MEGATREND UNIVERZITET

FAKULTET ZA KOMPJUTERSKE NAUKE

DOKTORSKA DISERTACIJA

UTICAJ BEZBEDNOSNIH RIZIKA U SAJBER PROSTORU NA POBOLJŠANJE FUNKCIONALNOSTI SIEM SOFTVERSKIH REŠENJA

Mentor:
Prof. Dr Nenad Kapor

Kandidat:
Aleksandar Kotevski

Beograd, 2024

Apstrakt

U savremenom digitalnom okruženju, sajber bezbednost predstavlja ključni faktor za očuvanje integriteta, poverljivosti i dostupnosti informacija. Ova disertacija istražuje uticaj bezbednosnih rizika u sajber prostoru na unapređenje funkcionalnosti rešenja za upravljanje bezbednosnim informacijama i događajima (SIEM). Analizirajući aktuelne pretnje i ranjivosti, rad identifikuje ključne izazove sa kojima se organizacije suočavaju u procesu detekcije i odgovora na incidecije.

Istraživanje obuhvata analizu postojećih SIEM rešenja i njihovih funkcionalnosti, kao i metodološki pristup za identifikaciju i klasifikaciju bezbednosnih rizika. Uvođenjem novih modela i tehnika, poput mašinskog učenja i analize velike količine podataka, disertacija prikazuje kako inovacije mogu doprineti poboljšanju efikasnosti i preciznosti SIEM sistema.

Kroz empirijska istraživanja i studije slučaja, ovaj rad demonstrira praktične primene unapređenih SIEM rešenja u različitim sektorima, naglašavajući značaj proaktivnog pristupa u identifikaciji pretnji. Rezultati istraživanja pružaju uvid u optimalne strategije za integraciju bezbednosnih rizika u dizajn i implementaciju SIEM alata, čime se doprinosi sveobuhvatnijem razumevanju sajber bezbednosti u dinamičnom i kompleksnom digitalnom pejzažu. Disertacija završava preporukama za buduća istraživanja i razvoj SIEM rešenja koja će biti otpornija na sveprisutne sajber pretnje.

Ključne reči: sajber bezbednost, digitalno okruženje, upravljanje bezbednosnim informacijama i događajima, analiza i klasifikacija.

Sadržaj

UVOD

U savremenom svetu, gde digitalna transformacija neprekidno oblikuje način na koji poslovne i društvene strukture funkcionišu, sajber bezbednost postaje ključni aspekt upravljanja organizacionim resursima. Sa porastom složenosti i učestalosti sajber napada, organizacije se suočavaju sa značajnim bezbednosnim rizicima koji mogu imati dalekosežne posledice na njihovu operativnost i reputaciju. U tom kontekstu, sigurnosni informacioni i događajni menadžment (SIEM) softveri se ističu kao esencijalni alati za detekciju, analizu i odgovor na sajber pretnje.

Uticaj bezbednosnih rizika u sajber prostoru na poboljšanje funkcionalnosti SIEM softverskih rešenja je značajan i višestruk. Kako se pretnje konstantno razvijaju i postaju sofisticiranije, tako se i zahtevi za SIEM rešenja moraju prilagođavati tim promenama.

Ukratko, bezbednosni rizici u sajber prostoru direktno utiču na razvoj i unapređenje SIEM softverskih rešenja, čineći ih sve sofisticiranijim i prilagodljivijim potrebama savremenih organizacija.

Ova disertacija istražuje interakciju između bezbednosnih rizika u sajber prostoru i unapređenja funkcionalnosti SIEM rešenja. Razumevanje kako različiti bezbednosni incidenti utiču na razvoj i optimizaciju SIEM alata predstavlja ne samo akademski izazov, već i praktičnu potrebu u kontekstu sve većih pretnji koje se pojavljuju u digitalnom okruženju. Kroz analizu postojećih rešenja i istraživanje novih pristupa, ovaj rad teži da pruži sveobuhvatan uvid u to kako organizacije mogu efikasnije koristiti SIEM softvere za upravljanje rizicima i jačanje svoje bezbednosne posture.

U prvom delu disertacije razmatraju se ključni koncepti i teorijske osnove sajber bezbednosti, dok drugi deo obuhvata analizu trenutnih SIEM rešenja i identifikaciju njihovih nedostataka. Na kraju, fokusiraćemo se na predloge za unapređenje funkcionalnosti ovih alata, uzimajući u obzir dinamične prirode sajber pretnji. Ova istraživanja doprinose razvoju teorijskog okvira i praktičnih smernica koje mogu poboljšati sposobnosti organizacija da se zaštite od sve sofisticiranijih sajber napada.

GLAVA 1: METODOLOŠKI OKVIR ISTRAŽIVANJA

1.1.Problem istraživanja

Organizacije se suočavaju s brzim razvojem i sve većim brojem sajber pretnji, što značajno utiče na njihove bezbednosne strategije. Kako bi se zaštitile od potencijalnih incidenata, mnoge organizacije koriste rešenja za upravljanje bezbednosnim informacijama i događajima (SIEM) koja im omogućavaju prikupljanje, analizu i korelaciju bezbednosnih podataka iz različitih izvora. Ipak, uprkos njihovoj važnosti, postojeća SIEM rešenja često se ne prilagođavaju dovoljno brzo i efikasno dinamičkim promenama u pejzažu bezbednosnih rizika.

Bezbednosni rizici u sajber prostoru postaju sve kompleksniji, sa novim vrstama napada koji se svakodnevno pojavljuju, kao što su ransomware, napadi na lanac snabdevanja, insider pretnje i drugi sofisticirani oblici sajber kriminala. Ovi rizici ne samo da izazivaju neposredne posledice po bezbednost informacija, već takođe dovode u pitanje i funkcionalnost postojećih SIEM rešenja. Postavlja se pitanje kako ovi rizici utiču na performanse SIEM alata i u kojoj meri trenutne metodologije analize i upravljanja incidentima mogu biti unapređene da bi se bolje suočile s novim izazovima.

Ključna istraživačka pitanja su:

1. Koji su ključni bezbednosni rizici u sajber prostoru koji utiču na rad SIEM sistema?

   Ovo pitanje istražuje specifične tipove pretnji koje predstavljaju izazove za SIEM rešenja, kao i to kako se ove pretnje razlikuju među industrijama i organizacijama.

2. Kako trenutni modeli i metode analize podataka u SIEM rešenjima mogu biti unapređeni da bi efikasnije odgovarali na nove pretnje?

   Istraživaće se kako postojeće metode analize logova i korelacije podataka mogu biti poboljšane, uključujući upotrebu mašinskog učenja i analitike u realnom vremenu.

3. Koje su najbolje prakse u integraciji automatizacije i veštačke inteligencije u SIEM rešenja, kako bi se poboljšala njihova funkcionalnost u kontekstu prepoznatih rizika?

   Ova pitanja će se fokusirati na ulogu automatizacije u ubrzanju procesa detekcije i odgovora na pretnje, kao i na mogućnosti koje veštačka inteligencija pruža za prediktivnu analizu.

4. Na koji način organizacije mogu implementirati proaktivne mere u SIEM rešenjima kako bi smanjile uticaj budućih bezbednosnih rizika?

   Ovo istraživanje će razmotriti strategije koje organizacije mogu uvesti za unapređenje svojih SIEM sistema, uključujući obuku zaposlenih, unapređenje politike bezbednosti i redovno testiranje sistema.

Analiziraće se trenutni trendovi u sajber pretnjama i njihov uticaj na efikasnost SIEM rešenja. Potom, istražiće se slabosti postojećih sistema u kontekstu dinamičkih rizika i identificirati područja za poboljšanje. Na kraju, razviće se preporuke za unapređenje funkcionalnosti SIEM rešenja, kako kroz tehnološka unapređenja, tako i kroz organizacione strategije.

Istraživanje će se oslanjati na kombinaciju kvalitativnih i kvantitativnih metoda. Kvalitativni deo obuhvatiće analizu literature i studije slučaja, dok će kvantitativni deo uključivati prikupljanje podataka putem anketa i intervjua sa stručnjacima iz industrije. Ova kombinacija omogućava sveobuhvatno razumevanje izazova i rešenja u oblasti SIEM-a.

Ovo istraživanje ima za cilj da doprinese razvoju efikasnijih SIEM rešenja koja su bolje prilagođena savremenim bezbednosnim rizicima. Razumevanje uticaja sajber pretnji na funkcionalnost ovih alata ključno je za unapređenje sposobnosti organizacija da se zaštite od sve složenijih i ozbiljnijih pretnji u sajber prostoru. Rezultati istraživanja će biti od značaja za akademsku zajednicu, praktičare u oblasti sajber bezbednosti, kao i za donosioca odluka unutar organizacija.

1.2.Predmet istraživanja

U svetu koji se brzo digitalizuje, organizacije se suočavaju s rastućim bezbednosnim rizicima u sajber prostoru. Ovi rizici, uključujući napade zlonamernog softvera, phishing napade, DDoS napade, kao i insider pretnje, predstavljaju značajan izazov za očuvanje informatičke bezbednosti. U tom kontekstu, rešenja za upravljanje bezbednosnim informacijama i događajima (SIEM) igraju ključnu ulogu u detekciji, analizi i odgovoru na ove pretnje.

Predmet ovog istraživanja je analiza kako različiti bezbednosni rizici utiču na razvoj i prilagođavanje funkcionalnosti SIEM softverskih rešenja. Istraživanje će se fokusirati na identifikaciju specifičnih pretnji koje zahtevaju unapređenje postojećih funkcionalnosti SIEM alata, kao i na razumevanje načina na koji se ova rešenja prilagođavaju novim izazovima u sajber prostoru.

Kroz analizu trenutnih trendova i pretnji, istraživanje će identifikovati ključne aspekte koje SIEM rešenja moraju obuhvatiti kako bi bila efikasna u prepoznavanju i odgovaranju na savremene bezbednosne izazove. Takođe, istraživanje će obuhvatiti i praktične aspekte implementacije ovih poboljšanja, uključujući analizu uspešnosti kroz studije slučaja iz različitih sektora.

Neophodno je razviti sveobuhvatan model koji definiše preporučene funkcionalnosti SIEM rešenja u skladu sa prepoznatim bezbednosnim rizicima, čime se doprinosi unapređenju njihove otpornosti i efikasnosti. Ovaj model će poslužiti kao vodič za buduće razvojne inicijative i strategije upravljanja bezbednošću, omogućavajući organizacijama da bolje zaštite svoje informacije i infrastrukturu.

1.3.Ciljevi istraživanja

Opšti cilj ovog istraživanja je da se ispita kako bezbednosni rizici u sajber prostoru utiču na funkcionalnost i efikasnost SIEM softverskih rešenja. Ovaj cilj uključuje analizu trenutnih izazova u identifikaciji i odgovoru na bezbednosne pretnje, kao i istraživanje mogućnosti za unapređenje ovih sistema.

Naučni cilj istraživanja je razvijanje novog okvira za evaluaciju i unapređenje funkcionalnosti SIEM rešenja na osnovu identifikovanih bezbednosnih rizika. Ovaj cilj podrazumeva:

- Analizu postojećih SIEM rešenja: Istraživanje trenutnih karakteristika i limita postojećih SIEM alata u kontekstu prepoznavanja i reagovanja na sajber pretnje.
- Ispitivanje bezbednosnih rizika: Kategorizacija i analiza najčešćih bezbednosnih rizika sa kojima se organizacije suočavaju, uključujući nove i evolutivne pretnje.
- Razvoj modela: Razvoj i validacija modela koji može pomoći organizacijama u optimizaciji SIEM rešenja na osnovu prepoznatih rizika.

Društveni cilj istraživanja je doprinos povećanju bezbednosti informatičkih sistema i zaštite podataka u organizacijama, što će rezultirati većim poverenjem korisnika i smanjenjem finansijskih gubitaka usled sajber napada. Ovaj cilj obuhvata:

- Edukaciju i svest: Promocija svesti o značaju zaštite informacija i korišćenju naprednih SIEM rešenja među organizacijama različitih veličina.
- Praktčna primena rezultata: Razvoj preporuka i smernica za implementaciju unapređenih SIEM rešenja koje će pomoći organizacijama u prevenciji i odgovoru na sajber napade.

Specifični ciljevi istraživanja su:

- Istraživanje pretnji: Identifikovati i klasifikovati bezbednosne rizike koji najviše utiču na funkcionalnost SIEM rešenja.
- Analiza podataka: Prikupiti i analizirati podatke o performansama postojećih SIEM alata u različitim scenarijima sajber napada.
- Razvijanje metrika: Razviti kvantitativne i kvalitativne metrike za ocenu efikasnosti SIEM rešenja u identifikaciji i upravljanju bezbednosnim incidentima.
- Simulacije napada: Sprovesti simulacije različitih tipova sajber napada kako bi se testirala otpornost SIEM rešenja i njihova sposobnost da se prilagode novim rizicima.
- Preporuke za implementaciju: Razviti konkretne preporuke za organizacije o tome kako da unaprede svoja SIEM rešenja u skladu sa identifikovanim bezbednosnim rizicima.

Ovi ciljevi će pomoći u izgradnji temeljnijeg razumevanja interakcije između sajber bezbednosti i tehnologije SIEM, doprinoseći ne samo naučnim saznanjima već i praktičnoj primeni u industriji.

1.4.Hipotetički okvir istraživanja

U svetlu rastućih pretnji u sajber prostoru, organizacije su sve više okrenute implementaciji i unapređenju SIEM rešenja. Ova disertacija istražuje kako specifični bezbednosni rizici utiču na razvoj i funkcionalnost ovih sistema, s ciljem identifikacije ključnih faktora koji doprinose poboljšanju efikasnosti SIEM softverskih rešenja.

Glavna hipoteza:

- GH: Povećani bezbednosni rizici u sajber prostoru direktno utiču na poboljšanje funkcionalnosti SIEM softverskih rešenja, čime se povećava njihova sposobnost identifikacije i odgovora na pretnje.

Pomoćne hipoteze:

- PH1: Organizacije koje redovno ažuriraju svoje SIEM softverske sisteme kao odgovor na nove bezbednosne rizike beleže značajno brže vreme odgovora na incidentne situacije.
- PH2: Postojanje analitičkih alata unutar SIEM rešenja, koji se fokusiraju na prepoznavanje specifičnih bezbednosnih rizika, povećava tačnost detekcije i smanjuje broj lažno pozitivnih alarmacija.
- PH3: Organizacije koje integrišu informacije o bezbednosnim rizicima u realnom vremenu u svoje SIEM rešenje postižu bolje performanse u upravljanju incidentima u poređenju sa onima koje ne koriste takve informacije.

Očekuje se da će istraživanje potvrditi glavnu hipotezu i pomoćne hipoteze, identifikujući ključne strategije koje organizacije mogu primeniti za unapređenje svojih SIEM rešenja u svetlu dinamičnih bezbednosnih rizika.

1.5.Metode istraživanja

Metode koje će se primenjivati u istraživanju su sledeće:

1. **Kvalitativna analiza:**
   - Intervjui sa stručnjacima: Sprovesti polustrukturirane intervjue sa IT stručnjacima i bezbednosnim analitičarima kako bi se prikupili uvidi o trenutnim izazovima i potrebama SIEM rešenja.
   - Studije slučaja: Analizirati konkretne primere organizacija koje su implementirale SIEM softver, fokusirajući se na identifikovane bezbednosne rizike i način na koji su ih rešavali.
2. **Kvantitativna analiza:**
   - Anketiranje: Provesti anketu među organizacijama koje koriste SIEM rešenja kako bi se prikupili podaci o učestalosti bezbednosnih rizika i ocenama funkcionalnosti SIEM alata.
   - Statistička analiza podataka: Koristiti deskriptivnu i inferencijalnu statistiku za analizu prikupljenih podataka iz anketa i studija slučaja, kako bi se identifikovale korelacije između bezbednosnih rizika i funkcionalnosti SIEM softvera.
3. **Eksperimentalna istraživanja:**
   - Simulacije: Sprovesti simulacije napada na sistem sa različitim SIEM rešenjima kako bi se ispitala njihova efikasnost u detekciji i odgovoru na bezbednosne rizike.
   - Prototipiranje: Razviti prototip unapređenog SIEM rešenja zasnovanog na identifikovanim potrebama i rizicima, a zatim testirati njegovu funkcionalnost u kontrolisanom okruženju.
4. **Literaturna analiza:**
   - Pregled postojećih istraživanja: Analizirati postojeću literaturu o SIEM rešenjima, bezbednosnim rizicima i najboljoj praksi kako bi se identifikovale postojeće praznine i potencijalna poboljšanja.

5. **Analiza trendova:**
    - Praćenje industrijskih izveštaja i trendova: Istraživati aktuelne trendove u sajber bezbednosti i njihov uticaj na razvoj SIEM tehnologija.

Kombinovanjem ovih metoda će se dobiti sveobuhvatan uvid u temu istraživanja i razviti preporuke za poboljšanje funkcionalnosti SIEM softverskih rešenja u kontekstu sve prisutnijih bezbednosnih rizika.

1.6.Očekivani rezultati i naučni doprinos

Očekivani rezultati i naučni doprinos rada na temu uticaja bezbednosnih rizika u sajber prostoru na poboljšanje funkcionalnosti SIEM[1] softverskih rešenja mogu se analizirati kroz nekoliko ključnih tačaka:

Očekivani rezultati:

1. **Analiza bezbednosnih rizika:**
    - Identifikacija i klasifikacija ključnih bezbednosnih rizika u sajber prostoru koji utiču na organizacije.
    - Razvijanje metodologije za procenu uticaja ovih rizika na funkcionalnost SIEM rešenja.
2. **Unapređenje SIEM funkcionalnosti:**
    - Predlozi za unapređenje postojećih SIEM alata, uključujući nove funkcionalnosti za detekciju i odgovor na rizike.
    - Razvoj modela koji integriše rizike u proces analize podataka i pravljenje izveštaja.
3. **Prakticne implementacije:**
    - Studije slučaja koje demonstriraju kako poboljšana SIEM rešenja mogu unaprediti bezbednost informacija.
    - Kreiranje protokola ili smernica za implementaciju novih funkcionalnosti.
4. **Evaluacija performansi:**
    - Kvantitativne i kvalitativne analize efekata primene unapređenih SIEM rešenja na organizacionu bezbednost.
    - Upitnici i intervjui sa stručnjacima za procenu poboljšanja u detekciji i reagovanju na incidente.
5. **Naučni doprinos:**
    - Teorijski okvir:
    - Razvijanje novog teorijskog okvira za analizu interakcije između bezbednosnih rizika i SIEM rešenja.
    - Povezivanje teorija iz oblasti sajber bezbednosti i menadžmenta rizika[2].
6. **Metodološki doprinos:**
    - Uvođenje inovativnih metoda istraživanja i analize koje bi mogle poslužiti kao osnova za buduća istraživanja u oblasti sajber bezbednosti.

[1] Lee, G. (2020). Enhancing SIEM Functionality with AI., str. 25-29

[2] Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework – Cynthia Brumfield (2021), str. 18-22.

7. **Interdisciplinarni pristup:**
    - Uključivanje perspektiva iz različitih oblasti, kao što su informacione tehnologije, menadžment i psihologija, za holistički pristup problemu.
8. **Praktične preporuke:**
    - Izrada smernica za organizacije o tome kako da unaprede svoje SIEM sisteme u skladu sa aktuelnim pretnjama u sajber prostoru.
    - Doprinos razvoju standarda i okvira u industriji za bezbednost informacija.

Ovaj rad ima za cilj ne samo da obogatiti teorijsko znanje u oblasti sajber bezbednosti, već i da pruži praktične alate i preporuke za organizacije, čime se doprinosi unapređenju opšteg nivoa bezbednosti u digitalnom okruženju.

GLAVA 2: ISTORIJSKI ASPEKT BEZBEDNOSNIH RIZIKA[3] U SAJBER PROSTORU

2.1. Istorijat odnosa bezbednosnih rizika u sajber prostoru i SIEM softverskih rešenja

Sajber prostor je postao neodvojivi deo savremenog života, a s njim su se pojavili i složeni bezbednosni rizici koji ugrožavaju organizacije širom sveta. Sa rastućim brojem sofisticiranih napada, od phishinga do naprednih persistentnih pretnji (APT[4]), potreba za efikasnim sistemima zaštite nikada nije bila veća. U ovom kontekstu, softverska rešenja za upravljanje informacijama i bezbednosnim događajima (SIEM[5]) su se pojavila kao ključni alati u arsenalima bezbednosnih stručnjaka.

Ova rešenja omogućavaju organizacijama da prate, analiziraju i odgovaraju na bezbednosne incidente u realnom vremenu, integrišući podatke iz različitih izvora i pružajući centralizovanu vidljivost. U ovom radu, istražićemo istorijat odnosa između bezbednosnih rizika u sajber prostoru i SIEM rešenja[6], osvetlićemo njihovu evoluciju kroz vreme i analizirati kako su se prilagodila novim izazovima i trendovima u svetu bezbednosti.

Početak 2000-ih: Rani razvoj SIEM rešenja

U početku, sajber bezbednost se fokusirala na zaštitu mrežnih perimetara koristeći firewalle i antivirusne alate. Kako su se pretnje razvijale, došlo je do potrebe za kompleksnijim alatima za prikupljanje i analizu podataka o bezbednosti. Tako su se pojavila SIEM rešenja, koja su omogućila organizacijama da centralizovano prate sigurnosne događaje i analize.

[3] Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press., str. 15-20

[4] Cybersecurity and Cyberwar: What Everyone Needs to Know – P.W. Singer, Allan Friedman (2014), str. 15-20.

[5] Security Information and Event Management (SIEM) Implementation – David Miller et al. (2010), str. 35-39.

[6] Security Information and Event Management (SIEM) Architecture – Omar Santos (2020), str. 51-55.

2005-2010: Rastuća kompleksnost pretnji

Sa porastom sofisticiranih napada, kao što su APT (Advanced Persistent Threats), organizacije su sve više shvatile značaj integracije različitih izvora podataka. SIEM rešenja su počela da uključuju mogućnosti za korelaciju događaja, što je omogućilo brže identifikovanje i reagovanje na pretnje[7].

2010-2015: Povećanje regulative i usklađenosti

U ovom periodu, sve veći broj regulativa (kao što su GDPR i HIPAA[8]) postavio je standarde za upravljanje bezbednosnim rizicima[9]. SIEM rešenja su postala ključna za ispunjavanje ovih zahteva, omogućavajući organizacijama da prate i beleže događaje u skladu sa zakonskim obavezama.

2015-2020: Razvoj AI i automatizacije

Kako su se napadi postajali sve sofisticiraniji, integracija veštačke inteligencije i mašinskog učenja u SIEM rešenja postala je standard. Ova tehnologija je omogućila brže otkrivanje anomalija[10] i automatizaciju odgovora na incidente, čime su se smanjili potencijalni bezbednosni rizici.

2020-sada: Zero Trust[11] i Cloud rešenja

U poslednjim godinama, koncept "Zero Trust" je postao popularan, podstičući organizacije da ne veruju ni jednoj unutrašnjoj ni spoljašnjoj jedinici bez provere. SIEM rešenja su se razvila da podrže ovaj model, integrišući se sa oblačnim tehnologijama i omogućavajući bolju vidljivost i kontrolu nad svim korisnicima i uređajima.

Odnos između bezbednosnih rizika u sajber prostoru i SIEM rešenja je evoluirao kroz vreme, od jednostavne zaštite do kompleksnih sistema koji koriste napredne analitičke tehnike. Ova rešenja su ključna za proaktivno upravljanje bezbednosnim rizicima i zaštitu organizacija od sve sofisticiranijih pretnji. U budućnosti, očekuje se dalji razvoj integracije AI, automatizacije i oblačnih rešenja, čime će se dodatno unaprediti efikasnost i responzivnost SIEM alata.

Trenutna Situacija: Bezbednosni Rizici u Sajber Prostoru i NextGen SIEM Rešenja

U današnjem digitalnom okruženju, bezbednosni rizici su postali složeniji i raznovrsniji nego ikada. Organizacije se suočavaju sa stalnim pretnjama, uključujući ransomware, phishing, insider napade i napade zasnovane na veštačkoj inteligenciji. Ove pretnje ne samo da su sve prisutnije, već su i sve sofisticiranije, što zahteva proaktivan i dinamičan pristup u upravljanju bezbednošću.

U ovoj situaciji, NextGen SIEM (naredna generacija SIEM) rešenja igraju ključnu ulogu. Ova moderna rešenja koriste napredne tehnologije, uključujući veštačku inteligenciju i mašinsko učenje, kako bi unapredila detekciju i odgovor na pretnje. Umesto da se oslanjaju isključivo na

[7] Practical Threat Intelligence and Data-Driven Threat Hunting – Valentina Costa-Gazcón, Jessica Reiser (2021), str. 29-33.
[8] Network Security Essentials: Applications and Standards – William Stallings (2017), str. 45-49.
[9] Cybersecurity: Law and Guidance – Helen Wong MBE (2018), str. 24-27.
[10] Khan, A. (2020). Anomaly Detection Using Machine Learning in Cybersecurity. O'Reilly Media., str. 34-39
[11] Zero Trust Networks: Building Secure Systems in Untrusted Networks – Evan Gilman, Doug Barth (2017), str. 35-39.

pravila i korelacije, NextGen SIEM alati analiziraju velike količine podataka u realnom vremenu[12], identifikujući obrasce koji ukazuju na potencijalne napade.

Ključni Elementi Trenutne Situacije:

Evolucija Pretnji: Napadi su postali sve više usmereni i ciljani, sa kradljivcima koji koriste sofisticirane tehnike kao što su socijalni inženjering[13] i zero-day exploit-i. Ovo povećava pritisak na organizacije da unaprede svoje bezbednosne strategije.

Integracija Podataka: NextGen SIEM rešenja omogućavaju integraciju podataka iz više izvora, uključujući oblačne servise, IoT uređaje i mobilne aplikacije. Ova holistička pristup omogućava organizacijama da imaju sveobuhvatan pregled svoje bezbednosne posture.

Automatizacija i Brzi Odgovor: Automatizacija procesa detekcije i odgovora je ključna prednost NextGen SIEM rešenja. Ova rešenja omogućavaju brže reagovanje na incidente, smanjujući vreme potrebno za otkrivanje i neutralizaciju pretnji.

Usmerenje na Zdravlje i Performanse: Pored tradicionalnog fokusiranja na detekciju pretnji, savremeni SIEM alati takođe prate performanse sistema i zdravlje mreže, što pomaže u identifikaciji potencijalnih ranjivosti pre nego što postanu ozbiljni problemi.

Prilagođavanje i Učenje: Napredni modeli mašinskog učenja omogućavaju NextGen SIEM rešenjima da se prilagode novim pretnjama i unaprede svoje performanse tokom vremena, što čini organizacije otpornijim na promenljive rizike.

Trenutna situacija u sajber prostoru zahteva od organizacija da neprestano reevaluiraju svoje bezbednosne strategije. NextGen SIEM rešenja se pokazala kao efikasna sredstva za borbu protiv sve složenijih pretnji, omogućavajući organizacijama da unaprede svoje sposobnosti detekcije, odgovora i upravljanja rizicima. Kako se pretnje nastavljaju razvijati, tako će i ova rešenja morati da evoluiraju, pružajući kompanijama potrebne alate za zaštitu njihovih podataka i infrastrukture.

Istorijat odnosa između bezbednosnih rizika u sajber prostoru i SIEM (Security Information and Event Management) softverskih rešenja oslikava evoluciju kako tehnologija, tako i pretnji sa kojima se organizacije suočavaju. U proteklih nekoliko decenija, sa brzim razvojem digitalnih tehnologija i rastećim brojem online pretnji, postalo je očigledno da tradicionalni alati za zaštitu više nisu dovoljni za obezbeđivanje sveobuhvatne bezbednosti.

U ranim fazama razvoja sajber bezbednosti, fokus je bio na zaštiti mrežnog perimetra[14] kroz osnovne alate kao što su firewalle i antivirusni programi. Kako su pretnje postajale složenije, sa pojavom APT napada i socijalnog inženjeringa, pojavila se potreba za sofisticiranijim rešenjima koja bi mogla da analiziraju i koreliraju velike količine podataka. Ovo je dovelo do razvoja SIEM softverskih rešenja, koja su omogućila centralizovano prikupljanje, analizu i upravljanje bezbednosnim događajima.

Tokom godina, SIEM rešenja su se prilagodila rastućim zahtevima tržišta i napredovale u funkcionalnosti. Uvođenje napredne analitike, veštačke inteligencije i mašinskog učenja dodatno je poboljšalo sposobnost ovih alata da brzo detektuju anomalije i reaguju na pretnje.

[12] Hartman, F. W. (2020). Real-Time SIEM Utilization. Packt., str. 29-32
[13] Black, D. (2018). Social Engineering Techniques and Countermeasures. Packt., str. 50-55
[14] Inside Network Perimeter Security – Stephen Northcutt et al. (2005), str. 39-43.

Ove inovacije su omogućile organizacijama da ne samo da reaguju na incidentne događaje, već i da prepoznaju potencijalne rizike pre nego što se pretvore u ozbiljne pretnje.

U svetlu rastućih regulativa i standarda u oblasti sajber bezbednosti, kao što su GDPR i HIPAA, SIEM rešenja su postala ključna u osiguravanju usklađenosti sa zakonskim zahtevima. Ova rešenja ne samo da pomažu u detekciji i odgovoru na pretnje, već takođe omogućavaju organizacijama da prate svoje bezbednosne prakse[15] i izveštavaju o incidentima, čime se osigurava transparentnost i poverenje.

Gledajući unapred, očekuje se da će se odnos između bezbednosnih rizika i SIEM rešenja i dalje razvijati. Sa pojavom novih tehnologija, poput oblačnih rešenja i IoT uređaja, organizacije će se suočiti sa dodatnim izazovima. NextGen SIEM rešenja, koja integriraju automatizaciju i orkestraciju, već predstavljaju odgovor na ove izazove, omogućavajući brži i efikasniji odgovor na pretnje.

U zaključku, istorijat odnosa između bezbednosnih rizika u sajber prostoru i SIEM softverskih rešenja oslikava kontinuiranu borbu protiv pretnji u digitalnom svetu. Dok pretnje postaju sve sofisticiranije, tako će se i alati za njihovu detekciju i upravljanje morati razvijati. Ova evolucija će biti ključna za očuvanje bezbednosti podataka i infrastrukture, omogućavajući organizacijama da se prilagode novim izazovima i ostanu otporne u sve dinamičnijem sajber okruženju.

2.2.Finansijski odnos[16] uticaja bezbednosnih pretnji[17] u sajber prostoru na SIEM softverska rešenja

Sajber bezbednost predstavlja jedan od najvažnijih aspekata savremenog poslovanja, a sve veće bezbednosne pretnje imaju značajan uticaj na način na koji organizacije pristupaju zaštiti svojih podataka i infrastrukture. Softverska rešenja za upravljanje informacijama i bezbednosnim događajima (SIEM) igraju ključnu ulogu u ovom procesu, omogućavajući organizacijama da detektuju, analiziraju i reaguju na bezbednosne incidente. Ovo poglavlje istražuje finansijski odnos između bezbednosnih pretnji u sajber prostoru i poboljšanja funkcionalnosti SIEM rešenja, osvetljavajući kako se ekonomski faktori prepliću sa potrebom za unapređenjem bezbednosnih alata.

Rastući Troškove Bezbednosti

Ekonomski Uticaj Napada

Prema različitim istraživanjima, troškovi sajber napada za organizacije mogu biti astronomični. Ove troškove čine direktni gubici, troškovi oporavka, pravni troškovi, kao i gubici reputacije. Na primer, napadi ransomware-a mogu zahtevati velike isplate, dok se troškovi oporavka od napada često mere u milionima dolara.

[15] Modern Cybersecurity Practices – Pascal Ackerman (2020), str. 33-36.
[16] Security Information and Event Management (SIEM) Implementation – David Miller et al. (2010), str. 35-39.
[17] Network Security Essentials: Applications and Standards – William Stallings (2017), str. 45-49.

Investicije u Bezbednost

Zbog ovih rizika, organizacije su primorane da povećaju svoja ulaganja u sajber bezbednost. U 2023. godini, globalna ulaganja u bezbednosne tehnologije procenjuju se na više od 150 milijardi dolara, a veliki deo ovih sredstava usmerava se na razvoj i implementaciju SIEM rešenja. Ove investicije su ključne za zaštitu organizacija od pretnji koje postaju sve sofisticiranije.

Razvoj i Unapređenje SIEM Rešenja

Inovacije u Tehnologiji

Rastući bezbednosni rizici podstiču inovacije u SIEM tehnologiji. Organizacije očekuju od ovih rešenja da ne samo da prate i beleže događaje, već i da pružaju analitiku u realnom vremenu, automatsku korelaciju podataka i mogućnosti predikcije pretnji. Očekivanja korisnika su sve veća, a tržište reaguje razvojem NextGen SIEM rešenja koja koriste veštačku inteligenciju i mašinsko učenje.

Automatska Detekcija i Odgovor

Napredna SIEM rešenja omogućavaju automatizaciju procesa detekcije i odgovora na incidente, što smanjuje vreme potrebno za reakciju i smanjuje potrebu za ljudskim resursima. Ove funkcionalnosti direktno smanjuju potencijalne troškove vezane za napade i povećavaju ukupnu bezbednost organizacija.

Usklađenost i Regulative

Povećani Zahtevi za Usklađivanje

Regulatorni zahtevi, poput GDPR-a i HIPAA-e, takođe igraju ključnu ulogu u oblikovanju investicija u SIEM rešenja. Organizacije su primorane da usklade svoje procese sa strogim zakonima, što dodatno povećava pritisak na njih da ulažu u napredne alate za analizu i upravljanje bezbednosnim događajima.

Troškovi Usklađenosti

Neusaglašenost može dovesti do značajnih finansijskih kazni, što čini ulaganje u SIEM rešenja ne samo kao zaštitu od pretnji, već i kao ekonomsku neophodnost. Na taj način, troškovi koji se odnose na usklađenost postaju deo sveobuhvatne strategije upravljanja rizicima.

Gubitak Reputacije i Potrošačko Poverenje

Ekonomske Posledice Gubitka Reputacije

U slučaju sigurnosnog incidenta, organizacije se suočavaju ne samo sa direktnim finansijskim gubicima, već i sa gubitkom reputacije koji može trajno uticati na njihov brend i poslovanje. Istraživanja pokazuju da je povraćaj potrošačkog poverenja nakon incidenta dugotrajan i skup proces.

Ulaganje u Proaktivnu Bezbednost

Zbog ovih potencijalnih posledica, organizacije su sve više fokusirane na proaktivne strategije zaštite, što uključuje i implementaciju naprednih SIEM rešenja koja omogućavaju prevenciju napada pre nego što se dogode.

Pristup Resursima i Talentima

Nedostatak Stručnjaka

Jedan od najvećih izazova u oblasti sajber bezbednosti je nedostatak kvalifikovanih stručnjaka. Očekuje se da će se potrebe za talentima povećati, što može dodatno povećati troškove organizacija. SIEM rešenja koja nude automatizaciju i olakšavaju rad bezbednosnim timovima postaju ključna u ovom kontekstu.

Obuka i Edukacija

Organizacije će morati da investiraju i u obuku i edukaciju svojih zaposlenih kako bi maksimalno iskoristile potencijal SIEM rešenja. Ovo dodatno naglašava ekonomski značaj ovih alata u kontekstu celokupne strategije upravljanja bezbednošću.

Finansijski Gubici u Privatnom i Javnom Sektoru zbog bezbednosnih Rizika u Sajber Prostoru

Bezbednosni rizici u sajber prostoru predstavljaju značajnu pretnju za organizacije širom sveta, uzrokujući ozbiljne finansijske gubitke kako u privatnom, tako i u javnom sektoru. Od phishing napada do ransomware-a i APT pretnji, troškovi oporavka od ovih incidenata mogu biti astronomski. Ovi gubici utiču na finansijsku stabilnost organizacija, a SIEM rešenja mogu doprineti smanjenju tih gubitaka.

Finansijski Gubici u Privatnom Sektoru

Privatni sektor je često na prvoj liniji fronta kada je reč o sajber napadima, a posledice mogu biti razorne. Prema nekim procenama, globalni troškovi sajber kriminala za privatne kompanije dostigli su više od 600 milijardi EUR godišnje.

Troškovi Oporavka: Organizacije moraju uložiti značajna sredstva u oporavak od napada, uključujući troškove pravnih usluga, istraživanja i povratka sistema u funkciju.

Gubici od Prestanaka Rada: Mnoge kompanije suočavaju se sa gubicima prihoda usled prekida poslovanja izazvanih napadima. Na primer, značajni napadi ransomware-a mogu paralizovati operacije, što rezultira direktnim finansijskim gubicima.

Gubitak Reputacije: Kada se informacije o napadu otkriju, gubitak reputacije može dovesti do smanjenja poverenja potrošača i investitora, što može trajno uticati na prihode.

Finansijski Gubici u Javnom Sektoru

Javni sektor takođe trpi velike finansijske gubitke usled sajber pretnji. Ove gubitke često dodatno otežavaju budžetska ograničenja i potrebna ulaganja u obnavljanje infrastrukture.

Troškovi Oporavka i Reforme: Napadi na vladine institucije često zahtevaju složene i skupe procese oporavka. Ove institucije mogu trošiti milione EUR-a na obnovu sistema i usklađivanje sa zakonodavstvom.

Gubici u Usmeravanju Resursa: Kada se resursi preusmere na oporavak od napada, javne usluge, kao što su obrazovanje i zdravstvo, mogu biti ozbiljno pogođene, što dovodi do dužih rokova i smanjenja kvaliteta usluga.

Uticaj na Nacionalnu Bezbednost: U slučaju napada na kritične infrastrukture, posledice mogu imati široke ekonomske i socijalne posledice, uključujući narušavanje sigurnosti građana.

SIEM (Security Information and Event Management) rešenja igraju ključnu ulogu u smanjenju finansijskih gubitaka izazvanih bezbednosnim pretnjama. Njihove funkcionalnosti obuhvataju:

- Proaktivna Detekcija Pretnji: SIEM rešenja omogućavaju organizacijama da detektuju potencijalne pretnje u realnom vremenu kroz analizu podataka i korelaciju događaja. Ovo proaktivno delovanje može sprečiti ili umanjiti ozbiljnost napada pre nego što se dogode.
- Brži Odgovor na Incidente[18]: Automatizacija odgovora na incidente[19] smanjuje vreme reakcije, što može značajno umanjiti troškove oporavka i prekida poslovanja. Brzi odgovori često minimiziraju obim štete.
- Integracija sa Obrazovanjem i Obukom: SIEM rešenja često uključuju alate za edukaciju zaposlenih, povećavajući njihovu svest o bezbednosnim rizicima i smanjujući verovatnoću ljudske greške koja može dovesti do incidenata.
- Usmeravanje Resursa: Korišćenjem SIEM rešenja, organizacije mogu bolje alocirati svoje resurse, smanjujući troškove vezane za višak zaposlenih u bezbednosnim timovima i omogućavajući im da se fokusiraju na strategije i inovacije.
- Poboljšanje Usklađenosti: SIEM rešenja pomažu organizacijama da se usklade sa regulatornim zahtevima, čime se smanjuje rizik od finansijskih kazni zbog neusaglašenosti.

Finansijski gubici prouzrokovani bezbednosnim pretnjama u sajber prostoru su značajni, sa dalekosežnim posledicama za privatni i javni sektor. Ulaganje u SIEM rešenja predstavlja ključni korak ka smanjenju ovih gubitaka, omogućavajući organizacijama da se proaktivno bore protiv pretnji, brže reaguju na incidente i optimizuju svoje resurse. Kako se sajber pretnje nastavljaju razvijati, tako će i značaj SIEM rešenja rasti, čineći ih neizostavnim delom strategije sajber bezbednosti svake organizacije.

U zaključku finansijski odnos između bezbednosnih pretnji u sajber prostoru i poboljšanja funkcionalnosti SIEM softverskih rešenja je kompleksan, ali neosporan. Rastući troškovi povezani sa napadima, obavezna usklađenost sa regulativama, i gubitak reputacije čine ulaganje u napredne bezbednosne alate ekonomskom neophodnošću. NextGen SIEM rešenja, koja koriste inovacije poput veštačke inteligencije i automatizacije, predstavljaju odgovor na izazove savremenog sajber prostora, omogućavajući organizacijama da smanje rizike i troškove, dok istovremeno poboljšavaju svoju sveukupnu bezbednost. Kako se tehnologija nastavlja razvijati, tako će i očekivanja organizacija rasti, postavljajući SIEM rešenja u središte strategija zaštite i upravljanja rizicima.

[18] Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents – Eric C. Thompson (2018), str. 52-56.
[19] Green, A. (2020). Automation in Security Operations Centers. Springer., str. 45-50

2.3 Faktori i sklonost riziku u odnosu sajber bezbednosti i funkcionalnosti SIEM rešenja

U poslednjim decenijama, sajber bezbednost je postala ključni aspekt poslovanja, javnih institucija i pojedinaca. Povećanje broja i složenosti sajber pretnji zahteva sveobuhvatan pristup zaštiti podataka i sistema. U tom kontekstu, rešenja za upravljanje bezbednosnim informacijama i događajima (SIEM) rešenja postaju centralni deo strategija sajber bezbednosti.

Bez obzira na industriju, organizacije su se suočavle s brojnim pretnjama koje mogu ugroziti njihovu funkcionalnost. U tom kontekstu, SIEM rešenja za upravljanje bezbednosnim informacijama i događajima igraju ključnu ulogu u otkrivanju, analizi i odgovoru na sajber pretnje. Razumevanje faktora koji utiču na rizik i sposobnost SIEM rešenja da se suoče s tim rizicima je od suštinskog značaja.

Sajber bezbednost je evoluirala od ranih dana interneta, kada su pretnje bile uglavnom motivisane znatiželjom ili igrom. Tokom 1980-ih i 1990-ih, razvoj mreža doveo je do pojave prvih virusa i crva, kao što su "Morris Worm" i "ILOVEYOU" virus. Ove pretnje su izazvale potrebu za boljim mehanizmima zaštite, što je dovelo do razvoja antivirusnog softvera i osnovnih sistema za detekciju upada.

Sa dolaskom 21. veka, kompleksnost pretnji je drastično porasla. Sajber napadi su postali organizovani, često sa finansijskim motivima. Razvoj društvenih mreža i mobilnih uređaja takođe je otvorio nove vektore za napade. U tom periodu, koncept SIEM rešenja je postao sve relevantniji, jer su organizacije počele da shvataju potrebu za centralizovanim sistemima koji mogu da prate, analiziraju i odgovore na sajber pretnje u realnom vremenu.

Razvoj SIEM rešenja

SIEM rešenja su se razvijala kroz nekoliko faza:

Prva generacija (rani 2000-ih): Ova rešenja su se fokusirala na prikupljanje i skladištenje logova iz različitih izvora[20]. Analiza je bila manualna, a odgovori na incidente spori i reaktivni.

Druga generacija (sredina 2000-ih): Sa razvojem algoritama za analizu i detekciju anomalija, SIEM rešenja su postala proaktivnija. Uvedena su pravila i korelacije kako bi se identifikovale sumnjive aktivnosti.

Treća generacija (2010-ih): Uvođenje veštačke inteligencije i mašinskog učenja omogućilo je napredniju analizu podataka i brže identifikovanje pretnji. Integracija sa drugim bezbednosnim alatima omogućila je brže odgovore.

Savremena SIEM rešenja: Današnja rešenja nude oblak opcije, automatsku analizu podataka i integraciju sa platformama za orkestraciju, omogućavajući brzo i efikasno upravljanje incidentima.

Sklonost riziku organizacije može varirati u zavisnosti od nekoliko faktora, uključujući:

[20] Adams, R. (2021). Trusted Threat Intelligence Sources. Packt., str. 20-25

- **Kultura organizacije:**

Organizacije koje smatraju sajber bezbednost prioritetom obično imaju nižu sklonost riziku. Ove organizacije često ulažu u obuku zaposlenih i napredne tehnologije.

- **Industrija:**

Neke industrije, poput finansijske ili zdravstvene, imaju višu sklonost riziku zbog obaveza usklađenosti i potencijalnih posledica napada.

- **Finansijski resursi:**

Organizacije s većim budžetima za IT bezbednost obično su bolje opremljene da se suoče s rizicima i implementiraju efikasna SIEM rešenja.

Faktori rizika[21] u sajber bezbednosti su mnogostruki:

1. **Tehnološki faktori:**
   - Složenost infrastrukture: Složenije IT okruženje, koje uključuje više sistema, aplikacija i mrežnih komponenti, povećava rizik od bezbednosnih propusta.
   - Zastarjela oprema i softver: Neaktuelni sistemi često sadrže ranjivosti koje mogu biti iskorišćene od strane napadača.
2. **Ljudski faktori:**
   - Nedostatak obuke: Radnici koji nisu adekvatno obučeni za prepoznavanje i upravljanje bezbednosnim pretnjama mogu postati "slaba karika" u bezbednosnom lancu.
   - Unutrašnji napadi: Insajderske pretnje[22], koje mogu biti namerne ili nenamerne, predstavljaju značajan rizik.
3. **Pravni i regulatorni faktori:**

Usaglašenost s propisima: Organizacije moraju poštovati različite regulative i standarde, poput GDPR-a ili HIPAA-e, što može uticati na način na koji implementiraju mere sajber bezbednosti.

4. **Faktori okoline:**

Geopolitička situacija: Globalne tenzije i sukobi mogu povećati broj sajber napada usmerenih na određene organizacije ili sektore.

U svetu sajber bezbednosti, merenje i određivanje stepena rizika su ključni koraci u razvoju efikasnih bezbednosnih strategija. Sa povećanjem složenosti i učestalosti sajber pretnji, organizacije moraju biti sposobne da precizno procene svoje ranjivosti i potencijalne posledice napada. U ovom kontekstu, Security Information and Event Management (SIEM) rešenja igraju ključnu ulogu u prikupljanju, analizi i upravljanju informacijama o pretnjama, omogućavajući organizacijama da identifikuju, ocenjuju i reše rizike.

[21] Cybersecurity for Beginners – Raef Meeuwisse (2017), str. 12-16.
[22] Smith, C. (2020). Managing Insider Threats in Organizations. CRC Press., str. 60-65

Merenje rizika u sajber bezbednosti obuhvata procese identifikacije, analize i ocene potencijalnih pretnji koje mogu ugroziti informacije, sisteme i infrastrukturu organizacije. Osnovne komponente ovog procesa uključuju:

Identifikacija pretnji: Ovo uključuje analizu potencijalnih izvora pretnji, kao što su hakeri, zlonamerni softver[23], insider pretnje i prirodne katastrofe. Razumevanje ko ili šta može napasti organizaciju je prvi korak ka merenju rizika.

Analiza ranjivosti[24]: Ovaj korak podrazumeva identifikaciju slabosti u sistemima i procesima organizacije koje bi mogle biti iskorišćene od strane napadača. To može uključivati tehničke ranjivosti, kao što su zastareli softver, kao i procese i procedure koji nisu adekvatno uspostavljeni.

Procena potencijalnog uticaja: Procena uticaja pretnji[25] može uključivati finansijske gubitke, gubitak reputacije, pravne posledice i operativne prekide. U ovom koraku, organizacije treba da razumeju koje su posledice po njih u slučaju uspešnog napada.

Kvantifikacija rizika: Ovaj proces uključuje kvantifikaciju verovatnoće da će određena pretnja iskorišćavati ranjivost i izračunavanje potencijalnog uticaja na osnovu verovatnoće. Metode za kvantifikaciju rizika mogu uključivati procene zasnovane na istorijskim podacima, analize scenarija i modeliranje.

Istorijski gledano, sajber bezbednost i razvoj SIEM rešenja su rezultat kontinuiranog odgovora na sve složenije pretnje. Razumevanje faktora rizika je ključno za izgradnju efikasne strategije zaštite. U dinamičnom svetu sajber pretnji, organizacije moraju neprekidno prilagođavati svoje pristupe i tehnologije kako bi osigurale sigurnost svojih podataka i sistema. U tom smislu, SIEM rešenja igraju ključnu ulogu, omogućavajući organizacijama da prepoznaju, analiziraju i reaguju na pretnje u realnom vremenu.

Posmatranje uticaja bezbednosnih rizika u sajber prostoru na poslovanje kompanija i rad organizacija drastično se promenilo tokom poslednjih nekoliko decenija. Dok su nekada rizici često bili viđeni kao marginalni problemi, danas su ključni aspekt strategijskog planiranja i operativnog upravljanja. Ova promena je rezultat evolucije tehnologije, povećanja složenosti sajber pretnji i rastuće svesti o važnosti sajber bezbednosti.

Nekada: Tradicionalno posmatranje

Minimalna svest o rizicima: U ranim danima interneta, mnoge kompanije nisu imale jasnu svest o sajber pretnjama. Rizici su često viđeni kao tehnički problemi koje treba rešavati IT timovi, a ne kao strateški izazovi.

Sistemi za zaštitu podataka: Organizacije su se oslanjale na osnovne zaštitne mere, kao što su antivirusni softver i jednostavni sistemi za lozinke. Mnogi su verovali da su te mere dovoljne za zaštitu podataka.

[23] Peterson, R. (2020). Malware Analysis Techniques and Prevention Strategies. Packt., str. 42-47
[24] Hughes, V. (2020). Vulnerability Analysis in Modern Networks. Apress.", str. 45-50
[25] Green, A. (2020). Assessing Cyber Threats: A Strategic Approach. Springer., str. 30-34

Reaktivni pristup: Reakcije na sajber napade bile su često reaktivne, bez prethodnog planiranja ili strategije. Nakon napada, organizacije su obično analizirale situaciju i pokušavale da shvate šta se desilo.

Ograničeni uticaj na poslovanje: Mnogi lideri su smatrali da sajber napadi retko direktno utiču na poslovne operacije ili reputaciju, pa su rizici često bili zanemarivani.

Danas: Savremeno posmatranje

Visoka svest o rizicima: Danas, gotovo svaka organizacija prepoznaje sajber pretnje kao ozbiljan rizik za poslovanje. Menadžment i odbori direktora aktivno se angažuju u razvoju strategija sajber bezbednosti.

Integrisani pristup: Sajber bezbednost više nije isključivo odgovornost IT odeljenja. Organizacije danas primenjuju holistički pristup koji uključuje sve nivoe poslovanja, od operacija do ljudskih resursa i pravnog odeljenja.

Proaktivan pristup: Mnoge organizacije usvajaju proaktivan pristup u identifikaciji i upravljanju rizicima. Ovo uključuje redovne procene rizika, simulacije napada (npr. pen-testovi) i kontinuirano obrazovanje zaposlenih.

Direktan uticaj na poslovanje: Danas, cyber napadi mogu imati direktne posledice na finansijske rezultate kompanija, reputaciju i poverenje kupaca. Napadi kao što su ransomware mogu dovesti do operativnih prekida, gubitka podataka i visokih troškova oporavka.

Regulatorna usklađenost[26]: Rastući broj zakona i regulativa, poput GDPR-a, zahteva od organizacija da uspostave robusne mere zaštite podataka. Neusaglašenost može dovesti do značajnih kazni i pravnih posledica.

Razvoj standardizacije upravljanja bezbednosnim rizicima u sajber prostoru postao je ključan zbog sveprisutne digitalizacije i rasta pretnji. U poslednjim decenijama, organizacije su sve više prepoznavale potrebu za sistematičnim pristupom u zaštiti svojih informacija i infrastrukture.

Ključni aspekti razvoja standardizacije:

- Globalni standardi: Organizacije kao što su ISO (Međunarodna organizacija za standardizaciju) razvijaju standarde poput ISO/IEC 27001, koji definiše zahteve za sisteme upravljanja bezbednošću informacija (ISMS). Ovi standardi omogućavaju organizacijama da uspostave, implementiraju i održavaju efektivne procese upravljanja rizicima.
- Framework-ovi: Razvijeni su različiti okviri[27], kao što je NIST Cybersecurity Framework, koji pomažu organizacijama da identifikuju, procene i upravljaju rizicima. Ovi okviri pružaju smernice i najbolje prakse koje olakšavaju pristup upravljanju rizicima.
- Prilagođavanje i usklađivanje: Standardizacija[28] omogućava organizacijama da se usklade sa regulativama i normama koje se razlikuju od zemlje do zemlje. Usklađivanje

[26] Martin, L. (2019). Regulatory Compliance in Cybersecurity., str. 33-37
[27] Cybersecurity: Law and Guidance – Helen Wong MBE (2018), str. 24-27.
[28] White, J. (2019). Standards in Cybersecurity: Best Practices. CRC Press., str. 28-32

sa zakonima o zaštiti podataka, kao što su GDPR u EU, postaje ključni deo strategije upravljanja rizicima.

- Edukacija i obuka: Standardi podstiču edukaciju zaposlenih o rizicima i najboljoj praksi u bezbednosti. Osvestiti zaposlene o potencijalnim pretnjama i načinima zaštite je ključni deo sveukupnog upravljanja rizicima.
- Kontinuirano unapređenje: Proces standardizacije nije statičan. Organizacije su ohrabrene da redovno revidiraju i unapređuju svoje strategije upravljanja rizicima kako bi se prilagodile novim pretnjama i tehnologijama.

Razvoj standardizacije upravljanja bezbednosnim rizicima u sajber prostoru predstavlja evoluciju u pristupu zaštiti informacija. Povezivanje globalnih standarda, okvira i lokalnih regulativa omogućava organizacijama da se efikasnije suoče sa sve kompleksnijim pretnjama u digitalnom svetu. Implementacija ovih standarda ne samo da štiti organizacije, već i doprinosi ukupnoj stabilnosti i poverenju u sajber prostor.

U današnjem kompleksnom sajber okruženju, razumevanje faktora rizika i uloga SIEM rešenja je ključno za zaštitu organizacija. SIEM rešenja pružaju neprocenjivu podršku u prepoznavanju i odgovoru na pretnje, ali uspeh zavisi od sposobnosti organizacije da razume i upravlja svojim rizicima. Integracija tehničkih rešenja s ljudskim faktorima i usklađenošću s regulativama može značajno smanjiti sklonost riziku i poboljšati ukupnu sajber bezbednost.

Posmatranje uticaja bezbednosnih rizika u sajber prostoru se značajno promenilo od marginalizovanog problema do centralnog pitanja strateškog planiranja i upravljanja rizicima. Organizacije danas shvataju da je sajber bezbednost ključna za održavanje konkurentnosti, zaštitu reputacije i osiguranje poverenja potrošača. Sa stalnim evolucijama pretnji, nastavak investicija u sajber bezbednost i proaktivan pristup postali su neophodni za uspešno poslovanje.

GLAVA 3: SAVREMENI ODNOS MENADŽMENTA PREMA UTICAJU BEZBEDNOSNIH RIZIKA U SAJBER PROSTORU

U savremenom poslovnom okruženju, menadžment organizacija suočava se sa brojnim izazovima vezanim za bezbednost u sajber prostoru. Razvoj tehnologije i digitalizacija poslovanja doneli su mnoge prednosti, ali i povećali rizike, što zahteva sveobuhvatan pristup upravljanju bezbednosnim rizicima[29]. Neophodno je istraživati odnos menadžmenta prema uticaju bezbednosnih rizika u sajber prostoru, naglašavajući ključne aspekte, strategije i preporuke za efikasno upravljanje tim rizicima.

Bezbednosni rizici u sajber prostoru uključuju pretnje kao što su hakerski napadi, malver, phishing, ransomware, krađa podataka i unutrašnje pretnje. Ove pretnje mogu imati ozbiljne posledice po finansijsko stanje organizacije, reputaciju, kao i pravnu odgovornost. Menadžment mora razumeti ove rizike i njihov potencijalni uticaj na poslovanje.

[29] Black, D. (2020). Risk Management Decision-Making in Cybersecurity., str. 35-39

Uloga menadžmenta u razumevanju i upravljanju uticajem bezbednosnih pretnji u sajber prostoru je višestruka:

- Procenjivanje rizika: Menadžment treba da sprovodi redovne procene rizika kako bi identifikovao i analizirao potencijalne pretnje. Ovo uključuje razumevanje vrednosti informacija i resursa, kao i ranjivosti sistema.
- Strategijsko planiranje: Upravni tim mora uključiti bezbednost u sajber prostoru u svoje strateško planiranje. To podrazumeva razvijanje politika i procedura koje se fokusiraju na prevenciju i odgovor na incidente.
- Odluke o investicijama: Menadžment je odgovoran za alokaciju resursa i investicija u bezbednosne tehnologije, obuke i razvoj. Pravilna procena gde uložiti sredstva može značajno smanjiti rizike.
- Kultura bezbednosti: Menadžment treba da promoviše kulturu bezbednosti unutar organizacije. To uključuje edukaciju zaposlenih o bezbednosnim praksama i podsticanje svesti o rizicima, što može pomoći u smanjenju ljudskih grešaka koje često predstavljaju slabost u bezbednosti.

Dalje, menadžment je odgovoran za sastavljanje strategije upravljanja bezbednosnim rizicima u sajber prostoru, što se može posmatrati na više nivoa:

- Razvijanje sveobuhvatnog plana: Menadžment treba da razvije i implementira planove za upravljanje incidentima, koji uključuju postupke za odgovor na napade, komunikaciju sa relevantnim stranama i procese oporavka.
- Tehnološka rešenja: Investiranje u modernu tehnologiju, kao što su sistemi za detekciju intruzija, antivirusni softver i rešenja za enkripciju, može značajno poboljšati bezbednost.
- Pristup zasnovan na riziku: Organizacije bi trebale da usvoje pristup zasnovan na riziku, koji se fokusira na identifikovanje i upravljanje najkritičnijim pretnjama, umesto da se bave svim rizicima podjednako.
- Obuka i svest: Stalna edukacija zaposlenih o najnovijim pretnjama i sigurnosnim praksama može smanjiti mogućnost uspešnih napada. Obuka treba biti redovna i prilagođena različitim ulogama unutar organizacije.

Odnos menadžmenta prema uticaju bezbednosnih rizika u sajber prostoru je ključno pitanje koje zahteva pažnju i strateško planiranje. Razumevanje rizika, procena posledica, proaktivan pristup i stvaranje kulture bezbednosti su neophodni za zaštitu organizacije. U svetu gde su sajber pretnje sveprisutne, efikasno upravljanje bezbednosnim rizicima postaje imperativ za održavanje poslovne stabilnosti i reputacije.

3.1. Uticaj dobrog menadžmenta na upravljanje bezbednosnim rizicima u sajber prostoru

Upravljanje bezbednosnim rizicima u sajber prostoru predstavlja jedan od ključnih izazova za organizacije svih veličina. Dobar menadžment igra presudnu ulogu u oblikovanju strategija i politika koje pomažu u prepoznavanju, proceni i mitigaciji tih rizika. U nastavku ćemo istražiti

kako kvalitetan menadžment utiče na upravljanje sajber bezbednosnim rizicima, i to kroz nekoliko ključnih aspekata.

Razvoj strategije i politike

Dobar menadžment postavlja temelj za razvoj sveobuhvatne sajber bezbednosne strategije. To uključuje definisanje jasnih ciljeva, politika i procedura koje će voditi organizaciju u prepoznavanju i odgovoru na bezbednosne pretnje. Menadžeri koji razumeju važnost sajber bezbednosti mogu efikasnije identifikovati kritične tačke u infrastrukturi i razviti strategije koje odgovaraju specifičnim potrebama i rizicima organizacije.

Edukacija i svest zaposlenih

Menadžment igra ključnu ulogu u promovisanju kulture bezbednosti unutar organizacije. Edukacija zaposlenih o potencijalnim sajber pretnjama, kao što su phishing napadi ili zlonamerni softver, može značajno smanjiti rizik od ljudskih grešaka koje često predstavljaju najslabiju kariku u bezbednosnom lancu. Organizacije koje ulažu u obuke i podizanje svesti svojih zaposlenih stvaraju otpornije radno okruženje.

Investicije u tehnologiju

Kvalitetan menadžment prepoznaje važnost ulaganja u savremene tehnologije za zaštitu podataka. To uključuje implementaciju sigurnosnih rešenja kao što su firewall-ovi, antivirusni programi, sistemi za detekciju upada i enkripcija podataka. Pravilno upravljanje resursima omogućava organizacijama da proaktivno pristupaju bezbednosnim izazovima, umesto da reaguju na incidentne situacije.

Procena i upravljanje rizicima

Dobar menadžment osigurava redovnu procenu bezbednosnih rizika, što uključuje analizu postojećih sigurnosnih protokola i identifikaciju potencijalnih ranjivosti. Razvijanje metodologija za ocenu rizika omogućava organizacijama da shvate verovatnoću i uticaj različitih pretnji, što im pomaže da prioritetizuju svoje napore i resurse na efikasniji način.

Reakcija na incidentne situacije

Menadžment ima ključnu ulogu u postavljanju plana reagovanja na incidentne situacije. Brza i efikasna reakcija na sajber napade može značajno umanjiti štetu i smanjiti vreme potrebno za oporavak. Uspostavljanje jasnih procedura, timova za odgovor na incidente i komunikacionih kanala osigurava da organizacija može brzo reagovati na pretnje i minimizirati posledice.

Pridržavanje regulativa i standarda

Upravljanje bezbednosnim rizicima takođe zahteva poštovanje relevantnih regulativa i standarda, kao što su GDPR, HIPAA ili PCI DSS. Dobar menadžment obezbeđuje da organizacija bude u skladu sa zakonskim okvirima, čime se smanjuje rizik od pravnih posledica i poboljšava reputacija kompanije. Uvođenje procedura koje su usklađene sa standardima pomaže u jačanju celokupnog okvira bezbednosti.

Kontinuirano poboljšanje

Sajber pretnje se stalno razvijaju, zbog čega je važno da organizacije budu proaktivne i da neprestano unapređuju svoje bezbednosne protokole. Dobar menadžment promoviše kulturu

stalnog poboljšanja, uključujući redovne revizije bezbednosnih praksi i implementaciju novih tehnologija i metoda. Ova strategija pomaže organizacijama da ostanu korak ispred potencijalnih pretnji.

Neki od primera dobrih praksi menadžmenta na upravljanje bezbednosnim rizicima u sajber prostoru navedeni su u nastavku.

Upravljanje bezbednosnim rizicima u sajber prostoru zahteva integraciju različitih strategija i pristupa. Kroz konkretne primere dobrih praksi menadžmenta, možemo bolje razumeti kako organizacije uspevaju da zaštite svoje podatke i infrastrukturu od potencijalnih pretnji. Ovi primeri ilustriraju ključne aspekte efikasnog menadžmenta i njihov uticaj na sajber bezbednost.

Stvaranje kulturološke svesti o bezbednosti

Primer:Google

Google je poznat po svojoj posvećenosti kulturi bezbednosti. Organizacija redovno sprovodi obuke za sve zaposlene o prepoznavanju i reagovanju na sajber pretnje. Kroz interaktivne radionice i simulacije, zaposleni uče kako da identifikuju phishing napade i druge vrste prevara. Takođe, Google je razvio program "Bezbednosni vežba", gde se zaposleni takmiče u rešavanju bezbednosnih problema, čime se dodatno podiže svest o važnosti bezbednosti.

Implementacija višefaktorske autentifikacije (MFA)

Primer:Microsoft

Microsoft je implementirao višefaktorsku autentifikaciju kao standardnu praksu za pristup svojim sistemima. Ova mera značajno smanjuje rizik od neovlašćenog pristupa, jer korisnici moraju da potvrde svoj identitet putem više metoda (npr. lozinka i biometrijski podaci ili SMS kod). Ova praksa ne samo da poboljšava bezbednost, već takođe podiže svest među korisnicima o važnosti dodatnih bezbednosnih slojeva.

Redovno testiranje i procena bezbednosti[30]

Primer:IBM

IBM sprovodi redovne testove penetracije i procene ranjivosti svojih sistema. Ovi testovi pomažu u identifikaciji potencijalnih slabosti pre nego što ih napadači iskoriste. Tim za sajber bezbednost koristi alate za automatizaciju kako bi izvršio široke analize, ali takođe angažuje i spoljne eksperte za dodatnu procenu. Ova praksa omogućava IBM-u da brzo reaguje na nove pretnje i da unapredi svoje bezbednosne protokole.

Razvoj plana odgovora na incidente

Primer:Target

Nakon velikog sajber napada 2013. godine, Target je uveo sveobuhvatan plan odgovora na incidente[31]. Ovaj plan uključuje uspostavljanje tima za brzo delovanje, koji se aktivira u slučaju sigurnosnog incidenta, kao i jasne procedure za komunikaciju sa klijentima i regulatornim

[30] The Basics of Hacking and Penetration Testing – Patrick Engebretson (2013), str. 35-38.
[31] White, L. (2019). Incident Response Planning for Cybersecurity. CRC Press., str. 38-43

telima. Target takođe investira u obuke i simulacije za svoj tim kako bi se osiguralo da su svi spremni da reaguju na efikasan način.

Proaktivan pristup analizi podataka

Primer:Cisco

Cisco koristi napredne analitičke alate kako bi identifikovao sumnjive aktivnosti u svom mrežnom saobraćaju. Korišćenjem veštačke inteligencije i mašinskog učenja, Cisco može da prepozna obrasce koji ukazuju na potencijalne pretnje i automatski reaguje na njih. Ova proaktivna strategija omogućava brže detekciju i smanjenje potencijalnih incidenata.

Pridržavanje industrijskih standarda i regulativa

Primer:Banke (npr. JPMorgan Chase)

Banke poput JPMorgan Chase strogo se pridržavaju finansijskih regulativa i standarda, kao što su PCI DSS (Payment Card Industry Data Security Standard) i GLBA (Gramm-Leach-Bliley Act). Ove regulative zahtevaju implementaciju jakih bezbednosnih protokola, a menadžment u ovim organizacijama osigurava da se svi zaposleni obučavaju i da se redovno sprovode revizije usklađenosti. Ovakve prakse ne samo da štite podatke klijenata, već i poboljšavaju reputaciju organizacije.

Angažovanje stručnjaka i saradnja sa partnerima

Primer:Facebook

Facebook često angažuje spoljne stručnjake za bezbednost kako bi unapredio svoje protokole i rešenja. Saradnja sa profesionalcima iz oblasti sajber bezbednosti omogućava im da dobiju uvid u najnovije pretnje i najbolje prakse. Takođe, Facebook redovno učestvuje u inicijativama zajednice i deljenju informacija sa drugim organizacijama, čime dodatno jača kolektivnu bezbednost.

Korišćenje simulacija i vežbi

Primer: U.S. Department of Defense (DoD)

Ministarstvo odbrane Sjedinjenih Američkih Država redovno sprovodi simulacije sajber napada kako bi pripremilo svoje timove za odgovaranje na realne pretnje. Ove vežbe omogućavaju identifikaciju slabih tačaka u odgovorima timova i pomažu u unapređenju strategija. Kroz ovakve simulacije, DoD može da osigura da su njegovi sistemi i timovi spremni za brzu reakciju na potencijalne napade.

Dobre prakse menadžmenta u upravljanju bezbednosnim rizicima u sajber prostoru obuhvataju različite strategije, od edukacije zaposlenih[32] do implementacije naprednih tehnologija. Organizacije koje se fokusiraju na proaktivan pristup, kontinuirano testiranje i razvoj kultura svesti o bezbednosti, uspevaju da minimiziraju rizike i zaštite svoje resurse. U svetu u kojem su pretnje sve prisutnije, ovakve prakse postaju neophodne za očuvanje sigurnosti i integriteta podataka.

[32] White, J. (2021). Role of Education in Cybersecurity. CRC Press., str. 40-45

Upravljanje bezbednosnim rizicima u sajber prostoru zahteva holistički pristup koji kombinuje tehničke, ljudske i organizacione aspekte. Dobar menadžment je ključan za uspostavljanje okvira koji omogućava organizacijama da se efikasno nose sa pretnjama i izazovima. Kroz edukaciju, strateško planiranje, investicije u tehnologiju i proaktivan pristup, organizacije mogu značajno smanjiti rizik od sajber napada i osigurati sigurnost svojih informacija i infrastrukture.

3.2. Uticaj lošeg menadžmenta na upravljanje bezbednosnim rizicima u sajber prostoru

U savremenom poslovanju, sajber bezbednost postaje sve važnija, a njen uspeh često zavisi od kvaliteta menadžmenta unutar organizacije. Loš menadžment može imati ozbiljne posledice po sposobnost organizacije da adekvatno upravlja bezbednosnim rizicima, što može dovesti do značajnih gubitaka, uključujući finansijske gubitke, gubitak reputacije i pravne posledice. U ovom tekstu istražićemo različite aspekte lošeg menadžmenta i njihov uticaj na sajber bezbednost.

Nedostatak strategije i plana

Jedna od najčešćih grešaka lošeg menadžmenta je odsustvo sveobuhvatne strategije sajber bezbednosti. Bez jasnog plana, organizacije se često suočavaju s problemima u prepoznavanju i prioritetizaciji bezbednosnih rizika. Menadžment koji ne prepoznaje važnost izrade strategije može zanemariti ključne aspekte zaštite, kao što su:

- Procena rizika: Organizacije bez jasno definisanih procedura za procenu rizika često ne mogu pravilno identifikovati i klasifikovati pretnje.
- Nedostatak resursa: Bez strategije, resursi se često neefikasno raspoređuju, što može dovesti do nedostatka potrebnih alata i obuka.

Nedovoljna edukacija i svest zaposlenih

Loš menadžment može rezultirati nedovoljnom edukacijom zaposlenih o sajber bezbednosti. Mnogi incidenti u sajber prostoru su posledica ljudskih grešaka, kao što su otvaranje phishing e-poruka ili korišćenje slabe lozinke. Ukoliko menadžment ne ulaže u obuke i podizanje svesti zaposlenih, organizacija postaje ranjivija na napade.

- Nesvesnost zaposlenih: Kada zaposleni nisu svesni potencijalnih pretnji, lakše mogu postati žrtve napada.
- Zanemarivanje obuka: Redovne obuke i simulacije mogu pomoći zaposlenima da prepoznaju pretnje, dok njihovo izostavljanje stvara opasnu atmosferu.

Nedostatak proaktivnog pristupa

Loš menadžment često ima reaktivni pristup bezbednosti, reagujući na incidente umesto da proaktivno identifikuje i rešava probleme. Ovaj pristup može dovesti do:

- Zagušenja u sistemu: Organizacije koje ne prate i ne analiziraju potencijalne pretnje često se suočavaju s višestrukim napadima pre nego što reše prethodne probleme.

- Kasno otkrivanje pretnji: Nedostatak proaktivnog nadzora[33] znači da se pretnje često ne otkrivaju na vreme, što otežava odgovor na napade.

Neefikasno upravljanje resursima

Menadžment koji ne uspeva da adekvatno upravlja resursima, bilo ljudskim ili tehnološkim, može ozbiljno ugroziti bezbednost organizacije. Neefikasna raspodela resursa može uključivati:

- Nedovoljno osoblja za bezbednost: Organizacije često potcenjuju potrebu za stručnjacima za bezbednost, što može dovesti do preopterećenja postojećih timova i smanjenja efikasnosti.
- Stare tehnologije: Korišćenje zastarelih sistema i softvera bez redovnog ažuriranja čini organizaciju ranjivijom na napade.

Loša komunikacija i koordinacija

Loš menadžment može dovesti do nedostatka komunikacije između različitih odeljenja unutar organizacije. Ova fragmentacija može rezultirati:

- Nejasnim protokolima: Kada se ne deli informacija o bezbednosnim pretnjama, različita odeljenja mogu primeniti različite pristupe, što otežava usklađivanje i koordinaciju.
- Smanjenom efikasnošću: Nedostatak međusobne saradnje može usporiti reakciju na incidente i smanjiti sposobnost organizacije da se brzo prilagodi novim pretnjama.

Pravo reagovanje na incidente

Upravljanje incidentima u sajber prostoru zahteva brzo i efikasno delovanje. Loš menadžment može dovesti do:

- Nejasnih procedura: Ako organizacija nema jasno definisane procedure za reagovanje na incidente, postoji rizik od kašnjenja u reakciji, što može rezultirati većim gubicima.
- Loše postavljeni timovi za odgovor: Timovi koji nisu adekvatno obučeni ili pripremljeni mogu biti nedovoljno efikasni u rešavanju problema, čime se povećava potencijalna šteta.

Pravo upravljanje pravnim i regulatornim zahtevima

Organizacije su često podložne različitim pravnim i regulatornim zahtevima u vezi sa zaštitom podataka. Loš menadžment može dovesti do:

- Neusaglašenosti: Organizacije koje ne prate promene u regulativama mogu se suočiti s pravnim posledicama, uključujući visoke kazne.
- Gubitak poverenja: Nepoštovanje regulativa može ugroziti reputaciju organizacije i smanjiti poverenje klijenata i partnera.

[33] Applied Network Security Monitoring: Collection, Detection, and Analysis – Chris Sanders, Jason Smith (2013), str. 42-46.

Upravljanje bezbednosnim rizicima u sajber prostoru zahteva pažljivo planiranje i sprovođenje strategija koje minimiziraju ranjivosti. Nažalost, mnoge organizacije ne uspevaju da primene efikasne prakse, što može dovesti do ozbiljnih sigurnosnih incidenata. Ovdje su neki od ključnih primera loših praksi menadžmenta i njihove posledice.

Nedostatak strategije sajber bezbednosti

Primer:Equifax

Jedan od najpoznatijih slučajeva lošeg menadžmenta u oblasti sajber bezbednosti desio se u 2017. godini kada je Equifax, jedna od najvećih kreditnih agencija u SAD-u, doživela veliki sigurnosni proboj. Nedostatak sveobuhvatne strategije sajber bezbednosti doveo je do kompromitacije podataka više od 147 miliona ljudi. Organizacija nije imala adekvatne protokole za ažuriranje svojih sistema, što je omogućilo napadačima da iskoriste poznate ranjivosti u softveru.

Neprovođenje redovnih obuka i edukacija zaposlenih

Primer:Yahoo

Yahoo je bio žrtva više sajber napada tokom 2013. i 2014. godine, što je rezultiralo gubitkom podataka o milijardama korisnika. Jedan od ključnih razloga za ovu situaciju bio je nedostatak edukacije i svesti zaposlenih o bezbednosti. Zaposleni nisu bili adekvatno obučeni za prepoznavanje phishing napada i drugih pretnji, što je dovelo do lakog kompromitovanja naloga i podataka.

Nedovoljno investiranje u tehnologiju

Primer:Heartland Payment Systems

Heartland Payment Systems, kompanija koja se bavi procesiranjem plaćanja, doživela je jedan od najvećih sigurnosnih proboja 2008. godine, kada su hakeri ukrali podatke o više od 100 miliona kartica. Loš menadžment se manifestovao kroz nedovoljno ulaganje u savremene tehnologije zaštite podataka, kao što su enkripcija i zaštita od zlonamernog softvera. Rezultat toga bio je ozbiljan gubitak podataka i ugled.

Neusaglašenost sa regulativama

Primer:Marriott International

Marriott je 2018. godine objavio da je došlo do proboja podataka u kojem su bili uključeni podaci o više od 500 miliona gostiju. Istraživanjem je utvrđeno da organizacija nije bila u skladu sa regulativama o zaštiti podataka, kao što je GDPR. Loš menadžment u ovoj situaciji pokazao je nedostatak pravih procedura za zaštitu podataka i reagovanje na pretnje, što je rezultiralo kaznama i gubitkom poverenja potrošača.

Zanemarivanje važnosti komunikacije

Primer:Sony Pictures

Nakon napada na Sony Pictures 2014. godine, postalo je jasno da je menadžment potcenio važnost komunikacije unutar organizacije. Nakon napada, informacije su curile u medije, a zaposleni nisu bili adekvatno obavešteni o situaciji ili kako da postupaju. Ova neorganizovanost je doprinela dodatnom oštećenju reputacije kompanije.

Nedostatak međusobne saradnje između timova

Primer:British Airways

British Airways doživeo je ozbiljan sajber napad 2018. godine koji je rezultirao otkrivanjem podataka o 380.000 korisnika. Analize su pokazale da je loša komunikacija između IT i bezbednosnih timova doprinela incidentu. Menadžment nije uspeo da uspostavi efikasne procese koji bi omogućili saradnju između timova, što je otežalo brzo reagovanje na pretnje.

Zastareli sistemi i softver

Primer:WannaCry napad

WannaCry ransomware napad iz 2017. godine ukazao je na probleme s zastarelim sistemima u organizacijama širom sveta. Mnoge kompanije nisu redovno ažurirale svoje operativne sisteme i softver, što je omogućilo napadačima da iskoriste ranjivosti. Ovaj incident je doveo do gubitaka u milijardama dolara i ukazao na loše upravljanje resursima i nedostatak strategije ažuriranja.

Loše prakse menadžmenta u upravljanju bezbednosnim rizicima u sajber prostoru mogu imati ogromne posledice. Organizacije koje žele da se zaštite od ovih pretnji moraju ulagati u efikasne menadžerske prakse i stvoriti kulturu sajber bezbednosti koja se prostire kroz sve nivoe poslovanja.

Loš menadžment može imati dalekosežne posledice po upravljanje bezbednosnim rizicima u sajber prostoru. Nedostatak strategije, slaba edukacija zaposlenih, neproaktivan pristup, loše upravljanje resursima, loša komunikacija i neusaglašenost s regulativama mogu dovesti do ozbiljnih sigurnosnih incidenata i značajnih gubitaka. Organizacije koje žele da zaštite svoje resurse i reputaciju moraju investirati u efikasan menadžment koji postavlja temelje za snažnu sajber bezbednost.

3.3. Uticaj zaposlenih na upravljanje bezbednosnim rizicima u sajber prostoru

Upravljanje bezbednosnim rizicima u sajber prostoru nije samo pitanje tehnologije i strategije; zaposlenici igraju ključnu ulogu u oblikovanju bezbednosne kulture i sposobnosti organizacije da se zaštiti od pretnji. Njihovo ponašanje, svest i znanje direktno utiču na nivo rizika s kojim se organizacija suočava. U nastavku ćemo detaljno razmotriti kako zaposlenici i njihovo ponašanje utiču na upravljanje bezbednosnim rizicima.

Ljudski faktor kao najslabija karika

Jedan od najznačajnijih aspekata u upravljanju bezbednosnim rizicima je prepoznavanje da su zaposleni često najslabija karika u bezbednosnom lancu. Mnogi sajber napadi se događaju zbog ljudskih grešaka, kao što su

- Otvaranje phishing e-poruka: Zaposleni često ne prepoznaju prevarantske poruke, što može dovesti do kompromitovanja naloga i podataka.
- Korišćenje slabih lozinki: Bez obzira na politiku lozinki, zaposleni često koriste lako pamtljive i slabe lozinke, što povećava rizik od neovlašćenog pristupa.

Edukacija i svest o bezbednosti

Svest zaposlenih o bezbednosnim pretnjama može značajno smanjiti rizike. Organizacije koje ulažu u edukaciju i obuku svojih zaposlenih ostvaruju bolje rezultate u prevenciji incidenata. Efikasne obuke mogu obuhvatati:

- Prepoznavanje pretnji: Učenje o prepoznavanju phishing napada, malware-a i drugih pretnji omogućava zaposlenima da postanu prvi zaštitni sloj bezbednosti.
- Pravilno korišćenje tehnologije: Edukacija o sigurnom korišćenju e-pošte, interneta i poslovnih aplikacija može smanjiti rizik od nepažnje ili grešaka.

Kultura bezbednosti

Organizacije koje razvijaju jaku kulturu bezbednosti uspevaju da podignu svest i odgovornost među zaposlenima. Ova kultura uključuje:

- Ohrabrivanje prijavljivanja incidenta: Zaposleni treba da se osećaju slobodnima da prijave sumnjive aktivnosti bez straha od kazne.
- Pohvale za dobre prakse: Prepoznavanje i nagrađivanje zaposlenih koji sprovode dobre bezbednosne prakse može povećati motivaciju i posvećenost.

Saradnja između timova

Saradnja između različitih timova unutar organizacije može poboljšati upravljanje bezbednosnim rizicima. Kada IT, HR i menadžment rade zajedno na razvoju i sprovođenju bezbednosnih politika, organizacija postaje otpornija. Zaposleni iz različitih sektora mogu doprineti razumevanju pretnji i podeli informacija, što dodatno jača bezbednost.

Uticaj radnog okruženja

Radno okruženje takođe igra značajnu ulogu u ponašanju zaposlenih. Na primer:

- Fleksibilnost i rad na daljinu: Rad na daljinu može povećati rizike ako zaposleni ne koriste adekvatne bezbednosne protokole ili privatne mreže. Organizacije moraju obezbediti jasne smernice za rad od kuće.
- Stres i pritisak: Povećan stres može uticati na koncentraciju i donošenje odluka, što može povećati verovatnoću grešaka u radu s tehnologijom.

Svest o društvenim inženjeringu

Društveni inženjering[34] predstavlja jedan od najčešćih metoda koje napadači koriste za kompromitovanje organizacija. Zaposleni koji nisu svesni ovih tehnika mogu lako postati žrtve. Edukacija o tehnikama društvenog inženjeringa, kao što su lažne telefonske pozive ili pretvaranje da su IT osoblje, može pomoći zaposlenima da budu oprezniji.

Upotreba privatnih uređaja

Upotreba privatnih uređaja (BYOD - Bring Your Own Device) može predstavljati značajan rizik za bezbednost organizacije. Ako zaposleni koriste svoje uređaje za pristup poslovnim podacima bez adekvatnih bezbednosnih mera, rizik od gubitka podataka se povećava. Organizacije bi trebalo da uspostave jasne politike o korišćenju privatnih uređaja i da obezbede alate za zaštitu podataka.

Ponašanje u slučaju incidenata

Kako zaposleni reaguju na bezbednosne incidente može značajno uticati na posledice. Na primer:

- Brza reakcija: Zaposleni koji su obučeni za pravilan postupak u slučaju incidenta mogu brzo prijaviti incident i umanjiti štetu.
- Nepovezivanje sa IT timom: Ako zaposleni ne obaveštavaju IT tim o incidentima, to može odložiti odgovor i povećati štetu.

Primer dobrih praksi zaposlenih i njihovog ponašanja na upravljanje bezbednosnim rizicima u sajber prostoru

U savremenom poslovanju, zaposleni igraju ključnu ulogu u održavanju sigurnosti podataka i infrastrukture. Dobre prakse koje zaposleni primenjuju mogu značajno smanjiti rizik od sajber napada i drugih bezbednosnih incidenata. U ovom tekstu, fokusiraćemo se na konkretne primere organizacija koje su uspešno implementirale efikasne prakse i kako je to uticalo na upravljanje bezbednosnim rizicima.

Kultura bezbednosti: Primer kompanije Cisco

Cisco Systems, globalni lider u tehnologiji i mrežnim rešenjima, stvorio je snažnu kulturu bezbednosti kroz sveobuhvatan pristup koji uključuje edukaciju, obuke i aktivno uključivanje zaposlenih. Njihov program "Be Secure" ima za cilj da podigne svest o bezbednosti među svim zaposlenima.

- Edukacija i obuka: Cisco redovno organizuje obuke o sajber bezbednosti, uključujući simulacije napada i vežbe za prepoznavanje pretnji. Zaposleni su upoznati sa različitim tipovima napada, kao što su phishing i ransomware, čime se povećava njihova svest i sposobnost reagovanja.
- Prijavljivanje incidenata: Cisco podstiče zaposlene da prijave sumnjive aktivnosti i potencijalne bezbednosne pretnje putem jednostavne platforme za prijavu. Ovaj pristup ne samo da pomaže u bržem otkrivanju pretnji, već i stvara otvorenu komunikaciju između zaposlenih i IT tima.

[34] Social Engineering: The Science of Human Hacking – Christopher Hadnagy (2018), str. 55-59.

- Nagrade za najbolje prakse: Zaposleni koji prepoznaju i prijave pretnje često su nagrađivani, što dodatno motiviše timove da budu proaktivni u očuvanju bezbednosti.

Proaktivan pristup: Primer kompanije Google

Google je poznat po svom proaktivnom pristupu bezbednosti. Organizacija se fokusira na razvoj alata i politika koje osnažuju zaposlene u prepoznavanju i sprečavanju bezbednosnih rizika.

- Višefaktorska autentifikacija: Google je implementirao višefaktorsku autentifikaciju kao standardnu praksu za sve zaposlene. Ova mera značajno smanjuje rizik od neovlašćenog pristupa, jer zahteva dodatne potvrde identiteta.
- Redovne vežbe: Zaposleni prolaze kroz redovne simulacije bezbednosnih incidenata, koje im pomažu da se pripreme za moguće napade. Ove vežbe uključuju testove na prepoznavanje phishing napada i učenje o reakciji u slučaju hakerskih proboja.
- Transparentnost i otvorena komunikacija: Google promoviše kulturu otvorenosti, gde zaposleni slobodno dele informacije o bezbednosnim pretnjama i uspešnim preventivnim merama. Ovaj pristup stvara zajednicu koja aktivno učestvuje u jačanju bezbednosti.

Saradnja i timski rad: Primer kompanije IBM

IBM je uspešno integrisao saradnju između različitih odeljenja kako bi poboljšao upravljanje bezbednosnim rizicima. Ova saradnja omogućava bolju koordinaciju i brže reagovanje na potencijalne pretnje.

- Interdisciplinarni timovi: IBM formira timove koji uključuju članove iz IT, pravnog, operativnog i ljudskih resursa, čime se osigurava da svi aspekti bezbednosti budu pokriveni. Ovi timovi redovno razmenjuju informacije i strategije.
- Deljenje znanja: Zaposleni su podstaknuti da dele iskustva i lekcije naučene iz prethodnih incidenata. Ova praksa pomaže u jačanju kolektivnog znanja o pretnjama i mogućim rešenjima.
- Simulacije i vežbe: IBM sprovodi redovne simulacije sajber napada koje uključuju sve relevantne timove. Ove vežbe omogućavaju zaposlenima da testiraju svoje veštine u realnim uslovima i identifikuju područja koja zahtevaju poboljšanje.

Svesnost o pretnjama: Primer kompanije JPMorgan Chase

JPMorgan Chase, jedna od najvećih finansijskih institucija na svetu, pokazala je kako svesnost o pretnjama među zaposlenima može značajno smanjiti rizike.

- Obuka o prepoznavanju pretnji: Kompanija pruža obuke za zaposlene o tehnikama društvenog inženjeringa i kako prepoznati sumnjive aktivnosti. Ova edukacija povećava svest o potencijalnim pretnjama i čini zaposlene opreznijima.
- Kampanje za podizanje svesti: JPMorgan Chase redovno sprovodi kampanje koje imaju za cilj podizanje svesti o sajber bezbednosti. Ove kampanje uključuju postere, email obaveštenja i interne radionice, što doprinosi jačanju bezbednosne kulture.

- Podsticanje odgovornosti: Organizacija podstiče zaposlene da preuzmu odgovornost za bezbednost informacija. Svi zaposleni su uključeni u bezbednosne politike i procedure, čime se stvara zajednički front protiv sajber pretnji.

Dobre prakse zaposlenih i njihovo ponašanje igraju ključnu ulogu u upravljanju bezbednosnim rizicima u sajber prostoru. Organizacije koje ulažu u edukaciju, saradnju i kulturu bezbednosti uspevaju da smanje rizike i zaštite svoje podatke i infrastrukturu. Primeri kompanija kao što su Cisco, Google, IBM i JPMorgan Chase ilustruju kako angažovanje zaposlenih može značajno unaprediti bezbednosne protokole i stvoriti otpornije organizacije. U svetu u kojem su sajber pretnje sve prisutnije, aktivno uključivanje zaposlenih u procese zaštite postaje imperativ za svaku organizaciju.

Sa druge strane, loše prakse zaposlenih i njihovo ponašanje predstavljaju značajan izazov za upravljanje bezbednosnim rizicima u sajber prostoru. Od nedostatka obuke do ignorisanja bezbednosnih politika, ovakvi primeri ukazuju na to koliko je važno imati efikasne programe obuke i jasan sistem komunikacije o bezbednosnim pitanjima. Organizacije koje žele da zaštite svoje resurse i podatke moraju aktivno raditi na podizanju svesti među zaposlenima i implementaciji strogih bezbednosnih politika. Samo kroz kolektivnu odgovornost i kontinuiranu edukaciju mogu se smanjiti rizici i zaštititi integritet organizacije.

Zaposleni su ključni faktor u upravljanju bezbednosnim rizicima u sajber prostoru. Njihovo ponašanje, svest i edukacija direktno utiču na nivo zaštite organizacije. Ulaganjem u edukaciju, razvoj kulture bezbednosti i efikasnu saradnju između timova[35], organizacije mogu značajno smanjiti rizik od sajber napada i osigurati sigurnost svojih podataka. Ova integracija ljudskog faktora u strategije bezbednosti je presudna za izgradnju otpornije organizacije u svetu prepunom pretnji.

GLAVA 4: STRATEŠKO UPRAVLJANJE BEZBEDNOSNIM RIZICIMA U SAJBER PROSTORU

Strateško upravljanje je proces planiranja, implementacije i evaluacije dugoročnih ciljeva i strategija unutar organizacije. Ono uključuje analizu unutarnjih i vanjskih faktora koji utječu na organizaciju, postavljanje ciljeva koji su usklađeni s njenom vizijom i misijom, te alokaciju resursa za ostvarenje tih ciljeva. Strateško upravljanje također podrazumijeva kontinuirano praćenje i prilagodbu strategija kako bi se odgovorilo na promjene u okruženju i osigurala održivost i konkurentnost organizacije.

Strateško upravljanje zasnovano na uticaju bezbednosnih rizika u sajber prostoru je sistematski pristup koji se fokusira na identifikaciju, analizu i minimizaciju sajber pretnji kako bi se zaštitili kritični resursi organizacije. Ovaj pristup obuhvata procenu rizika, razvoj strategija zaštite, planove za odgovor na incidente i kontinuirano praćenje, s ciljem očuvanja integriteta, poverljivosti i dostupnosti informacija, te osiguranja poslovne otpornosti i usklađenosti sa regulativama.

[35] White, L. (2020). Collaborative Cyber Threat Management. Syngress., str. 40-45

Pristup strateškom upravljanju zasnovan na upravljanju bezbednosnim rizicima fokusira se na identifikaciju, procenu i minimizaciju rizika koji mogu ugroziti organizaciju, njene informacije i sisteme. Ovaj pristup uključuje nekoliko ključnih koraka:

- Identifikacija rizika: Analiziranje potencijalnih pretnji, uključujući fizičke, tehničke i ljudske faktore, koji mogu uticati na bezbednost organizacije.
- Procena rizika: Kvalitativna i kvantitativna analiza rizika kako bi se utvrdila verovatnoća i potencijalni uticaj svakog rizika na poslovanje.
- Strategije upravljanja rizicima:
    - Prevencija: Implementacija mera za sprečavanje nastanka rizika, kao što su sigurnosne politike, obuka zaposlenih i tehničke zaštite.
    - Otkrivanje: Uvođenje sistema za ranog upozoravanja na pretnje ili incidente, kao što su alati za nadzor i analizu podataka.
    - Reakcija: Razvijanje planova za odgovor na incidente i obnavljanje poslovanja, uključujući krizne planove[36] i procedure oporavka.
- Kontinuirano praćenje i evaluacija: Stalno pratiti i procenjivati efikasnost implementiranih mera i strategija, te prilagoditi pristupe na osnovu promena u pretnjama ili poslovnom okruženju.
- Usklađenost s propisima: Osiguravanje da organizacija ispunjava relevantne zakonske i regulatorne zahteve vezane za bezbednost informacija.

Ovaj pristup omogućava organizacijama da izgrade otpornije poslovne modele, smanje potencijalne gubitke i povećaju poverenje klijenata i partnera.

Strateško upravljanje bezbednosnim rizicima u sajber prostoru postaje ključno zbog sveprisutne digitalizacije i rastuće kompleksnosti sajber pretnji. Organizacije moraju kontinuirano identifikovati i pratiti različite vrste sajber pretnji, kao što su malware, phishing, ransomware, i DDoS napadi. Razumevanje specifičnih pretnji koje mogu uticati na poslovanje je osnovni korak. Procena rizika uključuje analizu verovatnosti napada i njihovog potencijalnog uticaja na organizaciju. To može uključivati procene ranjivosti sistema, vrednovanje podataka koji se čuvaju, i identifikaciju kritičnih infrastruktura. Na osnovu procene rizika, organizacije trebaju razviti sveobuhvatne strategije zaštite koje mogu uključivati:

- Tehničke mere: Korišćenje antivirusnih programa, firewall-a, enkripcije i redovnog ažuriranja softvera.
- Organizacione politike: Postavljanje pravila o korišćenju tehnologije i obuka zaposlenih o sajber bezbednosti[37].
- Planovi za odgovor na incidente: Uključivanje procedura za brzo reagovanje na sajber napade, uključujući timove za upravljanje incidentima.

Redovno praćenje sajber okruženja i procena efikasnosti zaštitnih mera su ključni. To uključuje analizu logova, korišćenje alata za detekciju pretnji i izvođenje redovnih bezbednosnih proba. Organizacije moraju biti svesne i pridržavati se relevantnih zakona i regulativa vezanih za zaštitu podataka i sajber bezbednost, kao što su GDPR, HIPAA ili drugi lokalni propisi. Saradnja s drugim organizacijama, sektorima i vladinim agencijama može poboljšati

[36] White, K. (2021). Crisis Management in Cybersecurity. CRC Press., str. 50-55
[37] Wright, T. (2020). Cybersecurity Training Programs for Employees. Wiley., str. 40-45

sposobnost identifikacije i odgovora na pretnje. Deljenje informacija o pretnjama i najboljim praksama može ojačati ukupnu otpornost sektora.

Cilj pristupa strateškog upravljanja zasnovanog na uticaju bezbednosnih rizika u sajber prostoru je osiguranje sveobuhvatne zaštite organizacije od potencijalnih pretnji, dok se istovremeno minimiziraju negativni uticaji tih pretnji na poslovanje. Sveukupno, cilj je izgradnja sveobuhvatnog, proaktivnog pristupa koji omogućava organizacijama da se efikasno suoče sa dinamičnim sajber okruženjem.

Kako navodi izvor McKinsey & Company : ” Proaktivan pristup upravljanju sajber rizikom može pomoći organizacijama ne samo da zaštite svoju imovinu već i da steknu konkurentsku prednost”, dok Harvard Business Review navodi: ” Kompanije moraju da razmatraju sajber bezbednost ne samo kao problem tehnologije, već i kao poslovni rizik koji utiče na njihovu ukupnu strategiju.

Strateško upravljanje bezbednosnim rizicima u sajber prostoru zahteva holistički pristup, kombinovanje tehnologije, politike i ljudskog faktora. U svetu u kojem su sajber pretnje sve sofisticiranije, proaktivan i sveobuhvatan pristup je od suštinskog značaja za zaštitu organizacija i njihovih podataka.

4.1 Kratak istorijski pregled upravljanja bezbednosnim rizicima u sajber prostoru

Bezbednosni rizici u sajber prostoru odnose se na potencijalne pretnje i ranjivosti koje mogu ugroziti informacije, sisteme, mreže i infrastrukturu organizacija[38]. Ovi rizici obuhvataju širok spektar opasnosti koje mogu nastati usled zlonamernih aktivnosti, kao što su sajber napadi, ali i zbog nesreća, grešaka ili loših praksi u upravljanju tehnologijama.

U savremenom digitalnom okruženju, upravljanje bezbednosnim rizicima u sajber prostoru postalo je ključno za zaštitu organizacija od sve sofisticiranijih pretnji. Sa rastućom globalizacijom i povezanosti, sajber napadi su postali ne samo tehnološki izazov, već i ozbiljna pretnja poslovnim operacijama, reputaciji i poverenju korisnika. Istorijski gledano, bezbednost informacija nije bila prioritet sve do kraja 20. veka, kada su se prvi ozbiljniji incidenti ukazali na potrebu za sistematskim pristupima zaštiti podataka.

Od ranih dana kada su se računarstvo i mreže tek razvijali, do današnjih naprednih strategija kao što su modeli zasnovani na konceptu "Zero Trust", evolucija upravljanja bezbednosnim rizicima odražava složenost i dinamičnost sajber prostora. Ovaj istorijski pregled istražuje ključne etape u razvoju upravljanja bezbednosnim rizicima, osvetljava važne zakonske i tehničke aspekte, kao i izazove s kojima se organizacije suočavaju danas. Kroz razumevanje ovih aspekata, možemo bolje shvatiti kako efikasno upravljati rizicima i osigurati sigurnost informacija u svetu koji se brzo menja.

[38] Thompson, G. (2020). Network Security Requirements for Enterprises. Apress., str. 42-47

Istorijski pregled upravljanja bezbednosnim rizicima u sajber prostoru

Rani razvoj (1960-1980-e)

U ranim danima računarstva, bezbednost nije bila prioritet. Računari su se koristili pretežno u akademskim i vojnim krugovima. Prvi oblici bezbednosti fokusirali su se na fizičku zaštitu i pristupne kontrole.

- 1960-e: Razvoj prvih operativnih sistema doveo je do svesti o potrebi zaštite podataka. Uvođenje tehnika kao što su autentifikacija i kontrola pristupa počelo je da se razvija.
- 1970-e: Uvođenje koncepta "sajber kriminala" uzrokovano je sve većim korišćenjem mreža. Prvi dokumentovani sajber napad desio se 1982. godine kada su Rusi sabotirali sistem kanadske kompanije.

Formalizacija bezbednosti (1980-e-1990-e)

Tokom 1980-ih i 1990-ih, kako su se računari i mreže sve više povezivali, bezbednost podataka postala je ključno pitanje.

- 1986: Donet je Computer Fraud and Abuse Act u SAD-u, prvi zakon koji se bavio kompjuterskim prevarama i zloupotrebama.
- 1990-e: Razvoj interneta doveo je do eksponencijalnog povećanja pretnji. Pojava virusa i wormova, kao što su "Morris worm" 1988. godine, podstakla je razvoj antivirusnih softvera i proaktivnijeg pristupa bezbednosti.

Uspon cyber bezbednosti (2000-e)

S početkom novog milenijuma, bezbednost u sajber prostoru postala je vitalni deo strategije svake organizacije.

- 2001: Teroristički napadi 11. septembra u SAD-u doveli su do povećane svesti o bezbednosti, ne samo fizičkoj, već i digitalnoj. Osnovana je **Homeland Security Department**, koja je uključila i aspekte sajber bezbednosti.
- 2003: Uvođenje ISO/IEC 27001, standarda za upravljanje bezbednošću informacija, postavilo je temelje za sistematsko upravljanje bezbednosnim rizicima.
- 2004: NIST (National Institute of Standards and Technology) objavljuje prvi Cybersecurity Framework, pružajući organizacijama smernice za procenu i poboljšanje njihove bezbednosne prakse.

Evolucija i izazovi (2010-e)

Tokom 2010-ih, učestalost i sofisticiranost sajber napada drastično su porasli.

- 2013: Napadi poput Target i Yahoo ukazali su na ranjivosti velikih korporacija, što je rezultiralo usvajanjem strožih politika zaštite podataka i implementacijom višefaktorske autentifikacije.
- 2014: Sony Pictures hack osvetlio je problem unutrašnjih pretnji i značaj proaktivnog pristupa upravljanju rizicima.
- 2016: Pojava WannaCry ransomware napada pokazala je koliko je važno imati planove za odgovor na incidente i strategije za oporavak.

Savremeni pristupi (2020-e)

Danas, upravljanje bezbednosnim rizicima u sajber prostoru obuhvata širok spektar tehnika i strategija.

- Uspon Zero Trust modela: Organizacije sve više usvajaju pristup zasnovan na konceptu "nikome se ne veruje", što uključuje rigorozne provere identiteta i kontrolu pristupa.
- Regulativa i usklađenost**: Uvođenje zakona kao što je GDPR (General Data Protection Regulation) u Evropi postavilo je nove standarde zaštite podataka, čime se dodatno naglašava potreba za sistematskim upravljanjem rizicima.
- Veštačka inteligencija i analitika: Upotreba AI i mašinskog učenja postaje ključna u prepoznavanju i odgovoru na pretnje, omogućavajući brže i efikasnije upravljanje rizicima.

Upravljanje bezbednosnim rizicima u sajber prostoru evoluiralo je kroz različite faze, od osnovne zaštite fizičkih sistema do složenih, sistematskih pristupa koji uključuju tehnologiju, ljude i procese. Kako se pretnje razvijaju, tako će se i pristupi upravljanju rizicima morati prilagoditi, s ciljem očuvanja bezbednosti informacija i poslovnih operacija.
Sa ekonomskog stanovišta, bezbednosni rizici predstavljaju potencijalne pretnje koje mogu izazvati gubitke ili smanjenje vrednosti resursa unutar organizacije. Ovi rizici se javljaju u kontekstu ekonomskih odluka i strategija, i obuhvataju aspekte kao što su finansijski gubici, troškovi oporavka, reputacijski uticaji i pravne posledice.

Ključni aspekti bezbednosnih rizika sa ekonomskog stanovišta:

1. **Finansijski gubici:**
   - Direktni troškovi: Gubici nastali usled sajber napada, kao što su otkupi za vraćanje podataka ili troškovi popravke i obnavljanja sistema.
   - Indirektni troškovi: Troškovi koji se odnose na prekid poslovanja, gubitak prodaje i smanjenje produktivnosti.
2. **Troškovi upravljanja rizicima:**
   - Investicije u tehnologiju: Troškovi za implementaciju sigurnosnih rešenja, kao što su antivirusni programi, firewall-ovi i sistemi za detekciju upada.
   - Obuka zaposlenih: Troškovi obuka i edukacije zaposlenih o pravilima bezbednosti i prepoznavanju pretnji.
3. **Reputacijski rizici:**
   - Gubitak poverenja: Sajber incidenti mogu značajno smanjiti poverenje kupaca i partnera, što može uticati na prodaju i tržišni udeo.
   - Dugi rok: Gubici reputacije često se manifestuju kroz smanjenje klijenata ili povećanje troškova marketinga potrebnih za obnavljanje brenda.
4. **Pravni i regulatorni troškovi:**
   - Kazne i tužbe: Neuspeh u zaštiti podataka može dovesti do pravnih posledica i kazni, posebno u svetlu regulativa kao što je GDPR.
   - Troškovi usklađenosti: Troškovi povezani s implementacijom politika i procedura koje osiguravaju usklađenost s propisima o zaštiti podataka.

5. **Uticaj na poslovne odluke:**
    - Procena rizika: Organizacije moraju uzeti u obzir bezbednosne rizike prilikom donošenja ekonomskih odluka, kao što su ulaganja u nove tehnologije ili ekspanziju na nova tržišta.
    - Strategije mitigacije: Razvijanje strategija za upravljanje bezbednosnim rizicima može postati deo šire poslovne strategije, usmerene na dugoročnu održivost i otpornost.

Sa ekonomskog stanovišta, bezbednosni rizici nisu samo tehnički problem, već ključna komponenta poslovnog upravljanja. Efikasno upravljanje ovim rizicima može zaštititi organizaciju od značajnih gubitaka, poboljšati operativnu efikasnost i očuvati reputaciju, što je od vitalnog značaja za dugoročnu održivost i uspeh. Kroz sveobuhvatan pristup upravljanju rizicima, organizacije mogu optimizovati svoje resurse i stvoriti stabilno poslovno okruženje.

Tabela 1. Promene fokusa menadžmenta bezbednosnih rizika u sajber prostoru kroz istorijski kontekst

Period	Fokus menadžmenta bezbednosnih rizika	Ključne karakteristike
1960-e	Fizička sigurnost i pristupne kontrole	Ograničen broj korisnika, fokus na fizičku zaštitu računara.
1970-e	Osnovna zaštita podataka	Početak razumevanja sajber kriminala, razvoj autentifikacije.
1980-e	Razvoj zakonodavstva i pravnih okvira	Uvođenje zakona o kompjuterskim prevarama, rast svesti o sajber pretnjama.
1990-e	Antivirusna zaštita i proaktivne mere	Povećanje pretnji, razvoj antivirusnih programa i sistema za zaštitu.
2000-e	Strateško upravljanje i integracija IT bezbednosti	Uključivanje bezbednosti u poslovne strategije, razvoj standarda kao što je ISO 27001.
2010-e	Složenije strategije i fokus na organizacione politike	Povećana svest o pretnjama, razvoj planova za odgovor na incidente.
2020-e i nadalje	Proaktivan pristup i model "Zero Trust"	Integracija AI i mašinskog učenja, usmerenje na zaštitu podataka i usklađenost sa regulativama.

Opis promene fokusa

Rani periodi: Fokus se više oslanjao na fizičke mere zaštite i osnovne bezbednosne protokole.

1980-e i 1990-e: Razvoj tehnologije doveo je do povećanih pretnji, što je rezultiralo potrebom za razvojem antivirusnih rešenja.

2000-e: Strateško upravljanje bezbednošću postalo je ključno, s naglaskom na integraciju bezbednosti u celokupnu poslovnu strategiju.

2010-e do danas: Pristupi se sve više fokusiraju na proaktivne mere, uključujući moderne tehnologije i nove paradigme poput "Zero Trust", čime se stvara otpornije okruženje na sajber pretnje.

Strateško upravljanje bezbednosnim rizicima u sajber prostoru podrazumeva sveobuhvatan i proaktivan pristup koji uključuje identifikaciju, analizu, mitigaciju i monitoring rizika povezanih sa informacijama, sistemima i mrežama. Danas, strateško upravljanje bezbednosnim rizicima u sajber prostoru predstavlja dinamičan proces koji se neprestano prilagođava novim pretnjama i tehnologijama. Organizacije moraju usvojiti proaktivan pristup, gde je bezbednost integralni deo njihove strategije i kulture, kako bi se osigurala otpornost na sajber pretnje i očuvala integritet informacija.

U savremenom digitalnom svetu, strateško upravljanje bezbednosnim rizicima u sajber prostoru predstavlja ključno opredeljenje za svaku organizaciju koja želi da očuva svoju operativnu efikasnost, reputaciju i poverenje klijenata. Kako se pretnje stalno razvijaju i postaju sve sofisticiranije, organizacije ne mogu više da se oslanjaju na reaktivne mere zaštite. Umesto toga, proaktivan pristup koji uključuje identifikaciju, analizu, mitigaciju i monitoring rizika postaje neophodan.

Uspostavljanjem sveobuhvatnih strategija upravljanja rizicima, organizacije mogu bolje zaštititi svoje informacije, resurse i ljude, minimizirajući potencijalne gubitke i pravne posledice. Takođe, edukacija zaposlenih i razvijanje kulture bezbednosti unutar organizacije igraju ključnu ulogu u jačanju otpornosti na sajber napade[39].

Na kraju, strateško upravljanje bezbednosnim rizicima ne samo da obezbeđuje sigurnost podataka, već i doprinosi dugoročnoj održivosti i uspehu poslovanja. U svetu u kojem su digitalne tehnologije neizostavan deo svakodnevnog poslovanja, ulaganje u bezbednost predstavlja investiciju u budućnost.

4.2. Perspektive upravljanja bezbednosnim rizicima u sajber prostoru

Upravljanje bezbednosnim rizicima u sajber prostoru ima ključnu ulogu u zaštiti informacija, sistema i mreža od pretnji koje mogu ugroziti integritet, poverljivost i dostupnost podataka. Ono je od vitalnog značaja za očuvanje operativne efikasnosti i dugoročne održivosti organizacija.

Perspektive upravljanja bezbednosnim rizicima u sajber prostoru se konstantno menjaju u skladu sa promenama u poslovnom okruženju i društvu. Upravljanje bezbednosnim rizicima u sajber prostoru se neprestano razvija, kako se tehnologije, pretnje i regulatorni zahtevi menjaju. Ove perspektive pružaju uvid u buduće pravce i pristupe[40] koje organizacije mogu usvojiti za efikasnije upravljanje rizicima.

[39] Nelson, F. (2021). Building Resilience to Cyber Attacks. Wiley.", str. 42-46
[40] Hughes, V. (2021). Future Technologies in Cybersecurity. Apress., str. 40-45

Evolucija pretnji

Sa razvojem tehnologije, takođe se menjaju i metode napada. Napadi postaju sve sofisticiraniji i usmereni, što zahteva inovativne pristupe u upravljanju bezbednosnim rizicima. Organizacije će morati da:

- Prate trendove sajber kriminala: Razumevanje novih tehnika i strategija koje koriste napadači može pomoći u prevenciji incidenata.
- Unaprede mehanizme učenja iz pretnji: Korišćenje veštačke inteligencije i mašinskog učenja za analizu obrazaca ponašanja napadača.

Integracija veštačke inteligencije (AI) i mašinskog učenja

Tehnologije poput AI i mašinskog učenja nude mogućnosti za unapređenje upravljanja bezbednosnim rizicima:

- Automatizacija detekcije pretnji: AI može pomoći u identifikaciji neobičnih obrazaca u mrežnom saobraćaju i potencijalnim napadima u realnom vremenu.
- Proaktivan odgovor: Razvijanje sistema koji mogu automatski reagovati na pretnje, smanjujući vreme reakcije i potencijalne štete.

Model "Zero Trust"

Model "Zero Trust" postaje sve popularniji kao odgovor na tradicionalne pristupe bezbednosti:

- Nema povjerenja prema ničemu: Svaki pristup sistemima ili podacima zahteva autentifikaciju i autorizaciju, bez obzira na to da li dolazi iz unutrašnje ili spoljne mreže.
- Segmentacija mreže: Razvijanje mikro-segmentacije kako bi se ograničio pristup i smanjila mogućnost lateralnog kretanja napadača unutar mreže.

Pristup zasnovan na riziku

Organizacije se sve više oslanjaju na pristup zasnovan na riziku kako bi prioritetizovale resurse i napore:

- Evaluacija poslovnog uticaja: Razumevanje potencijalnog uticaja različitih pretnji na poslovne procese omogućava fokusiranje na najvažnije rizike.
- Dinamika resursa: Prilagođavanje investicija u bezbednost na osnovu trenutnog stanja rizika i pretnji.

Regulatorna i pravna usklađenost

Sa sve većim brojem zakonskih regulativa u vezi sa zaštitom podataka, kao što su GDPR i CCPA:

- Povećanje svesti o usklađenosti: Organizacije će morati da se fokusiraju na usklađenost sa sve strožim pravilima o zaštiti podataka.
- Uloga advokata u bezbednosti: Saradnja između pravnih timova i IT odeljenja postaje neophodna za razumevanje i implementaciju zakonskih zahteva.

Kultura bezbednosti i obuka

Svest o bezbednosti među zaposlenima je ključna za efikasno upravljanje rizicima:

- Redovne obuke: Organizacije će morati da implementiraju kontinuirane obuke i simulacije kako bi edukovale zaposlene o pretnjama i pravilima ponašanja.
- Razvijanje kulture bezbednosti: Stvaranje okruženja u kojem je bezbednost prioritet može smanjiti ljudske greške koje često vode do incidenata.

Saradnja i deljenje informacija

S obzirom na globalni karakter sajber pretnji, saradnja između organizacija i industrija postaje sve važnija:

- Deljenje informacija o pretnjama: Učešće u zajednicama za razmenu informacija o pretnjama može pomoći u unapređenju kolektivne bezbednosti.
- Partnerstva sa vladinim agencijama: Saradnja s vladinim institucijama može obezbediti dodatne resurse i informacije.

U budućnosti, upravljanje bezbednosnim rizicima u sajber prostoru biće definisano kroz nekoliko ključnih aspekata koji će odražavati evoluciju tehnologije, pretnji i pristupa bezbednosti. To e svakako biti shvaćeno kao sveobuhvatan, proaktivan i adaptivan proces koji se oslanja na moderne tehnologije, etičke standarde i saradnju. Ovaj pristup će omogućiti organizacijama da se efikasno suoče s rastućim izazovima u sajber bezbednosti, obezbeđujući zaštitu podataka i resursa u dinamičnom digitalnom okruženju.

Jedan od jasnih primera je i NIS2 direktiva[41] koja je usvojena u okviru Evropske unije, i predstavlja značajan korak ka jačanju sajber bezbednosti širom EU. Ova direktiva proširuje obaveze prethodne NIS (Direktiva o mrežnoj i informatičkoj sigurnosti) direktive, postavljajući jasnije i strožije zahteve za upravljanje bezbednosnim rizicima. NIS2 ima za cilj da poboljša otpornost na sajber pretnje u kritičnim sektorima, kao što su energija, transport, zdravstvo i digitalne usluge.

Proširenje obaveza i opsega

NIS2 direktiva uvodi širi spektar sektora i usluga koji su obuhvaćeni regulativom:

- Obuhvat više sektora: Svi pružaoci usluga u kritičnim sektorima, kao i digitalne usluge, sada imaju obavezu da uspostave odgovarajuće mere bezbednosti.
- Mali i srednji preduzetnici: Iako su veće kompanije najčešće na meti, mala i srednja preduzeća[42] koja pružaju kritične usluge takođe će biti podložna obavezama usklađenosti.

Povećane obaveze u vezi sa upravljanjem rizicima

NIS2 direktiva zahteva od organizacija da razviju sveobuhvatne strategije upravljanja rizicima:

- Procena rizika: Organizacije će morati da redovno sprovode procene rizika kako bi identifikovale potencijalne pretnje i ranjivosti.

[41] Green, A. (2021). Compliance Strategies for NIS2 Directive. Bloomsbury Professional., str. 30-35
[42] Johnson, P. (2021). Cybersecurity Support for Small Businesses. Wiley., str. 35-39

- Proaktivan pristup: Direktiva naglašava važnost proaktivnih mera za mitigaciju rizika, što uključuje implementaciju tehničkih i organizacionih mera zaštite.

Izveštavanje o incidentima

Jedna od ključnih stavki NIS2 direktive je obaveza izveštavanja o bezbednosnim incidentima:

- Brzo obaveštavanje: Organizacije su dužne da obaveštavaju relevantne vlasti o značajnim incidentima u roku od 24 sata.
- Standardizacija procedura: Uspostavljanje standardizovanih procedura za izveštavanje olakšaće razmenu informacija i brži odgovor na pretnje.

Saradnja i deljenje informacija

NIS2 direktiva naglašava potrebu za saradnjom između država članica i privatnog sektora:

- Zajednička platforma za deljenje informacija: Direktiva podstiče uspostavljanje mehanizama za razmenu informacija o pretnjama i najboljim praksama.
- Edukacija i obuka: Organizacije će biti ohrabrene da učestvuju u zajedničkim programima obuke i vežbama kako bi poboljšale kapacitete za odgovor na incidente.

Uloga nacionalnih[43] i evropskih agencija

NIS2 direktiva postavlja osnovu za jaču saradnju između nacionalnih i evropskih agencija:

- Jačanje kapaciteta: Države članice će morati da osnaže svoje nacionalne kapacitete za upravljanje rizicima i odgovor na incidente.
- Koordinacija na evropskom nivou: Uspostaviće se mehanizmi za koordinaciju i razmenu informacija na evropskom nivou, što će omogućiti efikasniji odgovor na transnacionalne pretnje.

Upravljanje bezbednosnim rizicima u sajber prostoru, u svetlu NIS2 direktive, postaje sveobuhvatan i obavezan proces za organizacije u EU. Ova direktiva ne samo da postavlja jasne zahteve, već i podstiče kulturu saradnje i deljenja informacija među svim akterima. Kako se pretnje nastavljaju razvijati, usvajanje proaktivnog pristupa upravljanju rizicima biće ključno za očuvanje bezbednosti i otpornosti organizacija.

Dalje, upravljanje bezbednosnim rizicima u sajber prostoru ne može se posmatrati samo kroz tehničke aspekte, već uključuje i ključnu ulogu ljudskih resursa. Ljudi su često najslabija karika u lancu bezbednosti, ali istovremeno i najvažniji faktor u održavanju visokog nivoa bezbednosti. Upravljanje bezbednosnim rizicima u sajber prostoru iz ugla ljudskih resursa naglašava važnost ljudskog faktora u bezbednosti organizacije. Kroz edukaciju, razvoj kulture bezbednosti, pažljivu selekciju i angažovanje zaposlenih, organizacije mogu značajno smanjiti rizike i unaprediti svoju ukupnu otpornost na sajber pretnje. Ljudi su ključni za implementaciju i održavanje bezbednosnih strategija, čineći ih neizostavnim partnerima u borbi protiv sajber kriminala.

Takođe perspektivu razvoja upravljanja bezbednosnim rizicima u sajber prostoru treba posmatrati i sa aspekta organizacione teorije i prakse. Upravljanje bezbednosnim rizicima u sajber prostoru iz perspektive organizacione teorije i prakse obuhvata analizu kako

[43] National Cybersecurity Strategies in Practice – D. Kovačević (2021), str. 30-35.

organizacione strukture, kulture i dinamika utiču na sposobnost organizacija da efikasno upravljaju rizicima. Ova perspektiva može se sagledati kroz nekoliko ključnih aspekata:

Organizaciona struktura i dizajn

Organizacije moraju razviti strukture koje omogućavaju efikasno upravljanje bezbednosnim rizicima:

- Centralizovane vs. decentralizovane strukture: Centralizovani modeli mogu olakšati koordinaciju i doslednost u sprovođenju bezbednosnih politika, dok decentralizovani modeli omogućavaju brže reakcije na lokalne pretnje.
- Uloga interdisiplinarnih timova: Formiranje timova koji uključuju članove iz različitih odeljenja (IT, pravni, ljudski resursi) može doprineti holističkom pristupu bezbednosti.

Kultura organizacije

Kultura organizacije igra ključnu ulogu u upravljanju bezbednosnim rizicima:

- Svesnost o bezbednosti: Organizacije koje razvijaju kulturu bezbednosti, gde su svi zaposleni svesni svojih uloga u zaštiti podataka, često su otpornije na napade.
- Podsticaj za prijavljivanje incidenata: Otvorena komunikacija i podsticanje zaposlenih da prijave potencijalne pretnje mogu pomoći u ranom otkrivanju problema.

Liderstvo[44] i strategija

Liderstvo ima značajnu ulogu u oblikovanju pristupa upravljanju rizicima:

- Zagovaranje bezbednosti na najvišem nivou: Kada rukovodstvo aktivno promoviše bezbednosne inicijative, organizacija dobija veći legitimitet i resurse za implementaciju bezbednosnih mera.
- Integracija bezbednosti u poslovne strategije: Uključivanje bezbednosti u šire poslovne strategije osigurava da se rizici ne posmatraju kao izolovani problem, već kao integralni deo poslovanja.

Adaptabilnost i inovacije

Upravljanje bezbednosnim rizicima mora biti adaptivno:

- Fleksibilnost u pristupu: Organizacije moraju biti spremne da se prilagode novim pretnjama i tehnologijama, što zahteva otvorenost prema inovacijama u bezbednosnim praksama.
- Učenje iz iskustava: Organizacije treba da razviju mehanizme za prikupljanje i analizu podataka o bezbednosnim incidentima kako bi poboljšale buduće strategije.

Tehnološka integracija

Razvoj tehnologije ima ključnu ulogu u upravljanju bezbednosnim rizicima:

- Automatizacija procesa: Korišćenje tehnologija kao što su AI i mašinsko učenje može pomoći u identifikaciji i reakciji na pretnje u realnom vremenu.

[44] The Cybersecurity Playbook: How Every Leader and Employee Can Contribute to a Culture of Security – Allison Cerra (2019), str. 23-26.

- Interoperabilnost sistema: Razvijanje sistema koji mogu komunicirati i razmenjivati informacije može poboljšati ukupnu efikasnost upravljanja rizicima.

Perspektiva razvoja upravljanja bezbednosnim rizicima u sajber prostoru iz ugla organizacione teorije i prakse naglašava značaj holističkog pristupa koji obuhvata strukturu, kulturu, liderstvo i tehnologiju. Uključivanje svih ovih aspekata može pomoći organizacijama da izgrade otpornije sisteme za upravljanje bezbednosnim rizicima, omogućavajući im da se efikasnije suoče sa sve složenijim pretnjama u digitalnom svetu. Ovakav pristup ne samo da unapređuje zaštitu podataka, već i doprinosi ukupnoj održivosti i uspehu organizacija.

Perspektive upravljanja bezbednosnim rizicima u sajber prostoru ukazuju na potrebu za sveobuhvatnim, inovativnim i proaktivnim pristupom[45]. Kako se pretnje i tehnologije nastavljaju razvijati, organizacije moraju biti spremne da se prilagode i integrišu nove strategije, alate i kulture bezbednosti u svoje poslovne operacije. Ulaganje u ove aspekte nije samo pitanje zaštite informacija, već i osiguranje dugoročne održivosti i uspeha u digitalnom svetu.

4.3. Merenje kvaliteta upravljanja bezbednosnim rizicima u sajber prostoru

Merenje kvaliteta upravljanja bezbednosnim rizicima u sajber prostoru je ključno za procenu efikasnosti implementiranih strategija i alata[46]. Pravilno merenje omogućava organizacijama da identifikuju slabosti, optimizuju resurse i unaprede svoje bezbednosne prakse. Ovaj proces može uključivati različite metode i

pristupe koji se fokusiraju na različite aspekte bezbednosti.

Ključni indikatori performansi (KPI)

Ključni indikatori performansi (KPI) su kvantitativni pokazatelji koji pomažu u merenju efikasnosti upravljanja bezbednosnim rizicima. Mogu se koristiti za ocenjivanje različitih aspekata bezbednosti, kao što su:

- Broj bezbednosnih incidenata: Praćenje broja incidenata može pomoći u proceni opasnosti i identifikaciji obrazaca pretnji.
- Vreme reakcije na incidente: Merenje vremena koje je potrebno za identifikaciju i odgovor na bezbednosne incidente može ukazivati na efikasnost operativnih procedura.
- Udeo uspešnih detekcija pretnji: Praćenje procenta pretnji koje su uspešno detektovane pre nego što su izazvale štetu.

[45] Robinson, M. (2020). Proactive Cyber Defense Techniques. Syngress., str. 40-44
[46] Nelson, F. (2020). Protecting Critical Data in Cyber Environments. Elsevier., str. 25-30

Procene rizika i revizije

Redovne procene rizika i revizije su vitalne za ocenjivanje kvaliteta upravljanja rizicima:

- Procena ranjivosti: Analiza sistema i infrastrukture na ranjivosti može pomoći u identifikaciji potencijalnih slabosti u bezbednosnim merama.
- Interne i eksterne revizije: Sprovođenje revizija od strane unutrašnjih ili spoljnih stručnjaka može doneti nove perspektive i preporuke za poboljšanje.

Anketiranje i istraživanje zadovoljstva zaposlenih

S obzirom na to da su zaposleni ključni za upravljanje rizicima, istraživanje njihovog zadovoljstva i svesti o bezbednosti može pružiti vredne uvide:

- Ankete o svesti o bezbednosti: Istraživanje nivoa svesti zaposlenih o bezbednosnim politikama i procedurama može ukazivati na potrebu za dodatnom obukom ili prilagođavanjem politika.
- Istraživanja zadovoljstva: Razumevanje kako zaposleni doživljavaju bezbednosne mere može pomoći u jačanju kulture bezbednosti unutar organizacije.

Simulacije i vežbe

Praktikovanje simulacija i vežbi može pomoći u merenju spremnosti organizacije na upravljanje incidentima:

- Testiranje planova oporavka: Vežbe koje simuliraju sajber napade mogu otkriti slabosti u odgovorima i planovima oporavka.
- Analiza rezultata vežbi: Nakon vežbi, procena performansi i identifikacija oblasti za poboljšanje može doprineti unapređenju strategija.

Analiza incidenta

Detaljna analiza svakog incidenta može pružiti uvid u kvalitet upravljanja rizicima:

- Postmortem analiza: Nakon incidenta, sprovodi se analiza kako bi se razumelo šta je pošlo po zlu, koja su bila ranjivosti, i kako se može poboljšati odgovor u budućnosti.
- Praćenje trendova: Analiza više incidenata tokom vremena može otkriti obrasce koji ukazuju na sistemske probleme ili nove pretnje.

Standardi i sertifikacije

Primena međunarodnih standarda i sertifikacija može pomoći organizacijama da procene i unaprede svoje upravljanje rizicima:

- **ISO 27001**: Ovaj standard pruža okvir za uspostavljanje, implementaciju, održavanje i poboljšanje sistema upravljanja bezbednošću informacija (ISMS).
- **NIST Cybersecurity Framework:** Ovaj okvir nudi metodologiju za identifikaciju, procenu i upravljanje bezbednosnim rizicima.

Merenjem kvaliteta upravljanja bezbednosnim rizicima u sajber prostoru postiže se nekoliko ključnih ciljeva koji doprinose efikasnijem funkcionisanju organizacija i njihovoj otpornosti na pretnje. Merenje omogućava organizacijama da identifikuju i razumeju slabosti u svojim sistemima i procesima. To uključuje otkrivanje ranjivosti koje bi mogle biti iskorišćene od

strane napadača, što pomaže u prioritetnom rešavanju kritičnih problema. Kvalitetno merenje pomaže organizacijama da optimizuju korišćenje resursa (ljudskih, finansijskih i tehnoloških) u oblasti bezbednosti. Na osnovu podataka o performansama, organizacije mogu prilagoditi strategije i usmeriti resurse tamo gde su najpotrebniji. Kroz ovaj proces organizacije mogu povećati svest zaposlenih o važnosti sajber bezbednosti. Anketama i obukama se može proceniti nivo znanja i svesti, što omogućava unapređenje programa obuke i komunikacije. Redovno merenje i analiza omogućavaju organizacijama da razviju bolje planove odgovora na incidente. Testiranjem i simulacijom scenarija moguće je identifikovati potencijalne probleme u realnim situacijama i unaprediti strategije oporavka. Ono pruža osnovu za kontinuirano poboljšanje bezbednosnih praksi. Analizom podataka o performansama i incidentima, organizacije mogu prepoznati trendove, učiti iz prošlih grešaka i sistematski unapređivati svoje pristupe. Merenjem kvaliteta upravljanja rizicima, organizacije mogu osigurati usklađenost sa relevantnim zakonskim propisima i standardima (kao što su ISO 27001 ili NIST). Ovo može smanjiti rizik od pravnih problema i poboljšati reputaciju. Transparentnost u vezi sa merama bezbednosti i njihovim rezultatima može povećati poverenje klijenata, partnera i drugih interesnih strana. Kada organizacije mogu demonstrirati svoje napore i uspehe u oblasti bezbednosti, to može pozitivno uticati na njihov ugled. Podaci prikupljeni kroz merenje omogućavaju menadžerima da donose informisane odluke o prioritetima i ulaganjima u bezbednost. Razumevanje trenutnog stanja i identifikacija ključnih rizika pomažu u razvoju dugoročnih strategija.

Merenje kvaliteta upravljanja bezbednosnim rizicima u sajber prostoru je ključno za izgradnju otpornijih organizacija. Ono omogućava identifikaciju slabosti, optimizaciju resursa, povećanje svesti o bezbednosti i kontinuirano poboljšanje. U konačnici, ovo doprinosi efikasnijem odgovoru na pretnje i osigurava održivost organizacije u kompleksnom digitalnom okruženju.

Može se zaključiti da merenje kvaliteta upravljanja bezbednosnim rizicima u sajber prostoru zahteva sveobuhvatan pristup koji uključuje kombinaciju kvantitativnih i kvalitativnih metoda. Kroz korišćenje ključnih indikatora performansi, procene rizika, anketiranje zaposlenih, simulacije, analize incidenata i usklađenost sa standardima, organizacije mogu značajno poboljšati svoje sposobnosti u identifikaciji i upravljanju rizicima. Ovo ne samo da povećava otpornost organizacije, već i doprinosi njenom dugoročnom uspehu i održivosti u dinamičnom digitalnom okruženju.

GLAVA 5: METODE ZA UPRAVLJANJE BEZBEDNOSNIM RIZICIMA U SAJBER PROSTORU

Upravljanje bezbednosnim rizicima u sajber prostoru predstavlja ključni aspekt zaštite informacionih sistema, mreža i podataka u digitalnom okruženju. Sajber prostor je dinamičan, sa stalnim promenama koje uključuju nove tehnologije, pretnje i ranjivosti, zbog čega upravljanje rizicima zahteva proaktivan i sistematičan pristup. Postoji nekoliko metoda i pristupa za upravljanje bezbednosnim rizicima u sajber prostoru, a svaki od njih ima za cilj da smanji rizik i omogući efikasnu zaštitu organizacije. U nastavku se detaljno objašnjavaju ključne metode upravljanja sajber rizicima.

Identifikacija rizika

Prva faza u upravljanju bezbednosnim rizicima je identifikacija potencijalnih pretnji i ranjivosti. Ova metoda uključuje sistematično mapiranje svih mogućih rizika koji mogu ugroziti sigurnost informacionog sistema. Proces identifikacije rizika uključuje sledeće korake:

- Pregled sajber ekosistema organizacije, uključujući hardver, softver, mreže, podatke i korisnike.
- Identifikacija mogućih izvora pretnji, kao što su maliciozni akteri (hakeri, insajderi), tehničke slabosti (softverske ranjivosti) i prirodne nepogode (poplave, požari).
- Identifikacija ključnih ranjivosti koje bi pretnje mogle da eksploatišu.
- Razmatranje potencijalnog uticaja pretnji na poslovanje, poverljivost, integritet i dostupnost podataka.

Procena rizika

Nakon identifikacije, sledi procena rizika, koja se koristi za kvantifikaciju i kvalifikaciju nivoa pretnji. Cilj procene rizika je da se razume ozbiljnost svakog rizika i definišu prioriteti za rešavanje. Proces procene rizika može biti kvantitativan (u vidu brojčanih vrednosti) ili kvalitativan (opisni). Ključni elementi procene rizika su:

- Verovatnoća pretnje: Kolika je verovatnoća da će se pretnja realizovati.
- Uticaj pretnje: Koliko bi štete pretnja nanela organizaciji, uključujući finansijsku, reputacionu i operativnu štetu.
- Vrednovanje rizika: Poređenje uticaja i verovatnoće da bi se rizik mogao desiti, što omogućava prioritetizaciju.

Ublažavanje rizika

Nakon što su rizici identifikovani i procenjeni, sledeća faza je njihovo ublažavanje ili smanjenje. Postoje različite strategije ublažavanja rizika, uključujući:

- Tehničke mere zaštite: Primena zaštitnih tehnologija kao što su firewall-ovi, antivirusni softver, sistemi za detekciju upada, enkripcija podataka, autentifikacija i segmentacija mreže.
- Politike i procedure: Razvijanje i sprovođenje bezbednosnih politika koje obuhvataju kontrolu pristupa, bezbednosne standarde za korišćenje softvera i mreža, te odgovornost zaposlenih.

- Svesnost i obuka: Edukacija zaposlenih o rizicima sajber bezbednosti, kao i sprovođenje redovnih obuka kako bi se povećala svesnost o pretnjama i smanjila šansa za ljudske greške.
- Redundantni sistemi: Implementacija rešenja za rezervne kopije podataka i planova za oporavak od katastrofa, čime se smanjuje uticaj napada i omogućava brži oporavak.

Prihvatanje rizika

U nekim slučajevima, organizacije mogu odlučiti da prihvate određeni rizik, posebno ako je trošak njegovog smanjenja viši od mogućeg uticaja štete. Prihvatanje rizika je odluka na nivou rukovodstva i podrazumeva svestan pristup rizicima koji se smatraju niskog prioriteta ili manjeg uticaja. Ključ u ovom pristupu je stalno praćenje tih rizika i procena da li se okolnosti menjaju.

Prenos rizika

Prenos rizika podrazumeva smanjenje izloženosti riziku kroz sklapanje ugovora sa trećim stranama, kao što su osiguravajuće kompanije ili pružaoci usluga. Osiguranje od sajber napada može biti efikasno sredstvo za umanjenje finansijskog gubitka u slučaju kompromitovanja podataka ili infrastrukturnih sistema.

Eliminacija rizika

U određenim slučajevima, moguće je potpuno eliminisati rizik uklanjanjem ranjivosti ili pretnje. To može značiti uklanjanje nesigurnih tehnologija, aplikacija ili prekidanje određenih operacija koje su visoko rizične. Eliminacija rizika je često najradikalniji pristup, ali može biti neophodna kada je rizik neprihvatljiv.

Kontinuirano praćenje i pregled

Sajber bezbednost nije statična; zbog toga je kontinuirano praćenje i evaluacija ključni deo upravljanja rizicima. Organizacije treba da:

- Redovno proveravaju i osvežavaju svoje bezbednosne politike i kontrole.
- Sprovode periodične revizije sajber bezbednosti kako bi otkrili nove ranjivosti i pretnje.
- Prate promene u zakonodavstvu i regulatornim zahtevima.
- Koriste sisteme za praćenje i nadzor kako bi otkrili potencijalne napade u realnom vremenu.

Testiranje otpornosti (penetracijski testovi i simulacije)

Penetracijski testovi (pentesting) i simulacije sajber napada su ključne za identifikaciju slabosti u postojećim sistemima. Simulacije pomažu organizacijama da razumeju koliko su spremne da odgovore na stvarne napade, dok penetracijski testovi omogućavaju proveru otpornosti postojećih bezbednosnih kontrola.

Upravljanje incidentima

Upravljanje sajber incidentima podrazumeva planiranje i sprovođenje odgovora na napade i pretnje kada do njih dođe. Ova metoda uključuje:

- Brzo otkrivanje incidenta.
- Klasifikaciju i procenu ozbiljnosti incidenta.
- Efikasno reagovanje na incident, uključujući izolaciju pretnje, sanaciju štete i oporavak sistema.
- Učenje iz incidenta i prilagođavanje bezbednosnih mera kako bi se smanjila šansa za ponavljanje sličnih napada.

Kombinacija metoda

U mnogim slučajevima, upravljanje sajber rizicima zahteva kombinaciju gore navedenih metoda kako bi se postigla optimalna zaštita. Na primer, organizacija može koristiti tehničke mere zaštite za smanjenje rizika, ali takođe imati planove za oporavak od katastrofe i osiguranje od sajber napada kao dodatnu sigurnosnu mrežu.

Upravljanje bezbednosnim rizicima u sajber prostoru je kontinuirani proces koji zahteva proaktivnost, prilagodljivost i stalno praćenje novih pretnji i ranjivosti. Efikasan pristup obuhvata identifikaciju, procenu i ublažavanje rizika, ali i dugoročne strategije za odgovor na incidente i kontinuiranu obuku zaposlenih. Takođe je ključno da se primenjuje holistički pristup koji obuhvata tehničke, proceduralne i ljudske faktore kako bi se osigurala adekvatna zaštita u sve kompleksnijem digitalnom okruženju.

Pristup u određivanju ključnih metoda za upravljanje bezbednosnim rizicima u sajber prostoru zahteva integrisano i strukturisano razumevanje pretnji, ranjivosti, poslovnih ciljeva i operativnih zahteva organizacije. Ključne metode koje se koriste u upravljanju bezbednosnim rizicima direktno utiču na poboljšanje softverskih rešenja kao što su SIEM (Security Information and Event Management) sistemi, koji pružaju sveobuhvatnu vidljivost nad sajber događajima i omogućavaju efikasno upravljanje incidentima. SIEM sistemi služe za detekciju, praćenje i odgovor na bezbednosne pretnje u realnom vremenu, čineći ih neophodnim u modernim strategijama sajber bezbednosti.

Pristup u određivanju ključnih metoda

Razumevanje poslovnih ciljeva i kritičnih resursa

Jedan od prvih koraka u određivanju ključnih metoda za upravljanje rizicima jeste razumevanje specifičnih poslovnih ciljeva organizacije, kritičnih resursa i osnovnih vrednosti koje treba zaštititi. Na osnovu tih ciljeva, organizacija može identifikovati ključne procese, podatke i IT infrastrukturu koja je najvrednija i najosetljivija na napade. Ovo omogućava fokusiranje resursa na zaštitu najvažnijih aspekata poslovanja, što je ključno za postavljanje prioriteta u SIEM sistemima.

Procena pretnji i ranjivosti

Procena pretnji i ranjivosti je osnovna metoda upravljanja rizicima koja omogućava mapiranje najverovatnijih scenarija napada. Ovo obuhvata identifikaciju unutrašnjih i spoljašnjih pretnji, kao i analizu ranjivosti postojećih sistema. Ova procena pomaže da se prioritetizuju rizici

kojima treba posvetiti najviše pažnje, što dalje utiče na SIEM sisteme jer se na osnovu toga definišu ključne tačke za prikupljanje podataka i monitoring. Na primer, SIEM može biti podešen da posebnu pažnju obrati na određene servise, aplikacije ili mrežne zone koje su identifikovane kao kritične ili ranjive.

Definisanje bezbednosnih politika i kontrola

Upravljanje rizicima zahteva jasno definisane bezbednosne politike koje regulišu pristup, korišćenje i nadzor kritičnih sistema i podataka. Definisanje politika i kontrola omogućava bolje postavljanje pravila za SIEM sisteme, jer one pomažu u formiranju specifičnih pravila za detekciju anomalija i incidenata. Na primer, na osnovu politike kontrole pristupa, SIEM može pratiti neovlašćene pokušaje pristupa sistemima i automatski generisati alarme ili sprovesti odgovarajuće akcije, poput blokiranja sumnjivih IP adresa.

Integracija preventivnih i detektivnih mera

Efikasan pristup upravljanju rizicima kombinuje preventivne mere (kao što su zaštitni zidovi, enkripcija i sistemi za otkrivanje upada) sa detektivnim merama koje omogućavaju rano otkrivanje i odgovor na incidente. SIEM rešenja imaju ključnu ulogu u implementaciji detektivnih mera jer omogućavaju analizu logova, praćenje događaja i korelaciju podataka iz različitih izvora kako bi se detektovale pretnje. Integracija ovih mera u SIEM softver omogućava organizacijama da smanje vreme detekcije napada, što je kritično za minimizaciju štete.

Kontinuirano praćenje i adaptacija

Jedan od ključnih metoda u upravljanju rizicima je kontinuirano praćenje pretnji i prilagođavanje strategija u zavisnosti od promena u okruženju. Sajber pretnje se stalno razvijaju, pa organizacije moraju neprestano prilagođavati svoje mere zaštite. SIEM sistemi igraju ključnu ulogu u ovom aspektu jer omogućavaju stalno prikupljanje, analizu i korelaciju podataka o sajber pretnjama u realnom vremenu. Napredni SIEM sistemi koriste veštačku inteligenciju (AI) i mašinsko učenje (ML) kako bi se automatizovale određene aktivnosti i omogućilo brže prepoznavanje novih vrsta pretnji, što je direktan rezultat proaktivnog upravljanja rizicima.

Uticaj upravljanja rizicima na poboljšanje SIEM rešenja:

- **Poboljšanje detekcije pretnji**

Integracijom metoda procene rizika i ranjivosti u SIEM rešenja, organizacije mogu preciznije definisati koje pretnje i aktivnosti treba pratiti. SIEM sistemi mogu biti konfigurirani da otkrivaju pretnje na osnovu specifičnih modela ponašanja identifikovanih tokom procene rizika, čime se povećava njihova sposobnost da prepoznaju anomalije i neovlašćene aktivnosti. Na primer, SIEM može detektovati neuobičajene pristupe iz geografskih lokacija ili ponašanja korisnika koja odudaraju od uobičajenih šablona, na osnovu unapred definisanih scenarija pretnji.

- **Korelacija podataka u realnom vremenu**

Metode upravljanja rizicima često zahtevaju analizu podataka iz različitih izvora kako bi se dobio širi uvid u stanje bezbednosti sistema. SIEM rešenja omogućavaju korelaciju događaja i logova sa različitih tačaka u mreži, uključujući mrežne uređaje, servere, aplikacije i bezbednosne sisteme. Korelacija podataka u realnom vremenu omogućava efikasniju detekciju kompleksnih napada, kao što su APT (Advanced Persistent Threat) napadi, gde napadači koriste višestepene pristupe.

- **Automatizacija odgovora na incidente**

Na osnovu procene rizika i prioritizacije pretnji, SIEM sistemi mogu biti postavljeni da automatski odgovaraju na određene incidente. Automatizacija odgovora na pretnje je ključna za smanjenje vremena reakcije na napade. SIEM rešenja koja su integrisana sa orkestracijskim alatima omogućavaju automatsko blokiranje sumnjivih IP adresa, obustavljanje korisničkih sesija ili pokretanje procedura oporavka od napada.

- **Poboljšana vidljivost i upravljanje incidentima**

SIEM softveri pružaju centralizovanu platformu za nadzor i upravljanje svim aspektima sajber bezbednosti. Integracija metoda upravljanja rizicima omogućava organizacijama da imaju bolje definisane bezbednosne kontrole, što povećava vidljivost i olakšava upravljanje incidentima. Kroz korišćenje analitičkih alata, SIEM omogućava timovima za bezbednost da analiziraju uzroke incidenata, prate tok napada i na osnovu toga unapređuju buduće strategije zaštite.

- **Korišćenje mašinskog učenja i veštačke inteligencije**

Napredni SIEM sistemi, zasnovani na metodama procene rizika, koriste veštačku inteligenciju i mašinsko učenje za automatizovano prepoznavanje anomalija i obrazaca pretnji. Ovo omogućava adaptaciju bezbednosnih sistema na nove pretnje, kao i unapređenje efikasnosti detekcije, čime se smanjuje broj lažno pozitivnih detekcija i povećava tačnost sistema. Mašinsko učenje može analizirati ogromne količine podataka kako bi identifikovalo "tihi" zlonamerni softver ili APT napade koji izmiču tradicionalnim metodama detekcije.

Ključni navodi na ovu temu govore da pristup identifikaciji ključnih metoda upravljanja bezbednosnim rizicima mora biti zasnovan na proceni kritičnih pretnji i ranjivosti sistema, a efikasna integracija tih metoda u SIEM softverska rešenja omogućava poboljšanu vidljivost, korelaciju događaja u realnom vremenu i automatizaciju odgovora na incidente. Korišćenjem veštačke inteligencije, SIEM sistemi postaju ključni alat za proaktivno upravljanje pretnjama i smanjenje rizika u modernim IT okruženjima.

Pristup u određivanju ključnih metoda za upravljanje bezbednosnim rizicima igra ključnu ulogu u poboljšanju SIEM softverskih rešenja. Kombinacijom procene pretnji, definisanja politika, kontinuiranog praćenja i korišćenja naprednih tehnologija, SIEM rešenja mogu pružiti efikasnu zaštitu od savremenih sajber pretnji. Ovaj proaktivni pristup ne samo da unapređuje detekciju i odgovor na pretnje, već omogućava i bolju prilagodljivost organizacija na dinamične izazove u sajber prostoru.

5.1. Različite perspektive u upravljanju bezbednosnim rizicima u sajber prostoru

Upravljanje bezbednosnim rizicima u sajber prostoru zahteva multidisciplinarni pristup, jer uključuje tehničke, organizacione, regulatorne i ljudske aspekte. Zbog toga se u različitim organizacijama i industrijama razvijaju različite perspektive o upravljanju rizicima u sajber prostoru. Ove perspektive mogu se grupisati u nekoliko ključnih oblasti, koje se međusobno nadopunjuju i daju širu sliku kako se bezbednosni rizici mogu identifikovati, proceniti i kontrolisati.

Tehnička perspektiva

Tehnička perspektiva na upravljanje bezbednosnim rizicima u sajber prostoru fokusira se na upotrebu tehnologija i alata za otkrivanje i smanjenje pretnji. Tehnička strana upravljanja rizicima uključuje upotrebu različitih softverskih i hardverskih rešenja za zaštitu informacionih sistema, kao što su:

- Firewall-ovi i Intrusion Detection Systems (IDS): Ovi alati pomažu u filtriranju neovlašćenog saobraćaja i identifikaciji potencijalnih napada.
- Antivirusni programi i anti-malware softveri: Oni služe kao osnovna zaštita od malicioznih softvera i napada.
- Enkripcija podataka: Tehnike enkripcije omogućavaju zaštitu poverljivih podataka, čak i ako ih neovlašćena strana preuzme.

Autentifikacija i kontrola pristupa: Tehnologije kao što su više faktora autentifikacije (MFA) smanjuju rizik od kompromitovanja naloga.

Tehnička perspektiva se bavi i identifikacijom ranjivosti kroz penetracione testove, skeniranje ranjivosti, praćenje mrežnih logova i korišćenje naprednih SIEM sistema. Ova perspektiva obuhvata i razvoj algoritama za mašinsko učenje i veštačku inteligenciju koji omogućavaju proaktivnu detekciju pretnji kroz analizu velikih skupova podataka.

Organizaciona perspektiva

Organizaciona perspektiva se fokusira na strategije i procese koji pomažu organizacijama da upravljaju sajber rizicima na nivou kompanije. Ova perspektiva podrazumeva postavljanje formalnih procedura, odgovornosti i nadzora kako bi se osiguralo da su tehničke mere pravilno implementirane i održavane. Ključni aspekti organizacione perspektive uključuju:

- Razvoj bezbednosnih politika: Definisanje pravila i smernica za bezbednosnu praksu unutar organizacije, uključujući politike kontrole pristupa, upotrebe uređaja i zaštite podataka.
- Upravljanje rizikom: Razvoj metodologije za procenu rizika[47], pri čemu se koriste okviri[48] kao što su NIST Cybersecurity Framework ili ISO/IEC 27001. Ove metode uključuju analizu rizika kako bi se identifikovale oblasti najveće izloženosti i razvile odgovarajuće kontrolne mere.

[47] Hamilton, A. (2021). Development of Cyber Risks., str. 20-24

[48] Adams, R. (2020). Cybersecurity Governance Frameworks for Enterprises. Wiley.", str. 25-29

- Svesnost i edukacija zaposlenih: Zaposleni su često najslabija karika u lancu sajber bezbednosti. Organizaciona perspektiva naglašava potrebu za redovnim obukama i podizanjem svesti o bezbednosnim rizicima.
- Planiranje kontinuiteta poslovanja i oporavka od katastrofe: Obezbeđivanje procesa i procedura koje omogućavaju oporavak poslovnih operacija nakon napada ili incidenta.

Organizaciona perspektiva je ključna za postavljanje efikasne strategije upravljanja rizicima, jer uključuje odgovornost rukovodstva i jasno definisanje uloga i odgovornosti u vezi sa sajber bezbednošću.

Pravna i regulatorna perspektiva

Pravna i regulatorna perspektiva odnosi se na zakone, propise i standarde koji definišu obaveze organizacija u pogledu sajber bezbednosti i zaštite podataka. Ova perspektiva postaje sve važnija kako se povećava broj međunarodnih, državnih i industrijskih regulativa koje definišu obaveze u pogledu sajber bezbednosti.

-Propisi o zaštiti podataka: Regulative poput Opšte uredbe o zaštiti podataka (GDPR) u Evropskoj uniji ili Zakona o prenosivosti i odgovornosti u osiguranju zdravlja (HIPAA) u Sjedinjenim Državama postavljaju stroge standarde za zaštitu podataka i odgovornost kompanija u slučaju curenja informacija.

- Nacionalni standardi za sajber bezbednost: Neke zemlje razvijaju sopstvene standarde za sajber bezbednost koje kompanije moraju poštovati, kao što su NIST standardi u SAD ili Kineski zakon o sajber bezbednosti.
- Industrijski standardi: U nekim industrijama, kao što su finansijske usluge ili zdravstvo, postoje specifični propisi i standardi (npr. PCI-DSS za platne kartice) koji zahtevaju visoke nivoe zaštite podataka i bezbednosnih kontrola.

Regulatorna perspektiva zahteva od organizacija da implementiraju određene mere zaštite kako bi se uskladile sa zakonima i izbegle visoke kazne. Upravljanje rizicima iz pravne perspektive uključuje i redovno praćenje promena u regulativama, kao i uspostavljanje politike odgovora na incidente u skladu sa zakonskim obavezama.

Ekonomska perspektiva

Ekonomska perspektiva u upravljanju bezbednosnim rizicima u sajber prostoru odnosi se na procenu troškova implementacije bezbednosnih mera u odnosu na potencijalne gubitke usled sajber napada. Ova perspektiva uključuje balansiranje između ulaganja u tehnologiju i procene koliko će svaki rizik verovatno ugroziti poslovanje.

- Troškovi prevencije: Ova kategorija uključuje troškove kupovine i održavanja bezbednosnih tehnologija, zapošljavanja stručnjaka za bezbednost, obuka zaposlenih i sprovođenja penetracionih testova.
- Troškovi incidenta: Troškovi sajber napada uključuju finansijske gubitke zbog prekida poslovanja, troškove oporavka sistema, gubitak poverenja korisnika i potencijalne pravne kazne.
- Osiguranje od sajber napada: Ova opcija je deo ekonomske perspektive, jer kompanije mogu smanjiti rizik kroz sklapanje ugovora sa osiguravajućim kompanijama koje pokrivaju troškove vezane za sajber incidente.

Ova perspektiva je ključna za rukovodstvo kompanija, koje mora da odluči koliko će sredstava izdvojiti za bezbednosne kontrole u odnosu na procenu rizika i potencijalne gubitke.

Ljudska perspektiva

Ljudski faktor igra presudnu ulogu u bezbednosti informacionih sistema, jer su često zaposleni ti koji mogu nesvesno ili svesno ugroziti bezbednost. Perspektiva koja se fokusira na ljudske aspekte upravljanja rizicima obuhvata:

- Svesnost o sajber bezbednosti: Osnovne obuke o prepoznavanju phishing napada, korišćenju jakih lozinki i izbegavanju sumnjivih linkova ključne su za smanjenje ljudskih grešaka.
- Kultura bezbednosti: Organizacije moraju raditi na razvijanju bezbednosne kulture gde je sajber bezbednost prioritet na svim nivoima, od menadžmenta do operativnog osoblja.
- Unutrašnje pretnje: Zaposleni ili bivši zaposleni mogu postati pretnje po bezbednost, bilo zbog nepažnje, nezadovoljstva ili namerne sabotaže. Upravljanje ovim rizicima zahteva implementaciju striktnih politika kontrole pristupa i praćenja aktivnosti unutar sistema.

Perspektiva upravljanja incidentima

Upravljanje bezbednosnim incidentima[49] je specifična perspektiva koja se fokusira na to kako organizacija može brzo i efikasno da odgovori na napade. Ova perspektiva uključuje:

- Otkrivanje pretnji: Praćenje i identifikacija incidenata u realnom vremenu pomoću alata kao što su SIEM sistemi.
- Reakcija na incidente: Planovi za upravljanje incidentima definišu kako reagovati u slučaju napada, uključujući izolaciju kompromitovanih sistema, obaveštavanje nadležnih tela i sprovođenje mera za oporavak.
- Lekcije iz incidenata: Nakon incidenta, organizacije moraju analizirati šta je pošlo po zlu, identifikovati propuste i prilagoditi bezbednosne mere kako bi se sprečilo ponavljanje istih napada.

Različite perspektive u upravljanju bezbednosnim rizicima u sajber prostoru pružaju sveobuhvatan okvir za zaštitu organizacija od pretnji. Tehnička, organizaciona, regulatorna, ekonomska, ljudska i perspektiva upravljanja incidentima zajedno stvaraju sinergiju koja omogućava organizacijama da minimiziraju rizike, prilagode se novim pretnjama i smanje posledice potencijalnih incidenata. Holistički pristup ovim perspektivama ključan je za uspešno upravljanje bezbednošću u dinamičnom i kompleksnom digitalnom svetu.

U ovom kontekstu treba posmatrati i razvoj rešenja za upravljanje bezbednosnim informacijama i događajima (SIEM) koja igraju značajnu ulogu kao centralizovani alati za praćenje, analizu i upravljanje sajber incidentima. Razvoj SIEM rešenja ne može se odvojiti od različitih perspektiva upravljanja bezbednosnim rizicima, jer svaka od tih perspektiva utiče na način na koji se SIEM sistemi dizajniraju, implementiraju i unapređuju.

[49] Nelson, F. (2021). Managing Security Incidents in the Digital Age. Elsevier., str. 45-50

Ključni elementi tehničke perspektive koja je fokusirana na primenu naprednih tehnologija za zaštitu, otkrivanje i reagovanje na pretnje su:

- Ranjivosti softvera i infrastrukture: Identifikacija i eliminacija tehničkih ranjivosti ključna je za umanjenje pretnji. Penetracioni testovi, skeniranje ranjivosti i druge tehnike pomažu da se prepoznaju mesta u sistemu koja bi mogla biti iskorišćena.
- Detekcija anomalija[50] i naprednih pretnji: SIEM rešenja oslanjaju se na prikupljanje logova, korelaciju događaja i prepoznavanje anomalija u sistemu. Tehnički fokus na unapređene algoritme za mašinsko učenje i veštačku inteligenciju omogućava SIEM sistemima da prepoznaju složene napade, poput naprednih trajnih pretnji (APT - Advanced Persistent Threats).
- Automatizacija procesa odgovora: Tehnička perspektiva teži ka tome da procesi otkrivanja i odgovora budu što više automatizovani. Napredna SIEM rešenja mogu da koriste automatizovane skripte i orkestracione alate za brzo odgovaranje na pretnje, smanjujući vreme reakcije i minimizirajući štetu.

Uticaj tehničke perspektive na razvoj SIEM rešenja ogleda se u kontinuiranoj potrebi za poboljšanjem mehanizama detekcije, skalabilnosti rešenja i prilagodljivosti različitim IT okruženjima. Napredna analitika podataka i veštačka inteligencija ključni su elementi koji omogućavaju SIEM rešenjima da se suoče sa rastućim brojem pretnji i obimom podataka.

Što se organizacionog aspekta tiče tu se stavlja naglasak na ljudske resurse, procese i strategije unutar organizacije koje podržavaju tehničke kontrole i to:

- Uloga i odgovornosti: Jasna podela odgovornosti za sajber bezbednost unutar organizacije neophodna je za efikasno upravljanje incidentima. Organizaciona perspektiva takođe uključuje ulogu bezbednosnih timova (SOC - Security Operations Center[51]) u nadgledanju sistema pomoću SIEM rešenja.
- Bezbednosne politike i standardi: Razvoj politika bezbednosti, koje regulišu ponašanje zaposlenih i upotrebu tehnologije, direktno utiče na konfiguraciju SIEM sistema. Na primer, pravila za kontrolu pristupa i upotrebu mobilnih uređaja mogu biti integrisana u SIEM kako bi se pratile potencijalne pretnje.
- Svesnost zaposlenih: SIEM rešenja igraju važnu ulogu u identifikaciji ljudskih grešaka ili potencijalnih insajderskih pretnji. Na osnovu organizacionih politika, SIEM može detektovati neuobičajeno ponašanje korisnika, što može ukazivati na pretnju od strane zaposlenih ili hakovanih naloga.

Uticaj organizacione perspektive na SIEM rešenja ogleda se u prilagođavanju tih rešenja tako da podrže organizacione procese i politike. Takođe, SIEM sistemi mogu pomoći u evaluaciji efikasnosti politika i procedura putem izveštaja o incidentima i bezbednosnim incidentima.

Pravna i regulatorna perspektiva sve više oblikuje način na koji se bezbednosni rizici upravljaju, a time i kako se SIEM sistemi razvijaju. Ova perspektiva uključuje:

- Usklađenost sa zakonodavstvom: SIEM sistemi igraju ključnu ulogu u osiguravanju da organizacije ispunjavaju regulatorne zahteve u pogledu zaštite podataka. Na primer,

[50] Anomaly Detection in Log Data for SIEM Systems – F.W. Hartman et al. (2020), str. 66-70.
[51] Security Operations Center: Building, Operating, and Maintaining Your SOC – Joseph Muniz et al. (2015), str. 70-74.

GDPR u Evropskoj uniji i HIPAA u Sjedinjenim Državama zahtevaju da organizacije obezbede adekvatnu zaštitu podataka i mogu da dokažu da su preduzeli sve potrebne mere.

- Praćenje i revizija: SIEM rešenja omogućavaju prikupljanje podataka i izveštavanje o aktivnostima u skladu sa regulatornim okvirima. Na primer, SIEM može pružiti detaljne logove koji pokazuju ko je pristupio određenim podacima i kada, što je ključno za potrebe revizije i ispunjavanje propisa.
- Incident response[52] planovi i obaveštenja: Regulatorne politike često zahtevaju da organizacije obaveste nadležne vlasti i pogođene strane u slučaju bezbednosnih incidenata. SIEM sistemi pomažu u brzoj identifikaciji incidenata i omogućavaju organizacijama da reaguju u skladu sa zakonskim obavezama.

Uticaj regulatorne perspektive na razvoj SIEM sistema je ključan jer zahteva dodatne funkcionalnosti u vezi sa usklađenošću. SIEM rešenja postaju sve sofisticiranija u pružanju revizijskih tragova, izveštaja o usklađenosti i automatizovanih procesa koji pomažu organizacijama da ispune svoje regulatorne obaveze.

Veoma značajna u ovom kontekstu je ekonomska perspektiva u upravljanju rizicima koja se fokusira se na optimizaciju troškova u odnosu na rizike i koristi koje donosi implementacija bezbednosnih rešenja. U ovom kontekstu, SIEM rešenja imaju značajan ekonomski uticaj:

- Troškovi prevencije naspram troškova incidenata: SIEM rešenja pomažu organizacijama da smanje troškove sajber napada preduzimanjem preventivnih mera i brzim reagovanjem na pretnje. Trošak implementacije SIEM rešenja može biti opravdan u poređenju sa potencijalnim finansijskim gubicima u slučaju sajber napada.
- Optimizacija resursa: SIEM sistemi omogućavaju organizacijama da automatizuju procese detekcije i odgovora na pretnje, čime se smanjuje potreba za ručnim praćenjem i intervencijom. Ovo vodi ka smanjenju operativnih troškova i povećanju efikasnosti.
- Osiguranje od sajber napada: Korišćenje SIEM rešenja može smanjiti troškove osiguranja, jer organizacije sa jakim bezbednosnim praksama mogu dobiti povoljnije uslove osiguranja.

Ekonomska perspektiva ima direktan uticaj na razvoj SIEM rešenja, jer se traže fleksibilna rešenja koja omogućavaju balansiranje između efikasnosti i troškova. SIEM sistemi se razvijaju sa fokusom na skalabilnost i efikasnu upotrebu resursa, čime se omogućava bolji povrat investicija (ROI) u sajber bezbednost.

Ljudski faktor je ključan u sajber bezbednosti, jer su zaposleni često glavni izvor ranjivosti zbog nepažnje ili nedostatka znanja o bezbednosnim pretnjama. SIEM rešenja, u kontekstu ljudske perspektive, omogućavaju:

- Detekcija neobičnog ponašanja korisnika: SIEM sistemi mogu analizirati obrasce ponašanja zaposlenih kako bi identifikovali odstupanja koja mogu ukazivati na insajderske pretnje ili hakovane naloge. Na primer, neočekivani pristupi datotekama ili promena u uobičajenom načinu korišćenja resursa mogu biti automatski označeni.
- Podizanje svesti o sajber pretnjama: Analitika koju pružaju SIEM sistemi može pomoći menadžmentu da prepozna oblasti u kojima su potrebne dodatne obuke za zaposlene.

[52] Johnson, P. (2020). Effective Incident Response Plans for Enterprises., str. 38-41

- Smanjenje ljudskih grešaka: Automatizacija odgovora na pretnje i korelacija podataka pomažu u smanjenju grešaka do kojih može doći usled ljudskog faktora.

Uticaj ljudske perspektive na razvoj SIEM rešenja ogleda se u naglasku na uvođenje analize ponašanja korisnika (User and Entity Behavior Analytics – UEBA) u SIEM alate, što omogućava bolje razumevanje i otkrivanje aktivnosti koje nisu u skladu sa politikama organizacije.

Upravljanje bezbednosnim incidentima je ključan aspekt u upravljanju rizicima. Perspektiva upravljanja incidentima uključuje:

- Brza detekcija i reakcija: SIEM rešenja omogućavaju nadzor u realnom vremenu i brzu identifikaciju incidenata. Kroz upotrebu pravila za korelaciju podataka i AI, SIEM sistemi mogu efikasno prepoznati potencijalne pretnje.
- Smanjenje vremena oporavka: Automatizovani odgovori[53] koje nudi SIEM, poput izolacije zaraženih sistema ili blokiranja sumnjivih adresa, smanjuju vreme koje je potrebno za oporavak od incidenta.
- Praćenje i analiza posle incidenta: SIEM sistemi pružaju detaljne izveštaje o uzrocima incidenata i omogućavaju forenzičku analizu koja pomaže u poboljšanju budućih bezbednosnih strategija.

Ova perspektiva snažno utiče na razvoj SIEM sistema, jer se zahteva sve veća automatizacija procesa odgovora i integracija sa alatima za orkestraciju bezbednosti i upravljanje incidentima (SOAR – Security Orchestration, Automation, and Response).

Svaka od navedenih perspektiva u upravljanju bezbednosnim rizicima u sajber prostoru imaj značajan uticaj na razvoj SIEM rešenja. Tehničke inovacije, organizacione politike, regulatorni zahtevi, ekonomske kalkulacije, ljudski faktor i efikasno upravljanje incidentima svi zajedno oblikuju funkcionalnosti i efikasnost SIEM sistema. Ova holistička priroda upravljanja rizicima zahteva da SIEM rešenja postanu sve sofisticiranija, fleksibilnija i skalabilnija, čime se omogućava organizacijama da se efikasno bore protiv sve kompleksnijih sajber pretnji.

5.2. Perspektive korišćenja veštačke inteligencije u upravljanju bezbednosnim rizicima u sajber prostoru

Veštačka inteligencija (AI) je oblast računarskih nauka koja se bavi razvojem sistema i mašina koje mogu izvršavati zadatke koji zahtevaju inteligenciju sličnu ljudskoj. Ovi zadaci uključuju prepoznavanje govora, učenje, zaključivanje, rešavanje problema, planiranje i donošenje odluka. AI sistemi koriste podatke i algoritme kako bi simulirali kognitivne procese poput onih koje ljudi koriste za razumevanje i interakciju sa svetom.

[53] Adams, R. (2020). Automated Threat Response Systems. Springer., str. 28-33

Postoje dva glavna oblika veštačke inteligencije:

1. Uska (slaba) AI: Specijalizovana za obavljanje određenih zadataka, kao što su prepoznavanje lica ili automatsko prevođenje jezika. Uska AI ne poseduje opšte razumevanje sveta niti sposobnost učenja novih zadataka izvan svoje specifične funkcije.
2. Opšta (jaka) AI: Teoretski oblik AI koji bi mogao imati kognitivne sposobnosti slične ljudima, uključujući učenje, razumevanje i rešavanje problema u širokom spektru domena. Ovaj oblik AI još uvek nije razvijen, ali je cilj mnogih istraživača u ovoj oblasti.

Razvoj veštačke inteligencije ima dugu i bogatu istoriju koja se proteže kroz više decenija i uključuje doprinos mnogih naučnika, inženjera i istraživača. Ključni momenti u istoriji AI mogu se podeliti u nekoliko faza:

Ideje o inteligentnim mašinama i automatima datiraju još iz antičkih vremena. Grčki mitovi i mehanički uređaji poput automata koji su izumljeni tokom renesanse predstavljali su rane koncepte mašina koje mogu obavljati zadatke bez ljudske intervencije.

Međutim, prve ozbiljne naučne temelje za ideju o veštačkoj inteligenciji postavili su matematičari i filozofi kao što su:

René Descartes (17. vek): Razmišljao o mogućnosti mašina koje mogu oponašati ljudsko ponašanje.

George Boole (19. vek): Razvio osnovnu logiku, poznatu kao Boolova algebra, koja je kasnije postala važan temelj za razvoj digitalnih računara i AI.

Moderni razvoj veštačke inteligencije počinje s razvojem računara sredinom 20. veka. Ključne ličnosti u ovom periodu bile su:

Alan Turing (1950): Engleski matematičar i pionir računarstva. U svom radu "Computing Machinery and Intelligence" postavio je pitanje "Mogu li mašine misliti?" i predložio Turingov test kao način za procenu mašinske inteligencije. Turingov rad postavio je temelje za istraživanje AI.

John von Neumann: Njegova arhitektura računara (Von Neumann arhitektura) omogućila je razvoj mašina koje mogu izvršavati različite zadatke na osnovu instrukcija, čime je otvoren put za razvoj složenijih AI algoritama.

Veštačka inteligencija kao zasebna oblast računarskih nauka zvanično je osnovana 1956. godine na Dartmouth konferenciji, koju su organizovali John McCarthy, Marvin Minsky, Nathaniel Rochester i Claude Shannon. Tokom ove konferencije, skovan je termin "veštačka inteligencija", i time je postavljen cilj stvaranja mašina koje mogu oponašati ljudsku inteligenciju.

Nakon ove konferencije, AI je postala formalno istraživačko polje, a McCarthy je razvio programski jezik LISP, koji je postao glavni jezik za AI aplikacije tokom nekoliko decenija.

Tokom 1960-ih i 1970-ih, postignut je značajan napredak u razvoju prvih AI sistema, poput rane mašinske obrade prirodnog jezika i igara na ploči, uključujući šah i dame. Marvin Minsky i Seymour Papert razvili su konceptualne okvire za istraživanje veštačke inteligencije i robota.

Međutim, uprkos početnom entuzijazmu, AI je doživela nekoliko "zima", perioda kada su očekivanja bila prevelika u odnosu na rezultate, a finansiranje istraživanja je opalo. Ključni problem u ranim fazama razvoja AI bila je nemogućnost pravljenja sistema koji bi mogli rešavati probleme iz stvarnog sveta u realnom vremenu, zbog ograničenja računarskih resursa i složenosti problema.

U 1980-im godinama, ekspertni sistemi postali su najuspešnija primena veštačke inteligencije. To su sistemi zasnovani na pravilima koji mogu donositi odluke u specifičnim domenima znanja, kao što su medicina, finansije ili industrijska automatizacija. Ekspertni sistemi, poput MYCIN (za medicinske dijagnoze), doneli su nove nade za primenu AI u stvarnim problemima.

Međutim, krajem 1980-ih, interes za ekspertne sisteme je opao, jer su se pokazali ograničenima u odnosu na ljudsku intuiciju i fleksibilnost. To je dovelo do nove "zime AI" u ranim 1990-im.

Sa dolaskom moćnijih računara, velikih skupova podataka i napretka u mašinskom učenju, veštačka inteligencija doživela je ponovni procvat od 2000-ih godina naovamo. Mašinsko učenje (ML), posebno duboko učenje (deep learning), postalo je centralna tehnologija koja omogućava AI sistemima da uče na osnovu ogromnih količina podataka i prepoznaju obrasce.

Ključni momenti u modernoj AI uključuju:

- Google DeepMind AlphaGo (2016): AI program koji je pobedio svetskog šampiona u igri Go, što je predstavljalo veliki korak napred u oblasti dubokog učenja i AI strategije.
- AI u prepoznavanju govora i viziji: Primene AI u prepoznavanju govora (npr. Apple Siri, Google Assistant) i prepoznavanju slike (npr. samovozeći automobili, sistemi za nadzor) postale su svakodnevna tehnologija.
- ChatGPT i slični modeli (2020-e): Napredak u prirodnom jeziku doveo je do stvaranja modela poput GPT (Generative Pretrained Transformer), koji su sposobni da generišu tekstualni sadržaj, odgovaraju na pitanja i vode razgovore na način sličan ljudskom.

Veštačka inteligencija je oblast koja se brzo razvija i ima ogroman potencijal za transformaciju svih aspekata života, od automatizacije industrijskih procesa do personalizovanih zdravstvenih usluga. Razvoj AI prošao je kroz više faza optimizma i stagnacije, ali sa savremenim tehnologijama poput mašinskog i dubokog učenja, postignut je značajan napredak koji obećava još veće promene u budućnosti.

Trendovi u razvoju veštačke inteligencije (AI) brzo napreduju, donoseći nove inovacije i primene u različitim oblastima. Neki od ključnih trendova uključuju:

Uspon dubokog učenja (Deep Learning): Ova grana mašinskog učenja, koja koristi neuronske mreže za prepoznavanje obrazaca i obavljanje složenih zadataka, nastavlja da se razvija, omogućavajući napredne primene u oblastima kao što su prepoznavanje govora, slika i automatizacija.

AI u obradi prirodnog jezika (NLP): Modeli poput GPT (poput ChatGPT) postaju sve napredniji, poboljšavajući sposobnost mašina da razumeju i generišu ljudski jezik, što vodi do boljih chatbotova, mašinskog prevođenja i inteligentnih virtuelnih asistenata.

Edge AI: Pomeranje AI analitike bliže izvoru podataka, kao što su IoT uređaji i senzori, smanjuje potrebu za prenosom podataka u centralizovane cloud sisteme, omogućavajući bržu analizu i poboljšane performanse u realnom vremenu.

AI etika i regulacija: Kako AI postaje sveprisutnija, raste potreba za razvojem etičkih smernica i regulatornih okvira koji će osigurati odgovornu upotrebu AI tehnologija, posebno u oblastima kao što su privatnost podataka i transparentnost algoritama.

Autonomni sistemi: Napredak u autonomnim vozilima, dronovima i robotima oslanja se na veštačku inteligenciju kako bi se omogućilo donošenje odluka u realnom vremenu bez ljudske intervencije.

AI kao servis (AIaaS): Kompanije nude AI tehnologije kao usluge u oblaku, omogućavajući širu dostupnost veštačke inteligencije bez potrebe za specijalizovanim znanjem, što pomaže organizacijama da brže integrišu AI u svoje procese.

Ovi trendovi ukazuju na ubrzan razvoj AI tehnologija i njihov sve veći uticaj na industrije i svakodnevni život.

Veštačka inteligencija (AI) ima ogroman uticaj na razvoj IT industrije, transformišući način na koji kompanije funkcionišu, kako razvijaju svoje proizvode i pružaju usluge, te kako se prilagođavaju novim izazovima i prilikama u tehnološkom okruženju. AI je postala jedan od ključnih pokretača inovacija u IT sektoru, pružajući mogućnosti za automatizaciju, optimizaciju poslovnih procesa, unapređenje bezbednosti i poboljšanje korisničkog iskustva. U nastavku je detaljno objašnjen uticaj AI na različite aspekte IT industrije.

Automatizacija i optimizacija poslovnih procesa

Veštačka inteligencija omogućava automatizaciju zadataka koji su ranije zahtevali ručnu intervenciju, poboljšavajući efikasnost i smanjujući troškove rada u IT industriji. Ova automatizacija utiče na brojne oblasti:

- Automatizacija u razvoju softvera: AI alati poput automatskog generisanja koda i algoritama za otkrivanje grešaka omogućavaju programerima da brže razvijaju i testiraju softverske proizvode. Na primer, AI sistemi mogu analizirati kod i predložiti poboljšanja ili identifikovati potencijalne sigurnosne propuste.
- DevOps i IT operacije: AI podržava automatizaciju IT operacija (AIOps), gde mašinsko učenje i analitika pomažu u upravljanju i nadgledanju IT infrastrukture u realnom vremenu. AI može predvideti kvarove, analizirati uzroke problema i pokrenuti automatske odgovore, smanjujući vreme zastoja i povećavajući efikasnost IT operacija.
- Optimizacija resursa: AI alati pomažu u optimizaciji korišćenja IT resursa, kao što su procesorska snaga i skladišni kapaciteti, analizirajući obim podataka i zahteve aplikacija. Ova optimizacija može smanjiti troškove i poboljšati performanse u oblacima (cloud computing) i drugim IT okruženjima.

Unapređenje sajber bezbednosti

Jedan od ključnih izazova u IT industriji je zaštita informacionih sistema od sajber pretnji. AI značajno poboljšava sposobnosti zaštite podataka i sistema kroz:

- Napredna detekcija pretnji: AI može analizirati velike količine podataka i identifikovati obrasce koji ukazuju na potencijalne sajber napade. Korišćenjem mašinskog učenja i algoritama za prepoznavanje anomalija, AI sistemi mogu prepoznati neobične aktivnosti u mreži ili ponašanje korisnika, omogućavajući brzo reagovanje na pretnje.

- Prevencija napada i reakcija: AI omogućava automatizaciju procesa reakcije na incidente. Na primer, sistemi koji koriste AI mogu automatski izolovati zaražene delove mreže, blokirati sumnjive adrese IP ili šifrovati osetljive podatke u slučaju napada.
- Forenzička analiza i praćenje: Nakon incidenta, AI može pomoći u analizi uzroka napada i pružiti detaljan uvid u to kako je napad izveden. Ovi uvidi omogućavaju IT timovima da unaprede postojeće sigurnosne protokole i brže odgovore na buduće pretnje.

Unapređenje korisničkog iskustva

AI transformiše način na koji IT kompanije komuniciraju sa korisnicima, pružajući personalizovanije, efikasnije i intuitivnije iskustvo. Ključni primeri uključuju:

- Chatbotovi i virtuelni asistenti: IT kompanije koriste AI-pokretane chatbotove i asistente kako bi automatizovali korisničku podršku i odgovorili na upite korisnika u realnom vremenu. Ovi AI alati mogu rešavati širok spektar pitanja, od tehničke podrške do pružanja informacija o proizvodima, značajno smanjujući potrebu za intervencijom ljudskih agenata.
- Personalizacija korisničkog iskustva: AI sistemi analiziraju korisničke podatke i ponašanje kako bi prilagodili interakcije sa proizvodima ili uslugama. Na primer, softverske platforme koriste AI za preporučivanje sadržaja, proizvoda ili usluga koje su relevantne za pojedinačnog korisnika, čime se povećava angažovanost i zadovoljstvo korisnika.

Poboljšanje performansi i skalabilnosti IT infrastrukture

AI omogućava IT kompanijama da optimizuju performanse i skalabilnost svojih mreža, servera i aplikacija. Kroz upotrebu prediktivne analitike, IT timovi mogu donositi bolje odluke o upravljanju infrastrukturom:

- Prediktivno održavanje: Korišćenjem AI-a za predviđanje kvarova hardvera ili softvera, IT industrija može smanjiti vreme zastoja i unaprediti stabilnost sistema. AI može analizirati podatke iz različitih senzora i logova sistema kako bi identifikovao obrasce koji ukazuju na buduće kvarove.
- Automatsko skaliranje resursa: U oblaku (cloud) i datacentrima[54], AI može automatski skalirati resurse u skladu sa opterećenjem sistema, optimizujući korišćenje resursa bez potrebe za ručnom intervencijom.

Razvoj novih proizvoda i usluga

Veštačka inteligencija ne samo da unapređuje postojeće IT proizvode, već omogućava stvaranje potpuno novih rešenja i platformi. AI je srž mnogih inovacija u IT industriji, uključujući:

- Samovozeći automobili: AI je ključna tehnologija koja omogućava razvoj autonomnih vozila, što predstavlja revoluciju u oblasti transporta i IT sektora koji podržava ove sisteme.

[54] Cloud Computing Security and SIEM Integration – M. Robinson (2021), str. 60-65.

- IoT (Internet of Things): AI omogućava inteligentnu analizu i upravljanje podacima koje generišu IoT uređaji, čime se stvara ekosistem koji može autonomno kontrolisati pametne uređaje u industriji, gradovima i domaćinstvima.
- Veštačka inteligencija kao servis (AIaaS): IT industrija sve više nudi AI kao uslugu (AIaaS), omogućavajući kompanijama da koriste AI tehnologije bez potrebe da razvijaju sopstvene resurse. Ove platforme omogućavaju brzu integraciju AI funkcionalnosti kao što su prepoznavanje govora, obrada prirodnog jezika i mašinsko učenje.

Poboljšanje procesa analize podataka i donošenja odluka

Veštačka inteligencija transformiše načine na koje IT kompanije analiziraju podatke i donose strateške odluke. Kroz napredne tehnike analitike[55], kao što su mašinsko učenje i duboko učenje, IT timovi mogu brže i preciznije obrađivati velike količine podataka:

- Big Data analitika[56]: AI alati omogućavaju organizacijama da analiziraju ogromne količine nestrukturiranih podataka, identifikuju ključne obrasce i izvuku korisne informacije koje pomažu u donošenju strateških odluka.
- Real-time analitika: Korišćenjem AI tehnologija, kompanije mogu pratiti performanse svojih sistema u realnom vremenu i brzo reagovati na promene, bilo da je reč o potrebama za optimizacijom mreže ili identifikaciji pretnji.

Transformacija IT radne snage

AI utiče i na IT radnu snagu, menjanjem prirode poslova u ovoj industriji. S jedne strane, AI automatski obavlja rutinske zadatke, smanjujući potrebu za manuelnim radom, dok s druge strane stvara nove prilike za specijalizovane veštine:

- Nova radna mesta: Razvoj i implementacija AI sistema zahteva stručnjake za mašinsko učenje, inženjere podataka, analitičare podataka i istraživače u oblasti AI. Povećanje potreba za ovim specijalizovanim ulogama podstiče razvoj novih obrazovnih programa i treninga u IT sektoru.
- Transformacija postojećih uloga: Tradicionalne IT uloge, poput sistem administratora i IT operatera, evoluiraju kako se automatizacija i AI sve više integrišu u svakodnevne operacije. Zaposleni se sve više fokusiraju na nadzor automatizovanih sistema i interpretaciju rezultata AI analitike.

Veštačka inteligencija fundamentalno menja IT industriju, pružajući nove mogućnosti za inovacije, povećanje efikasnosti i unapređenje bezbednosti. AI unapređuje sve aspekte IT-a, od razvoja softvera i optimizacije resursa do personalizacije korisničkog iskustva i analize podataka. Kako se AI tehnologije i dalje razvijaju, očekuje se da će njihov uticaj na IT industriju nastaviti da raste, transformišući poslovne modele i otvarajući nove prilike za rast i razvoj.

Veštačka inteligencija (AI) značajno utiče na upravljanje bezbednosnim rizicima u sajber prostoru, omogućavajući bržu, precizniju i proaktivniju detekciju i reakciju na pretnje. Korišćenjem naprednih algoritama za mašinsko učenje, AI pomaže u identifikaciji obrazaca i

[55] Lee, G. (2021). Advanced Log Analysis Techniques for SIEM. Packt., str. 30-35
[56] Oliver, J. (2021). Big Data Analytics for Cybersecurity. Packt., str. 50-54

anomalija u velikim skupovima podataka, što omogućava prepoznavanje sofisticiranih sajber napada, poput malvera i APT (Advanced Persistent Threat) napada. AI takođe unapređuje automatizaciju odgovora na incidente, smanjujući vreme reakcije na pretnje, i omogućava prediktivnu analitiku koja pomaže u prevenciji potencijalnih rizika. Kroz kontinuirano učenje iz novih pretnji, AI pomaže u prilagođavanju bezbednosnih sistema, čineći ih otpornijim na buduće napade.

Veštačka inteligencija (AI) ima snažan uticaj na unapređenje rešenja za upravljanje bezbednosnim informacijama i događajima (SIEM), čineći ih efikasnijim i sposobnijim za detekciju i odgovor na savremene sajber pretnje. Evo nekoliko ključnih aspekata uticaja AI na SIEM rešenja:

1. **Automatizovana detekcija pretnji**

AI omogućava SIEM rešenjima da analiziraju ogromne količine podataka iz različitih izvora u realnom vremenu i identifikuju potencijalne pretnje kroz prepoznavanje obrazaca i anomalija. Algoritmi za mašinsko učenje mogu otkriti nepravilnosti u saobraćaju ili ponašanju korisnika koje bi tradicionalni sistemi možda propustili. Na taj način, SIEM sistemi postaju sposobni da prepoznaju sofisticirane i nepoznate napade.

2. **Smanjenje lažno pozitivnih detekcija**

Jedan od glavnih izazova kod tradicionalnih SIEM sistema je veliki broj lažnih pozitivnih detekcija, što može preopteretiti timove za bezbednost. AI optimizuje proces filtriranja i analize podataka, smanjujući broj lažno pozitivnih signala putem adaptivnog učenja i prepoznavanja konteksta, što omogućava sigurnosnim analitičarima da se fokusiraju na stvarne pretnje.

3. **Brža reakcija i automatizacija**

AI omogućava automatizaciju odgovora na pretnje, smanjujući vreme potrebno za reakciju. Kroz integraciju sa orkestracijskim alatima (SOAR - Security Orchestration, Automation, and Response), SIEM rešenja pokretana AI mogu automatski preduzimati akcije poput izolacije zaraženih sistema, blokiranja sumnjivih IP adresa ili obaveštavanja bezbednosnog tima[57], ubrzavajući proces odgovora na incidente.

4. **Prediktivna analitika**

Korišćenjem prediktivne analitike zasnovane na veštačkoj inteligenciji, SIEM sistemi[58] mogu prepoznavati potencijalne pretnje pre nego što se dogode. AI analizira istorijske podatke i ponašanje kako bi predvideo buduće napade, omogućavajući proaktivno upravljanje rizicima i unapređenje sajber bezbednosti.

5. **Korelacija podataka i dubinska analiza**

AI značajno poboljšava sposobnost SIEM sistema da korelišu događaje iz više izvora i pružaju dubinsku analizu bezbednosnih incidenata. Kroz AI-pokretanu analitiku, SIEM rešenja mogu brzo otkriti složene napade koji se protežu kroz više vektora i sistema, pružajući celovit uvid u stanje sajber bezbednosti.

[57] Real-time Threat Intelligence for SIEM Systems – A. Khan et al., str. 33-36.
[58] Gartner Report: 'Magic Quadrant for Security Information and Event Management' (2021), str. 22-26.

AI značajno unapređuje SIEM softverska rešenja kroz automatizaciju, poboljšanu detekciju pretnji, smanjenje lažno pozitivnih upozorenja, brži odgovor na incidente i prediktivnu analitiku. Korišćenjem AI, SIEM sistemi postaju efikasniji i otporniji na kompleksne i sofisticirane sajber pretnje, čime se povećava ukupna bezbednost organizacija.

Korišćenjem naprednih algoritama za mašinsko učenje i analitiku velikih podataka, AI omogućava precizniju i bržu detekciju, analizu i reakciju na sve složenije sajber pretnje. AI pomaže u automatizaciji odgovora na incidente, predviđanju potencijalnih pretnji i smanjenju lažnih pozitivnih signala, čime se značajno poboljšava efikasnost sigurnosnih timova.

Perspektiva korišćenja AI[59] u sajber bezbednosti takođe naglašava važnost integracije sa postojećim sistemima, kao što su SIEM rešenja, čime AI postaje ključni alat za proaktivno upravljanje rizicima. Kako pretnje postaju sve sofisticiranije, uloga veštačke inteligencije postaje neophodna za unapređenje otpornosti na napade i održavanje sigurnosti u dinamičnom digitalnom okruženju. AI ima potencijal da preoblikuje načine na koje se sajber rizici identifikuju, upravljaju i rešavaju, pružajući organizacijama sposobnost da se efikasnije suoče sa izazovima savremenih pretnji u sajber prostoru.

5.3. Upravljanje bezbednosnim rizicima u sajber prostoru na nacionalnom nivou

Razvoj internet bezbednosti u Srbiji je u poslednjim godinama postao sve značajnija tema, kako se povećava digitalizacija i upotreba informacionih tehnologija u svim sferama društva, uključujući javni sektor, privredu, obrazovanje i privatne korisnike. Srbija se, kao i mnoge druge zemlje, suočava sa sve kompleksnijim pretnjama u sajber prostoru, što zahteva kontinuirani razvoj bezbednosnih politika, infrastrukture i svesti o sajber bezbednosti.

Regulativa i strateški okvir

U Srbiji je postavljen pravni i strateški okvir za unapređenje sajber bezbednosti, uglavnom usklađen sa evropskim standardima. Ključni dokumenti koji definišu razvoj internet bezbednosti u Srbiji uključuju:

- Zakon o informacionoj bezbednosti: Usvojen 2016. godine, ovaj zakon postavlja osnove za regulaciju sajber bezbednosti i obavezuje pravna lica, posebno pružaoce ključnih usluga, da preduzimaju mere zaštite svojih informacionih sistema. Zakon definiše i odgovornosti u slučaju incidenata i bezbednosnih pretnji.
- Strategija razvoja informacione bezbednosti (2021-2026): Ovaj dokument definiše nacionalne ciljeve i prioritete u vezi sa unapređenjem sajber bezbednosti, uključujući zaštitu kritične infrastrukture, jačanje kapaciteta državnih institucija i podizanje svesti o sajber pretnjama.
- Usklađivanje sa evropskom regulativom: Srbija je postavila temelje za usklađivanje svojih zakona sa evropskim zakonodavstvom, uključujući direktive poput NIS direktive (Direktiva o bezbednosti mrežnih i informacionih sistema).

[59] Artificial Intelligence in Cybersecurity – L. White (2020), str. 50-55.

Institucionalna podrška

Za koordinaciju aktivnosti u vezi sa internet bezbednošću u Srbiji zadužene su različite državne institucije:

- Kancelarija za IT i eUpravu: Ključna institucija koja razvija i implementira politike eUprave, ali i inicijative za povećanje bezbednosti u sajber prostoru.
- Nacionalni CERT (Computer Emergency Response Team)[60]: Osnovan u okviru RATEL-a (Regulatorna agencija za elektronske komunikacije i poštanske usluge), Nacionalni CERT je odgovoran za koordinaciju odgovora na sajber incidente, kao i za pružanje saveta i smernica pravnim i fizičkim licima u vezi sa sajber bezbednošću.
- MUP (Ministarstvo unutrašnjih poslova): Posebne jedinice Ministarstva unutrašnjih poslova (MUP) rade na borbi protiv sajber kriminala, prikupljanju digitalnih dokaza i reagovanju na sajber incidente.

Svesnost i edukacija

Jedan od ključnih izazova za razvoj internet bezbednosti u Srbiji je podizanje svesti o sajber pretnjama među građanima, privatnim kompanijama i državnim institucijama. Pokrenuto je nekoliko inicijativa i kampanja u cilju podizanja nivoa svesti o značaju internet bezbednosti:

- Obrazovni programi: Sve više obrazovnih institucija, uključujući fakultete i škole, uvodi predmete i kurseve posvećene sajber bezbednosti i digitalnoj pismenosti.
- Kampanje za podizanje svesti: Različite nevladine organizacije, kao i državne institucije, sprovode kampanje za podizanje svesti o sigurnom korišćenju interneta, posebno u vezi sa zaštitom privatnih podataka, prepoznavanjem phishing napada i zaštitom od malvera.

Tehnološki razvoj i ulaganja u sajber bezbednost

U Srbiji su sve prisutnije kompanije koje razvijaju rešenja za sajber bezbednost, a postoji i sve veći fokus na unapređenje tehnologija za zaštitu podataka i mreža. Neke ključne oblasti uključuju:

- Razvoj sigurnosnih rešenja: Pojavljuju se lokalne IT firme koje nude proizvode i usluge za zaštitu informacionih sistema, uključujući rešenja za enkripciju, antivirusne sisteme, zaštitu mreža i prevenciju curenja podataka.
- Digitalna transformacija privrede: Kako sve više kompanija prelazi na digitalne poslovne modele, raste i ulaganje u sigurnosne tehnologije, poput firewall-a, VPN-ova, sigurnosnih protokola i cloud zaštite.

Sajber pretnje i izazovi

Iako se internet bezbednost razvija, Srbija se suočava sa različitim vrstama sajber pretnji, uključujući:

- Ransomware napadi: Ovi napadi postaju sve učestaliji, ciljajući i privatni sektor i državne institucije.

[60] White, K. (2020). National CERT: Role in Cybersecurity., str. 35-38

- Phishing i socijalni inženjering: Napadi putem lažnih emailova i društvenih mreža sve više pogađaju građane i organizacije.
- Napadi na kritičnu infrastrukturu: Kao i u drugim zemljama, kritična infrastruktura[61] u Srbiji, uključujući energetski sektor, telekomunikacije i zdravstvo, postaje meta sajber napada.

Razvoj internet bezbednosti u Srbiji napreduje kroz usklađivanje sa evropskim standardima, jačanje institucija i povećanje svesti o sajber pretnjama. Iako je postignut značajan napredak u postavljanju regulatornog okvira i stvaranju infrastrukturne podrške, i dalje postoji potreba za daljim ulaganjem u tehnologije i edukaciju kako bi se Srbija adekvatno zaštitila od sve složenijih sajber pretnji.

U poslednjih nekoliko godina, Srbija je sprovela niz specifičnih inicijativa i projekata u oblasti sajber bezbednosti, usmerenih na jačanje kapaciteta za borbu protiv sajber pretnji, podizanje svesti o sajber rizicima i unapređenje zakonodavstva. Neke od ključnih inicijativa i projekata uključuju:

Jedan od najznačajnijih koraka u jačanju internet bezbednosti u Srbiji bio je formiranje Nacionalnog CERT-a, koji deluje u okviru Regulatorne agencije za elektronske komunikacije i poštanske usluge (RATEL). Nacionalni CERT je zadužen za koordinaciju odgovora na sajber incidente u zemlji, pružanje podrške institucijama, kompanijama i građanima u prevenciji i rešavanju sajber pretnji. Nacionalni CERT takođe organizuje redovne obuke i simulacije sajber napada kako bi unapredio pripremljenost relevantnih aktera na moguće incidente.

Srbija je intenzivirala saradnju sa međunarodnim organizacijama kao što su Europol i ENISA (Evropska agencija za sajber bezbednost), što je omogućilo bolju koordinaciju u borbi protiv sajber kriminala na međunarodnom nivou. Ova saradnja uključuje zajedničke operacije protiv sajber kriminalaca, razmenu informacija o pretnjama i najbolje prakse u vezi sa bezbednošću informacionih sistema.

Sprovedeno je nekoliko sajber vežbi i simulacija napada, kao što je CyberTesla, koja je fokusirana na unapređenje otpornosti ključnih sektora, poput finansijskog sektora, telekomunikacija i energetike. Ove vežbe pomažu u testiranju sposobnosti brzog reagovanja na kompleksne sajber incidente i poboljšavaju koordinaciju između različitih institucija i privatnog sektora.

Srbija je takođe unapredila svoj zakonodavni okvir u oblasti sajber bezbednosti. Zakon o informacionoj bezbednosti iz 2016. godine postavio je osnove za zaštitu informacionih sistema od sajber pretnji, dok su kasnije izmene zakona dodatno ojačale obaveze privatnog sektora, naročito u vezi sa zaštitom kritične infrastrukture i odgovorom na incidente. Implementacija ovog zakona prati standarde Evropske unije i pomaže u usklađivanju sa evropskom Direktivom o bezbednosti mreža i informacionih sistema (NIS Direktiva).

Projekat "Sajber Srbija" pokrenut je kao platforma za promociju sajber bezbednosti, podizanje svesti javnosti i jačanje kapaciteta institucija i kompanija u zemlji. Ovaj projekat uključuje obuke za IT profesionalce, organizovanje seminara, kao i edukaciju građana o prepoznavanju

[61] Oliver, J. (2021). Protecting Critical Infrastructure in Cybersecurity., str. 45-50

i prevenciji sajber pretnji. Cilj projekta je da se stvori kultura sajber bezbednosti na nacionalnom nivou, gde svaki korisnik interneta ima osnovno znanje o zaštiti podataka.

U saradnji sa univerzitetima i privatnim sektorom, Srbija je uvela niz obrazovnih programa usmerenih na sajber bezbednost. Fakulteti u Srbiji sada nude specijalizovane kurseve o sajber bezbednosti, a organizuju se i programi stručnog usavršavanja za IT stručnjake kroz različite obuke i sertifikacije. Centar za sajber bezbednost Srbije i slične organizacije organizuju seminare i konferencije na kojima se diskutuje o najnovijim trendovima i pretnjama u oblasti sajber bezbednosti.

Srbija sve više ulaže u javno-privatna partnerstva kako bi unapredila sajber bezbednost. Državne institucije sarađuju sa domaćim i međunarodnim IT kompanijama u razvoju novih tehnologija i implementaciji bezbednosnih rešenja. Kompanije kao što su Microsoft i Cisco pružaju tehničku podršku i znanje za razvoj naprednih rešenja za zaštitu mreža i podataka.

Srbija koristi finansijska sredstva iz fondova Evropske unije za unapređenje svoje sajber bezbednosti kroz učešće u projektima kao što su Horizon 2020 i slične inicijative. Ovi projekti omogućavaju Srbiji pristup najnovijim tehnologijama i znanju iz oblasti sajber bezbednosti, što dalje pomaže u jačanju otpornosti na sajber pretnje.

NIS2 regulativa (Direktiva o bezbednosti mreža i informacionih sistema 2) je novi zakonodavni okvir Evropske unije koji proširuje i unapređuje prethodnu NIS direktivu, a njen cilj je jačanje sajber bezbednosti i otpornosti kritične infrastrukture u državama članicama EU. Iako Srbija nije članica EU, kao zemlja koja teži usklađivanju sa evropskim standardima, NIS2 regulativa postavlja osnovu za buduće zakonske prilagodbe u oblasti sajber bezbednosti u Srbiji.

NIS2 regulativa postavlja strože zahteve za zaštitu kritičnih sektora, kao što su energetika, telekomunikacije, finansije i zdravstvo, te obuhvata širi spektar organizacija i uvodi strože mere za prevenciju, detekciju i odgovor na sajber incidente. Srbija već preduzima korake ka implementaciji standarda sličnih onima koje postavlja NIS2, kroz Zakon o informacionoj bezbednosti i rad Nacionalnog CERT-a, kako bi unapredila sajber bezbednost i poboljšala otpornost svojih kritičnih sistema na sajber pretnje.

Očekuje se da će Srbija, kroz dalje usklađivanje sa evropskim regulativama, prilagoditi svoje zakonodavstvo i prakse prema NIS2 standardima kako bi se povećala zaštita i sigurnost ključnih infrastruktura u digitalnom okruženju.

Srbija je u poslednjih nekoliko godina napravila značajne korake u jačanju sajber bezbednosti kroz niz inicijativa i projekata. Formiranjem Nacionalnog CERT-a, poboljšanjem zakonodavnog okvira, obrazovnim inicijativama i jačanjem međunarodne saradnje, država se sve više približava globalnim standardima u borbi protiv sajber pretnji. Iako još uvek postoje izazovi, ovi napori doprinose izgradnji sveobuhvatnog sistema sajber bezbednosti koji može efikasno odgovoriti na sve složenije pretnje u digitalnom okruženju.

5.4. Upravljanje bezbednosnim rizicima u sajber prostoru na međunarodnom nivou

Istorija bezbednosnih rizika u sajber prostoru na globalnom nivou počinje sa razvojem prvih računarskih mreža i interneta, koji su doneli nove ranjivosti i pretnje.

Sredinom 1970-ih pojavili su se prvi računarski virusi i zlonamerni softveri. Rani oblici malvera, poput "Creeper" virusa iz 1971. godine, bili su relativno bezopasni, ali su nagovestili potencijalne rizike. U ovom periodu, napadi su se uglavnom odvijali na pojedinačnim računarskim sistemima, a zaštitne mere bile su minimalne.

Kako je internet postajao globalno dostupan, sajber napadi su se intenzivirali. Mrežni crvi kao što je Morris worm iz 1988. godine prouzrokovali su velike poremećaje u internet infrastrukturi. U ovoj deceniji, pojavili su se napadi na web sajtove i mreže, a hakeri su postali ozbiljan bezbednosni problem. Takođe, pojavili su se DDoS napadi i prve ozbiljne krađe podataka.

Početak 21. veka doneo je značajan porast u sajber kriminalu. Pojavljuju se finansijski motivisani napadi, uključujući krađu identiteta i phishing napade. Crvi kao što su ILOVEYOU i SQL Slammer izazvali su haos na globalnom nivou, a organizovane kriminalne grupe počele su koristiti sajber prostor za krađu podataka i pranje novca. Ova decenija je označila početak sajber špijunaže i napada na vladine i vojne sisteme.

U 2010-im godinama, napadi su postali sve sofisticiraniji i politički motivisani. Stuxnet, prvi poznati sajber oružani napad, 2010. godine je ciljao iranske nuklearne objekte, označavajući početak sajber ratovanja. Napadi na kritičnu infrastrukturu postali su česti, kao i globalni napadi kao što su WannaCry i NotPetya 2017. godine, koji su oštetili kompanije i institucije širom sveta.

U tekućoj deceniji, ransomware napadi[62] su postali dominantna pretnja, posebno ciljajući zdravstvene ustanove, obrazovne institucije i ključnu infrastrukturu. Napadi poput onog na Colonial Pipeline 2021. godine pokazali su koliko su ranjive čak i vitalne industrije. Takođe, sajber špijunaža i geopolitički napadi sve više utiču na globalnu bezbednost.

Sajber bezbednosni rizici evoluirali od ranih, relativno bezopasnih napada do sofisticiranih, koordinisanih napada koji imaju ozbiljne posledice na globalnom nivou, kako za pojedince, tako i za organizacije i države.

Upravljanje bezbednosnim rizicima u sajber prostoru postalo je ključno pitanje za organizacije, vlade i pojedince širom sveta, jer sajber pretnje postaju sve složenije, učestalije i štetnije. Trendovi u ovoj oblasti reflektuju sveobuhvatan pristup koji kombinuje napredne tehnologije, regulatorne reforme, globalnu saradnju i osvešćenost o sajber bezbednosti. U nastavku su detaljno objašnjeni ključni trendovi koji oblikuju budućnost upravljanja bezbednosnim rizicima u sajber prostoru na globalnom nivou.

Jedan od najznačajnijih trendova u sajber prostoru je sve veća sofisticiranost napada. Napredne uporne pretnje (APT - Advanced Persistent Threats), ransomware napadi i multi-vektorski

[62] Thompson, P. (2021). Ransomware Response Strategies for Enterprises. Syngress., str. 30-35

napadi postali su glavni izazovi za organizacije. Ovi napadi često uključuju kompleksne tehnike, kao što su eksploatacija ranjivosti nultog dana, društveni inženjering, napadi na dobavljački lanac i sajber špijunaža.

Kao odgovor na to, globalna sajber bezbednosna zajednica ulaže u napredne tehnologije za odbranu, uključujući:

- Veštačku inteligenciju (AI) i mašinsko učenje (ML): Ove tehnologije pomažu u analizi velikih skupova podataka i identifikaciji obrazaca koji ukazuju na sajber pretnje. AI se koristi za detekciju anomalija u ponašanju korisnika i proaktivnu identifikaciju pretnji pre nego što one postanu ozbiljan problem.
- Zero Trust arhitektura: "Zero Trust" je pristup sajber bezbednosti u kojem nijedan entitet, bez obzira na lokaciju, ne dobija automatski poverenje. Ovaj koncept podrazumeva stalnu proveru identiteta korisnika i uređaja, kao i strogu kontrolu pristupa podacima.
- Kriptografija[63] postkvantnog računarstva: Kako kvantno računarstvo postaje realnost, organizacije sve više istražuju nove kriptografske metode koje će biti otporne na buduće pretnje koje kvantni računari mogu doneti.

Ransomware je postao jedna od najopasnijih i najprofitabilnijih sajber pretnji u poslednjoj deceniji. Grupa DarkSide i napad na Colonial Pipeline 2021. godine pokazali su koliko štete ovi napadi mogu naneti, ne samo finansijskim gubicima, već i u prekidu kritičnih infrastrukturnih usluga. Ransomware napadi sada često koriste modele "ransomware as a service" (RaaS), omogućavajući manje iskusnim kriminalcima da koriste gotove alate za napade.

Organizacije se suočavaju sa sve većom potrebom za:

- Proaktivnim upravljanjem ranjivostima: Redovno ažuriranje softvera, zakrpe za ranjivosti i stroge kontrole pristupa smanjuju šanse za uspeh ransomware napada.
- Oporavkom podataka i rezervnim kopijama: Organizacije sve više ulažu u strategije koje uključuju više nivoa rezervnih kopija kako bi mogle brzo da se oporave od napada bez plaćanja otkupnine.
- Obučavanjem zaposlenih: Veliki broj napada koristi tehnike društvenog inženjeringa, poput phishing-a, pa je edukacija zaposlenih ključni deo odbrane.
- Kritična infrastruktura, uključujući energetiku, zdravstvo, transport, vodosnabdevanje i telekomunikacije, postala je ključna meta sajber napada. Incidenti poput napada na Colonial Pipeline i Travelex pokazali su koliko je ranjiva ova infrastruktura. Kao odgovor, globalni trendovi u upravljanju bezbednosnim rizicima fokusiraju se na:
- Uvođenje specifičnih regulatornih okvira: Regulative kao što su NIS2 direktiva u EU i Executive Order on Improving the Nation's Cybersecurity u SAD postavljaju standarde za zaštitu kritične infrastrukture. Ove regulative obavezuju operatore kritičnih usluga da primene rigorozne mere zaštite.

[63] Cryptography and Network Security: Principles and Practice – William Stallings (2017), str. 67-70.

- Poboljšanje javno-privatne saradnje: Vlade širom sveta sve više sarađuju sa privatnim sektorom kako bi obezbedile deljenje informacija o pretnjama i poboljšale koordinaciju u slučaju incidenata. Ova saradnja omogućava brži odgovor i oporavak u slučaju napada na kritične sektore.

Uspon regulative i zakona o sajber bezbednosti

Sajber bezbednost postaje sve više regulisana oblast. Brojne zemlje uvode strože zakone i standarde kako bi osigurale da organizacije implementiraju adekvatne mere zaštite i odgovornosti u slučaju sajber incidenata. Ključni trendovi u ovoj oblasti uključuju:

GDPR i zaštita podataka: Evropska unija postavila je globalni standard sa General Data Protection Regulation (GDPR), koji postavlja stroge zahteve za zaštitu podataka i obaveštavanje o povredama podataka. Očekuje se da će slični zakoni biti usvojeni i u drugim delovima sveta.

NIS2 direktiva u EU: NIS2 proširuje regulativu za sajber bezbednost na veći broj sektora i uvodi strože kazne za organizacije koje ne ispune zahteve bezbednosti. Njena svrha je da poveća otpornost na sajber napade i poboljša zajedničku sigurnosnu odgovornost unutar EU.

Zakonske reforme u SAD-u: SAD je preduzela nekoliko koraka ka unapređenju sajber bezbednosti, uključujući naredbe i zakonske reforme koje podstiču privatni sektor da unapredi zaštitu, kao i poboljšanje odgovora na sajber incidente.

Globalni sajber rizici i napadi primorali su organizacije da povećaju ulaganja u bezbednosne tehnologije i stručnjake. Prema procenama, globalno tržište sajber bezbednosti će nastaviti da raste eksponencijalno, jer organizacije širom sveta prepoznaju sajber bezbednost kao jedan od ključnih faktora u zaštiti poslovanja i održavanju kontinuiteta. Neka od ključnih ulaganja uključuju:

Cloud sigurnosna rešenja: Sa sve većim prelaskom na cloud infrastrukture, organizacije ulažu u specifične cloud alate za detekciju pretnji, kontrolu pristupa i upravljanje podacima.

Cyber threat intelligence[64] (CTI): Organizacije se sve više oslanjaju na CTI, što im omogućava da proaktivno prate globalne pretnje i prilagode svoje odbrambene sisteme na osnovu najnovijih saznanja o sajber napadima.

Sajber osiguranje: Mnoge kompanije sada investiraju u sajber osiguranje kao dodatnu meru zaštite od finansijskih gubitaka nastalih usled sajber napada.

Ljudski faktor ostaje jedna od najslabijih karika u lancu sajber bezbednosti. U cilju smanjenja rizika povezanih sa društvenim inženjeringom, phishing napadima i internim pretnjama, organizacije širom sveta sve više ulažu u obuku zaposlenih. Ključne aktivnosti uključuju:

Redovne obuke o prepoznavanju pretnji: Programi obuke koji uključuju simulacije sajber napada, kao što su phishing testovi, pomažu zaposlenima da razviju veštine prepoznavanja pretnji.

[64] Practical Cyber Intelligence: How Action-Based Intelligence Can Be an Effective Response to Attacks – Wilson Bautista (2018), str. 45-48.

Sajber bezbednosne politike: Organizacije razvijaju sveobuhvatne bezbednosne politike koje uključuju stroge smernice za korišćenje interneta, društvenih mreža i ličnih uređaja na poslu, čime se smanjuju šanse za slučajni pristup malicioznim sajtovima i aplikacijama.

Veštačka inteligencija (AI) i automatizacija postali su ključni alat u sajber bezbednosti. Ovi alati omogućavaju organizacijama da brže identifikuju i odgovore na pretnje, automatski blokirajući napade ili preduzimajući druge odbrambene mere. Neki od glavnih trendova u ovoj oblasti su:

AI u analizi pretnji: AI sistemi mogu analizirati velike količine podataka u realnom vremenu, identifikujući obrasce koji ukazuju na napade, kao i ranjivosti koje bi napadači mogli da iskoriste.

Automatizovana reakcija na incidente: Automatizacija u okviru SOAR platformi omogućava bržu reakciju na incidente, smanjujući vreme potrebno za identifikaciju i odgovor na napad. Ove tehnologije takođe pomažu u smanjenju opterećenja na bezbednosne timove.

Kako sajber pretnje ne poznaju granice, sve je veći fokus na međunarodnoj saradnji u borbi protiv sajber kriminala. Organizacije poput Europola, NATO-a, Interpol-a, kao i saradnja između država, igraju ključnu ulogu u suzbijanju globalnih sajber pretnji. Neki od ključnih koraka u ovom trendu su:

Razmena informacija o pretnjama: Vlade i međunarodne organizacije sve više sarađuju u razmeni informacija o aktuelnim pretnjama, napadačima i metodama koje koriste. To pomaže u preventivnoj zaštiti globalnih sistema.

Zajedničke sajber vežbe i simulacije: Države i organizacije širom sveta organizuju zajedničke vežbe za sajber bezbednost, čime testiraju otpornost svojih sistema i poboljšavaju koordinaciju odgovora na napade.

Upravljanje bezbednosnim rizicima u sajber prostoru postalo je globalni prioritet zbog sve veće učestalosti i ozbiljnosti sajber napada. Ključni trendovi, uključujući usvajanje naprednih tehnologija poput AI, povećanje regulative, fokus na zaštitu kritične infrastrukture i međunarodnu saradnju, oblikuju budućnost sajber bezbednosti. Organizacije i vlade moraju kontinuirano prilagođavati svoje strategije kako bi bile spremne na nove pretnje i osigurale sigurnost svojih informacionih sistema u sve složenijem digitalnom okruženju.

Razvoj SIEM (Security Information and Event Management) rešenja direktno je oblikovan rastućim i sve složenijim bezbednosnim pretnjama u sajber prostoru. SIEM sistemi su postali centralna tačka u borbi protiv sajber napada, omogućavajući organizacijama da efikasno prate, detektuju i reaguju na pretnje u realnom vremenu. Kako pretnje postaju sve sofisticiranije, tako i SIEM rešenja moraju da evoluiraju kako bi odgovarala na nove izazove. U ovom tekstu istražujemo kako različite vrste sajber pretnji, od naprednih uporne pretnje (APT) do ransomware napada, oblikuju razvoj SIEM sistema i funkcionalnosti.

Uticaj bezbednosnih pretnji u sajber prostoru na razvoj SIEM rešenja na međunarodnom nivou je izuzetno snažan, jer se globalna priroda interneta i sajber pretnji odražava na sve industrije, organizacije i države. Sistemi za upravljanje bezbednosnim informacijama i događajima (SIEM) razvijeni su kao odgovor na potrebu za efikasnim i centralizovanim praćenjem, analizom i upravljanjem bezbednosnim incidentima. Kako su sajber pretnje evoluirale i postale

sofisticiranije, SIEM rešenja su se morala prilagoditi kako bi odgovarala na nove i složenije izazove.

Rast kompleksnosti i učestalosti sajber pretnji

Sajber pretnje su se u poslednjim decenijama značajno promenile i postale složenije i opasnije. Napadi poput ransomware-a, DDoS (Distributed Denial of Service), phishing-a, i naprednih upornh pretnji (APT), zahtevaju od organizacija složenija rešenja za praćenje i zaštitu. U tom kontekstu, SIEM rešenja su postala ključna tehnologija za detekciju i odgovaranje na ovakve pretnje.

Ransomware: Eksplozija ransomware napada, koji šifruju podatke i zahtevaju otkup, naterala je organizacije da integrišu alate za raniju detekciju pretnji. SIEM sistemi su morali da se prilagode kako bi prepoznali sumnjivo ponašanje koje vodi ka šifrovanju velikih količina podataka i blokirali napad pre nego što prouzrokuje štetu.

Napredne uporne pretnje (APT): APT napadi, koji traju duže vremenske periode i često koriste više faza napada, primorali su SIEM rešenja da integrišu alate za dubinsku analizu i detekciju anomalija. SIEM sistemi sada uključuju mogućnosti za dugoročno praćenje i korelaciju podataka kako bi otkrili ove "tihi" napade.

Proširivanje opsega i različitost izvora podataka

Kako su se sajber pretnje razvijale, tako je postala neophodna integracija sve većeg broja izvora podataka u SIEM sisteme. Organizacije su počele da koriste kompleksne IT infrastrukture, uključujući lokalne sisteme, cloud servise, mobilne uređaje, IoT (Internet of Things), i druge tehnologije. To je značilo da SIEM rešenja moraju da budu sposobna da prikupljaju, analiziraju i koreliraju podatke iz različitih izvora, u realnom vremenu.

Integracija podataka iz cloud servisa: Sa sve većim prelaskom na cloud rešenja, SIEM sistemi su morali da prošire svoju funkcionalnost na praćenje cloud infrastrukture. To uključuje integraciju podataka iz AWS, Microsoft Azure, Google Cloud i drugih platformi, čime se omogućava detekcija pretnji specifičnih za cloud okruženja, kao što su neovlašćeni pristup, curenje podataka ili nepravilna konfiguracija resursa.

IoT uređaji: IoT uređaji postaju sve veći cilj napadača, a njihova ranjivost i nesigurne konfiguracije zahtevaju praćenje kroz SIEM sisteme. IoT ekosistemi generišu ogromne količine podataka, što je SIEM rešenja nateralo da koriste napredne algoritme za filtriranje i analizu podataka u realnom vremenu.

Praćenje mobilnih uređaja: Kako se sve više poslovnih funkcija obavlja putem mobilnih uređaja, SIEM sistemi su morali da razviju sposobnost praćenja i analiziranja podataka generisanih putem mobilnih aplikacija, softverskih ažuriranja i mobilnih mreža kako bi otkrili potencijalne pretnje.

Automatizacija i orkestracija odgovora na incidente

Kako sajber pretnje postaju sve brže i kompleksnije, ručno praćenje i odgovor na incidente postaju neefikasni. Ovaj trend je podstakao razvoj SIEM sistema koji integrišu veći stepen automatizacije i orkestracije kako bi omogućili brži i precizniji odgovor na sajber pretnje.

SOAR integracija (Security Orchestration, Automation, and Response): SIEM sistemi sve češće uključuju SOAR funkcionalnosti koje omogućavaju automatizaciju odgovora na pretnje. Korišćenjem unapred definisanih pravila i akcija, SIEM može automatski pokrenuti odgovore na određene napade, kao što su izolacija kompromitovanih sistema, blokiranje sumnjivih IP adresa ili slanje obaveštenja bezbednosnim timovima.

Korišćenje veštačke inteligencije (AI) i mašinskog učenja (ML): Napredni SIEM sistemi koriste AI i mašinsko učenje za identifikaciju anomalija i pretnji koje tradicionalni sistemi ne bi prepoznali. AI analizira ogromne količine podataka, prepoznaje obrasce i predviđa potencijalne napade na osnovu prethodnih pretnji. AI takođe omogućava smanjenje broja lažnih alarma, jer uči da razlikuje normalne aktivnosti od sumnjivih.

Globalna regulativa i usklađenost sa zakonodavstvom

Međunarodna zakonska regulativa ima veliki uticaj na razvoj SIEM rešenja. Globalni zakoni i propisi o sajber bezbednosti, kao što su GDPR u Evropskoj uniji, NIS2 direktiva i zakoni poput CLOUD Act i CISA (Cybersecurity Information Sharing Act) u SAD, zahtevaju od organizacija da postave rigorozne mere za zaštitu podataka i detekciju pretnji.

Usklađenost sa GDPR-om: SIEM sistemi su morali da se prilagode kako bi pomogli organizacijama da ispunjavaju zahteve GDPR-a, naročito u pogledu zaštite podataka, obaveštavanja o povredi podataka i obrade ličnih informacija. SIEM rešenja sada uključuju napredne funkcionalnosti za praćenje podataka, generisanje izveštaja o prekršajima i reviziju događaja koji se odnose na lične podatke.

Zahtevi za bezbednost kritične infrastrukture: Regulative poput NIS2 direktive, koja se odnosi na zaštitu kritične infrastrukture, uključuju telekomunikacije, energetiku i finansijske sisteme. SIEM rešenja moraju omogućiti organizacijama u ovim sektorima da efikasno prate i reaguju na sajber napade, dok pružaju transparentne izveštaje o aktivnostima i usklađenosti sa zakonom.

Povećanje broja pretnji na kritičnu infrastrukturu

U protekloj deceniji, napadi na kritičnu infrastrukturu, kao što su energetika, vodosnabdevanje, telekomunikacije i zdravstvo, postali su sve učestaliji i sofisticiraniji. Globalni incidenti, poput napada na ukrajinsku elektroenergetsku mrežu 2015. godine i napad ransomware-om na Colonial Pipeline 2021. godine, podstakli su veći fokus na zaštitu kritičnih sistema.

Detekcija pretnji u industrijskim kontrolnim sistemima (ICS): SIEM rešenja sada integrišu alate specifične za praćenje i zaštitu industrijskih kontrolnih sistema (ICS). Kako se infrastruktura postepeno digitalizuje i povezuje s internetom, pretnje ovim sistemima rastu, pa je integracija ICS specifičnih detekcijskih alata u SIEM ključna za zaštitu.

Proaktivna odbrana i prediktivna analitika: Kako bi se bolje zaštitili ovi kritični sistemi, SIEM rešenja koriste naprednu analitiku podataka za predviđanje napada. Korišćenjem podataka o prethodnim napadima i anomalijama, SIEM sistemi mogu upozoriti na moguće pretnje pre nego što se one razviju u stvarne incidente.

Povećanje zahteva za transparentnost i reviziju

Organizacije širom sveta suočavaju se sa sve većim pritiskom da poboljšaju transparentnost u vezi sa sajber bezbednosnim aktivnostima i rizicima. Zahtevi za transparentnost dolaze od

regulatora, investitora i korisnika, koji očekuju jasne informacije o tome kako kompanije štite podatke i sisteme.

Izveštavanje i revizija u realnom vremenu: SIEM rešenja su razvijena kako bi pružila sveobuhvatan i automatizovan sistem za generisanje izveštaja o aktivnostima, incidenata i usklađenosti. Ovi izveštaji pomažu organizacijama da ispunjavaju zakonske obaveze, ali i da stvore jasnu sliku o stanju sajber bezbednosti za menadžment i akcionare.

Forenzička analiza posle incidenata: U slučaju sajber incidenata, SIEM rešenja omogućavaju detaljnu forenzičku analizu događaja, identifikaciju uzroka i planiranje budućih bezbednosnih politika. Ova sposobnost analize je posebno važna u pravnom i regulatornom kontekstu, jer pomaže u dokazivanju usklađenosti i minimiziranju pravnih posledica nakon napada.

Uticaj bezbednosnih pretnji na razvoj SIEM rešenja na međunarodnom nivou je ogroman, jer se tehnologija kontinuirano prilagođava kako bi odgovorila na sve sofisticiranije napade. Kompleksnost modernih sajber pretnji zahteva od SIEM sistema da postanu brži, inteligentniji i integrisani sa naprednim alatima kao što su AI, mašinsko učenje i automatizacija. Kako regulative postaju strože, a globalne pretnje sve češće, SIEM rešenja igraju ključnu ulogu u održavanju sajber bezbednosti na visokom nivou, omogućavajući organizacijama da efikasno upravljaju rizicima, zaštite kritičnu infrastrukturu i ispune zahteve za transparentnost.

5.5. Etički aspekt[65]

Upravljanje bezbednosnim rizicima u sajber prostoru nosi niz etičkih izazova zbog brzog razvoja tehnologija i složenosti koje one donose. Ovi izazovi uključuju balansiranje privatnosti, slobode izražavanja, odgovornosti za zaštitu korisnika, kao i pitanja transparentnosti i pravičnosti. Evo detaljnijeg pregleda etičkih aspekata upravljanja bezbednosnim rizicima u sajber prostoru:

Zaštita privatnosti[66]

Jedan od ključnih etičkih izazova u sajber bezbednosti jeste zaštita privatnosti korisnika. Organizacije koje upravljaju podacima korisnika moraju da obezbede da ti podaci budu zaštićeni od neovlašćenog pristupa, krađe ili zloupotrebe. Međutim, zaštita privatnosti može biti u sukobu sa potrebom da se nadgleda i kontroliše sajber prostor radi otkrivanja pretnji i ranjivosti. Balansiranje između zaštite privatnosti i bezbednosnih potreba zahteva pažljiv etički pristup kako bi se izbegla prekomerna intruzija u privatnost pojedinaca.

Transparentnost i odgovornost

Sistem upravljanja rizicima u sajber prostoru mora biti transparentan kako bi korisnici bili informisani o načinima na koje se njihovi podaci prikupljaju, koriste i čuvaju. Nedostatak transparentnosti može dovesti do zloupotreba ili gubitka poverenja. Takođe, organizacije koje upravljaju sajber bezbednošću moraju biti odgovorne za bilo kakve greške, kao što su curenje

[65] Ethics in Cybersecurity Practices – F. Nelson (2021), str. 39-42.
[66] Peterson, R. (2020). Privacy Issues in Cybersecurity. CRC Press., str. 25-29

podataka ili hakerski napadi, što često dovodi do dilema u vezi sa time ko snosi odgovornost za oštećenja – korisnici, tehnološke kompanije ili država.

Postoji stalni sukob između potrebe za povećanom sajber bezbednošću i očuvanja slobode korisnika, uključujući slobodu izražavanja i pristup informacijama. Na primer, države mogu nametnuti strože zakone o nadzoru u cilju zaštite od sajber pretnji, ali to može dovesti do suzbijanja slobode govora ili ograničavanja pristupa određenim informacijama na internetu. Etika nalaže da se razmotre posledice po društvo, te da bezbednosne mere ne ugrožavaju osnovna prava.

Tehnologije sajber bezbednosti često imaju nejednak uticaj na različite grupe ljudi. Digitalna nejednakost može dovesti do toga da određene zajednice budu ranjivije na sajber napade, dok one sa boljim resursima mogu imati bolju zaštitu. Takođe, algoritmi za otkrivanje pretnji mogu biti pristrasni, što može stvoriti nepravdu prema određenim korisnicima ili grupama. Etika zahteva da sistemi sajber bezbednosti budu dizajnirani i implementirani na pravičan način, kako bi se smanjile ove nejednakosti.

Važan etički izazov jeste kako organizacije koriste tehnologije za prevenciju zlonamernih aktivnosti u sajber prostoru. U nastojanju da zaštite svoje sisteme, kompanije i države koriste napredne tehnike praćenja i identifikacije potencijalnih pretnji, ali te tehnike mogu voditi u problematične prakse, poput masovnog nadzora ili zloupotrebe tehnologija u represivne svrhe. Etika upravljanja rizicima zahteva jasne granice između legitimnih bezbednosnih mera i preteranog nadzora.

Postoji etička odgovornost za sprečavanje zloupotrebe sajber tehnologija u svrhe kao što su hakerski napadi, cybercrime, ransomware i drugi oblici zlonamernog ponašanja. Organizacije koje razvijaju ili koriste sajber bezbednosne alate moraju preuzeti odgovornost za načine na koje ti alati mogu biti upotrebljeni, s obzirom na to da neodgovorno rukovanje tehnologijama može prouzrokovati veliku štetu.

Sajber prostor ne poznaje granice, pa je međunarodna saradnja ključna u upravljanju bezbednosnim rizicima. Etika nalaže da države i organizacije poštuju međunarodne norme, izbegavajući aktivnosti poput sajber špijunaže ili kibernetičkih napada na infrastrukture drugih zemalja. Potreba za stvaranjem zajedničkih etičkih standarda u međunarodnim okvirima postaje sve veća kako bi se smanjile tenzije i sukobi u sajber prostoru.

Sve veća upotreba veštačke inteligencije[67] (AI) u sajber bezbednosti donosi dodatne etičke izazove, posebno u vezi sa automatizacijom donošenja odluka. Algoritmi mogu donositi odluke o tome koje aktivnosti su sumnjive ili predstavljaju pretnju, što može imati posledice po pojedince i organizacije. Odluke zasnovane na AI moraju biti transparentne, nepristrasne i u skladu sa etičkim principima kako bi se izbegle diskriminacija ili nepravda.

Upravljanje bezbednosnim rizicima u sajber prostoru zahteva duboko razumevanje etičkih izazova. Tehnološki napredak uvek mora biti u skladu sa osnovnim ljudskim pravima, transparentnošću, pravičnošću i odgovornošću. Samo etički utemeljeni pristupi omogućavaju pravičan i siguran sajber prostor, gde se bezbednosne mere ne koriste na štetu pojedinaca ili zajednica.

[67] Robinson, M. (2021). Artificial Intelligence in Modern Security Systems. Springer., str. 55-60

Upotreba veštačke inteligencije (AI) za smanjenje bezbednosnih rizika u sajber prostoru donosi brojne prednosti, ali istovremeno otvara niz etičkih pitanja koja se tiču privatnosti, transparentnosti, pristrasnosti i odgovornosti. AI se sve češće koristi za otkrivanje sajber pretnji, upravljanje incidentima i analizu ponašanja korisnika, ali njeno korišćenje zahteva pažljivo razmatranje etičkih implikacija. Evo detaljnijeg uvida u etički aspekt upotrebe AI za smanjenje bezbednosnih rizika:

1. **Privatnost i masovni nadzor**

Jedan od ključnih etičkih izazova u upotrebi AI za sajber bezbednost jeste zaštita privatnosti korisnika. AI sistemi često analiziraju velike količine podataka kako bi identifikovali pretnje i anomalije, što može uključivati obradu osjetljivih informacija o korisnicima. Postavlja se pitanje koliko podataka je potrebno prikupiti i obraditi da bi AI efikasno smanjio bezbednosne rizike, a da se pritom ne naruši privatnost pojedinaca. Masovni nadzor i prikupljanje podataka mogu narušiti osnovna prava na privatnost, što zahteva balansiranje između potrebe za bezbednošću i prava na privatnost.

2. **Transparentnost i odgovornost algoritama**

AI sistemi za sajber bezbednost često rade na složenim algoritmima i mašinskom učenju, što ih čini manje transparentnim. Odluke koje AI donosi, kao što su identifikacija sumnjivih aktivnosti ili određivanje prioriteta za bezbednosne incidente, mogu biti nejasne ili teško razumljive ljudskim korisnicima. Ovo vodi do pitanja transparentnosti u odlučivanju i toga da li krajnji korisnici imaju dovoljno informacija o načinu na koji AI funkcioniše. Etika nalaže da AI sistemi budu što transparentniji, kako bi korisnici mogli razumeti kako se donose odluke, i da postoji jasna odgovornost za eventualne greške ili zloupotrebe.

3. **Pristrasnost algoritama**

Algoritmi veštačke inteligencije nisu imuni na pristrasnost, jer se treniraju na osnovu podataka koji mogu sadržati pristrasnosti prema određenim grupama ili pojedincima. Ovaj problem je posebno izražen u sajber bezbednosti, gde AI može pogrešno identifikovati pretnje na osnovu faktora kao što su etnička pripadnost, geografska lokacija ili obrasci ponašanja. Ako su podaci koji se koriste za obuku AI sistema pristrasni, AI može nepravedno označiti određene korisnike ili aktivnosti kao pretnju, što može dovesti do nepravde i diskriminacije. Zato je etički važno da AI sistemi budu dizajnirani na način koji minimizuje pristrasnost i osigurava pravičnost.

4. **Autonomija AI sistema**

Još jedno važno etičko pitanje odnosi se na autonomiju AI sistema u donošenju odluka. Kako se AI tehnologije usavršavaju, raste potencijal da sistemi donose ključne bezbednosne odluke bez ljudske intervencije. Autonomne odluke AI sistema, kao što su blokiranje mrežnih aktivnosti, identifikacija zlonamernih napada ili deaktiviranje korisničkih naloga, mogu imati ozbiljne posledice. Ova autonomija zahteva pažljivo razmatranje kako bi se obezbedilo da ljudi zadrže kontrolu nad ključnim odlukama i da postoji mehanizam za ljudsku reviziju u slučajevima kada AI napravi grešku.

5. **Odgovornost za greške i zloupotrebe**

Veštačka inteligencija nije nepogrešiva i može napraviti greške u prepoznavanju sajber pretnji ili upravljanju rizicima. Pitanje odgovornosti je važno: ko je odgovoran kada AI napravi grešku

koja može rezultirati sajber napadom ili gubitkom podataka? Da li odgovornost snosi organizacija koja koristi AI, proizvođač AI sistema ili sam algoritam? Ovo pitanje postaje posebno složeno kada AI sistemi postaju sve autonomniji i kada se ljudska intervencija smanjuje. Etika nalaže da postoji jasan okvir odgovornosti koji će obezbediti zaštitu korisnika i osigurati da greške budu adekvatno ispravljene.

6. Upotreba AI za preduzimanje preventivnih akcija

AI se koristi ne samo za otkrivanje pretnji, već i za preduzimanje preventivnih akcija, kao što su blokiranje sumnjivih veza, izolacija mrežnih segmenata ili preduzimanje drugih bezbednosnih mera. Ove akcije mogu imati ozbiljan uticaj na korisnike, posebno ako su preuranjene ili zasnovane na pogrešnim informacijama. Etika nalaže da preventivne mere budu pažljivo kontrolisane i da ne nanose štetu korisnicima ili njihovom poslovanju, posebno kada nema jasnih dokaza da su stvarno ugroženi.

7. Dvojna upotreba AI tehnologija

Tehnologije veštačke inteligencije mogu imati dvojnu upotrebu – dok se koriste za legitimne svrhe poput sajber bezbednosti, mogu biti zloupotrebljene za napade, špijunažu ili masovni nadzor. Zbog toga, etički okvir upotrebe AI mora uključivati kontrolu nad načinom na koji se ove tehnologije razvijaju i distribuiraju, kako bi se sprečila njihova zloupotreba u sajber kriminalu ili u neetičkim praksama nadzora.

8. Uticaj na ljudsku radnu snagu

AI automatski obavlja zadatke koje su ranije izvršavali ljudi, kao što su otkrivanje pretnji i analiza logova. Iako ovo povećava efikasnost, zamena ljudske radne snage AI sistemima može dovesti do etičkih dilema u vezi sa gubitkom radnih mesta u oblasti sajber bezbednosti. Ovaj prelazak na AI postavlja pitanje kako obezbediti da radnici koji su pogođeni automatizacijom dobiju priliku za prekvalifikaciju i nove mogućnosti, čime bi se smanjile negativne socijalne posledice.

9. AI i ljudsko poverenje

Poverenje u veštačku inteligenciju je ključno za njen uspeh u smanjenju sajber bezbednosnih rizika. Korisnici moraju biti sigurni da AI sistemi rade u njihovom interesu i da će ih zaštititi bez narušavanja njihovih prava. Održavanje poverenja zahteva transparentnost u vezi sa radom AI sistema, jasne etičke smernice i odgovornost za greške. Ako korisnici nemaju poverenja u AI, efekti smanjenja sajber rizika mogu biti umanjeni jer se korisnici mogu odupreti implementaciji ovih tehnologija.

Etika igra centralnu ulogu u upotrebi veštačke inteligencije za smanjenje bezbednosnih rizika u sajber prostoru. Ključni etički izazovi uključuju zaštitu privatnosti, transparentnost, pravičnost, odgovornost za greške i mogućnost zloupotrebe tehnologija. Kako AI postaje sve važniji u sajber bezbednosti, neophodno je razvijati etičke standarde i regulative koje će osigurati da ove tehnologije rade u službi društva, a ne na njegovu štetu.

Sajber prostor postaje sve složeniji i dinamičniji, a time i pretnje po bezbednost sve učestalije i sofisticiranije. Kao odgovor na te pretnje, "next-gen" SIEM softverska rešenja se razvijaju kako bi omogućila bolje praćenje, detekciju i odgovor na sajber napade. Ova rešenja kombinovanjem naprednih tehnologija kao što su veštačka inteligencija (AI), mašinsko učenje

(ML) i analitika u realnom vremenu omogućavaju organizacijama da budu proaktivnije u upravljanju bezbednosnim rizicima. Međutim, kako se "next-gen" SIEM alati razvijaju, postavljaju se važna etička pitanja u vezi sa načinom na koji se ovi sistemi koriste, kako utiču na privatnost korisnika, koje su granice automatizacije i koja je odgovornost programera i organizacija u upravljanju ovim alatima. U nastavku je detaljna analiza ključnih etičkih aspekata koji utiču na razvoj i implementaciju "next-gen" SIEM rešenja.

Razvoj sledeće generacije (NextGen) SIEM softverskih rešenja može značajno unaprediti sposobnost organizacija da upravljaju sajber bezbednosnim rizicima, ali dolazi sa nizom etičkih izazova. Ključni etički aspekti uključuju zaštitu privatnosti, pravičnost algoritama, autonomiju sistema, odgovornost za greške i potencijal za zloupotrebu tehnologije. Da bi se osiguralo da razvoj ovih sistema bude u skladu sa etičkim normama, neophodno je uspostaviti jasne smernice koje balansiraju bezbednosne potrebe sa zaštitom osnovnih ljudskih prava.

5.6. Perspektive pristupa i legitimiteta

Bezbednosni rizici u sajber prostoru postaju sve kompleksniji sa brzim napretkom digitalnih tehnologija, globalizacijom i rastućom zavisnošću od informacionih i komunikacionih sistema. Ovi rizici predstavljaju izazove koji obuhvataju širok spektar pitanja – od zaštite privatnosti i podataka, preko ekonomskih i političkih posledica, do pretnji nacionalnoj bezbednosti. Perspektive pristupa ovim rizicima i pitanje legitimiteta uticaja mere preduzetih da bi se ovi rizici mitigovali, predstavljaju ključne tačke rasprava u savremenoj sajber bezbednosti.

Perspektive pristupa bezbednosnim rizicima u sajber prostoru

Perspektive pristupa bezbednosnim rizicima u sajber prostoru zavise od različitih faktora, uključujući tehničke kapacitete, regulatorne okvire, društvene norme, ekonomske prioritete i globalne odnose moći. Postoje četiri glavna pristupa koja se koriste za suočavanje sa bezbednosnim rizicima u sajber prostoru:

a) Tehnički pristup

Tehnički pristup zasniva se na razvijanju i primeni naprednih tehnologija koje mogu sprečiti, otkriti i odgovoriti na sajber pretnje. Ovaj pristup obuhvata implementaciju softverskih rešenja poput antivirusnih programa, vatrozida, šifrovanja podataka, kao i naprednih sistema za otkrivanje upada (IDS), sistema za upravljanje informacijama i događajima (SIEM), te veštačke inteligencije (AI) za detekciju anomalija.

Prednosti tehničkog pristupa:

- Brza i efikasna reakcija: Tehnološka rešenja omogućavaju brzo otkrivanje i neutralisanje pretnji, posebno kada su automatizovana.
- Skalabilnost: Tehnološke platforme mogu se skalirati kako bi pokrile velike sisteme i mreže, omogućavajući organizacijama da odgovore na globalne sajber pretnje.

- Automatizacija zaštitnih mera: Primena AI[68] i mašinskog učenja omogućava sistemima da se unapred programiraju za prepoznavanje novih vrsta pretnji.

Ograničenja tehničkog pristupa:

- Nedostatak ljudske intuicije: Iako su AI sistemi sposobni za brzo prepoznavanje obrazaca, često im nedostaje intuitivno razumevanje koje dolazi sa ljudskim iskustvom.
- Zavisnost od pravilne implementacije: Tehnološki alati zavise od pravilne implementacije i redovnog ažuriranja, a slabosti u tim aspektima mogu učiniti sistem ranjivim.
- Visoki troškovi: Implementacija sofisticiranih tehničkih rešenja može biti skupa, posebno za manje organizacije.

b) Regulatorni pristup

Regulatorni pristup zasniva se na kreiranju pravnih i institucionalnih okvira koji regulišu ponašanje u sajber prostoru. Države i međunarodne organizacije uspostavljaju zakone, standarde i smernice koje obavezuju pojedince, kompanije i druge entitete da usvoje određene mere sajber bezbednosti.

Prednosti regulatornog pristupa:

- Jasni standardi: Zakoni i regulative postavljaju jasne standarde kojih se svi učesnici u sajber prostoru moraju pridržavati.
- Odgovornost i sankcije: Regulatorni okvir omogućava uvođenje odgovornosti i kazni za organizacije koje ne poštuju zahteve bezbednosti.
- Promocija kolektivne bezbednosti: Regulativa može podstaći saradnju između različitih sektora i država, čime se unapređuje kolektivna otpornost na sajber napade.

Ograničenja regulatornog pristupa:

- Sporo prilagođavanje: Zakonodavni proces je često spor, dok se sajber pretnje brzo razvijaju i menjaju.
- Nedostatak globalne usklađenosti: Različite zemlje imaju različite zakonske okvire, što otežava globalnu koordinaciju u borbi protiv sajber kriminala.
- Kompleksnost implementacije: Pravne regulative mogu biti komplikovane za primenu, naročito u tehnički složenim okruženjima.

c) Društveni pristup

Društveni pristup podrazumeva edukaciju korisnika, podizanje svesti o bezbednosnim rizicima i promovisanju kulture sajber bezbednosti. Fokus je na ljudskom faktoru, jer mnogi bezbednosni incidenti u sajber prostoru nastaju zbog ljudske greške ili nepažnje.

Prednosti društvenog pristupa:

- Povećana svest korisnika: Edukacija i obuka korisnika smanjuju rizik od phishing napada, socijalnog inženjeringa i drugih pretnji koje iskorišćavaju ljudske slabosti.

[68] White, L. (2021). Practical Applications of AI in Cybersecurity. Packt., str. 50-55

- Lako primenjivo: Edukacija i osvešćivanje su često jednostavni i relativno jeftini u poređenju sa implementacijom tehnoloških rešenja.
- Smanjenje grešaka: Kultura sajber bezbednosti unutar organizacija može značajno smanjiti broj incidenata uzrokovanih greškom zaposlenih.

Ograničenja društvenog pristupa:

- Ograničen domet: Neki korisnici, naročito u manje razvijenim sredinama, mogu imati ograničen pristup edukaciji o sajber bezbednosti.
- Nepredvidivost ljudskog ponašanja: I pored edukacije, ljudske greške su i dalje neizbežne, pa ovaj pristup ne može u potpunosti neutralisati rizike.
- Međunarodni pristup[69]

S obzirom na globalnu prirodu interneta i sajber pretnji, međunarodna saradnja postaje ključna u borbi protiv sajber kriminala i terorizma. Države, organizacije i privatni sektor sve više sarađuju na stvaranju međunarodnih standarda i protokola za sajber bezbednost.

Prednosti međunarodnog pristupa:

- Globalna koordinacija: Sajber kriminal često prevazilazi granice država, pa je međunarodna saradnja ključna za efikasno praćenje i suzbijanje pretnji.
- Povećana otpornost: Deljenjem informacija i resursa, zemlje i organizacije mogu zajedno brže i efikasnije odgovoriti na pretnje.
- Razvoj zajedničkih standarda: Međunarodni sporazumi i organizacije mogu pomoći u uspostavljanju zajedničkih standarda i protokola za sajber bezbednost.

Ograničenja međunarodnog pristupa:

- Nedostatak univerzalnog konsenzusa: Različite zemlje mogu imati različite prioritete i pristupe sajber bezbednosti, što otežava postizanje globalnog dogovora.
- Geopolitičke tenzije: Međunarodni odnosi i geopolitički sukobi mogu ometati saradnju u borbi protiv sajber pretnji.

Legitimitet uticaja bezbednosnih rizika u sajber prostoru

Pitanje legitimiteta u upravljanju bezbednosnim rizicima u sajber prostoru odnosi se na to da li su mere i pristupi koji se koriste za smanjenje tih rizika etički, pravno i društveno prihvatljivi. Ovaj legitimitet se može posmatrati kroz nekoliko ključnih dimenzija:

a) Legalni legitimitet

Legitimnost preduzetih mera često zavisi od njihovog usklađivanja sa nacionalnim zakonima i međunarodnim pravnim okvirima. Mnoge države su usvojile zakone o zaštiti podataka (npr. GDPR u Evropskoj uniji) koji regulišu kako organizacije mogu koristiti i čuvati podatke korisnika.

[69] The Role of International Standards in Cybersecurity – J. White (2019), str. 40-45.

Kritični izazovi legalnog legitimiteta:

- Balans između bezbednosti i sloboda: Zakonodavci se suočavaju sa izazovom balansiranja između potrebe za zaštitom društva od sajber pretnji i očuvanja osnovnih sloboda, kao što su privatnost i sloboda izražavanja.
- Sukobi zakona: Različiti pravni okviri u različitim državama mogu dovesti do sukoba, naročito kada kompanije posluju na globalnom tržištu.

b) Etnički legitimitet

Etnička pitanja uključuju moralne aspekte preduzetih bezbednosnih mera u sajber prostoru. Mere koje se koriste za smanjenje rizika moraju biti u skladu sa osnovnim ljudskim pravima.

Ključni etički izazovi:

- Privatnost: Sve mere koje se preduzimaju moraju poštovati privatnost korisnika. Masovni nadzor, bez odgovarajućih zakonskih osnova, može biti smatran neetičkim.
- Pravičnost i nepristrasnost: Tehnologije i politike sajber bezbednosti[70] ne smeju nepravedno ciljati određene grupe korisnika.

c) Društveni legitimitet

Mere koje organizacije preduzimaju moraju biti društveno prihvatljive. Ukoliko javnost smatra da su mere koje se koriste za smanjenje bezbednosnih rizika u sajber prostoru preterane ili invazivne, može doći do gubitka poverenja u institucije i tehnologije.

Ključni društveni izazovi:

- Transparentnost: Organizacije moraju jasno komunicirati sa javnošću o merama koje preduzimaju kako bi smanjile rizike, što povećava poverenje u te sisteme.
- Angažovanje korisnika: Građani i korisnici moraju biti uključeni u procese donošenja odluka kako bi mere koje se preduzimaju bile društveno legitimne.

Perspektive pristupa bezbednosnim rizicima u sajber prostoru kreću se od tehničkih do regulatornih, društvenih i međunarodnih rešenja. Svaki pristup ima svoje prednosti i ograničenja, a njihova efikasnost zavisi od konteksta u kojem se primenjuju. Pitanje legitimiteta ovih mera uključuje razmatranje pravnih, etičkih i društvenih faktora, sa posebnim fokusom na transparentnost, odgovornost i očuvanje osnovnih prava korisnika. Samo uz poštovanje ovih principa, mere za smanjenje sajber rizika mogu biti efikasne i društveno prihvatljive.

[70] Wright, T. (2021). Developing Cybersecurity Policies. CRC Press., str. 37-42

GLAVA 6: INTEGRACIJA SIEM[71] SOFTVERSKIH REŠENJA

SIEM softverska rešenja za upravljanje bezbednosnim informacijama i događajima predstavljaju jednu od ključnih tehnologija u modernoj sajber bezbednosti. Ovi sistemi omogućavaju organizacijama da prate, analiziraju i reaguju na bezbednosne događaje u realnom vremenu, što značajno poboljšava njihovu sposobnost da se suoče sa sajber pretnjama. SIEM rešenja kombinuju funkcionalnosti upravljanja bezbednosnim informacijama (SIM – Security Information Management) i upravljanja bezbednosnim događajima (SEM – Security Event Management) kao bi pružili sveobuhvatan uvid u aktivnosti unutar mreže i sistema.

Evo detaljnog opisa SIEM softverskih rešenja, njihovih glavnih funkcionalnosti, prednosti, izazova, i njihovog mesta u modernom sajber bezbednosnom okruženju:

1. Osnovne funkcionalnosti SIEM sistema

SIEM sistemi imaju niz funkcionalnosti koje omogućavaju efikasno upravljanje bezbednosnim događajima i informacijama. Njihova glavna uloga je prikupljanje, agregacija i korelacija podataka o bezbednosnim događajima iz različitih izvora, analiziranje tih podataka u realnom vremenu i preduzimanje odgovarajućih akcija kada se detektuju pretnje.

- Prikupljanje i agregacija podataka

SIEM sistemi prikupljaju ogromne količine podataka iz različitih izvora u organizaciji, kao što su:

- Mrežni uređaji (ruteri, vatrozidi, prekidači)
- Sistemi za zaštitu krajnjih tačaka (antivirusni softver, IDS/IPS sistemi)
- Sistemi za autentifikaciju (Active Directory, LDAP)
- Sistemi za upravljanje bazama podataka

-Aplikacije i serveri (npr. web serveri, aplikacioni serveri) Prikupljeni podaci uključuju logove, događaje i bezbednosne informacije koje SIEM sistem agregira u centralizovanu bazu podataka radi daljeg procesuiranja.

- Korelacija podataka

Jedna od ključnih funkcionalnosti SIEM rešenja je korelacija podataka, gde sistem analizira prikupljene informacije iz različitih izvora i povezuje ih kako bi identifikovao potencijalne pretnje. Korelacioni engine koristi unapred definisana pravila i algoritme za prepoznavanje obrazaca koji ukazuju na bezbednosne incidente.

Na primer, ako SIEM sistem detektuje neobične pokušaje pristupa iz udaljenih lokacija, zajedno sa neuobičajenim ponašanjem korisnika (poput pristupa kritičnim resursima koje korisnik obično ne koristi), sistem može prepoznati potencijalni pokušaj kompromitovanja korisničkog naloga.

- Detekcija anomalija

[71] Thompson, P. (2020). SIEM Integration with Other Cybersecurity Tools., str. 40-45

Savremeni SIEM sistemi koriste analitiku zasnovanu na mašinskom učenju i detekciju anomalija kako bi identifikovali neuobičajene aktivnosti koje mogu ukazivati na pretnje. Detekcija anomalija uključuje praćenje uobičajenog ponašanja u mreži ili aplikacijama i prepoznavanje devijacija od tog ponašanja. Ova funkcionalnost je posebno korisna za prepoznavanje naprednih sajber napada, kao što su APT (Advanced Persistent Threat) napadi, koji mogu proći ispod radara tradicionalnih sistema.

- Upozorenja i reagovanje na incidente

SIEM sistemi generišu upozorenja u realnom vremenu kada otkriju sumnjive aktivnosti ili pretnje. Ova upozorenja mogu biti konfigurisana da se automatski šalju bezbednosnim timovima ili da se pokrenu određene akcije (npr. blokiranje IP adrese, prekidanje sesije, privremeno deaktiviranje korisničkog naloga). Takođe, SIEM rešenja često integrišu funkcionalnosti automatizovanog odgovora na incidente (SOAR – Security Orchestration, Automation and Response), što omogućava brže reagovanje na pretnje.

- Upravljanje logovima i forenzika

SIEM sistemi omogućavaju centralizovano upravljanje logovima i dugoročno čuvanje logova sa različitih sistema, što je korisno za analize i forenzičke istrage u slučaju bezbednosnih incidenata. Ovi logovi omogućavaju analitičarima da istraže tačne uzroke napada i identifikuju slabe tačke u mrežnoj infrastrukturi. Dugoročno skladištenje logova je takođe važno zbog usaglašenosti sa regulativama, kao što su GDPR, HIPAA, PCI DSS i druge.

- Izveštavanje i usaglašenost sa regulativama

SIEM sistemi obezbeđuju detaljne izveštaje o bezbednosnim incidentima, aktivnostima i usaglašenosti sa regulativama. Ovi izveštaji su neophodni za ispunjavanje zahteva za bezbednosne audite i prikazivanje dokaza o usaglašenosti sa propisima. Sistemi mogu automatski generisati izveštaje na dnevnom, nedeljnom ili mesečnom nivou, kao i po zahtevu.

2. Komponente SIEM rešenja[72]

SIEM sistemi su složena rešenja koja se sastoje od nekoliko ključnih komponenti, od kojih svaka igra specifičnu ulogu u bezbednosnom ekosistemu organizacije.

Prikupljači podataka (Data Collectors)

- Prikupljači podataka su agenti ili servisi koji prikupljaju logove i događaje sa različitih izvora u mreži. Oni prikupljaju podatke sa krajnjih tačaka, servera, mrežnih uređaja i drugih relevantnih izvora i prenose ih u centralni SIEM sistem za dalju analizu.

Skladištenje podataka

- SIEM sistemi često koriste centralizovane baze podataka ili distribuirana skladišta podataka kako bi skladištili ogromne količine logova i bezbednosnih informacija. Ove baze podataka moraju biti optimizovane za brzo pretraživanje i analizu kako bi omogućile efikasan rad sistema.

[72] Hartman, F. W. (2020). Components of Effective SIEM Systems. Elsevier., str. 66-70

Korelacioni engine

- Korelacioni engine je ključna komponenta SIEM sistema koja omogućava analizu podataka u realnom vremenu. Ovaj engine primenjuje pravila i algoritme za identifikaciju obrazaca i događaja koji ukazuju na potencijalne pretnje ili sumnjive aktivnosti.

Interfejs za upravljanje i analitiku

- SIEM rešenja imaju interfejs za upravljanje koji omogućava analitičarima i bezbednosnim stručnjacima da pregledaju upozorenja, pretražuju logove, kreiraju izveštaje i konfigurišu pravila za detekciju pretnji. Moderni SIEM sistemi obično koriste intuitivne grafičke korisničke interfejse (GUI) sa nadzornim pločama (dashboards) koje pružaju sveobuhvatan pregled bezbednosne situacije u organizaciji.

3. Prednosti SIEM rešenja

SIEM sistemi donose niz ključnih prednosti organizacijama koje se suočavaju sa sve složenijim pretnjama u sajber prostoru:

- Centralizovano upravljanje bezbednošću
- Jedna od najvećih prednosti SIEM rešenja je centralizovano upravljanje bezbednosnim događajima. Bez obzira na broj uređaja, aplikacija ili mrežnih segmenata, SIEM sistemi omogućavaju centralizovano praćenje i analizu svih bezbednosnih događaja, čime se povećava efikasnost bezbednosnih timova.
- Realno-vremenska detekcija pretnji
- Zahvaljujući mogućnostima korelacije podataka i detekcije anomalija, SIEM sistemi omogućavaju detekciju pretnji u realnom vremenu[73], što značajno smanjuje vreme potrebno za otkrivanje i odgovor na sajber napade.
- Usaglašenost sa regulativama
- SIEM rešenja olakšavaju usaglašenost sa industrijskim i pravnim regulativama koje zahtevaju stalno praćenje, izveštavanje i čuvanje bezbednosnih podataka. Organizacije mogu generisati prilagođene izveštaje koji ispunjavaju zahteve specifičnih regulativa, čime se smanjuju rizici od pravnih i finansijskih sankcija.
- Forenzička analiza
- SIEM sistemi pružaju detaljnu forenzičku analizu nakon bezbednosnog incidenta, omogućavajući bezbednosnim timovima da identifikuju tačan tok napada i izgrade strategije za prevenciju budućih incidenata.

4. Izazovi SIEM rešenja

Iako SIEM sistemi donose značajne prednosti, oni se takođe suočavaju sa nizom izazova:

- Složenost i troškovi implementacije
- SIEM rešenja su često kompleksna za implementaciju i zahtevaju značajna sredstva za inicijalnu instalaciju, konfiguraciju i održavanje. Organizacije moraju imati obučen kadar kako bi upravljao i optimizovao SIEM sistem.
- Lažno pozitivna upozorenja

[73] Edwards, R. (2021). Real-time Threat Detection Techniques in SIEM Systems. Elsevier., str. 50-55

- Jedan od najvećih izazova u radu sa SIEM sistemima je veliki broj lažnih pozitivnih upozorenja, koji mogu preopteretiti bezbednosne timove i otežati prepoznavanje pravih pretnji. Precizna podešavanja i redovno ažuriranje pravila mogu smanjiti ovaj problem, ali zahtevaju stalnu pažnju i optimizaciju.
- Velike količine podataka

S obzirom na to da SIEM sistemi prikupljaju ogromne količine podataka, organizacije se često suočavaju sa izazovom upravljanja i analize tih podataka. Bez efikasne analize, podaci mogu postati pretežak teret za sistem i izazvati kašnjenja u detekciji pretnji.

5. Next-gen SIEM: Budućnost SIEM rešenja

Savremena i napredna SIEM rešenja poznata kao "Next-gen SIEM" integrišu veštačku inteligenciju, mašinsko učenje i analitiku u oblaku kako bi se izborila sa rastućim izazovima u sajber prostoru. Ova rešenja omogućavaju:

- Prediktivnu analitiku: Predviđanje potencijalnih pretnji na osnovu analize obrazaca.
- Integraciju sa SOAR platformama: Automatizovan odgovor na incidente i orkestraciju bezbednosnih procedura.
- Bolju detekciju naprednih pretnji[74]: Napredni algoritmi[75] koji se bore sa APT i drugim sofisticiranim napadima.

SIEM softverska rešenja predstavljaju vitalni deo moderne sajber bezbednosti, omogućavajući organizacijama da upravljaju velikim količinama podataka, detektuju pretnje u realnom vremenu i reaguju na incidente. Iako se suočavaju sa izazovima poput složenosti implementacije i lažnih pozitivnih upozorenja, "next-gen" SIEM sistemi pružaju sve naprednija rešenja koja uključuju veštačku inteligenciju i automatizaciju, čime organizacije postaju otpornije na sajber pretnje.

6.1. ARMADA: Primer NexGen SIEM softverskog rešenja

ARMADA je NextGen SIEM sistem za nadzor i otkrivanje svih vrsta sajber napada koji trenutno pruža automatsku zaštitu. Sistem kao što je ARMADA neophodan je za izgradnju bezbednosnih procesa i infrastrukture za korporacije i finansijske institucije, vojne i vladine organizacije, kao i za industrijski IoT i tzv. pametne mreže.

ARMADA SIEM pruža:

- Zaštitu kritične infrastrukture i podataka od oštećenja, neovlašćene upotrebe i napada.
- Zaštitu ključnih poslovnih procesa za državne institucije, banke, operatere telekomunikacija, kompanije itd.
- Zaštitu finansijskih transakcija i sprečavanje krađa.
- Zaštitu poslovne komunikacije i dokumenata.
- Zaštitu ličnih identiteta i integriteta ličnih usluga.

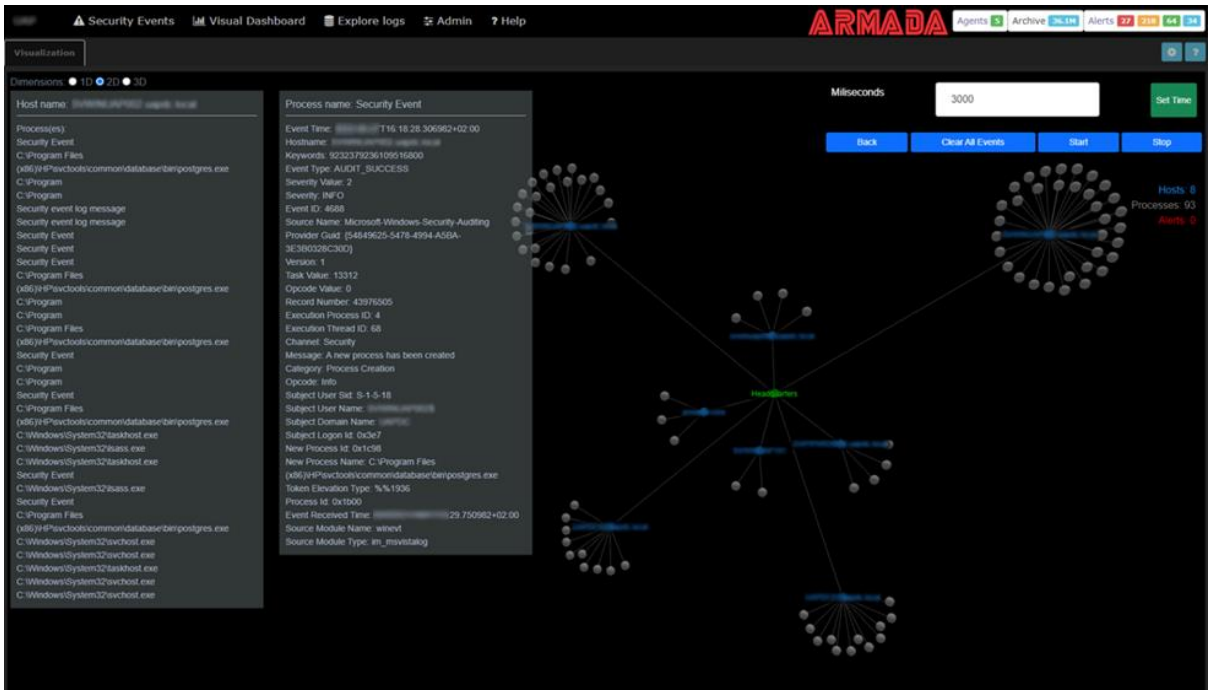
[74] Green, A. (2020). Advanced Threat Detection in Cyber Defense. Syngress., str. 34-38
[75] Smith, C. (2021). Advanced Threat Detection Algorithms., str. 30-34

Osnovne karakteristike ARMADA SIEM sistema su:

- Obrađuje ogromne količine podataka; obrađuje milijarde događaja svakog dana, analizirajući neograničenu količinu podataka.
- Korelacija u realnom vremenu; potrebno je manje od 3ms za otkrivanje napada ili abnormalnog ponašanja i reagovanja u skladu sa tim.
- Zamke za ”hakere”; unutrašnje zamke se postavljaju u okviru sistema da bi prevarile i uhvatile uljeze.
- Detekcija nepoznatih pretnji; spoljne zamke dobijaju znanje o novim napadima i napadačima širom sveta i blokiraju ih u realnom vremenu.
- Vizuelna rekonstrukcija i forenzika; gleda se šta svaki zaposleni radi unutar sistema ili spolja i to u realnom vremenu ili unazad istorijski.
- Automatska zaštita; svaki napadač je blokiran u realnoj jedinici vremena čim se pokaže njegovo zlonamerno ponašanje.

ARMADA SIEM prikuplja spoljne informacije o trenutnim napadima uživo, kao i unutrašnje informacije o ljudima i uređajima unutar štićene mreže, povezuje ih u realnom vremenu i reaguje za manje od 3 milisekunde. Poznate vrste napada prepoznaju se pravilima korelacije, dok se najnoviji, još uvek nepoznati tipovi napada blokiraju na osnovu podataka o pretanjama u realnom vremenu. Čaki i ako postojeći antivirus ili ”firewall” ne mogu da identifikuju napad (potrebno im je više vremena za ažuriranje potpisa), ARMADA SIEM takav napad može da blokira.

Slika 1. Grafička interpretacija događaja i veza u realnom vremenu ARMADA SIEM sistema



Ključne prednosti ARMADA SIEM SISTEMA u odnosu na konkurentska rešenja:

- Vreme otkrivanja napada je manje od 3 milisekunde, što je oko 10.000 puta brže od najefikasnijeg konkurentskog sistema.

- Postavljanje zamki i njihovo korišćenje za učenje u realnom vremenu o novim, nepoznatim IP napadima i novim metodama napada, kako sistem bio proaktivan u zaštiti imovine i podataka čak i od nepoznatih vrsta napada.
- ARMADA SIEM pomaže da se izvrši više od 100 različitih antivirusnih provera bilo kojih proceas ikada pokrenutih u štićenim sistemima.
- Svako može da razume događaje samim gledanjem kanala za rekonstrukciju u video zapisu.

Tehnička prednost postignuta je sledećim parametrima:

- Arhitektura zasnovana na mikroservisima, potpuno skalabilna.
- Obrada logova u realnom vremenu.
- Više od 15.000 događaja u sekundi na jednoj viruelnoj mašini.
- Kompletna infrastruktura organizacije radi na jednoj virtuelnoj mašini.
- Neograničeno skladištenje logova kojem se lako pristupa.
- Neograničene analize retrospektivnih događaja.

SIEM ARMADA osigurava da kroz automatizciju korisnik bude maksimalno proaktivan:

- Praćenje u realnom i prošlom vremenu korisnikovih administratora.
- Nadgledanje, otkrivanje i reagovanje protiv napada za 3 milisekunde.
- Otkrivanje nestandardnog ponašanja korisnika ili strukture mrežnog saobraćaja koja mo-e predstavljati izvor opasnosti u bliskoj budućnosti.

Otkrivanje slabosti u arhitekturi i uspostavljanje mrežne i uslužne infrastrukture.

SIEM ARMADA daje vizuelni prikaz čime pojednostavljuje tehnološku složenost:

- Složenost i heterogenost infrastrukture.
- Masovno nadgledanje aktivnosti (veliki broj uređaja, korisnika, mrežnih elemenata ili IoT senzora stvara milione događaja).
- Neophodno integrisano znanje o različitim operativnim sistemima, mrežnim elementima i uslužnim platformama.

SIEM ARMADA koristi se u oba domena zaštite, odnosno koriste ga takozvani Blue Team i Red Team.

Blue Team koristi SOC (Security Operations Center) kao eksterni IT bezbednosni centar, koji koristi napredne alate, kao i platformu Cyber Surveillance System ARMADA, koja predstavlja sledeću generaciju SIEM proizvoda i ima dosta jedinstvenih funkcija. Pruža zaštitu 24/7, naprednu analitiku i forenziku u realnom vremenu svakom korisniku, bez obzira na složenost IT sistema, aktivnost ili izloženost napadima.

Red Team se sastoji od etičkih hakera i radi prethodno odobren napad, dizajniran da meri koliko je bezbedna mreža, aplikacije, sredstva itd. organizacije od napada u stvarnom svetu.Njihova procena će otkriti tehnološke i fizičke ranjivosti. Tokom procene, Red Team će pokrenuti opasne scenarije kako bi otkrio potencijalne slabosti u vašim proizvodima, IT infrastrukturi, mreži i zaposlenima.Red Teamće pokušati da probije i istraži slabosti na svim nivoima i sredstvima vaše organizacije. Za razliku od tradicionalnog PT-a(Penetration Testa), koji će se uglavnom fokusirati na testiranu aplikaciju, angažovanje Red Team-a bi moglo da zahteva

kreiranje alata za upadu informacioni sistem, email-oveza phishing napade, maliciozne payloade, exploite, hardverske trojance, kreiranje avatara i prikupljanje obaveštajnih podataka o organizaciji i infiltriranje u njeno okruženje.

Na kraju procene organizaciji se uručuje izveštaj u kome se pominju sva utvrđena kršenja, ranjivosti ili slabosti. Izveštaj takođe uključuje sugestije i preporuke za sanaciju kako bi se svi pronađeni bezbednosni propusti odmah sanirali.

Cilj je da se unese otpornost u okruženja klijenata koji se suočavaju sa sve većom potrebom za bezbednošću.

ARMADA NextGen SIEM rešenje je savremeni sistem dizajniran za organizacije koje žele unapređenu i proaktivnu zaštitu od sajber pretnji. Korišćenjem napredne tehnologije, veštačke inteligencije i mašinskog učenja, ARMADA omogućava skalabilnu, prilagodljivu i efikasnu detekciju i odgovor na pretnje, smanjujući rizik od ozbiljnih sigurnosnih incidenata. Sve ove karakteristike čine ga ključnim rešenjem za organizacije koje žele da unaprede svoj nivo sigurnosti i održe konkurentsku prednost u sve složenijem sajber okruženju.

6.1.1. Studija slučaja implementacije ARMADA NextGen SIEM softverskog rešenja

Klijent: Velika finansijska institucija iz Beograda koja pruža bankarske i finansijske usluge širom regiona.

Izazov: Institucija je suočena sa sve većim brojem sofisticiranih sajber napada, uključujući APT i pokušaje krađe podataka. Postojeći sigurnosni sistemi nisu bili efikasni u otkrivanju i odgovoru na ove pretnje u realnom vremenu.

Cilj: Implementacija naprednog SIEM sistema za sveobuhvatnu zaštitu, brzo otkrivanje i odgovor na sajber pretnje, čime bi se zaštitila kritična infrastruktura[76] i poverljivi podaci klijenata.

Rešenje: Implementiran je NextGen SIEM ARMADA softver, prilagođen potrebama institucije. ARMADA je omogućila napredno praćenje, detekciju i odgovor na sajber pretnje, koristeći sledeće funkcionalnosti:

- Analiza i obrada velike količine podataka: Analiza milijardi događaja dnevno za sveobuhvatan uvid u potencijalne pretnje.
- Korelacija u realnom vremenu: Detekcija i reakcija na pretnje u manje od 3 milisekunde.
    - Zamke za hakere: Korišćenje zamki za obmanu i hvatanje uljeza.
- Vizuelna rekonstrukcija i forenzika: Real-time retrospektivna analiza aktivnosti unutar sistema.
- Automatska remedijacija: Blokiranje napadača u realnom vremenu čim je detektovano zlonamerno ponašanje.

[76] Oliver, J. (2021). Critical Infrastructure Protection. CRC Press., str. 40-45

Rezultati:

Nakon implementacije ARMADA sistema, postignuti su značajni rezultati:

- Povećana bezbednost: Efikasno otkrivanje i blokiranje sajber napada.
- Smanjeno vreme reakcije: Brzo reagovanje na incidente.
- Poboljšana usklađenost: Usklađenost sa najnovijim regulativama i standardima sajber bezbednosti.
- Ojačana infrastruktura: Zaštita kritične infrastrukture i podataka klijenata.

Povratna informacija klijenta: Implementacija NextGen SIEM ARMADA sistema bila je prelomna tačka za organizaciju. Poboljšana je sposobnost da se otkriju i odgovori na pretnje, te je značajno povećano poverenje klijenata u sposobnost da se zaštitie njihovi podaci.

Zaključak: NextGen SIEM ARMADA sistem je omogućio finansijskoj instituciji efikasnu borbu protiv sofisticiranih sajber pretnji. Sa naprednim mogućnostima detekcije i reakcije u realnom vremenu, ARMADA je osigurala sveobuhvatnu zaštitu i povećala otpornost organizacije na sajber napade.

6.2. ARMADA AI Engine modul: Primer projekta uspešne implementacije AI Engine modula u NexGen SIEM alat

Tabela 2. Osnovni podaci o projektu

PODACI O APLIKANTU			
1. Naziv projekta	ARMADA AI Engine Module		
2. Vrednost projekta u USD	Ukupna vrednost projekta	Vrednost granta za koji se aplicira	Iznos sopstvenog učešća aplikanta
	60.000	50.000	10.000
3. Naziv MMSPP	Advanced Cyber Security doo Beograd - Vračar		
4. Matični broj	21558796		
5. PIB	111876558		
6. Adresa	Rudnička 8, Beograd		
7. E-mail	office@acs.co.rs		
8. Kontakt osoba i kontakt telefon	Aleksandar Kotevski +38163257578		
9. Datum registracije MMSPP	20.02.2020.		
10. Vlasnici *(ukoliko ima više vlasnika navesti njihovo učešće u vlasništvu privrednog društva)*	Aleksandar Kotevski		
11. Šifra delatnosti	6202 – Konsultantske delatnosti u oblasti informacione tehnologije		
12. Web sajt	https://www.acs.co.rs/		
13. Nalog na društvenim mrežama	https://rs.linkedin.com/company/advanced-cyber-security-doo		
14. Poslovni prihod u RSD	2021.	2022.	2023.
	7.880.000	9.940.000	21.163.000
15. Neto dobit u RSD	2021.	2022.	2023.
	341.000	14.000	1.897.000

Rezime projekta

Cilj ovog projekta je implementacija AI modula[77] u postojeći alat za sajber bezbednost radi poboljšanja detekcije i odgovora na pretnje. Osnovni fokus je na razvoju i integraciji naprednih algoritama mašinskog učenja i dubokog učenja kako bi se unapredila sposobnost prepoznavanja i predviđanja sajber napada, kao i efikasnijeg upravljanja incidentima.

Ključni koraci projekta:

Analiza postojećeg stanja: Detaljna analiza postojećeg alata za sajber bezbednost kako bi se identifikovali nedostaci i potencijalne oblasti poboljšanja.

Definisanje zahteva: Definisanje specifičnih zahteva za AI modul, uključujući tipove pretnji koje će biti detektovane, performanse sistema, resurse potrebne za implementaciju i integraciju sa postojećim alatom.

Razvoj AI modula: Razvoj AI modula koji će koristiti napredne tehnike mašinskog učenja i dubokog učenja za detekciju i predikciju sajber pretnji. Ovo uključuje izbor odgovarajućih algoritama, prikupljanje i obradu podataka, trening modela i evaluaciju performansi.

Integracija u postojeći alat: Integracija AI modula u postojeći alat za sajber bezbednost uz minimalne prepravke i optimizaciju kako bi se osigurala kompatibilnost i stabilnost sistema.

Testiranje i validacija: Testiranje performansi AI modula na simuliranim i stvarnim sajber napadima kako bi se proverila efikasnost detekcije i odgovora na pretnje. Validacija rezultata u stvarnom svetu radi verifikacije funkcionalnosti.

Očekivani rezultati:

Poboljšana detekcija sajber pretnji: Implementacija AI modula će rezultirati boljom detekcijom sajber pretnji, uključujući i ranije otkrivanje novih i nepoznatih napada.

Brži odgovor na incidente: Integracija AI tehnologija omogućiće automatsko reagovanje na sajber pretnje u realnom vremenu, smanjujući vreme reakcije i minimizirajući štetu.

Smanjenje lažnih alarma: Napredni algoritmi mašinskog učenja će pomoći u smanjenju lažnih alarma i boljoj diferencijaciji između stvarnih pretnji i benignih aktivnosti.

Povećana efikasnost timova za sajber bezbednost: Kroz automatizaciju procesa detekcije i odgovora, timovi za sajber bezbednost će moći efikasnije da upravljaju incidentima i resursima.

Kontinuirano unapređenje sistema: Implementacija AI modula omogućiće kontinuirano učenje i adaptaciju sistema na nove vrste pretnji kroz analizu novih podataka i iterativno poboljšanje algoritama.

Ukupno, implementacija AI modula u alat za sajber bezbednost ima za cilj da unapredi sposobnost detekcije i odgovora na sajber pretnje, doprinoseći povećanju sigurnosti i stabilnosti sistema.

[77] Harris, T. (2021). Integrating AI in SIEM Systems., str. 44-48

Kompetencije i kapaciteti aplikanta

Advanced Cyber Security je kompanija koju su 2020 godine osnovali stručnjaci sa dugogodišnjim međunarodnim iskustvom u oblasti sajber bezbednosti, bivši zaposleni u Vladi Republike Srbije, kao i privatnim kompanijama koji se bave informacionom bezbednošću. Kompanija nudi dugogodišnje iskustvo u praktikovanju ofanzivne i defanzivne sajber bezbednosti u okviru javnog i privatnog sektora koji zauzimaju ključne pozicije. Članovi tima prepoznaju ranjivosti sistema, znajući tačno kako ih neko može iskoristiti i pretvarajući ih u bezbedno okruženje otporno na bilo kakve napade, malver ili štetne događaje. Na kraju procene korisniku se uručuje izveštaj u kome su navedena sva utvrđena kršenja, ranjivosti ili slabosti uključujući sugestije i preporuke za sanaciju kako bi se svi pronađeni bezbednosni propusti odmah sanirali.

Glavni proizvodi odnosno usluge uključuju:

- Zaštitu od spyware softvera – štetnog softvera sa namenom da presreće ili preuzima kontrolu nad računarom bez znanja ili dozvole korisnika.
- Brzo pravljenje rezervne kopije podataka na oblaku (Cloud-u).
- Zaštita baza podataka.
- Zaštita svih novčanih transakcija.
- Zaštita od računarskih programa koji su dizajnirani za slanje nepoželjne pošte.
- Veštačka inteligencija koja je napravljena da brine o sajber bezbednosti korisnika.
- Zaštita sajber bezbednosti klijenata korisnika.
- Zaštita pomoću tehnologija prepoznavanja lica osoba.
- Pravljenje rezervne kopije podataka u planirano vreme.
- Skeniranje aktivnih uređaja na mreži.
- Zaštita od potencijalnih sajber pretnji koje utiču na funkcionisanje procesora (CPU).
- Alati koji omogućavaju vraćanje IT infrastructure u stanje pre katastrofe.
- Zaštita razmene poruka unutar kompanije.
- Plan sajber zaštite u kompanijama.
- Zaštita svih transakcija koje se odvijaju preko mobilnih telefona.
- Zaštita POS terminala za plaćanje kreditnim krarticama.
- Zaštita logistike transporta podataka.
- Dvadesetčetvoročasovna podrška sedam dana u nedelji.

Kompanija je dosada uspešno realizovala sledeće projekte:

- Horizon 2020 – Puzzle Framework

Inovativnost

Sistem ARMADA predstavlja napredni softverski alat za obradu bezbednosnih podataka namenjen prikupljnju i obradi podataka o sajber bezbednosti, napravljen na proverenim principima upravljanja bezbednosnim incidentima i događajima (Security Information and Event Management).Sistem ARMADA poruža dvadesetčetvoročasovnu zaštitu, naprednu analitiku i forenziku u realnom vremenu svakom korisniku, bez obzira na složenost IT sistema, aktivnost ili izloženost napadima i predstavlja snažan alat koji u radu koristi tzv. Blue Team u

okviru SOC-a[78]. Inovacija se odnosi na razvoj AI engine modula koji će klasifikovati napade i prepoznavati sve anomalije i razjasniti korisniku prirodu napada i dati preporuku kako da se odnosi prema konkretnoj situaciji.

Pored navedenog u okviru kompanije deluje i tzv. Red Team koji se sastoji od etičkih hakera koji rade prethodno odobreni napad, dizajniran da meri Koliko je bezbedna mreža, aplikacije i sredstva organizacije od napada u stvarnom svetu. Njihgova procena otkriva tehnološke i fizižke ranjivosti, gde se tokom procene pokreću opasni scenariji kako bi se otkrile potencijalne slabosti u proizvodima, IT infrastrukturi, mreži i zaposlenima. Razvoj i implementacija inovacije stvorila bi dodatnu vrednost za korisnike budući da za razliku od tradicionalnog Penetration testa, koji se uglavnom fokusira na testiranu aplikaciju, angažovanje Read Team-a zahteva kreiranje alata za upad u informacioni system, email-ove za phishing napade, maliciozne payloade, exploite, hardverske trojance, kreiranje avatara i prikupljanje obaveštajnih podataka o organizaciji i infiltriranje u njeno okruženje.

Relevantnost projekta implementacije AI modula u sajber bezbednosti za nacionalne, regionalne ili globalne prioritete je veoma visoka zbog sve većeg broja sajber napada koji predstavljaju ozbiljnu pretnju za državnu, poslovnu i ličnu bezbednost. Efikasna zaštita od sajber pretnji postaje sve važnija kako bi se sačuvali podaci, infrastruktura i funkcionalnost društva u celini. Implementacija AI tehnologija u sajber bezbednosti može značajno unaprediti sposobnost detekcije, analize i reagovanja na sajber pretnje, čime se doprinosi jačanju bezbednosti i stabilnosti na nacionalnom, regionalnom i globalnom nivou.

Problem koji rešavamo ovim projektom je nedostatak efikasnih alata za praćenje i detekciju sajber pretnji u realnom vremenu. Mnoge organizacije, posebno velike korporacije i vladine institucije, suočavaju se sa sve većim brojem sofisticiranih sajber napada koji mogu naneti ozbiljnu štetu njihovoj infrastrukturi i podacima.

Uvođenjem AI modula u alat za sajber bezbednost omogućavamo organizacijama da automatski analiziraju velike količine podataka i identifikuju sumnjive aktivnosti koje bi mogle ukazivati na potencijalnu pretnju. Na taj način, organizacije mogu brže reagovati na sajber napade i preduzeti odgovarajuće mere zaštite pre nego što dođe do ozbiljnih posledica.

Ova inovacija je posebno korisna za IT timove, bezbednosne stručnjake i menadžere informacione bezbednosti koji su odgovorni za zaštitu organizacija od sajber pretnji. Korišćenjem AI tehnologije, oni mogu efikasnije upravljati sajber bezbednošću i smanjiti rizik od napada.

Tehnološki proces

U okviru projekta radi će se na razvoju AI engine modula koji će biti implementiran u system ARMADA, a koji će koristiti prednost veštačke inteligencije u procesu otkrivanja i sprečavanja sajber napada na infrastrukturu korisnika.

Tehnološki proces razvoja odvijaće se u sledećim fazama:

- Prva faza će se sastojati od prikupljanja podataka i procesa učenja od logova AI engine modula da prepozna šta su konkretne anomalije;

[78] Wright, T. (2021). SOC Automation Techniques for Enhanced Efficiency. Packt., str. 38-42

- Druga faza će se sastojati od pravljenja tzv. rulova za sistem ARMADA, a na osnovu naučenih modela;
- Treća i završna faza odnosiće se na razjašnjenje korisniku o konkretnim događajima, kao i preporuku korisniku o mogućim rešenjima, odnosno fazu prikazivanja i testiranja.

Sistem ARMADA je napredan i kompleksan sistem koji naprednu analitiku i forenziku u realnom vremenu svakom korisniku, bez obzira na složenost IT sistema, aktivnost ili izloženost napadima.. Inovacija će stvoriti dodatnu vrednost za korisnike budući da se odnosi na razvoj AI engine modula koji će klasifikovati napade i prepoznavati sve anomalije i razjasniti korisniku prirodu napada i dati preporuku kako da se odnosi prema konkretnoj situaciji.

Razvoj i implementacija inovacije stvorila bi dodatnu vrednost za korisnike budući da za razliku od tradicionalnog Penetration testa, koji se uglavnom fokusira na testiranu aplikaciju, pruža uvid u sve potencijalne slabosti IT infrastructure korisnika i time minimizira potencijalne pretnje i mogućnost nastanka štetnih dejstava na samoj IT infrastrukturi korisnika.

Uticaj

Uvođenje AI engine modula u alat za sajber bezbednost ARMADA će imati značajan uticaj na poslovanje i poslovne performanse kompanije. Prvo, implementacija ovog projekta će povećati produktivnost zaposlenih tako što će omogućiti brže i efikasnije rešavanje problema sajber bezbednosti. AI engine će moći da automatski detektuje i reaguje na potencijalne pretnje, umesto da zaposleni moraju ručno da analiziraju velike količine podataka.

Takođe, implementacija AI engine modula će smanjiti troškove kompanije jer će eliminisati potrebu za angažovanjem dodatnog osoblja ili ulaganjem u skupu sajber bezbednosnu opremu. AI engine će moći da obavlja posao koji bi inače zahtevao više ljudi, i to sa većom tačnošću i efikasnošću.

Pored toga, implementacija ovog projekta će povećati prihode kompanije jer će poboljšati reputaciju kompanije u pogledu sajber bezbednosti. Klijenti će imati veće poverenje u kompaniju koja koristi napredne tehnologije za zaštitu njihovih podataka, što može dovesti do povećanja broja klijenata i poslova.

Ukupno gledano, implementacija AI engine modula u alat za sajber bezbednost ARMADA će dovesti do pozitivnih promena u poslovanju kompanije, povećavajući produktivnost, smanjujući troškove i povećavajući prihode. Ova inovacija će omogućiti kompaniji da bude konkurentnija na tržištu i da se efikasnije nosi sa sajber pretnjama i bori se sa sajber napadima.

Tržišni potencijal

Tržište sajber bezbednosti u Srbiji je u porastu, s obzirom na sve veći broj pretnji i napada na digitalne sisteme i podatke. Primarno tržište su private kompanije i javne odnosno državne organizacije koje žele da zaštite svoje informacije i infrastrukturu od sajber napada, kao i pojedinci koji žele da osiguraju svoju privatnost na internetu

Prepreke za ulazak na tržište sajber bezbednosti u Srbiji mogu biti visoki troškovi ulaganja u tehnologiju i obuku zaposlenih, nedostatak stručnjaka sa specifičnim znanjem iz oblasti sajber bezbednosti, kao i nedovoljna svest o značaju zaštite podataka i informacija.

Prema Nacionalnom indeksu sajber bezbednosti (NCSI), koji meri nivo sajber bezbednosti u državama širom sveta, Srbija se trenutno nalazi na 51. mestu, sa ukupnim skorom od 0.516. Iako se statistika značajno promenila u odnosu na prethodne godine, Srbija je već neko vreme intenzivno na testu razvijenosti sajber bezbednosti.

Stvarnost tržišta u razvoju govori u prilog rasta potražnje za sajber osiguranjem, te prema izveštajima svetske kompanije za osiguranje i reosiguranje „Swiss Re", stope sajber osiguranja porasle su za 30 do 40 odsto u prethodnoj godini, a očekuje se da će porasti za čak 50 procenata.

Potencijal za rast na tržištu sajber bezbednosti u Srbiji je veliki, s obzirom na sve veći broj digitalnih pretnji i napada. Prema istraživanju kompanije PwC, tržište sajber bezbednosti u Srbiji je u porastu i očekuje se da će rasti po stopi od 8 do 10% godišnje u narednom periodu. Takođe, prema istraživanju kompanije Kaspersky Lab, Srbija se nalazi među prvih 10 zemalja u Evropi po broju sajber napada, što dodatno ukazuje na potrebu za jačom zaštitom i sigurnošću digitalnih sistema u zemlji.

Potencijalni klijenti u oblasti sajber bezbednosti i zaštite podataka na internetu u Srbiji mogu biti:

- Privatna preduzeća i kompanije koje žele da zaštite svoje poslovne informacije, podatke o klijentima i transakcije
- Državne institucije i organizacije koje čuvaju osetljive podatke građana i nacionalnu bezbednost
- Finansijske institucije kao što su banke, osiguravajuće kompanije i investicione firme koje čuvaju velike količine novca i osetljive finansijske informacije
- IT kompanije koje pružaju usluge razvoja softvera, hostinga ili održavanja IT sistema i žele da zaštite svoje klijente od sajber napada
- Korisnici interneta koji žele dodatnu zaštitu svojih ličnih podataka, kao što su privatne osobe, blogeri, influenseri i mala preduzeća
- Organizacije koje se bave istraživanjem i razvojem, kao što su univerziteti, laboratorije i naučne institucije koje čuvaju osetljive naučne podatke i patente
- Proizvodne kompanije koje žele da zaštite svoje poslovne tajne, dizajne proizvoda i procese proizvodnje od konkurencije i krađe intelektualne svojine
- Glavni kupci su private kompanije, kao i javne odnosno državne institucije koje intenzivno rade na zaštiti svojih podataka (zbog prirode ugovora nije moguće imenovati konkretne organizacije).

Konkurencija

Glavni konkurenti na tržištu sajber bezbednosti i zaštite podataka na internetu u Srbiji su domaće i strane kompanije koje se bave pružanjem usluga i proizvoda u oblasti informacione bezbednosti. Neke od poznatih kompanija koje se ističu na tržištu su E-Smart Systems, ComTrade, Infostud Security, kao i globalne kompanije poput Symantec, McAfee, Kaspersky Lab, Cisco i druge.

Ulazak novih konkurenata na tržište sajber bezbednosti u Srbiji je moguć, s obzirom na rastuću potrebu za zaštitom podataka i informacija na internetu. Razvoj tehnologije i sve veći broj pretnji na internetu mogu dovesti do povećanog interesovanja kompanija i pojedinaca za uslugama i proizvodima u oblasti sajber bezbednosti, što može otvoriti prostor za ulazak novih

igrača na tržište. Međutim, ulazak novih konkurenata može biti izazovan zbog već prisutnih kompanija koje imaju razvijenu reputaciju i veliki broj klijenata.

Posebno je bitno istaći da Kompanija nema direktne konkurente budući da ima specifičan proizvod, zatim da se radi o inovativnoj Kompaniji koja je razvila sopstveno rešenje iz oblasti sajber bezbednosti.

Distribucija

Proizvod ARMADA distribuiran je klijentima kroz različite kanale distribucije kako bi se osiguralo da bude dostupna širokom spektru korisnika.

Jedan od načina distribucije mogao bi biti direktna prodaja putem online platformi ili direktnog kontakta sa potencijalnim klijentima. Takođe, možemo koristiti i partnerstva sa drugim kompanijama koje već imaju uspostavljene kanale distribucije u industriji sajber bezbednosti.

Kako bi naš proizvod ARMADA i ostale usluge bili prepoznati na ciljanim tržištima, fokusirali bismo se na edukaciju potencijalnih korisnika o važnosti sajber bezbednosti i rizicima povezanim sa nedovoljnom zaštitom podataka. Takođe bismo se trudili da naš proizvod bude jednostavan za korišćenje i prilagođen potrebama korisnika.

Neophodno je istaći da Kompanija organizuje obuke I treninge u saradnji sa Privrednom Komorom Srbije, nacionalnim CERT-om, a I sama ima status poslovnog CERT-a.

Procena tražnje

Industrija sajber bezbednosti postaje sve važnija širom sveta, uključujući i Srbiju. Uzimajući u obzir sve veći broj sajber napada i rastuću digitalizaciju poslovanja, potražnja za sajber bezbednosnim rešenjima značajno raste.

Razlozi za očekivanu potražnju:

- Povećani broj sajber napada: prema podacima iz 2023. godine, Srbija je zabeležila značajan porast sajber napada, posebno u bankarskom sektoru, državnim institucijama i privatnim preduzećima. Ransomware napadi, phishing i DDoS napadi su najčešći oblici napada.
- Regulativa i usklađenost:sa uvođenjem novih zakonskih regulativa kao što su GDPR (General Data Protection Regulation) i lokalne regulative o zaštiti podataka, kompanije su primorane da poboljšaju svoje bezbednosne mere.
- Digitalizacija i rad na daljinu: pandemija COVID-19 je ubrzala prelazak na digitalne operacije i rad na daljinu, što je dodatno povećalo potrebu za efikasnim sajber bezbednosnim rešenjima.

Procena Potražnje

Potražnja za sajber bezbednosnim proizvodima i uslugama može se proceniti kroz nekoliko ključnih faktora:

- Anketa među preduzećima:istraživanje koje obuhvata preduzeća različitih veličina i sektora može pružiti uvid u trenutne potrebe i planirane investicije u sajber bezbednost.
- Analiza tržišta:podaci o rastu IT sektora, broju registrovanih sajber incidenata i budžetima za IT bezbednost mogu pomoći u kvantitativnoj proceni potražnje.

- Konsultacije sa industrijskim stručnjacima:razgovori sa stručnjacima za sajber bezbednost i IT sektor mogu pružiti kvalitativne uvide u trendove i buduće potrebe.

Relevantni Trendovi Potražnje

- Cloud bezbednost:sa sve većim usvajanjem cloud tehnologija[79], raste potražnja za rešenjima koja osiguravaju bezbednost podataka u cloud okruženju.
- Zero Trust arhitektura:modeli bezbednosti zasnovani na "Zero Trust" pristupu postaju sve popularniji, zahtevajući striktne verifikacije identiteta i pristupa.
- Veštačka inteligencija i automatizacija:upotreba AI i mašinskog učenja za prepoznavanje i reagovanje na sajber pretnje u realnom vremenu je u porastu.

Plasman na Inostrano Tržište

- Analiza tržišta:pre ulaska na inostrano tržište, sprovedena je detaljna analizu tržišta, uključujući istraživanje konkurenata, regulative i potreba potencijalnih klijenata.
- Sertifikacije i usklađenost:Kompanija je osigurala da proizvodi i usluge ispunjavaju međunarodne standarde i regulative je ključne za uspešan plasman.
- Partnerstva: pokrenuta je saradnja sa lokalnim distributerima i IT kompanijama koja može olakšati ulazak na nova tržišta.

Kvantitativni Podaci

Prema istraživanju IDC-a iz 2023. godine, globalno tržište sajber bezbednosti je vredelo preko 150 milijardi dolara, sa godišnjim rastom od 10-12%. U Srbiji, očekuje se da tržište sajber bezbednosti raste po stopi od 8-10% godišnje, s obzirom na rastuću digitalizaciju i sve veću svest o sajber pretnjama.

Postojeći i potencijalni Klijenti u Srbiji su banke I finansijske institucije, državne institucije, telekomunikacione kompanije, edukativne ustanove, E-commerce kompanije i drugi.

Potražnja za sajber bezbednosnim rešenjima u Srbiji raste usled povećane digitalizacije, sve većeg broja sajber napada i regulatornih zahteva. Kroz analizu tržišta, anketiranje preduzeća i konsultacije sa stručnjacima, moguće je precizno proceniti potražnju i uspešno plasirati proizvode i usluge kako na domaćem tako i na inostranom tržištu.

Marketinški pristup

Najefikasniji marketinški i prodajni pristup za proizvode iz oblasti sajber bezbednosti i zaštite podataka na internetu uključuje kombinaciju strateških kanala i alata koji se fokusiraju na specifične potrebe ciljanog tržišta:

Identifikacija ciljanog tržišta

Prvi korak je identifikacija ciljanog tržišta. Ovo uključuje:

- Industrijski sektori (npr. finansije, zdravstvena zaštita, e-trgovina, IT kompanije)
- Veličina preduzeća (npr. mala i srednja preduzeća, korporacije)
- Geografski regioni (npr. specifične zemlje ili regije sa posebnim regulativama o zaštiti podataka)

[79] Cook, N. (2020). Security Challenges of Cloud Computing. Apress., str. 28-33

Kreiranje personalizovanog sadržaja

Za ovakvo tržište, edukativni i informativni sadržaj je ključan:

- Blogovi i članci koji obrađuju aktuelne pretnje i najbolje prakse u sajber bezbednosti.
- Beli papiri i e-knjige koje detaljno objašnjavaju specifične aspekte zaštite podataka.
- Webinari i online treninzi sa stručnjacima koji nude dubinske analize i studije slučaja.

Digitalni marketing

- SEO (optimizacija za pretraživače): Optimizacija sajta i sadržaja za ključne reči povezane sa sajber bezbednošću.
- PPC (plaćeno oglašavanje): Korišćenje Google Ads i LinkedIn Ads za ciljanje specifičnih demografskih grupa i industrijskih sektora.
- E-mail marketing: Segmentacija liste potencijalnih klijenata i slanje personalizovanih e-mail kampanja sa relevantnim informacijama i ponudama.
- Društveni mediji: Aktivno prisustvo na platformama kao što su LinkedIn, Twitter i Reddit. LinkedIn je posebno efikasan za B2B marketing, dok se Twitter može koristiti za praćenje i reagovanje na aktuelne događaje u sajber bezbednosti.

Alati za automatizaciju marketinga

- HubSpot: Za integraciju e-mail marketinga, CRM-a, praćenje leadova i analitiku.
- Marketo: Za naprednu segmentaciju, automatizaciju kampanja i analitiku performansi.
- Salesforce Pardot: Fokusiran na B2B marketing automatizaciju sa snažnim CRM integracijama.

Direktna prodaja i odnosi sa klijentima

- Sales Team: Obučavanje prodajnog tima za tehničke aspekte proizvoda kako bi mogli da odgovore na kompleksna pitanja klijenata.
- Account-Based Marketing (ABM): Fokusiranje na ključne račune sa personalizovanim pristupom, uključujući demo prezentacije i probne periode.

Partnerski programi i saradnje

Saradnja sa IT konsultantskim firmama i provajderima IT usluga može proširiti doseg i obezbediti dodatne kanale distribucije.

Prisustvo na događajima i sajmovima

Učešće na relevantnim konferencijama, sajmovima i industrijskim događajima kao izlagač ili sponzor. Ovi događaji omogućavaju direktnu interakciju sa potencijalnim klijentima i industrijskim stručnjacima.

Public Relations (PR)

Korišćenje PR agencija za promociju proizvoda kroz objave za medije, članke i intervjue u relevantnim IT i biznis publikacijama.

Kombinovanjem ovih strategija i kanala planiramo efikasno dopreti do ciljanog tržišta, edukovati ga o važnosti svojih proizvoda i na kraju generisati kvalifikovane leadove koji se mogu konvertovati u korisnike.

Tabela3. Rizici projekta

Vrsta rizika	Opis rizika	Upravljanje rizikom *(Ko je radnje su preduzete / biće preduzete za upravljanje ovim rizikom.)*	Opišite potencijalni efekat na projekat ukoliko bi se dogodio budući događaj	
			Unesite verovatnoću na osnovu skale: 1-niska; 3-srednja; 5-visoka.	Unesite uticaj na osnovu skale: 1-nizak; 3-srednji; 5-visoki.
Tehnološki rizik	Neuspeh u integraciji AI modula sa postojećim sajber bezbednosnim alatom ili neadekvatne performanse AI algoritama	Sprovođenje opsežnih testiranja i simulacije i angažovanje stručnjaka Kontinuirano praćenje I optimizacija AI modula	3	5
Finansijski rizik	Prekoračenje budžeta zbog visokih troškova implementacije	Detaljno planiranje budžeta faznog pristupa sa predviđenim troškovima Redovno praćenje troškova	1	5
Operativni rizik	Problemi u radu AI modula, netačne detekcije,lažno pozitivni odnosno negativni rezultati	Postavljanje procedura za brzo rešavanje problema Implementacija proverenih algoritama i redovno ažuriranje modela	1	3
Ekološki i socijalni rizik	Potencijalni negativan uticaj na privatnost korisnika I etičke dileme u vezi sa upotrebom AI tehnologije	Praćenje i usklađivanje sa zakonima I regulativama o zaštiti podataka I implementacija stroge politike privatnosti I zaštite podataka Transparentno objašnjavanje načina rada AI modula korisnicima	1	3
Tržišni rizik	Neuspeh prihvatanja AI modula na tržištu, nizak prihod odnosno neuspeh u postizanju planiranog povraćaja investicije	Istraživanje tržišta Testiranje korisničkog iskustva i prilagođavanje potrebama tržišta	1	3
Regulatorni rizik	Promene u zakonskim regulativama koje se odnose na upotrebu AI	Praćenje svih zakonskih okvira I regulativa Potencijalno angažovanje pravnih stručnjaka radi usklađenosti sa zakonima	1	3

Model generisanja prihoda

Generisanje prihoda kroz implementaciju AI modula u alat za sajber bezbednost može se postići kroz nekoliko ključnih strategija:

- Povećanje vrednosti proizvoda: dodavanjem AI funkcionalnosti alat postaje sofisticiraniji i efikasniji. AI može pomoći u bržem prepoznavanju pretnji, automatizaciji odgovora i smanjenju lažnih pozitivnih rezultata, što povećava vrednost alata za krajnje korisnike.
- Nove funkcionalnosti i servisi: AI modul može doneti nove funkcionalnosti koje nisu bile moguće sa tradicionalnim metodama. Na primer, prediktivna analitika, automatsko otkrivanje nepoznatih pretnji i personalizovani bezbednosni saveti. Ove nove funkcije mogu se ponuditi kao deo premium paketa ili dodatnih servisa.

- Smanjenje operativnih troškova:automatizacija određenih aspekata sajber bezbednosti pomoću AI može smanjiti potrebu za manuelnim intervencijama i tako smanjiti troškove operacija. Ušteda može biti direktno reinvestirana ili iskorišćena za konkurentske prednosti na tržištu.

Cenovna strategija

Subscription-based (Pretplata):naplata mesečne ili godišnje pretplate koja uključuje AI modul. Različiti nivoi pretplate mogu nuditi različite nivoe pristupa AI funkcionalnostima, od osnovnog detektovanja pretnji do napredne prediktivne analitike i automatizacije.

- Licenciranje po korisniku ili uređaju: cena može zavisiti od broja korisnika ili uređaja koji koriste alat. Veće organizacije koje koriste alat za veći broj korisnika ili uređaja plaćaju više.
- Performance-based pricing:model naplate zasnovan na performansama AI modula. Na primer, naplata može biti povezana sa brojem uspešno detektovanih i sprečenih pretnji ili sa procentom smanjenja lažnih pozitivnih rezultata.
- Custom pricing za velike klijente:za velike kompanije i organizacije, može se ponuditi prilagođena cena koja uključuje dodatne usluge, kao što su personalizovana podešavanja, dodatna podrška i obuka zaposlenih.
- Pay-per-use:naplata na osnovu korišćenja, gde korisnici plaćaju na osnovu broja skeniranih fajlova, broja izvršenih analiza ili drugih merljivih parametara korišćenja AI modula.

Doprinos prihodu

Implementacija AI modula može značajno doprineti generisanju prihoda na sledeće načine:

- Povećanje broja korisnika:poboljšane funkcionalnosti privlače nove korisnike koji traže napredna rešenja za sajber bezbednost.
- Zadržavanje postojećih korisnika: povećana efikasnost i nove funkcionalnosti pomažu u zadržavanju postojećih korisnika, smanjujući churn rate.
- Unakrsna prodaja i nadogradnje:postojeći korisnici mogu biti motivisani da nadograde na skuplje planove ili kupe dodatne servise.
- Diferencijacija na tržištu: inovativne AI funkcionalnosti mogu diferencirati alat od konkurencije, omogućavajući naplatu premijum cena.

Ovim strategijama se osigurava održiv model prihoda koji se oslanja na vrednost koju AI donosi korisnicima, istovremeno omogućavajući fleksibilnost u pristupu različitim segmentima tržišta.

Tabela 4. Faze implementacije projekta sa pripadajućim indikatorima

FAZA I INDIKATORI	Rezultat faze I 25.02.2025 *(Uneti datum završetka faze)*	Način validacije	Vrednost u USD
Faza I *Prikupljanje podataka i učenje*			
Indikator 1.1 *Završeno punjenje baze podataka svih anomalija*	*Kreiran fajl sa bazom podataka*	*Izveštaj o klasifikaciji i broju anomalija i sajber pretnji koje su upisane u bazu*	*10.000*
Indikator 1.2 *Učenje o postojećim sajber pretnjama i anomalijama na osnovu kojih će se prepoznati nove sajber pretnje koje se ne nalaze u postojećoj bazi*	*Dopunjen postojeći fajl sa bazom podataka novim anomalijama i sajber pretnjama koje se nisu do sada nalazile u bazi i koje su obležene*	*Izveštaj o klasifikaciji i broju anomalija i sajber pretnji koje su upisane u bazu*	*15.000*

FAZA II INDIKATORI	Rezultat faze II 25.06.2025 *(Uneti datum završetka faze)*	Način validacije	Vrednost u USD
Faza II *Kreiranje korelacionih pravila na osnovu naučenih modela*			
Indikator 2.1 *Kreirani kodovi u Python-u koji predstavljaju korelaciona pravila za prepoznavanje anomalija i sajber pretnji koji su naučeni u Fazi I*	*Kreirani fajlovi sa kodovima u Python-u koji predstavljaju korelaciona pravila za prepoznavanje anomalija i sajber pretnji koji su naučeni u Fazi I*	*Izveštaj o kreiranim korelacionim pravilima sa svim detaljima koji oni nose u sebi*	*30.000*

FAZA III INDIKATORI	Rezultat faze III 25.10.2025 *(Uneti datum završetka faze)*	Način validacije	Vrednost u USD
Faza III *Prikaz i testiranje AI engine modula*			
Indikator 3.1 *Uspešan rad AI engine modula u prepoznavanju i klasifikaciji anomalija i sajber pretnji*	*Funkcionalan AI engine modul*	*Demonstracija rada AI engine modula*	*5.000*

Budžet projekta

Tabela 5. Struktura budžeta projekta

R.Broj	Opis troškova	Jedinica mere	Količina	Cena po jedinici (sa PDV-om)	Ukupno (u USD)
1	Troškovi zarada zaposlenih				
1.1	Projektni menadžer	mesec	12	2.000	24.000
1.2	Data Scientist	mesec	12	1.500	18.000
2	Troškovi usluga				
2.1	Konsultantske usluge	sat	100	50	5.000
2.2	Testiranje i validacija	paket	1	5.000	5.000
3	Troškovi opreme				
3.1	Serveri i mrežna oprema	set	1	6.000	6.000
3.2	Softverske licence	paket	1	2.000	2.000
4	Troškovi materiala				
4.1	Kancelarijski materijal	paket	1	1.000	1.000
4.2	Potrošni materijal	paket	1	500	500
5	Troškovi marketinga				
5.1	Digitalni marketing	kampanja	2	2.500	5.000
5.2	PR aktivnosti	kampanja	2	1.500	3.000
6	Ostali troškovi				
6.1	Putovanja i obuke	paket	1	3.000	3.000
6.2	Administrativni troškovi	mesec	12	500	6.000
UKUPNO					**60.000**

Tabela 6. Opis budžeta projekta

R.Broj	Opis troškova	Narativni opis budžeta
1	Troškovi zarada zaposlenih	
1.1	Projektni menadžer	Projektni menadžer će biti ključan za upravljanje i realizaciju projekta. Njihova zarada je planirana na mesečnom nivou tokom trajanja projekta (12 meseci).
1.2	Data Scientist	Data Scientist će biti ključan za upravljanje i realizaciju projekta. Njihova zarada je planirana na mesečnom nivou tokom trajanja projekta (12 meseci).
2	Troškovi usluga	
2.1	Konsultantske usluge	Konsultantske usluge će biti angažovane za specifične zadatke
2.2	Testiranje i validacija	testiranje i validacija osigurati da AI modul funkcioniše prema očekivanjima
3	Troškovi opreme	
3.1	Serveri i mrežna oprema	Nabavka servera, mrežne opreme i softverskih licenci je neophodna za razvoj i testiranje AI modula.
3.2	Softverske licence	Nabavka servera, mrežne opreme i softverskih licenci je neophodna za razvoj i testiranje AI modula.
4	Troškovi materiala	
4.1	Kancelarijski materijal	Kancelarijski i potrošni materijal su potrebni za svakodnevno poslovanje.
4.2	Potrošni materijal	Kancelarijski i potrošni materijal su potrebni za svakodnevno poslovanje.
5	Troškovi marketinga	
5.1	Digitalni marketing	Digitalni marketing i PR aktivnosti su planirani za promociju projekta i povećanje svesti o novim AI funkcionalnostim
5.2	PR aktivnosti	Digitalni marketing i PR aktivnosti su planirani za promociju projekta i povećanje svesti o novim AI funkcionalnostim
6	Ostali troškovi	
6.1	Putovanja i obuke	Putovanja i obuke su potrebni za stručno usavršavanje tima
6.2	Administrativni troškovi	Administrativni troškovi vezani za operativne poslove projekta.
UKUPNO		**60.000**

Zaključak

Uspešna implementacija AI Engine modula u SIEM ARMADA alat može se sagledati kroz više dimenzija: tehničke, organizacione i poslovne benefite, kao i širi kontekst razvoja IT infrastrukture i sigurnosnih sistema.

Jedna od ključnih tehničkih prednosti implementacije AI Engine modula u SIEM ARMADA alat jeste značajno unapređenje u prepoznavanju, detekciji i odgovoru na sigurnosne pretnje. Tradicionalni SIEM sistemi, iako veoma korisni za prikupljanje i analizu podataka, oslanjaju se na pravila i statičke mehanizme, što može dovesti do propuštanja novih i sofisticiranih pretnji. AI Engine donosi mogućnost adaptivnog učenja iz istorijskih podataka, što omogućava alatki da prepozna anomalije i potencijalne napade čak i kada oni nisu definisani u postojećim pravilima.

Ovaj modul takođe može unaprediti efikasnost alata kroz automatsku korelaciju incidenata. Korišćenjem naprednih algoritama za mašinsko učenje, AI Engine može automatski analizirati velike količine podataka u realnom vremenu, identifikovati sumnjive aktivnosti, grupisati ih i prezentovati kao potencijalne sigurnosne incidente sa visokim prioritetom. Ovo značajno smanjuje vremenski okvir za detekciju pretnji i omogućava timovima za odgovor na incidente (IRT) da se fokusiraju na najkritičnije događaje.

Implementacija AI Engine modula u SIEM ARMADA alat zahteva i određene promene unutar organizacije, naročito kada je u pitanju edukacija osoblja i prilagođavanje novih radnih procesa. Međutim, ovaj modul omogućava veću automatizaciju procesa monitoringa, smanjujući potrebu za ručnom analizom podataka i minimizirajući tzv. „fatigue alerts“ koje su česte kod standardnih SIEM alata. Zaposleni zaduženi za sigurnost informacija mogu više vremena posvetiti proaktivnom radu na strategijama prevencije, što je ključna prednost u današnjem okruženju gde pretnje postaju sve sofisticiranije.

Što se tiče usklađenosti sa zakonodavstvom, implementacija AI Engine modula može poboljšati način na koji organizacije upravljaju sigurnosnim incidentima i kako ih prijavljuju nadležnim organima. Automatizovani alati sa naprednom analitikom omogućavaju preciznije praćenje incidenata i pravovremeno ispunjavanje regulatornih zahteva, što je kritičan aspekt u mnogim industrijama.

Iz poslovne perspektive, implementacija AI Engine modula u SIEM ARMADA alat donosi niz koristi koje direktno doprinose poslovnim ciljevima. Brža i preciznija detekcija pretnji smanjuje rizik od oštećenja reputacije kompanije usled sigurnosnih incidenata, dok proaktivno upravljanje bezbednosnim rizicima može umanjiti potencijalne finansijske gubitke. Takođe, bolja efikasnost u radu bezbednosnih timova može dovesti do smanjenja operativnih troškova, jer AI modul omogućava prepoznavanje i rešavanje problema pre nego što postanu ozbiljni.

U isto vreme, mogućnost skaliranja AI Engine modula omogućava organizacijama da se prilagode rastućim zahtevima kada je reč o obimu podataka i složenosti pretnji. Kako se poslovni ekosistem razvija i povećava obim podataka, organizacije mogu koristiti AI Engine za održavanje visoke razine sigurnosti bez značajnih dodatnih investicija u ljudske resurse.

Na kraju, implementacija AI Engine modula u SIEM ARMADA alat treba posmatrati kao deo šireg trenda integracije veštačke inteligencije u sisteme sajber bezbednosti. Sa napretkom tehnologije, pretnje postaju sve kompleksnije, pa su tradicionalni pristupi sve manje efikasni. Upotreba AI u kombinaciji sa SIEM sistemima pruža budući pravac razvoja, gde se predviđa još veća automatizacija, ali i inteligentniji odgovor na pretnje u realnom vremenu.

Osim toga, kako kompanije sve više usvajaju cloud infrastrukture i internet stvari (IoT), modularni sistemi poput AI Engine-a postaće ključni deo IT bezbednosnih strategija. U tom smislu, kompanije koje rano implementiraju ovakve sisteme dobiće konkurentsku prednost u osiguravanju svog poslovanja od savremenih sajber pretnji.

Uspešna implementacija AI Engine modula u SIEM ARMADA alat ne predstavlja samo tehničko unapređenje već transformaciju načina na koji organizacije pristupaju sajber bezbednosti. Ova implementacija omogućava organizacijama da postanu proaktivnije, efikasnije i bolje opremljene za suočavanje sa sve složenijim sigurnosnim izazovima. Sa napretkom tehnologije i sve većim brojem pretnji, ovakva rešenja postaju neophodna kako bi se osigurala dugoročna stabilnost i sigurnost poslovanja.

6.3. Strateške prednosi korišćenja NextGen SIEM softverskih rešenja

Strateške prednosti korišćenja NextGen SIEM rešenja[80] mogu se sagledati kroz nekoliko ključnih aspekata koji značajno unapređuju sajber bezbednost i poslovne performanse organizacije.

Proaktivna detekcija i prevencija pretnji[81]

NextGen SIEM rešenja koriste naprednu analitiku, veštačku inteligenciju i mašinsko učenje kako bi omogućili proaktivnu detekciju potencijalnih pretnji. To omogućava organizacijama da prepoznaju anomalije i reaguje na pretnje pre nego što eskaliraju u ozbiljne incidente. Tradicionalni SIEM sistemi uglavnom reaguju na već prepoznate obrasce, dok NextGen SIEM identifikuje i nepoznate pretnje i napade.

Automatizacija odgovora na incidente

Automatizacija je ključna prednost NextGen SIEM-a, jer omogućava brži i precizniji odgovor na pretnje. Automatizovano otkrivanje, korelacija događaja i generisanje alarmi smanjuje vreme potrebno za detekciju i reakciju na incidente, što omogućava sigurnosnim timovima da efikasnije upravljaju resursima i smanjuju oštećenje od pretnji. Automatizacija takođe smanjuje broj lažnih pozitivnih detekcija, čime se smanjuje "fatigue alert", odnosno preopterećenost incidentima koji nisu stvarni.

Skalabilnost i prilagodljivost

NextGen SIEM rešenja su izuzetno skalabilna, što znači da mogu da rastu u skladu sa potrebama organizacije. Ovo je važno u savremenim IT okruženjima gde se količina podataka eksponencijalno povećava, a sa tim i rizik od napada. Takođe, ova rešenja se lako integrišu sa postojećim sigurnosnim sistemima i infrastruktrom, omogućavajući da se efikasno prilagode specifičnim potrebama i zahtevanim kapacitetima kompanije.

Napredna analitika i vizualizacija podataka

NextGen SIEM sistemi koriste napredne alate za analizu podataka, omogućavajući kompanijama bolji uvid u tokove podataka, uzroke incidenata i uzorke pretnji. Ovi alati pružaju mogućnost vizualizacije bezbednosnih podataka na način koji olakšava donošenje strateških odluka o upravljanju rizicima i ulaganjima u sajber bezbednost.

Smanjenje troškova i operativne efikasnosti

Automatizacija i napredna analitika koje nudi NextGen SIEM značajno smanjuju potrebu za ručnim procesima i intervencijama, čime se direktno smanjuju operativni troškovi bezbednosnih timova. Time se postiže optimalna raspodela resursa, a poslovanje postaje efikasnije jer sistem može automatski otkrivati i neutralisati pretnje pre nego što one ugroze poslovne procese.

[80] Hughes, V. (2021). Strategic Advantages of Modern SIEM Solutions., str. 32-36
[81] Lee, G. (2021). Intrusion Detection and Prevention Techniques. Wiley., str. 45-49

Poboljšanje usklađenosti sa regulatornim zahtevima

NextGen SIEM rešenja su dizajnirana da pomažu organizacijama u ispunjavanju regulatornih zahteva i standarda bezbednosti. Omogućavaju detaljno praćenje i evidenciju incidenata, čime se olakšava ispunjavanje propisa, kao što su GDPR, HIPAA, PCI DSS, i drugi, u zavisnosti od industrije. Ovako sistematizovana evidencija pomaže u demonstraciji usklađenosti tokom inspekcija ili audita.

Kvalitetnija saradnja između timova

NextGen SIEM sistemi omogućavaju centralizovan pristup podacima o bezbednosnim incidentima, što poboljšava saradnju između različitih timova unutar organizacije. Analitički alati i izveštaji omogućavaju IT, bezbednosnim, kao i poslovnim timovima da dele uvide i zajednički rade na prevenciji i odgovoru na pretnje. Na ovaj način, kompanija može brže i efikasnije reagovati na bezbednosne izazove.

Prilagođavanje novim tehnologijama

Kako se sajber okruženje neprestano menja i pretnje postaju sofisticiranije, NextGen SIEM sistemi omogućavaju organizacijama da budu spremne za buduće izazove. Sa rastom upotrebe IoT uređaja, oblaka i hibridnih okruženja, fleksibilnost ovih sistema u prilagođavanju i detekciji napada na ovim novim platformama postaje ključna. NextGen SIEM je u stanju da prepozna pretnje koje ciljaju specifične segmente infrastrukture, omogućavajući bolju zaštitu celokupnog sistema.

Strateške prednosti korišćenja NextGen SIEM rešenja leže u proaktivnosti, efikasnosti i skalabilnosti koje ovo rešenje donosi. Omogućava organizacijama da na efikasan način upravljaju sajber rizicima, obezbede usklađenost sa propisima, i optimizuju svoje operacije uz niže troškove. S obzirom na rastuću složenost pretnji i tehnološke infrastrukture, NextGen SIEM rešenja predstavljaju ključni element u održavanju sigurnosti, stabilnosti i dugoročne održivosti poslovanja.

6.4. Donošenje strateških odluka o upravljanju bezbednosnim rizicima na osnovu NextGen SIEM softverskih rešenja

Uvod u NextGen SIEM softverska rešenja: Next-Generation Security Information and Event Management (NextGen SIEM) softverska rešenja predstavljaju evoluciju tradicionalnih SIEM sistema, koji služe za prikupljanje, analizu i korelaciju bezbednosnih događaja iz različitih izvora u mreži. Ova napredna verzija SIEM sistema integriše mogućnosti poput veštačke inteligencije (AI), mašinskog učenja (ML), automatizacije odgovora na incidente, te podrške za analizu velikih podataka, čime omogućava bržu i precizniju detekciju, analizu i mitigaciju bezbednosnih pretnji.

Razumevanje bezbednosnih rizika u kontekstu NextGen SIEM rešenja: Bezbednosni rizici u IT infrastrukturi se odnose na mogućnost da pretnje ili ranjivosti ugroze poslovne sisteme, podatke ili operacije organizacije. Tradicionalni pristupi identifikaciji ovih rizika oslanjali su se na reaktivne mere, gde su analitičari morali manuelno analizirati uzorke i incidente. NextGen

SIEM rešenja omogućavaju proaktivnu identifikaciju i praćenje pretnji u realnom vremenu koristeći napredne tehnike analize podataka i automatizovane alate za detekciju anomalija.

Ključni faktori za donošenje strateških odluka o upravljanju bezbednosnim rizicima:

- Prikupljanje podataka i vidljivost:

NextGen SIEM rešenja prikupljaju ogromne količine podataka sa različitih tačaka unutar organizacione mreže (uređaji, serveri, aplikacije, korisnici, cloud infrastruktura). Ovi podaci omogućavaju menadžerima da imaju potpunu vidljivost nad svim događajima unutar mreže i da uoče potencijalne bezbednosne rizike u realnom vremenu.

- Analiza pretnji[82] i predviđanje:

Uz podršku veštačke inteligencije i mašinskog učenja, NextGen SIEM sistemi analiziraju ponašanje korisnika, aplikacija i mrežnih uređaja kako bi detektovali anomalije i predvideli potencijalne bezbednosne incidente. Strateške odluke se donose na osnovu ove analize, omogućavajući organizacijama da se fokusiraju na ključne pretnje i spreče potencijalne napade pre nego što se dogode.

- Upravljanje rizikom na osnovu prioriteta:

NextGen SIEM omogućava klasifikaciju bezbednosnih rizika prema njihovoj ozbiljnosti i potencijalnom uticaju na poslovanje. Na primer, pretnje se mogu rangirati na osnovu kritičnosti, čime se omogućava donošenje strateških odluka koje resurse prioritetno koristiti za mitigaciju najopasnijih rizika. Ova strategija osigurava efikasno raspoređivanje resursa i brzi odgovor na incidente.

- Automatizacija odgovora na incidente:

Jedna od najvećih prednosti NextGen SIEM rešenja je mogućnost automatizacije odgovora na pretnje. Automatizovani procesi omogućavaju brzu reakciju na prepoznate rizike, poput blokiranja sumnjivih korisnika, izolacije ugroženih sistema ili obaveštavanja sigurnosnih timova o kritičnim događajima. Ova automatizacija smanjuje vreme reakcije i omogućava organizacijama da efikasnije upravljaju rizicima.

- Regulatorna usklađenost i izveštavanje:

NextGen SIEM rešenja pružaju alate za praćenje i dokumentovanje usklađenosti sa regulatornim okvirima (GDPR, HIPAA, PCI DSS). Donošenje strateških odluka mora uključivati razmatranje ovih zahteva kako bi organizacija izbegla potencijalne kazne zbog kršenja pravila o privatnosti i sigurnosti podataka[83]. SIEM pomaže u dokumentovanju napora preduzetih u cilju upravljanja rizicima, što je ključno za regulatorne inspekcije i audite.

- Stalno unapređenje putem učenja i prilagođavanja:

Pošto NextGen SIEM sistemi koriste mašinsko učenje, oni se stalno prilagođavaju i unapređuju na osnovu novih podataka o pretnjama. Strateško upravljanje bezbednosnim rizicima postaje

[82] Threat Landscape 2021 – ENISA Report, str. 27-30.
[83] Verizon Data Breach Investigations Report (2021), str. 31-34.

dinamičan proces, gde se odluke prilagođavaju u skladu sa razvojem novih pretnji, promenom poslovnog okruženja i napretkom tehnologija.

Proces donošenja strateških odluka:

- Identifikacija i procena rizika:

Prvi korak u donošenju strateških odluka jeste identifikacija potencijalnih pretnji i ranjivosti unutar organizacione IT infrastrukture. NextGen SIEM u ovom procesu igra ključnu ulogu, pružajući dubinsku analizu i korelaciju podataka, omogućavajući prepoznavanje rizika koji možda nisu bili očigledni.

- Razvoj scenarija i planiranje odgovora:

Nakon identifikacije rizika, ključna je simulacija različitih scenarija i određivanje mogućih posledica po poslovanje. Strateške odluke treba da budu zasnovane na planovima odgovora koji uključuju kako kratkoročne mere (brzi odgovori na incidente), tako i dugoročne strategije (upravljenje dugoročnim rizicima i jačanje bezbednosne arhitekture).

- Implementacija mera:

U ovoj fazi, menadžeri implementiraju mere za smanjenje prepoznatih rizika. NextGen SIEM omogućava automatizovane alate za sprovođenje mera, kao što su primena novih politika pristupa, enkripcija podataka, ili unapređenje bezbednosne infrastrukture.

- Praćenje i evaluacija:

Nakon implementacije, ključno je kontinuirano praćenje efektivnosti mera. NextGen SIEM omogućava stalni nadzor u realnom vremenu, praćenje performansi i evaluaciju primenjenih rešenja. Strateške odluke se prilagođavaju na osnovu dobijenih podataka o efikasnosti zaštite.

Prednosti NextGen SIEM u donošenju strateških odluka o upravljanju bezbednosnim rizicima:

- Brža detekcija i odgovor na pretnje: Korišćenje naprednih analitičkih tehnika omogućava ranije otkrivanje pretnji i smanjuje vreme potrebno za reakciju.
- Bolja koordinacija između timova: Automatizacija i centralizovano upravljanje incidentima omogućavaju efikasniju saradnju između IT i bezbednosnih timova.
- Smanjenje troškova: Automatizovani procesi smanjuju potrebu za manuelnim radom, što smanjuje troškove operacija i unapređuje efikasnost.
- Povećana usklađenost sa regulativama: Poboljšano praćenje i izveštavanje omogućavaju lakše ispunjavanje regulatornih zahteva.

NextGen SIEM rešenja predstavljaju moćan alat za upravljanje bezbednosnim rizicima u savremenim IT okruženjima. Donošenje strateških odluka zasnovano na ovim rešenjima omogućava organizacijama da predvide, prepoznaju i efikasno odgovore na pretnje, čime se smanjuje potencijalna šteta po poslovanje i povećava ukupna sigurnost i usklađenost sa zakonodavnim okvirima.

GLAVA 7: UPRAVLJANJE BEZBEDNOSNIM RIZICIMA U SAJBER PROSTORU U SRBIJI

7.1. Razvoj upravljanja rizicima u sajber prostoru u Srbiji

Sajber bezbednost je jedan od najvažnijih izazova sa kojim se suočavaju države, organizacije i pojedinci u digitalnoj eri. Srbija, kao zemlja u procesu digitalne transformacije, suočava se sa rastućim rizicima u sajber prostoru, gde su napadi sve učestaliji i sofisticiraniji. Upravljanje bezbednosnim rizicima u sajber prostoru postalo je ključni prioritet za vladu, privatni sektor i građane Srbije, jer je od vitalnog značaja za zaštitu kritične infrastrukture, podataka i digitalnih usluga. Ovaj dokument će obraditi razvoj sajber bezbednosti u Srbiji, trenutnu situaciju u ovoj oblasti i perspektive za budućnost.

Istorijski razvoj sajber bezbednosti u Srbiji

Razvoj upravljanja bezbednosnim rizicima u sajber prostoru u Srbiji može se podeliti u nekoliko faza:

Prethodna faza (pre 2000-tih)

Pre 2000. godine, sajber bezbednost nije bila prioritet u Srbiji. Internet penetracija je bila na niskom nivou, a većina poslovanja i komunikacije obavljala se putem tradicionalnih, analognih sredstava. Upravljanje bezbednosnim rizicima se fokusiralo na fizičku bezbednost i zaštitu podataka unutar lokalnih mreža. Malo je organizacija imalo politiku informacione bezbednosti, a uopšte nisu postojali zakonski okviri koji bi regulisali ovu oblast.

Period digitalne tranzicije (2000–2010)

Početkom 2000-ih, Srbija se suočava sa ubrzanom digitalizacijom i većom dostupnošću interneta. U ovom periodu dolazi do rasta broja internet korisnika i ekspanzije telekomunikacionih usluga. Pitanje sajber bezbednosti počinje da dobija na značaju, pre svega u bankarskom sektoru i vladinim institucijama, ali još uvek ne postoji sveobuhvatan pravni okvir.

Prvi pokušaji regulacije: U ovoj fazi dolazi do inicijalnih pokušaja regulacije u oblasti informacione bezbednosti. Bankarski sektor, kao jedan od prvih koji se suočava sa rizicima sajber napada, uvodi unutrašnje standarde za zaštitu podataka, ali to ostaje na nivou internih politika, dok zakonodavstvo još uvek ne reaguje u dovoljnoj meri.

Konsolidacija i razvoj pravnog okvira (2010–2020)

U ovom periodu dolazi do značajnijih iskoraka u razvoju sajber bezbednosti u Srbiji, kako sa aspekta pravne regulative, tako i sa stanovišta tehničkih kapaciteta i podizanja svesti o rizicima.

- Zakon o informacionoj bezbednosti (2016): Ključni trenutak u razvoju sajber bezbednosti u Srbiji predstavlja usvajanje Zakona o informacionoj bezbednosti 2016. godine, koji je prvi sveobuhvatan zakon koji se bavi ovom temom. Ovaj zakon postavlja temelje za kreiranje nacionalne strategije sajber bezbednosti i osnivanje institucija koje će se baviti upravljanjem sajber rizicima.

- Osnivanje CERT timova: U ovom periodu dolazi i do formiranja timova za reagovanje na sajber incidente, poznatih kao CERT (Computer Emergency Response Team), na nacionalnom nivou, kao i u okviru ključnih državnih institucija i većih preduzeća. CIRT timovi su zaduženi za praćenje, otkrivanje i reagovanje na sajber incidente u realnom vremenu.
- EU integracije i usklađivanje s regulativom: Srbija je u ovom periodu počela intenzivno da radi na usklađivanju sa standardima Evropske unije, što je rezultiralo usvajanjem normi iz Direktive NIS (Network and Information Systems) koja reguliše obaveze u vezi sa zaštitom kritične infrastrukture i digitalnih usluga.

Sadašnje stanje upravljanja bezbednosnim rizicima u sajber prostoru u Srbiji

Trenutno stanje u oblasti sajber bezbednosti u Srbiji karakteriše mešavina unapređenih pravnih okvira, rastuće svesti o rizicima, ali i izazova koji proizlaze iz neadekvatnih resursa i brzog razvoja pretnji.

Pravni okvir i institucionalna podrška

Danas, Srbija ima relativno stabilan pravni okvir koji reguliše sajber bezbednost:

- Zakon o informacionoj bezbednosti definiše obaveze pravnih lica, kao i obavezne tehničke i organizacione mere za zaštitu podataka.
- Strategija sajber bezbednosti Republike Srbije za period 2017–2021 je postavila osnovne pravce delovanja u oblasti zaštite od sajber pretnji i usklađivanja sa EU standardima.
- Osnovane su ključne institucije poput nacionalnog CERT tima, koji imaju centralnu ulogu u koordinaciji i nadzoru sajber bezbednosti na nivou države.

Rast broja sajber napada i pretnji

Sajber pretnje u Srbiji rastu iz godine u godinu. Prema podacima iz različitih izvora, tokom 2022. i 2023. godine registrovan je porast DDoS (Distributed Denial of Service) napada, ransomware pretnji i napada na kritičnu infrastrukturu, kao što su energetski sistemi, banke i telekomunikacioni operateri.

- Bankarski sektor: Jedan od najugroženijih sektora u Srbiji je finansijski sektor, gde su ransomware napadi i pokušaji krađe identiteta postali učestali. Institucije su počele da ulažu značajne resurse u unapređenje sajber zaštite, ali incidenti i dalje predstavljaju značajan problem.
- Državne institucije: Napadi na državne sisteme su takođe u porastu, što se može povezati sa većim oslanjanjem na digitalizovane usluge u javnoj administraciji. Elektronska uprava i sistemi koji upravljaju ličnim podacima građana postaju česte mete.

Nedostatak stručnog kadra i resursa

Jedan od glavnih izazova u Srbiji je nedostatak obučenih stručnjaka za sajber bezbednost. Prema podacima, većina organizacija u privatnom i javnom sektoru suočava se sa manjkom profesionalaca koji imaju specijalizovana znanja u oblasti sajber bezbednosti, što otežava proaktivno upravljanje bezbednosnim rizicima.

Obuka i edukacija: Postoji određeni napredak u edukaciji kadra za sajber bezbednost, ali je potrebno još veće angažovanje obrazovnih institucija i specijalizovanih centara za obuku. IT fakulteti počinju da nude kurseve i specijalizacije u ovoj oblasti, ali je broj diplomiranih kadrova i dalje nedovoljan da zadovolji potrebe tržišta.

Javna svest o sajber bezbednosti

Jedan od ključnih elemenata u upravljanju sajber rizicima je podizanje svesti o bezbednosnim pretnjama među širim slojevima društva. Iako je svest u privatnom sektoru i državnim institucijama značajno porasla, mnogi građani i dalje nisu dovoljno informisani o rizicima kao što su krađa identiteta, phishing napadi ili zaštita ličnih podataka u digitalnom svetu.

Perspektive i budući razvoj upravljanja bezbednosnim rizicima u sajber prostoru u Srbiji

Perspektive upravljanja bezbednosnim rizicima u sajber prostoru u Srbiji zavise od nekoliko ključnih faktora: daljeg razvoja pravnog okvira, tehnoloških inovacija, međunarodne saradnje i ulaganja u ljudske resurse.

Dalji razvoj pravnog okvira i usklađivanje sa EU regulativom

S obzirom na to da Srbija teži članstvu u Evropskoj uniji, očekuje se dalji razvoj zakona i propisa u oblasti sajber bezbednosti u skladu sa EU normama. Direktiva NIS2, koja je nadogradnja na postojeću NIS direktivu, očekuje se da bude usvojena i implementirana u pravni sistem Srbije u narednim godinama. To će uključivati strože zahteve za zašte podataka, obavezno prijavljivanje sajber incidenata i jačanje kapaciteta za odgovore na pretnje u okviru ključnih sektora kao što su finansije, energetika, zdravstvo i telekomunikacije. Uvođenje ovih mera će omogućiti veći stepen usklađenosti sa evropskim standardima, što će dodatno povećati poverenje u bezbednost digitalne infrastrukture u Srbiji.

Tehnološki napredak i digitalna transformacija

Dalji razvoj tehnologije, uključujući veštačku inteligenciju (AI), mašinsko učenje (ML), i blockchain tehnologije[84], pruža nove mogućnosti za unapređenje upravljanja bezbednosnim rizicima. Ove tehnologije mogu pomoći u automatizaciji detekcije pretnji, analizi velikih podataka u realnom vremenu i brzoj reakciji na incidente. Ulaganja u digitalnu transformaciju unutar privrede i javnog sektora zahtevaju da se paralelno razvijaju i mehanizmi za sajber zaštitu.

Na primer, primena veštačke inteligencije može značajno unaprediti identifikaciju obrazaca ponašanja u okviru mreža i korisničkih aktivnosti, čime bi se ubrzalo prepoznavanje anomalija koje ukazuju na potencijalne napade. Blockchain tehnologija može unaprediti bezbednost transakcija i zaštitu podataka, posebno u sektorima kao što su finansije i e-uprava.

Međunarodna saradnja

Međunarodna saradnja je ključni faktor u jačanju sajber bezbednosti u Srbiji. Sajber pretnje su globalne, pa je saradnja sa međunarodnim organizacijama, poput NATO-a, Evropske unije i Saveta Evrope, od velikog značaja. Srbija je već deo nekoliko inicijativa koje se odnose na borbu protiv sajber kriminala, kao što je Budimpeštanska konvencija o sajber kriminalu. Dalje

[84] Edwards, R. (2021). Blockchain Technology in Cybersecurity. Elsevier., str. 22-26

učešće u regionalnim i globalnim inicijativama, kao i razmena informacija o pretnjama sa drugim zemljama, doprinosi izgradnji otpornijeg sajber prostora.

Saradnja sa tehnološkim gigantima i kompanijama koje se bave sajber bezbednošću, kao i integracija sa globalnim platformama za razmenu sajber pretnji (Cyber Threat Intelligence), pomoći će u unapređenju kapaciteta Srbije za prepoznavanje i reagovanje na sajber napade.

Ulaganje u ljudske resurse i edukaciju

Kako bi se Srbija uspešno suočila sa sve složenijim sajber pretnjama, neophodna su dalja ulaganja u ljudske resurse. Potrebno je nastaviti razvoj specijalizovanih programa za obuku stručnjaka za sajber bezbednost, kako na univerzitetima, tako i kroz programe kontinuiranog obrazovanja za IT stručnjake i državne službenike.

Univerziteti i tehničke škole igraju ključnu ulogu u razvoju budućih stručnjaka za sajber bezbednost. Neophodno je povećati broj studijskih programa posvećenih sajber bezbednosti i jačati saradnju između obrazovnih institucija i industrije. Ova saradnja može pomoći da se obrazovni programi usklade sa realnim potrebama tržišta, što će obezbediti kvalitetan kadar za upravljanje sajber rizicima.

Takođe, neophodno je povećati ulaganja u podizanje svesti o sajber bezbednosti među građanima, privatnim preduzećima i javnim institucijama. Ovo obuhvata kampanje edukacije o osnovnim principima bezbednog korišćenja interneta, zaštiti ličnih podataka i prepoznavanju potencijalnih pretnji, kao što su phishing i maliciozni softver.

Jačanje nacionalne kritične infrastrukture

Kritična infrastruktura, kao što su energetski sistemi, vodovod, saobraćaj i telekomunikacije, sve više zavisi od digitalnih sistema. Zbog toga, upravljanje bezbednosnim rizicima u ovim sektorima postaje ključni zadatak države. Srbija već ulaže napore u zaštitu ovih sistema kroz primenu Zakona o kritičnoj infrastrukturi i zakonske regulative vezane za informacionu bezbednost.

U budućnosti, neophodno je proširiti obim zaštitnih mera i osigurati implementaciju najnovijih tehnologija za zaštitu kritičnih sistema. To uključuje primenu naprednih rešenja za detekciju i prevenciju pretnji, kao i povećanje kapaciteta za odgovor na napade u realnom vremenu. Dodatno, saradnja sa privatnim sektorom, koji upravlja značajnim delom kritične infrastrukture, biće od suštinskog značaja.

Razvoj sajber otpornosti i kontinuiteta poslovanja

Jedna od najvažnijih perspektiva u razvoju sajber bezbednosti u Srbiji je jačanje sajber otpornosti organizacija i državnih institucija. Sajber otpornost podrazumeva sposobnost sistema da se oporave od napada i nastave sa radom uz minimalne posledice po poslovanje i pružanje usluga.

Ovaj koncept uključuje:

- Planiranje kontinuiteta poslovanja (Business Continuity Planning – BCP): Razvoj BCP planova osigurava da organizacije mogu brzo reagovati na incidente, smanjiti gubitke i nastaviti sa radom. Uključuje i redovne vežbe i testove kako bi se proverila efikasnost ovih planova.

- Disaster Recovery: Planovi za oporavak od sajber napada treba da budu sastavni deo svake organizacije. U budućnosti, veći fokus na razvoju rešenja za automatski oporavak i brz povratak na normalno poslovanje biće ključan za održavanje stabilnosti i sigurnosti poslovanja.

Upravljanje bezbednosnim rizicima u sajber prostoru u Srbiji je oblast koja je značajno napredovala u poslednjoj deceniji, ali i dalje zahteva kontinuirani razvoj. Usvajanjem relevantne regulative, unapređenjem tehničkih kapaciteta i povećanjem svesti o sajber pretnjama, Srbija postavlja temelje za bezbedniji digitalni prostor.

Međutim, predstojeći izazovi, kao što su rastuća složenost sajber napada, nedostatak stručnog kadra i potreba za jačanjem kritične infrastrukture, zahtevaju dalja ulaganja i strateško planiranje. Perspektive razvoja sajber bezbednosti u Srbiji uključuju povećanje međunarodne saradnje, primenu inovativnih tehnologija, jačanje pravnog okvira i usklađivanje sa evropskim normama. Ulaganjem u obrazovanje i podizanjem svesti o sajber rizicima, Srbija može postati otpornija na buduće pretnje i izgraditi snažniji digitalni ekosistem za građane i preduzeća.

7.2. Odnos zaposlenih[85] prema sajber bezbednosti u Srbiji

Sajber bezbednost je postala ključni faktor za uspešno poslovanje organizacija širom sveta, pa tako i u Srbiji. U eri sve veće digitalizacije, pretnje u sajber prostoru postaju sve kompleksnije i sofisticiranije, što zahteva visok stepen svesti i odgovornosti svih zaposlenih unutar organizacija. Odnos zaposlenih prema sajber bezbednosti direktno utiče na sposobnost organizacija da se odbrane od sajber napada i upravljaju rizicima vezanim za bezbednost informacija. Ovaj dokument analizira različite aspekte odnosa zaposlenih u Srbiji prema sajber bezbednosti, uključujući nivo svesti, ponašanje, obrazovne potrebe i ključne izazove sa kojima se suočavaju organizacije u pogledu angažovanja zaposlenih u zaštiti informacija.

Značaj zaposlenih u sajber bezbednosti

Upravljanje sajber bezbednošću nije samo tehnički izazov, već uključuje ljudski faktor kao ključni element u zaštiti organizacije od pretnji. Bez obzira na nivo tehnološke zaštite koja se primenjuje, zaposleni ostaju prva linija odbrane. U praksi, mnogi sajber napadi, kao što su phishing, socijalni inženjering, pa čak i ransomware napadi, često počinju eksploatacijom ljudske greške ili nemarnosti.

Zaposleni koji nisu dovoljno edukovani ili koji nisu svesni sajber pretnji mogu nenamerno ugroziti bezbednost organizacije. To može uključivati otvaranje zlonamernih e-mail poruka, korišćenje nesigurnih lozinki ili ignorisanje sigurnosnih protokola. Shodno tome, edukacija i podizanje svesti zaposlenih predstavljaju ključne korake u stvaranju bezbednosne kulture u organizacijama.

[85] Edwards, R. (2020). Employee Attitudes Towards Cyber Threats., str. 28-32

Svest zaposlenih o sajber pretnjama u Srbiji

Opšti nivo svesti o sajber pretnjama

Iako su pretnje sajber bezbednosti sve prisutnije, svest zaposlenih u Srbiji o ovim rizicima i dalje varira u zavisnosti od sektora i veličine organizacije. Prema istraživanjima, veće organizacije, posebno one u finansijskom sektoru i IT industriji, imaju viši nivo svesti o sajber bezbednosti među zaposlenima. S druge strane, male i srednje organizacije često nemaju jasno definisane bezbednosne politike, a zaposleni u tim kompanijama često nisu dovoljno obučeni o pretnjama u sajber prostoru.

Zaposleni u državnim institucijama takođe pokazuju varijacije u nivou svesti o sajber pretnjama. U institucijama koje imaju direktnu odgovornost za kritičnu infrastrukturu (poput energetike, telekomunikacija i finansija), postoji veći nivo edukacije i svesti o bezbednosnim pretnjama. Međutim, u manjim državnim institucijama ili na nižim administrativnim nivoima, sajber bezbednost često nije prioritet.

Nedostatak znanja i obrazovanja

Jedan od ključnih izazova sa kojim se suočava većina organizacija u Srbiji je nedostatak formalnog obrazovanja zaposlenih o sajber bezbednosti. Tradicionalni obrazovni programi u Srbiji tek nedavno su počeli da integrišu teme vezane za informacione tehnologije i sajber bezbednost, a mnogi zaposleni koji su već u radnom odnosu nemaju formalno obrazovanje o ovoj oblasti.

Često se dešava da zaposleni nemaju osnovno znanje o tome kako prepoznati sajber pretnje, kao što su phishing e-mailovi, maliciozni softveri ili sumnjive web stranice. Zbog ovoga, organizacije su primorane da same sprovode interne edukacije i obuke kako bi povećale nivo znanja zaposlenih.

Podizanje svesti o sajber pretnjama

Sve više organizacija u Srbiji prepoznaje važnost podizanja svesti zaposlenih o sajber bezbednosti. Različite inicijative, poput obuka, radionica i kampanja unutar kompanija, pomažu zaposlenima da postanu svesni sajber pretnji i pravilnog ponašanja u digitalnom okruženju. Ipak, ove aktivnosti često nisu sistematične ili kontinuirane, što umanjuje njihov efekat.

Jedan od glavnih faktora koji doprinosi povećanju svesti zaposlenih je pojava konkretnih pretnji ili incidenata. Kada organizacija doživi sajber napad ili bude pogođena bezbednosnim incidentom, često dolazi do povećanja pažnje zaposlenih i veće angažovanosti na primeni sigurnosnih pravila.

Ponašanje zaposlenih i bezbednosni rizici

Česta ponašanja koja ugrožavaju sajber bezbednost

Niz uobičajenih ponašanja zaposlenih može ugroziti bezbednost organizacije. Ovo uključuje:

- Korišćenje slabih lozinki: Jedna od najčešćih pretnji je korišćenje jednostavnih i lako predvidljivih lozinki. Mnogi zaposleni u Srbiji koriste lozinke kao što su "123456" ili "password", a ove lozinke su lako ranjive na brute force napade.

- Ponovna upotreba lozinki: Mnogi zaposleni koriste iste lozinke za različite naloge i aplikacije, što povećava rizik od upada u sistem. U slučaju kompromitovanja jednog naloga, napadači mogu dobiti pristup i drugim ključnim sistemima.
- Neprepoznavanje phishing pretnji: Zaposleni često nisu u stanju da prepoznaju phishing e-mailove, što dovodi do toga da nesvesno dele poverljive informacije, kao što su podaci o pristupu ili finansijske informacije, sa napadačima.
- Preuzimanje i instalacija sumnjivog softvera: Mnogi zaposleni preuzimaju aplikacije ili softverske dodatke sa nesigurnih izvora, ne shvatajući da to može uključivati maliciozni softver koji omogućava napadačima pristup mrežama i podacima organizacije.

Kultura sigurnosne svesti u organizacijama

Organizacije koje podstiču kulturu sigurnosne svesti među zaposlenima imaju veće šanse da smanje rizike od sajber napada. Kultura sajber bezbednosti podrazumeva da svi zaposleni, od najnižeg do najvišeg nivoa, razumeju važnost bezbednosti i aktivno učestvuju u zaštiti informacija.

Kultura bezbednosti mora biti proaktivna i uključivati redovne treninge, simulacije sajber napada i stalnu komunikaciju o potencijalnim pretnjama. Kompanije koje integrišu sajber bezbednost u svakodnevni rad, kao deo korporativne kulture, beleže manji broj incidenata i uspešnije se nose sa pretnjama.

Socijalni inženjering i manipulacija zaposlenima

Socijalni inženjering, tehnika kojom napadači manipulišu zaposlenima kako bi dobili pristup poverljivim informacijama, predstavlja sve češći oblik sajber napada u Srbiji. Napadači koriste emocionalne ili psihološke taktike kako bi prevarili zaposlene da otkriju lozinke, otvore maliciozne dokumente ili kliknu na linkove koji sadrže maliciozni softver.

Zaposleni su često nesvesni sofisticiranosti ovakvih napada i mogu pasti pod uticaj prevarnih e-mailova ili telefonskih poziva. Organizacije moraju obučavati zaposlene kako da prepoznaju i odole pokušajima socijalnog inženjeringa.

Edukacija zaposlenih o sajber bezbednosti

Interni treninzi i obuke

Kako bi podigli nivo svesti i obučili zaposlene da se zaštite od sajber pretnji, mnoge kompanije u Srbiji organizuju interne obuke i treninge. Ove obuke mogu uključivati osnovne veštine prepoznavanja phishing pretnji, pravilnu upotrebu lozinki, kao i obuku o pravilima za korišćenje e-mail sistema i mrežnih resursa.

Efektivni treninzi uključuju:

- Simulacije sajber napada: Ove simulacije omogućavaju zaposlenima da se suoče sa realističnim scenarijima sajber pretnji i nauče kako da pravilno reaguju.
- Redovni testovi i vežbe: Organizacije bi trebalo da sprovode redovne testove kako bi proverile nivo svesti i obučile zaposlene na primerima iz stvarnog života.

S obzirom na to da svi zaposleni nemaju isti nivo odgovornosti i pristup osetljivim podacima[86], organizacije treba da razvijaju prilagođene programe obuke. Na primer, zaposleni u IT sektoru ili oni koji rade sa kritičnim podacima zahtevaju napredniju obuku u vezi sa bezbednosnim praksama, dok osnovni nivo svesti treba da bude obezbeđen za sve članove organizacije.

- Uloga menadžmenta: Menadžment mora biti obučen ne samo za prepoznavanje pretnji, već i za usvajanje politika koje podstiču proaktivnu sajber bezbednost i spremnost na reagovanje u slučaju incidenata.
- Specijalizovani treninzi za IT stručnjake: IT osoblje mora biti upoznato sa najnovijim alatima i tehnikama za otkrivanje i prevenciju sajber napada. Ovi treninzi mogu uključivati napredne tehnike za monitoring mreža, identifikaciju malicioznih aktivnosti i korišćenje softverskih rešenja za sajber bezbednost.

Sertifikacije i kontinuirano obrazovanje

U svetu sajber bezbednosti, znanja i tehnike brzo zastarevaju zbog stalnog razvoja novih pretnji i tehnologija. Zato je važno da se zaposleni u Srbiji podstaknu da se kontinuirano obrazuju i stiču međunarodno priznate sertifikate u oblasti sajber bezbednosti, poput:

- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)
- CompTIA Security+

Kontinuirano obrazovanje omogućava zaposlenima da budu u toku sa novim trendovima i tehnologijama u oblasti sajber bezbednosti, čime se organizacije bolje pripremaju za suočavanje sa novim pretnjama.

Izazovi u implementaciji sajber bezbednosnih politika među zaposlenima

Otpor promenama

Jedan od glavnih izazova u implementaciji sajber bezbednosnih politika među zaposlenima u Srbiji je otpor promenama. U mnogim organizacijama, zaposleni su naviknuti na određene načine obavljanja posla i mogu percipirati nove bezbednosne politike kao dodatni teret ili složenost koja otežava svakodnevni rad. Na primer, primena multifaktorske autentifikacije[87], obavezno ažuriranje lozinki ili redovne provere bezbednosnih procedura može izazvati nezadovoljstvo.

Organizacije moraju raditi na komunikaciji i obrazovanju zaposlenih o važnosti ovih mera, ističući kako one štite ne samo organizaciju, već i pojedince od potencijalnih gubitaka i incidenata. Promene moraju biti implementirane postepeno, uz podršku i obuku zaposlenih kako bi se smanjio otpor.

Nedostatak vremena i resursa

Mnoge organizacije, posebno male i srednje preduzeća, suočavaju se sa ograničenim resursima kada je reč o implementaciji sveobuhvatnih programa sajber bezbednosti. Često je izazov posvetiti dovoljno vremena i sredstava za obuku zaposlenih, dok se istovremeno održava

[86] Anderson, S. (2019). Handling Sensitive Data in Modern Enterprises. Elsevier.", str. 20-25
[87] Thompson, P. (2020). Multi-Factor Authentication for Enhanced Security. Apress., str. 38-43

redovno poslovanje. Takođe, manjim firmama često nedostaju interni IT resursi ili stručnjaci za sajber bezbednost koji bi mogli efikasno da sprovedu potrebne mere.

U ovom kontekstu, organizacije moraju pronaći balans između redovnih operacija i ulaganja u bezbednost, dok manji budžeti mogu biti kompenzovani primenom osnovnih sigurnosnih politika, kao što su obavezno korišćenje jakih lozinki i redovno ažuriranje softvera.

Pravila BYOD (Bring Your Own Device)

Praksa BYOD, gde zaposleni koriste svoje lične uređaje za pristup poslovnim mrežama, sve je učestalija u Srbiji. Iako ova praksa omogućava veću fleksibilnost zaposlenih, ona takođe povećava rizik od sajber pretnji. Lični uređaji mogu biti manje bezbedni od korporativnih uređaja, posebno ako nisu podložni istim pravilima i kontrolama bezbednosti.

Organizacije moraju usvojiti jasne politike koje regulišu korišćenje ličnih uređaja za radne svrhe, kao i implementirati odgovarajuće tehničke mere, poput enkripcije podataka i aplikacija za upravljanje mobilnim uređajima (Mobile Device Management – MDM), kako bi smanjile rizike.

Studije slučaja: incidenti izazvani ljudskom greškom

Phishing napad na državnu instituciju

Jedan od najupečatljivijih primera napada putem phishinga u Srbiji desio se kada je zaposleni u državnoj instituciji nehotice otvorio maliciozan e-mail i kliknuo na link koji je omogućio hakerima pristup mreži. Kao rezultat, napadači su kompromitovali poverljive informacije. Iako je institucija imala tehničke mere zaštite, nedovoljna obuka zaposlenih o prepoznavanju phishing pretnji doprinela je incidentu.

Greška zaposlenih u bankarskom sektoru

Jedan slučaj iz bankarskog sektora pokazuje kako ljudske greške mogu dovesti do značajnih bezbednosnih propusta. Zaposleni je nenamerno podelio lozinke za interni sistem putem nesigurne e-mail komunikacije, što je omogućilo napadačima da dobiju pristup kritičnim podacima o korisnicima. Ovaj incident naglašava potrebu za rigoroznijom obukom zaposlenih o bezbednosnim procedurama.

Perspektive i budući koraci

Podizanje svesti i kontinuirano obrazovanje

Jedna od najvažnijih perspektiva za poboljšanje odnosa zaposlenih prema sajber bezbednosti u Srbiji je kontinuirano obrazovanje i podizanje svesti. Potrebno je da organizacije prepoznaju da obuka zaposlenih nije jednokratan proces, već kontinuiran napor. Redovne radionice, kursevi i sertifikacione obuke bi trebalo da postanu standardna praksa, posebno kako bi se zaposleni upoznali sa novim oblicima pretnji koji se stalno razvijaju.

Razvoj sigurnosne kulture

Sistemsko usvajanje sajber bezbednosti kao deo organizacione kulture je ključno za uspešno upravljanje rizicima. Ovo uključuje ne samo formalnu obuku, već i svakodnevnu praksu koja uključuje menadžere i zaposlene u zajedničkoj odgovornosti za bezbednost podataka.

Zaposleni treba da budu podstaknuti da prijave bezbednosne prekršaje ili sumnjive aktivnosti bez straha od posledica, čime se stvara proaktivna kultura zaštite.

Tehnološke inovacije u zaštiti ljudskog faktora

Pored edukacije, organizacije treba da se oslanjaju i na tehnološka rešenja koja mogu da smanje uticaj ljudske greške. Na primer, korišćenje naprednih sistema za detekciju pretnji (npr. AI i mašinsko učenje), multifaktorske autentifikacije, i enkripcije podataka može pomoći u zaštiti informacija čak i u slučaju kada zaposleni naprave grešku.

Regulatorna podrška i usklađivanje sa EU standardima

Kako se Srbija postepeno usklađuje sa standardima Evropske unije, zakonodavni okvir će igrati ključnu ulogu u regulisanju odgovornosti zaposlenih i organizacija prema sajber bezbednosti. Zakoni poput GDPR-a (Opšta uredba o zaštiti podataka) uvode strože standarde zaštite podataka i propisuju visoke kazne za organizacije koje ne uspeju da zaštite podatke na odgovarajući način. Ovi standardi motivišu organizacije da ozbiljno pristupe edukaciji zaposlenih i zaštiti podataka.

Sajber bezbednost postaje sve važnija tema u modernom poslovanju, kako u svetu, tako i u Srbiji. Brz tehnološki razvoj i digitalizacija poslovnih procesa doneli su nove prilike za napredak, ali i povećali rizik od sajber pretnji. Odnos zaposlenih prema sajber bezbednosti igra ključnu ulogu u zaštiti kompanija i institucija od ovih pretnji. Na osnovu analize odnosa zaposlenih u Srbiji prema sajber bezbednosti, može se izvesti nekoliko važnih zaključaka.

Jedan od glavnih problema je nedovoljna svest zaposlenih o značaju sajber bezbednosti. Iako su sajber pretnje, kao što su hakerski napadi, krađa podataka i širenje malvera, sve učestaliji, mnogi zaposleni još uvek ne shvataju dovoljno ozbiljno opasnosti koje dolaze sa neodgovornim korišćenjem IT sistema. Nedostatak znanja i edukacije na ovu temu rezultira time da mnogi zaposlenici nesvesno postaju slabe karike u bezbednosnom lancu. Phishing napadi, zloupotreba lozinki i nepažljivo rukovanje poverljivim podacima često se događaju zbog nedovoljne obuke o osnovnim bezbednosnim protokolima.

U mnogim organizacijama u Srbiji sajber bezbednost se još uvek ne posmatra kao prioritet na nivou menadžmenta. Ukoliko rukovodstvo ne postavi sajber bezbednost kao strateški cilj i ne razvije politike koje će zaposlene obavezati da slede standardizovane bezbednosne prakse, teško je očekivati da će pojedinci samostalno inicirati promene u svom ponašanju. Uvođenje obavezne obuke, periodičnih testova i simulacija sajber napada može značajno poboljšati svest zaposlenih o opasnostima i njihovoj ulozi u zaštiti poslovanja.

Uvođenje redovne i kvalitetne obuke zaposlenih o sajber bezbednosti od suštinskog je značaja za smanjenje rizika od napada. Trenutno, u mnogim kompanijama u Srbiji, obuka iz oblasti sajber bezbednosti ili ne postoji, ili je minimalna i nedovoljna. Stalna edukacija o novim pretnjama, bezbednosnim praksama i alatima za zaštitu može unaprediti ponašanje zaposlenih. Programi edukacije ne bi trebalo da budu jednokratni, već kontinuirani, sa fokusom na praktične aspekte zaštite – kao što su upravljanje lozinkama, prepoznavanje phishing mejlova i pravilno čuvanje poverljivih podataka.

Pored edukacije, važno je zaposlenima obezbediti odgovarajuće alate i tehnološke resurse za sprovođenje bezbednosnih praksi. Uvođenje naprednih bezbednosnih rešenja, poput višefaktorske autentifikacije, enkripcije podataka i redovnih bezbednosnih provera, može

pomoći zaposlenima da lakše usvoje i primene bezbednosne mere. Pored toga, postavljanje jasnih procedura i smernica za prijavu sumnjivih aktivnosti i bezbednosnih incidenata omogućava zaposlenima da budu aktivni učesnici u zaštiti organizacije.

Jedan od ključnih aspekata odnosa zaposlenih prema sajber bezbednosti je razumevanje njihove lične odgovornosti. Sajber bezbednost nije samo zadatak IT sektora, već zajednička odgovornost svih zaposlenih. Svaki pojedinac koji koristi digitalne alate i ima pristup osetljivim podacima mora biti svestan svojih dužnosti i potencijalnog uticaja svog ponašanja na bezbednost cele organizacije.

Kultura sajber bezbednosti u Srbiji još uvek prolazi kroz fazu formiranja. Za postizanje održivih rezultata, potrebno je raditi na promeni mentaliteta zaposlenih, gde će se sajber bezbednost posmatrati kao svakodnevna praksa, a ne kao nešto što se odnosi samo na specifične događaje ili incidente. Uspeh u ovoj oblasti zavisi od integracije bezbednosnih praksi u svakodnevne poslovne aktivnosti, kao i od toga koliko će sajber bezbednost postati sastavni deo organizacione kulture.

Odnos zaposlenih prema sajber bezbednosti u Srbiji ima ključnu ulogu u zaštiti organizacija od pretnji u digitalnom svetu. Iako svest o sajber pretnjama raste, mnoge organizacije se suočavaju sa izazovima kao što su nedovoljno obrazovanje, otpor prema promenama i manjak resursa. Kako bi se uspešno suočili sa ovim izazovima, organizacije moraju da ulažu u kontinuiranu edukaciju zaposlenih, razvoj sigurnosne kulture i primenu tehnoloških rešenja koja smanjuju uticaj ljudske greške.

Odnos zaposlenih prema sajber bezbednosti u Srbiji pokazuje da postoji prostor za značajna unapređenja, posebno u oblastima edukacije, podrške od strane menadžmenta i implementacije adekvatnih tehnoloških rešenja. Kako pretnje postaju sve sofisticiranije, tako i odgovornost zaposlenih raste, pa je neophodno stvoriti okruženje u kojem će sajber bezbednost biti prioritet i deo svakodnevne rutine. Samo sa sinhronizovanim naporima svih zaposlenih, kompanije u Srbiji mogu da ostvare visok nivo zaštite i smanje rizik od sajber pretnji.

7.3. Odnos privrednih subjekata u Srbiji prema sajber bezbednosti

Odnos privrednih subjekata, banaka i osiguravajućih kompanija prema sajber bezbednosti u Srbiji je tema koja postaje sve relevantnija u poslednjih nekoliko godina, kako globalni trendovi digitalizacije utiču na privredu i ekonomiju, a pretnje sajber napadima postaju sve izraženije. Ovaj tekst detaljno razmatra kako različiti akteri iz privrednog sektora Srbije pristupaju sajber bezbednosti, uključujući izazove sa kojima se suočavaju, mere koje preduzimaju, kao i regulatorni okvir koji ih obavezuje.

Privredni subjekti u Srbiji i sajber bezbednost[88]

Privredni subjekti u Srbiji, poput malih, srednjih i velikih preduzeća, suočavaju se sa rastućim rizicima u sajber prostoru. Zbog ubrzane digitalizacije poslovnih procesa, uključujući e-

[88] Wright, T. (2021). Business Sector Cybersecurity Approaches., str. 40-45

trgovinu, digitalne platforme, automatizovane sisteme za upravljanje podacima i povezivanje sa međunarodnim tržištima, preduzeća su postala meta sajber kriminalaca. Sajber napadi mogu dovesti do gubitka podataka, narušavanja poslovne reputacije, finansijskih gubitaka i, u najtežim slučajevima, potpunog zaustavljanja poslovnih operacija.

Glavni izazovi:

- Nedovoljna svest o rizicima: Mnoga preduzeća, naročito mala i srednja, nisu dovoljno svesna rizika koje sa sobom nose sajber napadi. Nedostatak edukacije i informacija o vrstama napada i mogućim posledicama često dovodi do nedovoljnog ulaganja u sajber bezbednost.
- Ograničeni resursi: Manja preduzeća često nemaju resurse da ulažu u složene bezbednosne sisteme ili angažuju stručnjake za sajber bezbednost. Često koriste jednostavne i standardne IT sisteme, što ih čini ranjivijim.
- Kritična infrastruktura: Preduzeća koja rade sa osetljivim podacima, kao što su ona iz oblasti zdravstva, energetike, telekomunikacija i transporta, moraju da ulažu u napredne sisteme sajber zaštite kako bi zaštitila kritičnu infrastrukturu.

Mere za unapređenje sajber bezbednosti:

- Ulaganje u IT infrastrukturu: Sve više kompanija u Srbiji počinje da ulaže u jačanje svoje IT infrastrukture, koristeći napredne antiviruse, firewall sisteme, VPN mreže i enkripciju podataka.
- Edukacija zaposlenih: S obzirom na to da su zaposleni često najslabija karika u lancu sajber bezbednosti, mnoge kompanije ulažu u edukaciju o prepoznavanju pretnji (npr. phishing) i o tome kako da pravilno reaguju.
- Saradnja sa specijalizovanim firmama: Neke kompanije odlučuju se za saradnju sa specijalizovanim IT firmama koje pružaju usluge konsaltinga i bezbednosne procene.

Banke i sajber bezbednost

Bankarski sektor u Srbiji ima posebnu ulogu kada je u pitanju sajber bezbednost, s obzirom na to da upravlja velikim količinama osetljivih finansijskih podataka. Banke su prirodne mete sajber kriminalaca zbog mogućnosti brzog sticanja finansijske koristi kroz krađu podataka ili izvršavanje prevara.

Glavni izazovi:

- Finansijski gubici: Bankarski sektor se suočava sa značajnim finansijskim gubicima u slučaju uspešnih sajber napada. Gubitak poverenja korisnika može dodatno ugroziti reputaciju banke, što dugoročno dovodi do pada prihoda.
- Usaglašavanje sa regulativama: Banke moraju da se pridržavaju strogih regulativnih okvira koje propisuju međunarodne i domaće institucije, kao što su Zakon o zaštiti podataka o ličnosti (GDPR) i drugi propisi vezani za finansijske usluge. Usaglašenost sa ovim propisima zahteva značajna ulaganja u bezbednosne sisteme.
- Napadi na digitalne kanale: Banke su u sve većoj meri usmerene na digitalizaciju svojih usluga kroz internet i mobilno bankarstvo, što stvara dodatne ranjivosti u sistemu.

Mere za unapređenje sajber bezbednosti:

- Korišćenje naprednih alata za detekciju pretnji: Banke investiraju u napredne sisteme za detekciju pretnji (npr. SIEM - Security Information and Event Management sistemi) kako bi u realnom vremenu pratile i analizirale potencijalne bezbednosne pretnje.
- Multifaktorna autentifikacija: Jedna od najvažnijih mera koju banke preduzimaju jeste implementacija multifaktorne autentifikacije (MFA), čime se osigurava dodatni nivo zaštite prilikom pristupa bankarskim servisima.
- Penetracioni testovi: Banke redovno sprovode simulirane sajber napade kako bi identifikovale slabosti u svom sistemu i unapredile bezbednost.

Osiguravajuće kompanije i sajber bezbednost

Osiguravajuće kompanije u Srbiji takođe su značajno pogođene pretnjama iz sajber prostora, s obzirom na to da upravljaju velikim količinama podataka o svojim korisnicima, uključujući finansijske podatke i osetljive lične informacije. Pored zaštite sopstvenih podataka, ove kompanije sve više postaju deo ekosistema sajber osiguranja, pružajući osiguranje kompanijama koje su izložene rizicima sajber napada.

Glavni izazovi:

- Zaštita podataka korisnika: Kao i banke, osiguravajuće kompanije upravljaju velikom količinom podataka koji su osetljivi i na meti sajber kriminalaca. Neovlašćeni pristup ovim podacima može dovesti do kršenja poverljivosti i ozbiljnih reputacionih i finansijskih posledica.
- Kompleksnost podataka: Osiguravajuće kompanije često upravljaju različitim tipovima podataka (npr. medicinski, finansijski, lični podaci), što komplikuje proces njihove zaštite.
- Razvijanje tržišta sajber osiguranja: Kako sajber napadi postaju sve učestaliji, osiguravajuće kompanije sve više nude specifične polise koje pokrivaju posledice sajber napada. Ove polise pomažu preduzećima da ublaže finansijske gubitke nastale usled sajber incidenata.

Mere za unapređenje sajber bezbednosti:

- Implementacija GDPR propisa: Usaglašenost sa regulativama kao što je GDPR ključna je za osiguravajuće kompanije. Ove firme investiraju u sisteme za zaštitu podataka, kao i u procese koji osiguravaju pravilno upravljanje ličnim podacima.
- Sajber osiguranje: Osiguravajuće kompanije razvijaju polise sajber osiguranja koje pokrivaju troškove oporavka nakon sajber napada, uključujući troškove pravne pomoći, sanaciju štete i naknadu gubitaka zbog prekida poslovanja.

Regulatorni okvir za sajber bezbednost u Srbiji[89]

Srbija je prepoznala značaj sajber bezbednosti i preduzela je korake da uspostavi regulatorni okvir koji bi obavezao preduzeća, banke i osiguravajuće kompanije na preduzimanje adekvatnih bezbednosnih mera. Ključni zakonodavni okvir uključuje:

[89] Cook, N. (2020). Cybersecurity in Serbia: Challenges and Strategies., str. 42-47

- Zakon o informacionoj bezbednosti: Ovaj zakon obavezuje pravne subjekte, naročito one koji se bave pružanjem usluga kritične infrastrukture (npr. telekomunikacije, finansijske usluge), na implementaciju sistema za zaštitu od sajber pretnji.
- Nacionalna strategija za sajber bezbednost: Nacionalna strategija pruža smernice za razvoj sajber bezbednosti u zemlji i postavlja ciljeve za zaštitu kritičnih infrastruktura i osnaživanje institucija za borbu protiv sajber kriminala.
- Zakon o zaštiti podataka o ličnosti: Sličan GDPR-u, ovaj zakon obavezuje pravne subjekte da štite podatke korisnika i propisuje stroge kazne u slučaju kršenja privatnosti.

Odnos privrednih subjekata, banaka i osiguravajućih kompanija prema sajber bezbednosti u Srbiji postaje sve ozbiljniji, s obzizirom na sve učestalije sajber napade i sve strože regulatorne zahteve. Iako mnoge kompanije, naročito mala i srednja preduzeća, još uvek nisu u potpunosti svesne obima pretnji, jasno je da postoji sve veća potreba za ulaganjima u sajber bezbednost. Banke i osiguravajuće kompanije, koje su već podložne striktnim regulativama, preduzimaju značajne korake kako bi se zaštitile od potencijalnih napada, dok sve više preduzeća uvodi nove tehnologije i procese za zaštitu svojih sistema i podataka.

Ključna komponenta ovog procesa je edukacija i podizanje svesti o sajber bezbednosti na svim nivoima – od rukovodstva do zaposlenih. Bez adekvatne svesti i obučenosti, čak i najnapredniji tehnološki sistemi mogu biti ugroženi. Takođe, saradnja sa specijalizovanim firmama, kao i implementacija nacionalnih i međunarodnih standarda, omogućava privrednim subjektima da bolje odgovore na savremene pretnje.

U budućnosti se očekuje dalji razvoj sajber osiguranja i dodatno pooštravanje regulativa koje će privrednim subjektima nametnuti nove obaveze, ali i podstaknuti ulaganja u savremene sisteme zaštite. Samo uz multidisciplinarni pristup – uključujući tehničke mere, regulativu, edukaciju i osiguranje – privreda Srbije će moći da se uspešno izbori sa izazovima sajber bezbednosti i očuva integritet i sigurnost svojih podataka i poslovnih procesa.

7.4. Odnos javnih preduzeća i Vladinih institucija u Srbiji prema sajber bezbednosti

Odnos javnih preduzeća i vladinih institucija u Srbiji prema sajber bezbednosti postaje sve relevantniji, s obzirom na to da se ove organizacije bave velikim količinama kritičnih i poverljivih informacija od značaja za funkcionisanje države i društva. Ove institucije su često meta sajber napada, što može izazvati ozbiljne posledice ne samo po njihovu infrastrukturu, već i po širu javnost i državnu sigurnost. U nastavku sledi detaljan pregled stanja sajber bezbednosti u javnim preduzećima i vladinim institucijama u Srbiji, sa naglaskom na izazove, mere i regulativni okvir.

Javna preduzeća i sajber bezbednost

Javna preduzeća u Srbiji su ključni subjekti u oblastima kao što su energetika, transport, telekomunikacije i komunalne usluge. S obzirom na to da upravljaju kritičnom infrastrukturom, bilo kakva ranjivost u njihovim sistemima može imati ozbiljne posledice za celokupno društvo.

Prekid u snabdevanju energijom, saobraćajni kolaps ili ometanje telekomunikacionih usluga mogu dovesti do destabilizacije države i značajnih ekonomskih gubitaka.

Glavni izazovi:

- Zastarela infrastruktura: Mnogi IT sistemi u javnim preduzećima koriste zastarele tehnologije koje nisu u skladu sa savremenim standardima sajber bezbednosti. Nedostatak modernizacije i prilagođavanja novim pretnjama predstavlja ozbiljnu ranjivost.
- Nedostatak kvalifikovanog kadra: Uprkos povećanju svesti o značaju sajber bezbednosti, mnoga javna preduzeća nemaju dovoljno stručnog kadra za adekvatno upravljanje i zaštitu njihovih IT sistema. Nedostatak resursa za obuku i zadržavanje stručnjaka dodatno komplikuje situaciju.
- Kompleksnost mreža: Javna preduzeća često upravljaju velikim i kompleksnim IT mrežama koje se protežu kroz više sektora i regiona. Ova kompleksnost otežava zaštitu svih aspekata infrastrukture i povećava mogućnost za sajber napade.
- Nedovoljno testiranje ranjivosti: Nedostatak proaktivnog testiranja ranjivosti, kao što su penetracioni testovi, dovodi do toga da mnoge pretnje ostanu neprimećene sve dok ne dođe do napada.

Mere za unapređenje sajber bezbednosti:

- Modernizacija IT infrastrukture: Neka javna preduzeća u Srbiji počinju da investiraju u modernizaciju svojih IT sistema, prelazeći na savremene tehnologije, uključujući cloud computing, enkripciju podataka i napredne sisteme zaštite.
- Edukacija i obuka zaposlenih: Sve veći broj javnih preduzeća ulaže u edukaciju zaposlenih o osnovnim principima sajber bezbednosti. S obzirom na to da ljudski faktor često predstavlja najslabiju tačku, obuka je ključna za minimiziranje grešaka koje mogu dovesti do bezbednosnih incidenata.
- Saradnja sa privatnim sektorom: Javna preduzeća sve više sarađuju sa privatnim IT firmama kako bi obezbedila ekspertske usluge i konsultacije u vezi sa sajber bezbednošću. Ova partnerstva omogućavaju pristup naprednim alatima za zaštitu i prevenciju napada.
- Kontinuirano praćenje i unapređenje sistema: Uvođenje alata za nadzor i detekciju pretnji u realnom vremenu omogućava javnim preduzećima da brže reaguju na potencijalne pretnje i minimiziraju štetu.

Vladine institucije i sajber bezbednost

Vladine institucije u Srbiji, uključujući ministarstva, agencije i druge državne organe, imaju ključnu ulogu u očuvanju sajber bezbednosti na nacionalnom nivou. One upravljaju osetljivim podacima građana i ključnim informacijama koje su od vitalnog značaja za funkcionisanje države. Pretnje sajber napadima usmerene na državne institucije mogu ozbiljno ugroziti nacionalnu bezbednost, političku stabilnost i poverenje građana u institucije.

Glavni izazovi:

- Ciljani napadi: Vladine institucije su često meta sofisticiranih sajber napada koje sprovode različiti akteri, uključujući strane države, haktiviste i organizovane

kriminalne grupe. Ovi napadi obuhvataju špijunažu, krađu podataka, sabotažu i propagandu.

- Zakonodavni i regulatorni izazovi: Uprkos postojanju zakonskog okvira za sajber bezbednost, nedostatak dosledne primene regulativa može predstavljati problem. Takođe, brzina kojom se sajber pretnje razvijaju često premašuje tempo usvajanja novih zakona i regulativa.
- Nedovoljni resursi: Kao i kod javnih preduzeća, mnoge vladine institucije suočavaju se sa problemom nedostatka finansijskih i kadrovskih resursa za jačanje sajber bezbednosti. Ovo otežava implementaciju modernih tehnologija zaštite i jačanje operativnih sposobnosti.

Mere za unapređenje sajber bezbednosti:

- Nacionalni CERT: Nacionalni centar za odgovor na sajber incidente (CERT) igra ključnu ulogu u koordinaciji odgovora na sajber napade u državnim institucijama. Ovaj centar prikuplja informacije o sajber pretnjama, pruža savete o zaštiti i organizuje obuke za državne službenike.
- Primena naprednih sigurnosnih standarda: Vladine institucije sve više usvajaju međunarodne sigurnosne standarde kao što su ISO 27001 kako bi ojačale svoje sisteme za zaštitu podataka i informacijskih sistema.
- Digitalizacija sa sigurnosnim fokusom: Kako se sve više vladinih usluga digitalizuje (npr. e-uprava, online prijave, digitalno plaćanje poreza), sve veći akcenat se stavlja na sigurnosne aspekte ove digitalizacije. Implementacija sigurnih komunikacionih kanala, dvofaktorne autentifikacije i enkripcije postaje standard u pružanju digitalnih usluga.
- Saradnja sa međunarodnim partnerima: Srbija sarađuje sa brojnim međunarodnim organizacijama i zemljama na polju sajber bezbednosti. Ova saradnja omogućava razmenu informacija o pretnjama, unapređenje sigurnosnih praksi i obuku kadrova.
- Redovno testiranje sistema: Sprovode se simulacije sajber napada i penetracioni testovi u okviru vladinih institucija kako bi se identifikovale slabosti u sistemu i unapredile preventivne mere.

Regulatorni okvir za sajber bezbednost u vladinim institucijama i javnim preduzećima

Vladine institucije i javna preduzeća u Srbiji posluju u skladu sa specifičnim zakonskim i regulatornim okvirom koji definiše njihove obaveze u vezi sa sajber bezbednošću. Glavne komponente ovog regulatornog okvira uključuju:

- Zakon o informacionoj bezbednosti: Ovaj zakon postavlja osnove za sajber bezbednost i obavezuje vladine institucije i javna preduzeća da implementiraju odgovarajuće bezbednosne mere za zaštitu svojih informacionih sistema.
- Zakon o zaštiti podataka o ličnosti: Slično kao u privatnom sektoru, javne institucije[90] su dužne da se pridržavaju propisa o zaštiti podataka o ličnosti, kako bi obezbedile sigurnost podataka građana kojima upravljaju.
- Nacionalna strategija za sajber bezbednost: Ova strategija pruža okvir za jačanje kapaciteta u oblasti sajber bezbednosti u Srbiji, sa posebnim fokusom na zaštitu državne infrastrukture i informacija.

[90] Thompson, G. (2020). Public Institutions and Cybersecurity., str. 47-50

Odnos javnih preduzeća i vladinih institucija u Srbiji prema sajber bezbednosti postaje sve složeniji i zahteva sveobuhvatan pristup. Iako postoje izazovi poput zastarele tehnologije, nedostatka kadra i ciljanih napada, institucije preduzimaju korake kako bi se unapredila sigurnost informacionih sistema. Modernizacija IT infrastrukture, edukacija kadrova, saradnja sa privatnim sektorom i međunarodnim partnerima, kao i primena nacionalnih i međunarodnih bez bednosnih standarda, predstavljaju ključne elemente u unapređenju sajber bezbednosti.

Vladine institucije i javna preduzeća u Srbiji postaju sve svesnija ozbiljnosti sajber pretnji i neophodnosti proaktivnog delovanja. Uvođenjem Nacionalnog CERT-a, primenom sigurnosnih protokola i tehnologija, kao i saradnjom na međunarodnom nivou, Srbija pokazuje opredeljenost da unapredi svoju sajber bezbednost. Međutim, ostaje izazov da se ubrza digitalna transformacija i usvajanje novih tehnologija, istovremeno osiguravajući njihovu bezbednost.

U budućnosti će dalji razvoj zakonskog i regulatornog okvira, kao i povećanje ulaganja u bezbednosnu infrastrukturu, biti presudni za održavanje stabilnosti i sigurnosti u sajber prostoru. Javna preduzeća i državne institucije moraju kontinuirano prilagođavati svoje strategije kako bi odgovorile na nove i sve sofisticiranije sajber pretnje, čime će doprineti ne samo zaštiti svoje infrastrukture, već i očuvanju sigurnosti cele države i njenih građana.

7.5. Nacionalni CERT (Computer Emergency Response Team) i njegova uloga u sajber bezbednosti u Srbiji

Nacionalni CERT (Computer Emergency Response Team) u Srbiji, koji funkcioniše u okviru Regulatorne agencije za elektronske komunikacije i poštanske usluge (RATEL), ključna je institucija koja se bavi sajber bezbednošću u zemlji. Njegova osnovna uloga je koordinacija odgovora na sajber incidente, pružanje podrške u sprečavanju i saniranju napada, kao i podizanje svesti o sajber pretnjama i zaštitnim merama među svim ključnim akterima u Srbiji uključujući privatni, javni i državni sektor.

Osnivanje i funkcionalni okvir Nacionalnog CERT-a

Nacionalni CERT Srbije osnovan je u skladu sa Zakonom o informacionoj bezbednosti iz 2016. godine, koji je usvojen kao deo nacionalne strategije za unapređenje sajber bezbednosti. RATEL, kao nezavisna regulatorna agencija, dobio je ovlašćenja da osnuje i upravlja Nacionalnim CERT-om, sa zadatkom da nadgleda, prikuplja informacije i koordinira aktivnosti u vezi sa sajber incidentima na nacionalnom nivou.

Nacionalni CERT se bavi zaštitom kritične informacione infrastrukture, što uključuje državne i privatne subjekte čiji IT sistemi igraju ključnu ulogu u funkcionisanju države i društva. Ovi subjekti uključuju oblasti poput energetike, telekomunikacija, finansijskog sektora, zdravstva, saobraćaja, i drugih ključnih sektora koji su ranjivi na sajber napade.

Uloga Nacionalnog CERT-a u sajber bezbednosti

Nacionalni CERT ima višestruku ulogu u sajber bezbednosti Srbije, koja uključuje sledeće ključne zadatke:

Detekcija i odgovor na sajber incidente

Nacionalni CERT prikuplja i analizira informacije o sajber pretnjama i incidentima koji se dešavaju u zemlji, uključujući prijave od javnih i privatnih organizacija, kao i globalne informacije o sajber pretnjama. On prati i obaveštava relevantne institucije o potencijalnim pretnjama i rizicima, što omogućava brži odgovor na incidente. U slučaju sajber napada, CERT koordinira odgovor, pomaže organizacijama da ublaže štetu i pruža tehničku podršku u obnovi sistema.

Razmena informacija i koordinacija sa drugim institucijama

Jedna od ključnih uloga Nacionalnog CERT-a jeste razmena informacija i saradnja sa drugim domaćim i međunarodnim sajber bezbednosnim organizacijama. On uspostavlja veze sa CERT-ovima iz drugih zemalja, međunarodnim organizacijama i sektorima kako bi osigurao da Srbija ima pristup najnovijim informacijama o globalnim sajber pretnjama i napadima. Ova razmena informacija omogućava Srbiji da bude deo globalnog sistema sajber bezbednosti i da efikasnije odgovara na pretnje.

Podizanje svesti i edukacija

Nacionalni CERT ima važnu ulogu u edukaciji i podizanju svesti o sajber bezbednosti u Srbiji. On organizuje obuke, seminare, radionice i savetovanja za javne i privatne organizacije, kao i za širu javnost. Glavni cilj ovih aktivnosti je da se podigne nivo svesti o sajber pretnjama i da se osigura da svi akteri razumeju osnovne principe zaštite podataka i IT sistema.

Izrada preporuka i smernica

Kako bi unapredio nivo sajber bezbednosti u Srbiji, Nacionalni CERT redovno izrađuje i objavljuje preporuke i smernice za javna preduzeća, privatni sektor, državne institucije i građane. Ove preporuke se odnose na tehničke i organizacione mere zaštite, kao što su pravila za upravljanje pristupom, implementacija bezbednosnih protokola[91], pravilna upotreba enkripcije, i postupci u slučaju incidenata.

Koordinacija sa sektorom kritične infrastrukture

Jedan od najvažnijih zadataka Nacionalnog CERT-a jeste koordinacija sajber bezbednosti za sektore koji čine kritičnu infrastrukturu u zemlji. To uključuje energetiku, zdravstvo, transport, vodovod, telekomunikacije i druge sektore. Nacionalni CERT pruža podršku ovim sektorima u proceni ranjivosti, sprovođenju testiranja bezbednosti i izradi planova za odgovor na incidente.

Regulatorni okvir i zakonske obaveze

Nacionalni CERT deluje u skladu sa Zakonom o informacionoj bezbednosti, koji definiše obaveze javnih i privatnih institucija u vezi sa zaštitom informacijskih sistema. Zakon obavezuje sve pravne subjekte koji pružaju usluge od opšteg interesa da prijavljuju sajber

[91] Green, A. (2020). Implementing Security Protocols in Organizations. Springer., str. 34-39

incidente Nacionalnom CERT-u. Takođe, zakon propisuje stroge kazne za nepoštovanje ovih pravila, čime se osigurava ozbiljnost pristupa sajber bezbednosti.

Uz Zakon o informacionoj bezbednosti, Nacionalni CERT takođe radi u skladu sa Zakonom o zaštiti podataka o ličnosti, koji je u velikoj meri usklađen sa evropskim GDPR standardom. Ovaj zakon obavezuje sve organizacije da preduzmu odgovarajuće tehničke i organizacione mere za zaštitu podataka korisnika, a Nacionalni CERT pruža podršku u sprovođenju tih mera, naročito u slučajevima kada dođe do curenja ili kompromitacije podataka.

Saradnja sa međunarodnim institucijama

Nacionalni CERT Srbije uspostavlja intenzivnu saradnju sa međunarodnim organizacijama i drugim nacionalnim CERT-ovima. Ova saradnja je od suštinskog značaja za brzo delovanje u slučaju globalnih sajber incidenata, kao i za razmenu znanja o novim metodama zaštite i alatima za detekciju pretnji. Srbija je članica različitih međunarodnih mreža i foruma za sajber bezbednost, što omogućava integraciju u globalni sistem sajber zaštite i razmenu relevantnih informacija sa partnerskim državama.

Izazovi sa kojima se Nacionalni CERT suočava

Iako Nacionalni CERT ima ključnu ulogu u zaštiti Srbije od sajber pretnji, suočava se sa nekoliko izazova:

- Nedostatak resursa i kadra: Kao i mnogi drugi timovi koji se bave sajber bezbednošću u svetu, Nacionalni CERT se suočava sa nedostatkom kvalifikovanog kadra i resursa. Broj sajber pretnji raste iz godine u godinu, a kapaciteti za brzo delovanje su ograničeni.
- Brzina evolucije pretnji: Sajber pretnje se brzo razvijaju i postaju sve sofisticiranije, što zahteva stalno prilagođavanje i unapređenje znanja i tehnologija koje se koriste u odbrani.
- Usaglašavanje sa međunarodnim standardima: Kako bi ostala konkurentna i dobro povezana na međunarodnom nivou, Srbija mora da kontinuirano unapređuje svoje regulative i standarde, što predstavlja izazov za usklađivanje sa evropskim i globalnim normama.

Nacionalni CERT Srbije, u okviru RATEL-a, igra ključnu ulogu u održavanju sajber bezbednosti na nacionalnom nivou. Kroz detekciju i odgovor na incidente, koordinaciju sa domaćim i međunarodnim institucijama, kao i kroz podizanje svesti i edukaciju, ovaj tim je postao centralna tačka za sajber bezbednost u zemlji. Iako se suočava sa brojnim izazovima, Nacionalni CERT nastavlja da unapređuje svoju ulogu i kapacitete kako bi Srbija mogla efikasno da odgovori na sve složenije sajber pretnje i očuva sigurnost svoje kritične infrastrukture, podataka i sistema.

7.6. Funkcija i doprinos posebnih CERT-ova u Srbiji

Pored Nacionalnog CERT-a koji deluje pod okriljem RATEL-a, u Srbiji postoji nekoliko posebnih CERT-ova (Computer Emergency Response Team) koji imaju specifične funkcije unutar različitih sektora, organizacija i institucija. Ovi posebni CERT-ovi igraju ključnu ulogu

u unapređenju sajber bezbednosti, jer su usmereni na specifične potrebe sektora kao što su kritična infrastruktura, finansijski sektor, energetika i drugi važni sistemi. Njihov zadatak je ne samo da odgovore na incidente, već i da proaktivno spreče napade i obezbede bezbednosne protokole prilagođene specifičnim izazovima sa kojima se suočavaju.

Šta su posebni CERT-ovi?

Posebni CERT-ovi u Srbiji funkcionišu kao operativni timovi za odgovor na sajber incidente unutar organizacija, sektora ili industrijskih grana. Oni su specijalizovani za upravljanje incidentima, pružanje tehničke podrške, obuku i savetovanje, kao i za unapređenje bezbednosnih politika specifičnih za svoje okruženje. Postojanje ovih posebnih timova omogućava veću decentralizaciju odgovora na incidente i bolju koordinaciju unutar kritičnih sektora. Takođe, posebni CERT-ovi olakšavaju saradnju između organizacija i Nacionalnog CERT-a, koji služi kao centralni koordinacioni organ za sajber bezbednost.

Glavne funkcije posebnih CERT-ova

Posebni CERT-ovi u Srbiji imaju nekoliko ključnih funkcija koje doprinose opštoj sajber bezbednosti u zemlji. Njihove aktivnosti uključuju sledeće:

1. **Prevencija i upravljanje incidentima**

Kao i Nacionalni CERT, posebni CERT-ovi imaju zadatak da preduprede sajber incidente i reaguju na njih kada dođe do napada. To podrazumeva nadgledanje mreža, prikupljanje informacija o pretnjama, analiziranje uzroka incidenata, te obezbeđivanje tehničke pomoći u slučaju kompromitacije sistema. Oni takođe razvijaju planove za vanredne situacije, tako da se organizacije mogu brzo oporaviti nakon napada.

2. **Održavanje sajber bezbednosnih politika**

Posebni CERT-ovi kreiraju specifične bezbednosne politike koje su prilagođene industrijskom ili sektorskom okruženju u kojem deluju. Oni analiziraju rizike specifične za određene sektore i predlažu adekvatne mere za njihovo umanjenje. Na primer, u sektoru energetike ili telekomunikacija, bezbednosne politike moraju biti izuzetno robusne zbog značaja tih sektora za stabilnost države.

3. **Koordinacija sa Nacionalnim CERT-om i drugim subjektima**

Posebni CERT-ovi redovno razmenjuju informacije sa Nacionalnim CERT-om i srodnim timovima u zemlji i inostranstvu. Ova koordinacija je od ključnog značaja za širenje saznanja o sajber pretnjama i incidentima, kao i za unapređenje odbrambenih mehanizama. Kada se incidenti identifikuju na lokalnom ili sektorskom nivou, posebni CERT-ovi obaveštavaju Nacionalni CERT, koji dalje može preduzeti mere na nacionalnom nivou ili obavestiti međunarodne partnere.

4. **Obuka i podizanje svesti**

Posebni CERT-ovi igraju ključnu ulogu u obuci zaposlenih unutar sektora ili organizacija koje štite. Organizuju radionice, simulacije napada i obuke kako bi podigli nivo svesti o sajber bezbednosti i unapredili veštine zaposlenih u pogledu prepoznavanja i reagovanja na pretnje. Oni pružaju smernice za upravljanje digitalnim resursima i razvijaju sigurnosne prakse prilagođene specifičnim potrebama sektora.

5. **Proaktivna zaštita i testiranje**

Osim reagovanja na incidente, posebni CERT-ovi sprovode proaktivne mere zaštite kao što su penetracioni testovi (pentesting) i simulacije sajber napada. Ovi testovi omogućavaju organizacijama da unaprede svoje sisteme na osnovu identifikovanih ranjivosti pre nego što dođe do pravih incidenata.

Primeri posebnih CERT-ova u Srbiji

U Srbiji su neki od najvažnijih posebnih CERT-ova formirani u sektorima koji su ključni za funkcionisanje državne infrastrukture i ekonomije. Evo nekoliko primera:

1. **Finansijski sektor**

Finansijski sektor u Srbiji, koji uključuje banke, osiguravajuće kompanije i finansijske institucije, ima svoj posebni CERT koji je zadužen za sajber bezbednost unutar ovog sektora. S obzirom na visoki nivo pretnji kao što su finansijske prevare, phishing napadi i krađa podataka, finansijski CERT ima specifične zadatke u zaštiti finansijskih sistema. Ovaj tim se bavi detekcijom i reakcijom na napade koji uključuju finansijske transakcije i podatke, pružajući podršku bankama u upravljanju bezbednosnim rizicima.

2. **Energetski sektor**

Energetski sektor, uključujući elektrane, distributivne mreže i naftne kompanije, je od ključne važnosti za nacionalnu bezbednost Srbije. CERT za energetski sektor bavi se bezbednosnim izazovima specifičnim za industrijsku kontrolnu infrastrukturu, kao što su SCADA sistemi (Supervisory Control and Data Acquisition), koji su veoma osetljivi na sajber napade. Timovi unutar ovog sektora su odgovorni za obezbeđivanje stabilnog i sigurnog snabdevanja energijom, a incidenti u ovom sektoru mogu imati širok uticaj na nacionalnu ekonomiju i svakodnevni život.

3. **Telekomunikacioni sektor**

S obzirom na značaj telekomunikacija za povezivanje infrastruktura i svakodnevne poslovne i lične aktivnosti građana, telekomunikacioni sektor ima poseban CERT koji prati i reaguje na pretnje u ovoj oblasti. Napadi na telekomunikacione mreže mogu destabilizovati druge sektore, pa je njihova zaštita od ključnog značaja. Telekomunikacioni CERT igra ključnu ulogu u detekciji i neutralisanju napada kao što su DDoS (Distributed Denial of Service) napadi, ometanje mreža, kao i u zaštiti podataka korisnika usluga.

4. **Državne institucije i javna preduzeća**

CERT-ovi unutar državnih institucija kao što su ministarstva, vladine agencije i javna preduzeća imaju poseban fokus na zaštitu državnih informacija i kritične infrastrukture. Ovi timovi usko sarađuju sa Nacionalnim CERT-om kako bi osigurali da se pretnje identifikuju i saniraju pre nego što ozbiljno ugroze rad institucija ili infrastrukturu. U obzir se uzima i zaštita osetljivih podataka građana, koji se nalaze u državnim bazama podataka.

Doprinos posebnih CERT-ova sajber bezbednosti u Srbiji

Posebni CERT-ovi daju ogroman doprinos unapređenju sajber bezbednosti na više nivoa. Neki od glavnih doprinosa uključuju:

- Brža reakcija na incidente: Zbog svoje specifične usmerenosti i stručnosti, posebni CERT-ovi mogu brže reagovati na sajber incidente unutar sektora i pružiti neposrednu tehničku podršku organizacijama.
- Smanjenje rizika za kritičnu infrastrukturu: Posebni CERT-ovi omogućavaju bolju zaštitu kritičnih infrastrukturnih sistema od specifičnih pretnji. Na primer, energetski sektor ili finansijski sektor mogu biti ranjiviji na određene vrste napada, a posebni CERT timovi mogu bolje prepoznati i prilagoditi odbranu.
- Unapređenje svesti i stručnosti: Kroz obuku i obaveštavanje zaposlenih i menadžmenta, posebni CERT-ovi pomažu organizacijama da unaprede svoje kapacitete za prepoznavanje i reagovanje na sajber napade.
- Saradnja sa Nacionalnim CERT-om: Posebni CERT-ovi deluju kao veza između specifičnih sektora i Nacionalnog CERT-a, što omogućava bolju razmenu informacija i koordinisane akcije na nacionalnom nivou.

Posebni CERT-ovi u Srbiji predstavljaju ključnu komponentu u strategiji sajber bezbednosti. Njihova specifična usmerenost prema sektorima kao što su finansije, energetika, telekomunikacije i državna administracija omogućava fleksibiln

GLAVA 8: REZIME REZULTATA ISTRAŽIVANJA

Empirijsko istraživanje je metodološki pristup koji se bazira na prikupljanju, analizi i interpretaciji podataka iz stvarnog sveta, kako bi se testirale hipoteze ili otkrile zakonitosti. Ono koristi posmatranje, eksperimente, ankete, ili merenje kao metode za prikupljanje podataka, a rezultati su često kvantitativni, ali mogu biti i kvalitativni.

Cilj empirijskog istraživanja je da pruži objektivne, proverljive informacije koje potvrđuju ili opovrgavaju teorije ili pretpostavke, i time doprinese razumevanju pojava na temelju stvarnih dokaza, umesto spekulacija ili teorijskih modela.

8.1 Rezime rezultata istraživanja

U cilju prikupljanja podataka sprovedeno je detaljno empirijsko istraživanje s ciljem prikupljanja relevantnih podataka o percepciji i iskustvima korisnika, organizacija i stručnjaka u vezi sa sajber pretnjama i bezbednosnim rizicima.

Anketiranje ispitanika

Kao jedan od glavnih metoda prikupljanja podataka korišćeno je anketiranje, koje je obuhvatilo tri grupe ispitanika:

- IT stručnjaci i bezbednosni eksperti (20% uzorka)
- Zaposleni u javnim i privatnim organizacijama (50% uzorka)
- Korisnici interneta iz opšte populacije (30% uzorka)

Ukupno je anketirano 500 ispitanika putem online upitnika koji je obuhvatao 25 pitanja, podeljenih u nekoliko tematskih celina:

- Svest o sajber pretnjama
- Iskustva sa sajber napadima
- Bezbednosne prakse i navike
- Posledice sajber napada na poslovanje i privatne živote
- Percepcija efikasnosti postojećih mera sajber zaštite

Anketa je bila dostupna četiri nedelje, a odgovori su prikupljeni anonimno, kako bi se osigurala iskrenost ispitanika.

Intervjui sa stručnjacima

Pored ankete, sprovedeno je 10 dubinskih intervjua sa stručnjacima iz oblasti sajber bezbednosti, koji su dali uvid u složenost bezbednosnih rizika, najčešće metode napada, kao i efikasnost trenutnih odbrambenih strategija u Srbiji i regionu. Intervjui su trajali u proseku 60 minuta i obrađivali su teme kao što su:

- Najčešće ranjivosti sistema
- Trendovi u sajber napadima
- Preporuke za unapređenje sajber zaštite

Studije slučaja

Za dublju analizu uticaja sajber rizika na organizacije, korišćene su tri studije slučaja koje su analizirale stvarne sajber incidente u velikim kompanijama i državnim institucijama. Studije su obuhvatile:

- Tip napada (ransomware, phishing, DDoS)
- Finansijske i reputacione posledice
- Reakcije i mere oporavka nakon napada

Podaci iz ankete

- 65% zaposlenih u privatnom sektoru izjavilo je da su njihove kompanije bile meta sajber napada u poslednje dve godine.
- 40% ispitanika iz opšte populacije navelo je da koristi iste lozinke za više različitih naloga.
- 80% IT stručnjaka smatra da su trenutne mere zaštite nedovoljne i da su kompanije u Srbiji značajno ranjive na sofisticirane sajber napade.
- 55% ispitanika izjavilo je da nisu adekvatno obučeni za prepoznavanje phishing prevara.

Zaključci na osnovu prikupljenih podataka

Na osnovu prikupljenih podataka iz anketa, intervjua i studija slučaja, analiza je pokazala visok nivo svesti o sajber rizicima, ali i značajan nedostatak u obuci zaposlenih, tehničkoj zaštiti i strategijama oporavka od napada. Većina organizacija prepoznaje pretnje, ali ne ulaže dovoljno u adekvatne preventivne mere.

Ovi podaci će poslužiti kao osnova za formulaciju preporuka za poboljšanje sajber bezbednosti u Srbiji, kako na nivou organizacija, tako i u širem društvenom kontekstu.

Demografski podaci ispitanika

Tabela 7. Prikaz polne strukture ispitanika

Pol	Broj ispitanika	Procenat
Muškarci	296	59,2
Žene	204	40,8

Polnu strukturu ispitanika možemo i grafički ilustrovati.

Grafik 1. Zastupljenost polne strukture ispitanika

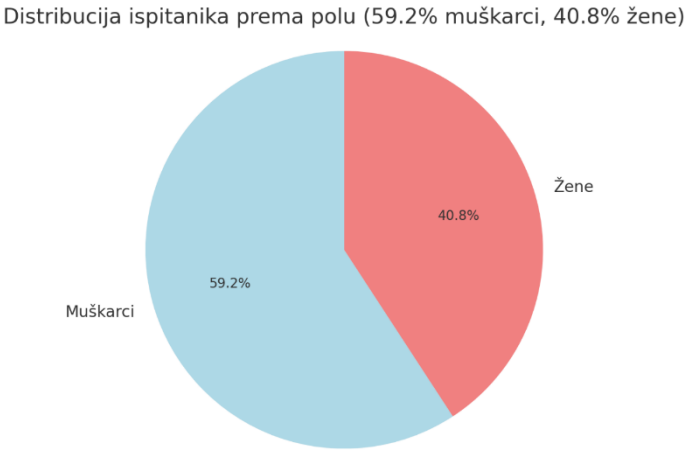


Tabela 8. Starosna struktura ispitanika

Starosna kategorija	Broj ispitanika	Procenat
18-25	81	16
26-30	119	24
31-35	100	20
36-40	59	12
41-45	41	8
46-50	30	6
51-55	30	6
56-60	20	4
61-65	20	4

Grafik 2. Grafički prikaz starosne strukture ispitanika

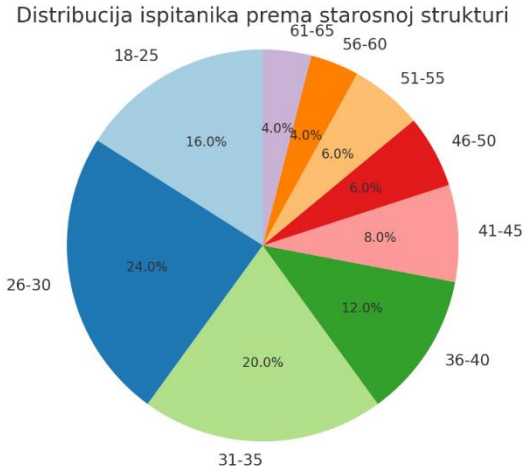


Tabela 9. Stepen obrazovanja ispitanika

Stepen obrazovanja	Broj ispitanika	Procenat
Osnovna škola	5	1
Srednja škola	150	30
Visoka škola	245	49
Master	75	15
Doktorat	25	5

Grafik 3. Stepen obrazovanja ispitanika

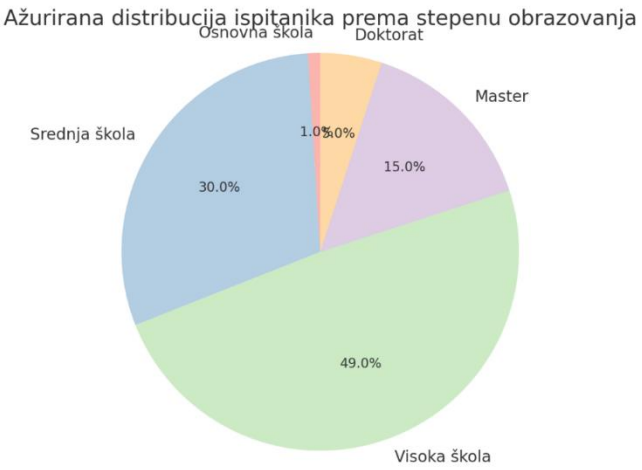
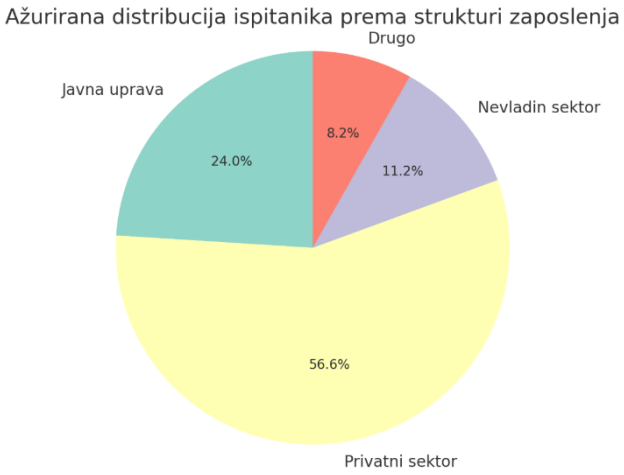


Tabela 10. Zaposlenje ispitanika

Struktura zaposlenja	Broj ispitanika	Procenat
Javna uprava	120	24
Privatni sektor	283	56.6
Nevladin sektor	56	11.2
Drugo	41	8.2

Grafik 4. Grafički prikaz strukture zaposlenja ispitanika



8.2 Ispitivanje stavova ispitanika

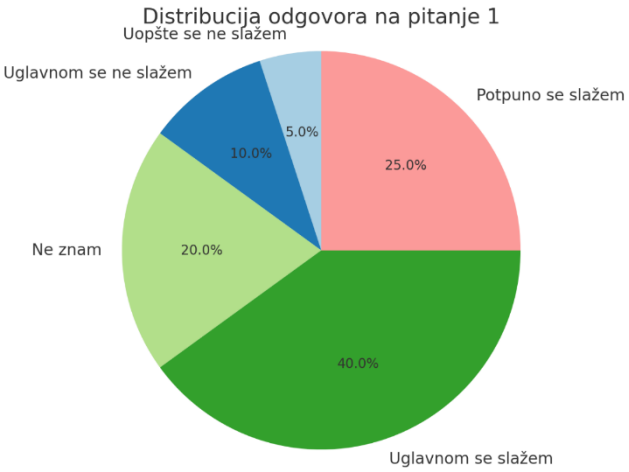
8.2.1 Svest o sajber pretnjama

8.2.1.1 Da li smatrate da su sajber pretnje ozbiljan rizik za organizacije danas?

Tabela 11. Odgovori ispitanika

Odgovor	Broj ispita	Procenat
Uopšte se ne slažem	26	5
Uglavnom se ne slažem	49	10
Ne znam	99	20
Uglavnom se slažem	101	40
Potpuno se slažem	125	25

Grafik 5. Grafički prikaz odgovora

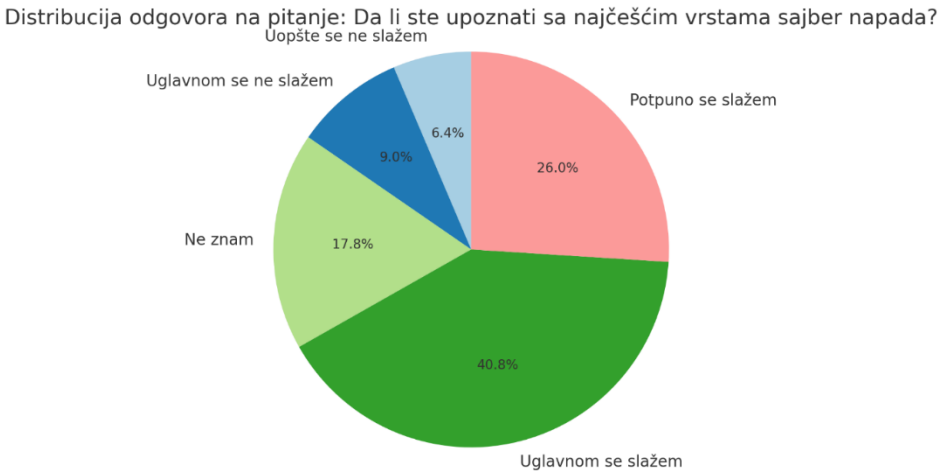


8.2.1.2 Da li ste upoznati sa najčešćim vrstama sajber napada?

Tabela 12. Odgovori ispitanika

Odgovor	Broj ispitanika	Procenat
Uopšte se ne slažem	32	6.4
Uglavnom se ne slažem	45	9
Ne znam	89	17.8
Uglavnom se slažem	204	40.8
Potpuno se slažem	130	26

Grafik 6. Grafički prikaz odgovora

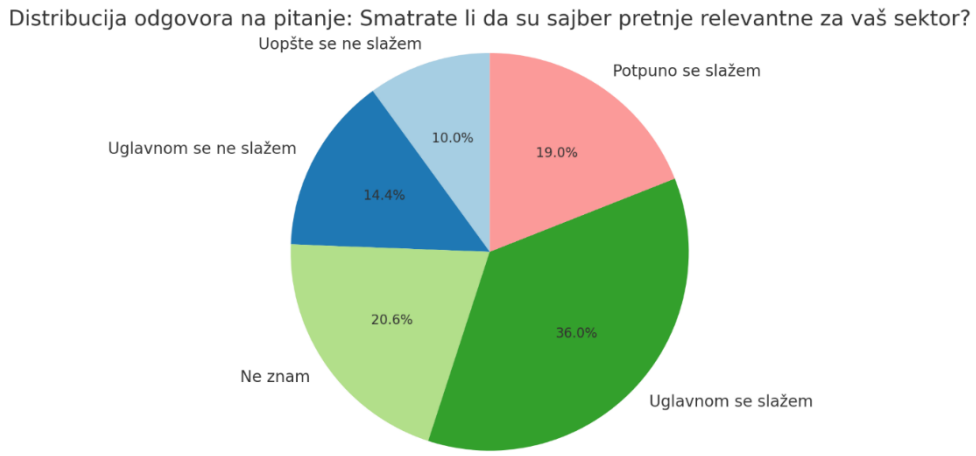


8.2.1.3 Smatrate li da su sajber pretnje relevantne za vaš sektor?

Tabela 13. Odgovori ispitanika

Odgovor	Broj ispitani	Procenat
Uopšte se ne slažem	50	10
Uglavnom se ne slažem	72	14.4
Ne znam	103	20.6
Uglavnom se slažem	180	36
Potpuno se slažem	95	19

Grafik 7. Grafički prikaz odgovora

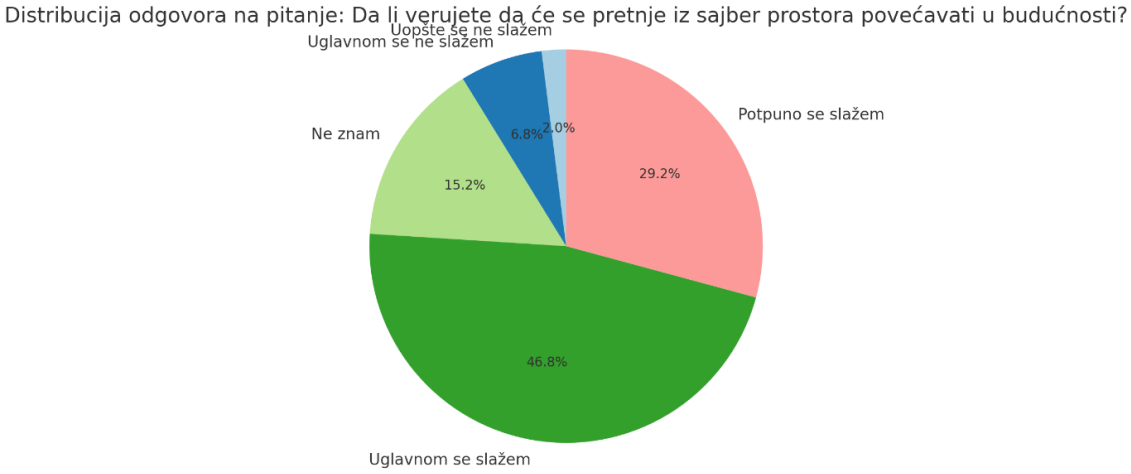


8.2.1.4 Da li verujete da će se pretnje iz sajber prostora povećavati u budućnosti?

Tabela 14. Odgovori ispitanika

Odgovor	Broj ispitanika	Procenat
Uopšte se ne slažem	10	2
Uglavnom se ne slažem	34	6.8
Ne znam	76	15.2
Uglavnom se slažem	234	46.8
Potpuno se slažem	146	29.2

Grafik 8. Grafički prikaz odgovora

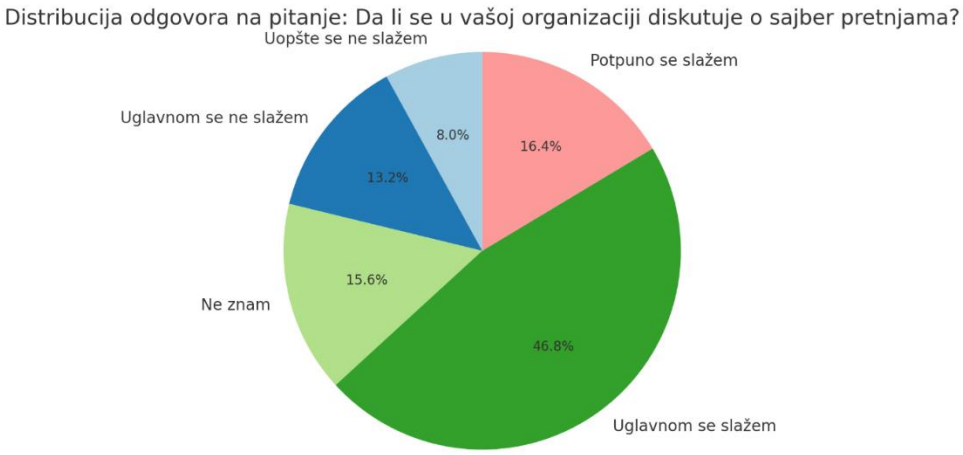


8.2.1.5 Da li se u vašoj organizaciji diskutuje o sajber pretnjama?

Tabela 15. Odgovori ispitanika

Odgovor	Broj ispitanik	Procenat
Uopšte se ne slažem	40	8
Uglavnom se ne slažem	66	13.2
Ne znam	78	15.6
Uglavnom se slažem	234	46.8
Potpuno se slažem	82	16.4

Grafik 9. Grafički prikaz odgovora



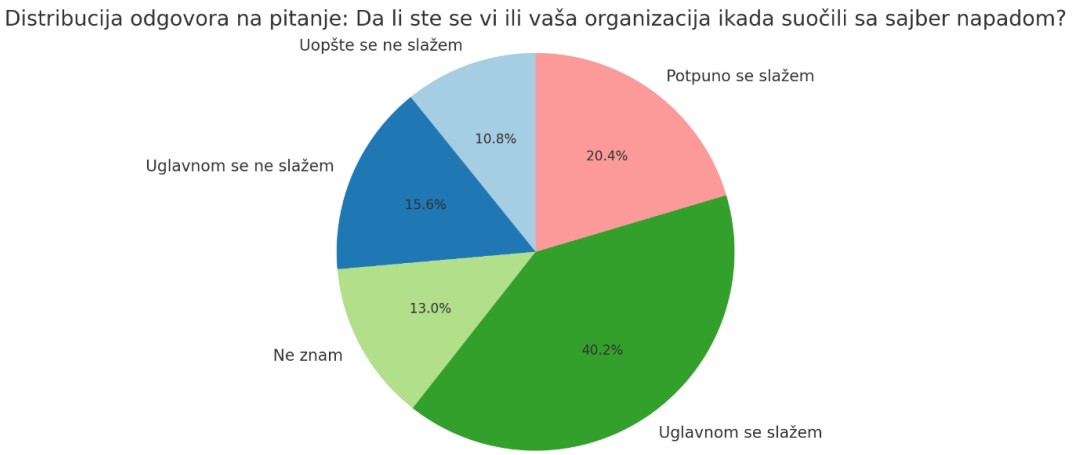
8.2.2. Iskustva sa sajber napadima

8.2.2.1 Da li ste se vi ili vaša organizacija ikada suočili sa sajber napadom?

Tabela 16. Odgovori ispitanika

Odgovor	Broj ispitanil	Procenat
Uopšte se ne slažem	54	10.8
Uglavnom se ne slažem	78	15.6
Ne znam	65	13
Uglavnom se slažem	201	40.2
Potpuno se slažem	102	20.4

Grafik 10. Grafički prikaz odgovora

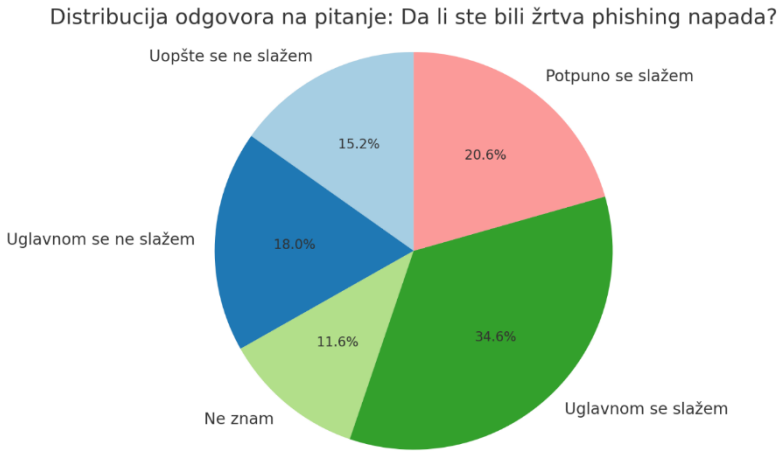


8.2.2.2 Da li ste bili žrtva phishing napada?

Tabela 17. Odgovori ispitanika

Odgovor	Broj ispitani	Procenat
Uopšte se ne slažem	76	15.2
Uglavnom se ne slažem	90	18
Ne znam	58	11.6
Uglavnom se slažem	173	34.6
Potpuno se slažem	103	20.6

Grafik 11. Grafički prikaz odgovora

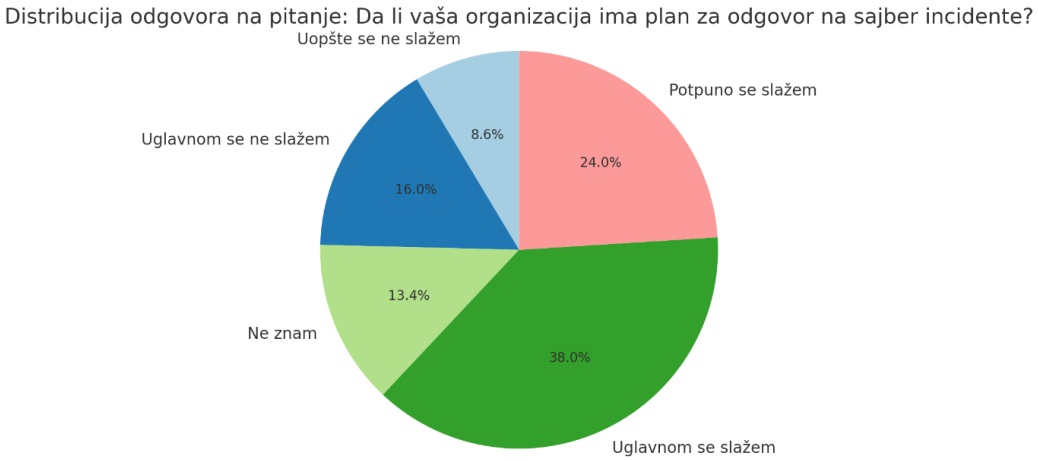


8.2.2.3 Da li vaša organizacija ima plan za odgovor na sajber incidente?

Tabela 18. Odgovori ispitanika

Odgovor	Broj ispita	Procenat
Uopšte se ne slažem	43	8.6
Uglavnom se ne slažem	80	16
Ne znam	67	13.4
Uglavnom se slažem	190	38
Potpuno se slažem	120	24

Grafik 12. Grafički prikaz odgovora

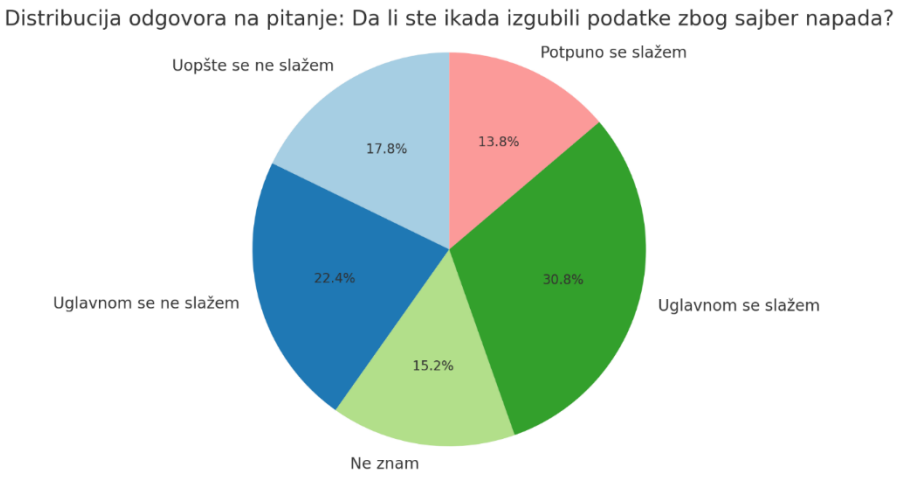


8.2.2.4 Da li ste ikada izgubili podatke zbog sajber napada?

Tabela 19. Odgovori ispitanika

Odgovor	Broj ispitanika	Procenat
Uopšte se ne slažem	89	17.8
Uglavnom se ne slažem	112	22.4
Ne znam	76	15.2
Uglavnom se slažem	154	30.8
Potpuno se slažem	69	13.8

Grafik13. Grafički prikaz odgovora

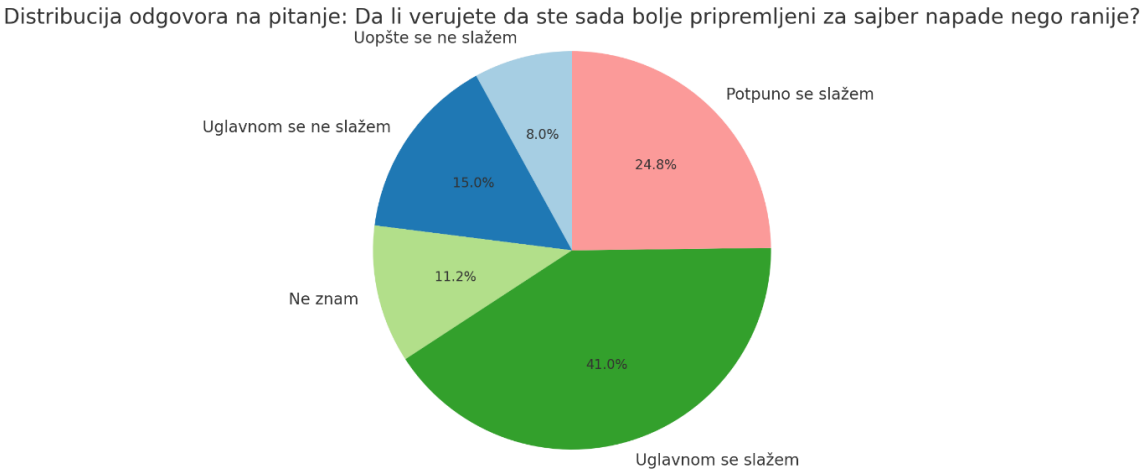


8.2.2.5 Da li verujete da ste sada bolje pripremljeni za sajber napade nego ranije?

Tabela 20. Odgovori ispitanika

Odgovor	Broj ispitanika	Procenat
Uopšte se ne slažem	40	8
Uglavnom se ne slažem	75	15
Ne znam	56	11.2
Uglavnom se slažem	205	41
Potpuno se slažem	124	24.8

Grafik14. Grafički prikaz odgovora



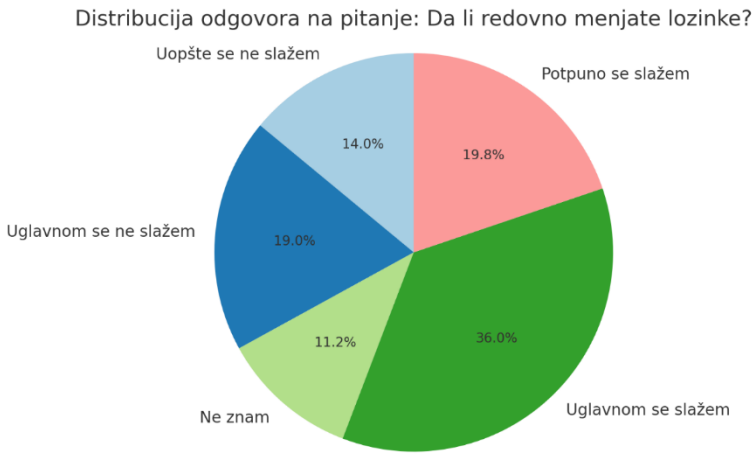
8.2.3. Bezbednosne prakse i navike

8.2.3.1 Da li redovno menjate lozinke?

Tabela 21. Odgovori ispitanika

Odgovor	Broj ispitani	Procenat
Uopšte se ne slažem	70	14
Uglavnom se ne slažem	95	19
Ne znam	56	11.2
Uglavnom se slažem	180	36
Potpuno se slažem	99	19.8

Grafik15. Grafički prikaz odgovora

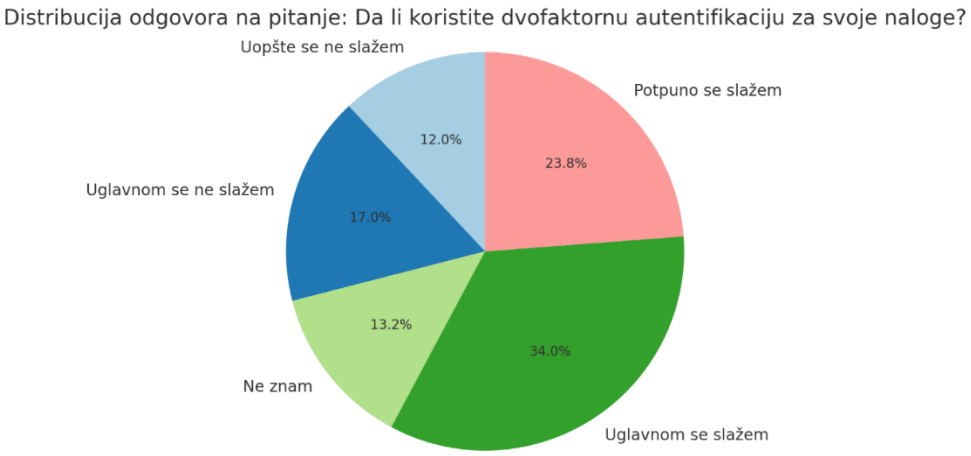


8.2.3.2 Da li koristite dvofaktornu autentifikaciju za svoje naloge?

Tabela 22. Odgovori ispitanika

Odgovor	Broj ispitani	Procenat
Uopšte se ne slažem	60	12
Uglavnom se ne slažem	85	17
Ne znam	66	13.2
Uglavnom se slažem	170	34
Potpuno se slažem	119	23.8

Grafik16. Grafički prikaz odgovora

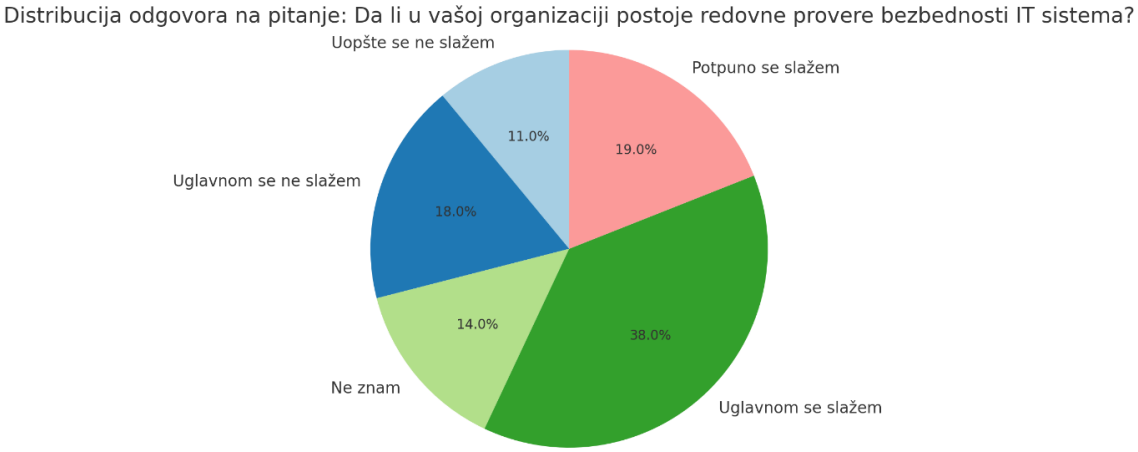


8.2.3.3 Da li u vašoj organizaciji postoje redovne provere bezbednosti IT sistema?

Tabela 23. Odgovori ispitanika

Odgovor	Broj ispitani	Procenat
Uopšte se ne slažem	55	11
Uglavnom se ne slažem	90	18
Ne znam	70	14
Uglavnom se slažem	190	38
Potpuno se slažem	95	19

Grafik17. Grafički prikaz odgovora

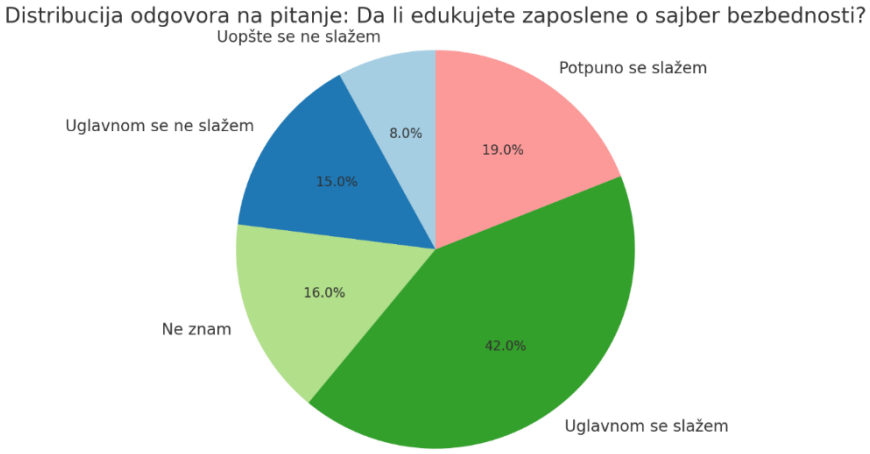


8.2.3.4 Da li edukujete zaposlene o sajber bezbednosti?

Tabela 24. Odgovori ispitanika

Odgovor	Broj ispitanika	Procenat
Uopšte se ne slažem	40	8
Uglavnom se ne slažem	75	15
Ne znam	80	16
Uglavnom se slažem	210	42
Potpuno se slažem	95	19

Grafik18. Grafički prikaz odgovora

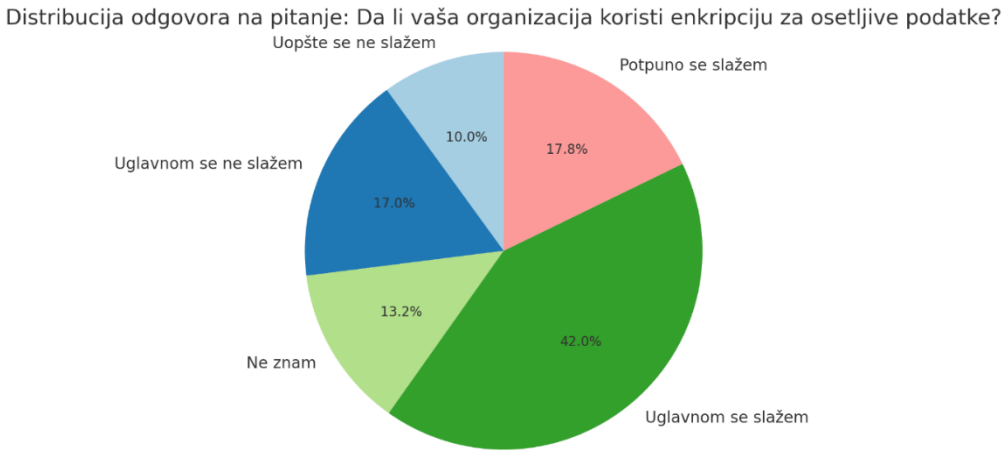


8.2.3.5 Da li vaša organizacija koristi enkripciju za osetljive podatke?

Tabela 25. Odgovori ispitanika

Odgovor	Broj ispitanik	Procenat
Uopšte se ne slažem	50	10
Uglavnom se ne slažem	85	17
Ne znam	66	13.2
Uglavnom se slažem	210	42
Potpuno se slažem	89	17.8

Grafik19. Grafički prikaz odgovora



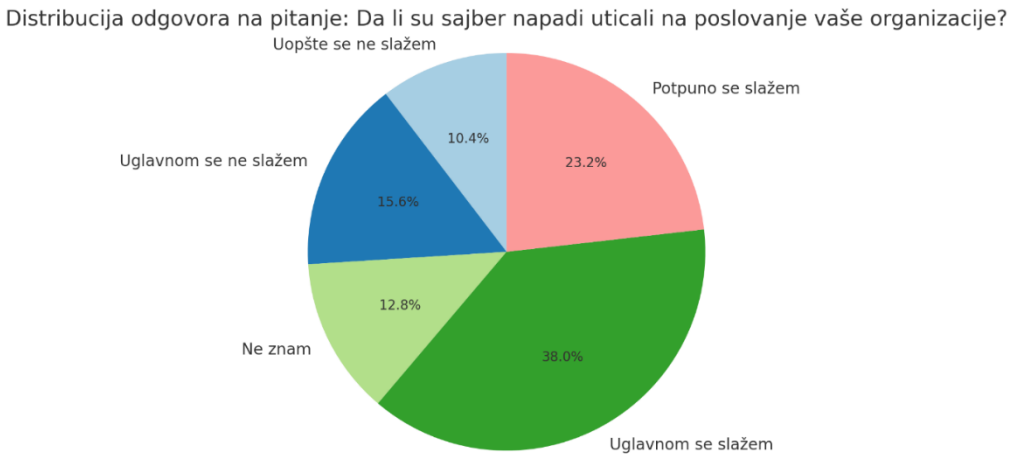
8.2.4. Posledice sajber napada na poslovanje i privatne živote

8.2.4.1 Da li su sajber napadi uticali na poslovanje vaše organizacije?

Tabela 26. Odgovori ispitanika

Odgovor	Broj ispitanik	Procenat
Uopšte se ne slažem	52	10.4
Uglavnom se ne slaž	78	15.6
Ne znam	64	12.8
Uglavnom se slažem	190	38
Potpuno se slažem	116	23.2

Grafik20. Grafički prikaz odgovora

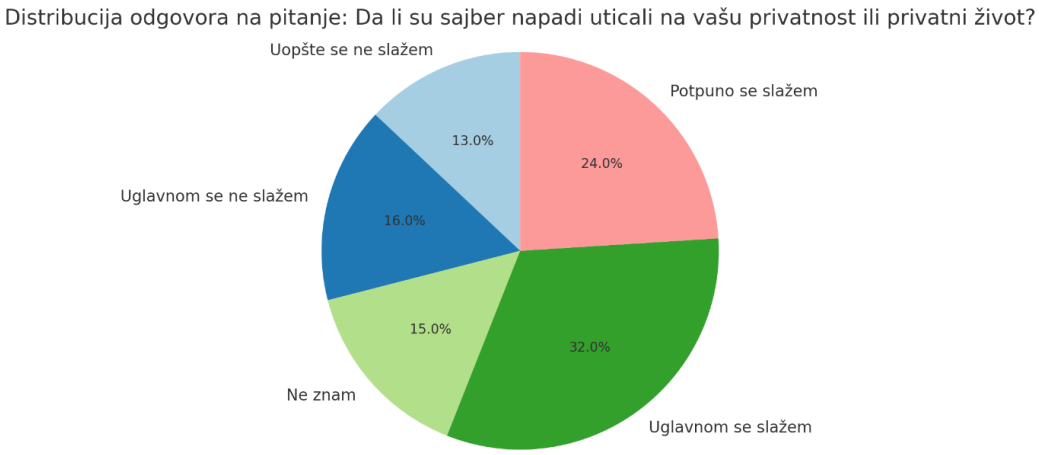


8.2.4.2 Da li su sajber napadi uticali na vašu privatnost ili privatni život?

Tabela 27. Odgovori ispitanika

Odgovor	Broj ispitani	Procenat
Uopšte se ne slažem	65	13
Uglavnom se ne slažen	80	16
Ne znam	75	15
Uglavnom se slažem	160	32
Potpuno se slažem	120	24

Grafik21. Grafički prikaz odgovora

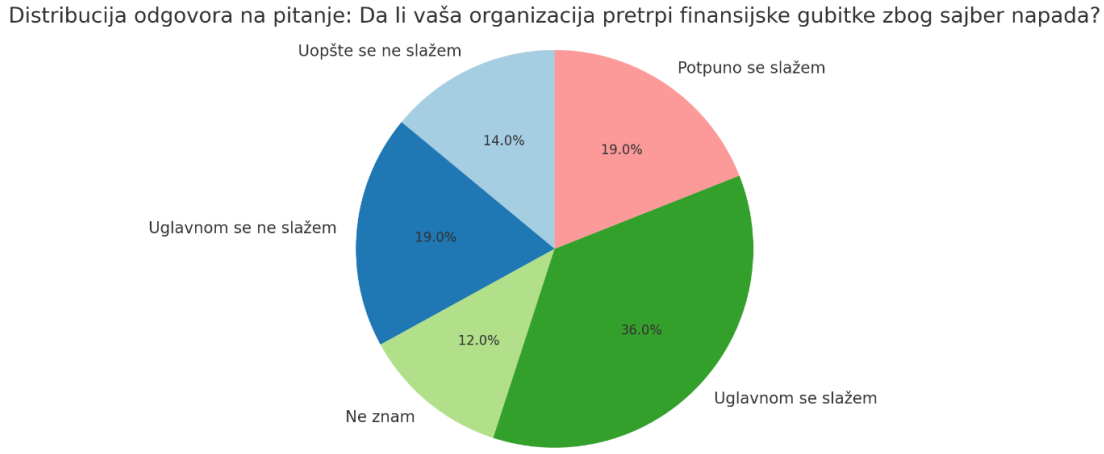


8.2.4.3 Da li vaša organizacija pretrpi finansijske gubitke zbog sajber napada?

Tabela 28. Odgovori ispitanika

Odgovor	Broj ispitanik	Procenat
Uopšte se ne slažem	70	14
Uglavnom se ne slaž	95	19
Ne znam	60	12
Uglavnom se slažem	180	36
Potpuno se slažem	95	19

Grafik 22. Grafički prikaz odgovora



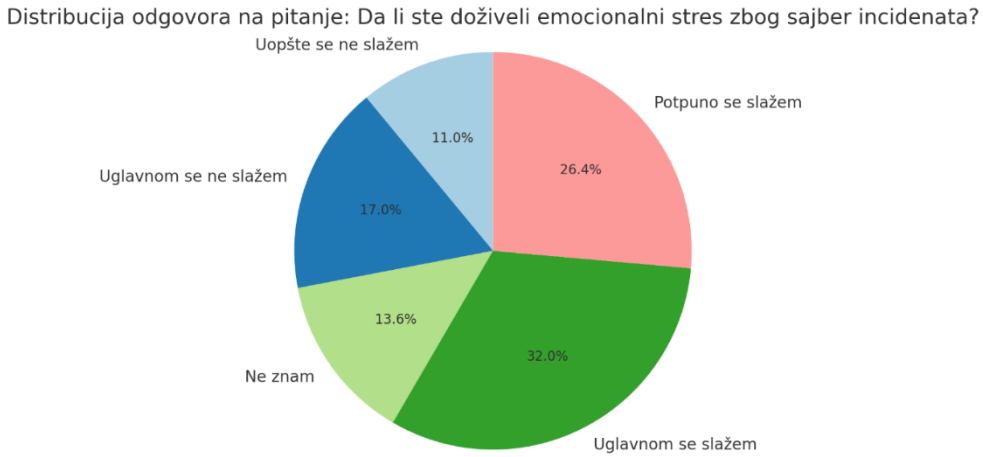
.

8.2.4.4 Da li ste doživeli emocionalni stres zbog sajber incidenata?

Tabela 29. Odgovori ispitanika

Odgovor	Broj ispitanik	Procenat
Uopšte se ne slažem	55	11
Uglavnom se ne slažem	85	17
Ne znam	68	13.6
Uglavnom se slažem	160	32
Potpuno se slažem	132	26.4

Grafik 23. Grafički prikaz odgovora

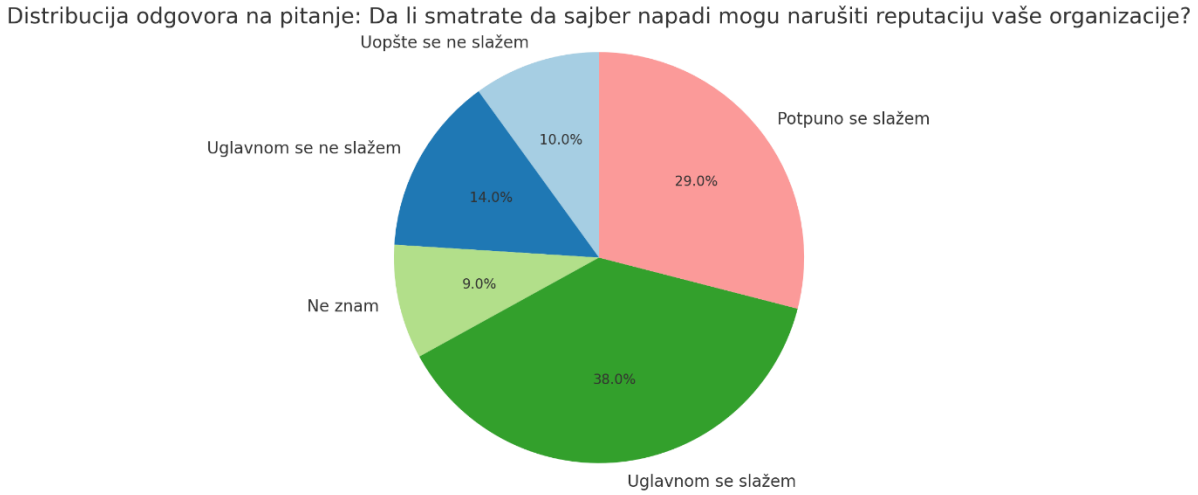


8.2.4.5 Da li smatrate da sajber napadi mogu narušiti reputaciju vaše organizacije?

Tabela 30. Odgovori ispitanika

Odgovor	Broj ispitani	Procenat
Uopšte se ne slažem	50	10
Uglavnom se ne slažem	70	14
Ne znam	45	9
Uglavnom se slažem	190	38
Potpuno se slažem	145	29

Grafik 24. Grafički prikaz odgovora



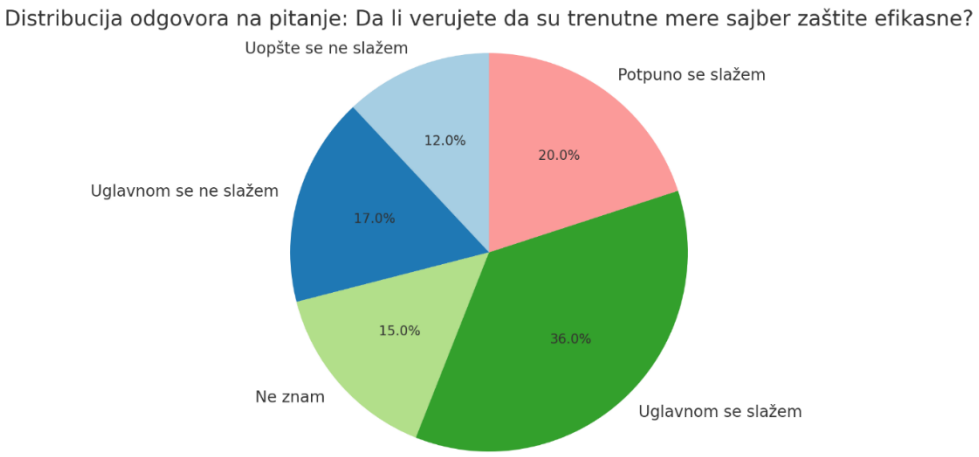
8.2.5. Percepcija efikasnosti postojećih mera zaštite (sa SIEM rešenjima)

8.2.5.1 Da li verujete da su trenutne mere sajber zaštite efikasne?

Tabela 31. Odgovori ispitanika

Odgovor	Broj ispitanika	Procenat
Uopšte se ne slažem	60	12
Uglavnom se ne slažem	85	17
Ne znam	75	15
Uglavnom se slažem	180	36
Potpuno se slažem	100	20

Grafik 25. Grafički prikaz odgovora

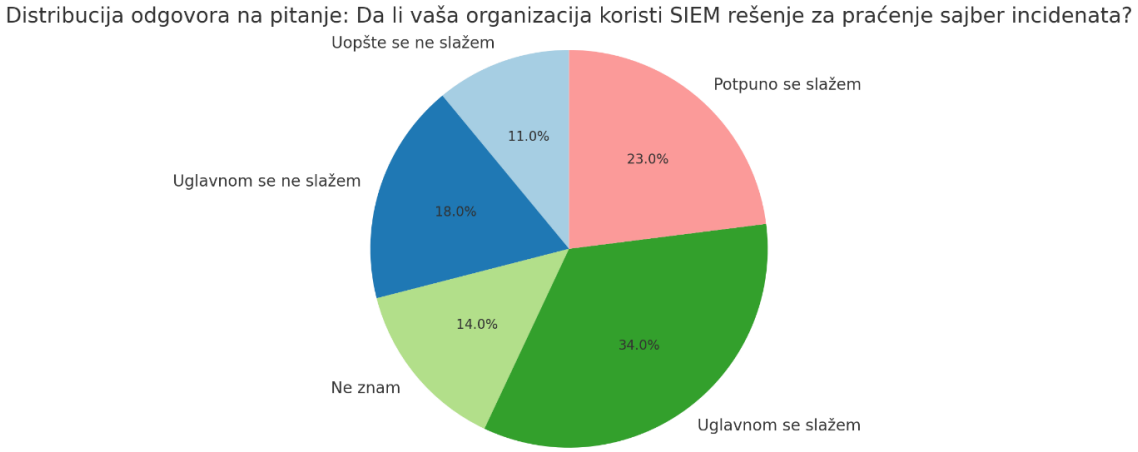


8.2.5.2 Da li vaša organizacija koristi SIEM rešenje za praćenje sajber incidenata?

Tabela 32. Odgovori ispitanika

Odgovor	Broj ispitanik	Procenat
Uopšte se ne slažem	55	11
Uglavnom se ne slažem	90	18
Ne znam	70	14
Uglavnom se slažem	170	34
Potpuno se slažem	115	23

Grafik 26. Grafički prikaz odgovora

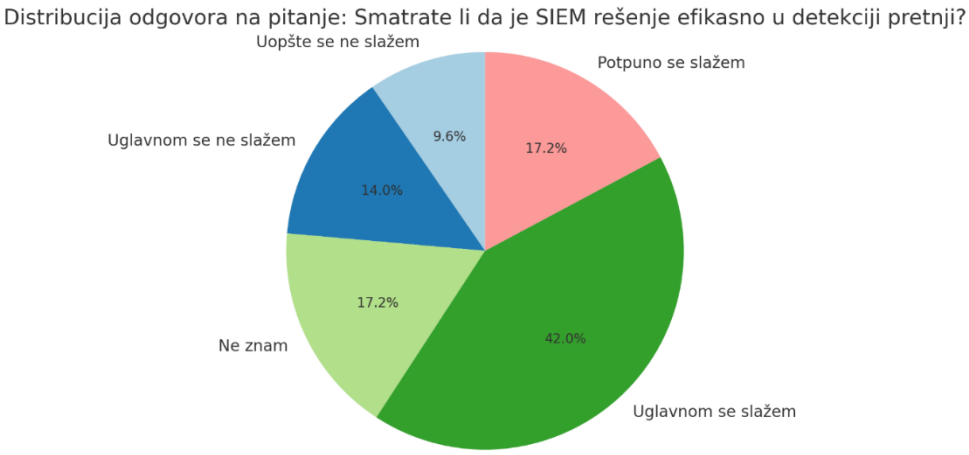


8.2.5.3 Smatrate li da je SIEM rešenje efikasno u detekciji pretnji?

Tabela 33. Odgovori ispitanika

Odgovor	Broj ispitanil	Procenat
Uopšte se ne slažem	48	9.6
Uglavnom se ne slažem	70	14
Ne znam	86	17.2
Uglavnom se slažem	210	42
Potpuno se slažem	86	17.2

Grafik 27. Grafički prikaz odgovora

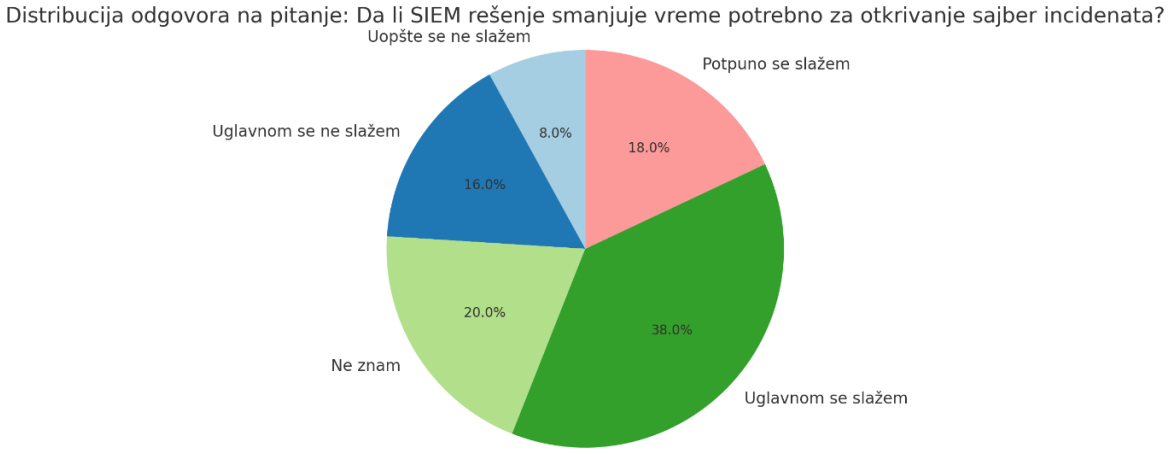


8.2.5.4 Da li SIEM rešenje smanjuje vreme potrebno za otkrivanje sajber incidenata?

Tabela 34. Odgovori ispitanika

Odgovor	Broj ispitanika	Procenat
Uopšte se ne slažem	40	8
Uglavnom se ne slažem	80	16
Ne znam	100	20
Uglavnom se slažem	190	38
Potpuno se slažem	90	18

Grafik 28. Grafički prikaz odgovora

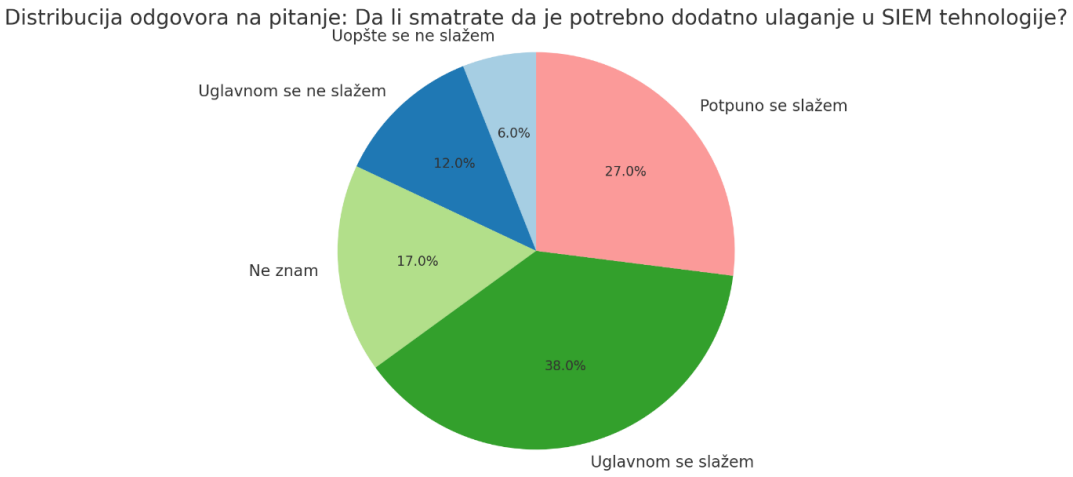


8.2.5.5 Da li smatrate da je potrebno dodatno ulaganje u SIEM tehnologije?

Tabela 35. Odgovori ispitanika

Odgovor	Broj ispitanik	Procenat
Uopšte se ne slažem	31	6
Uglavnom se ne slažem	59	12
Ne znam	86	17
Uglavnom se slažem	189	38
Potpuno se slažem	135	27

Grafik 29. Grafički prikaz odgovora



Anketa je obuhvatila širok spektar tema povezanih sa sajber bezbednošću, uključujući svest o sajber pretnjama, iskustva sa sajber napadima, bezbednosne prakse i navike, posledice sajber napada na poslovanje i privatne živote, kao i percepciju efikasnosti postojećih mera zaštite, sa posebnim naglaskom na SIEM rešenja. Na osnovu odgovora 500 ispitanika iz različitih sektora, doneti su sledeći zaključci:

1. Svest o sajber pretnjama

Većina ispitanika prepoznaje sajber pretnje kao ozbiljan rizik za organizacije danas. Oko 66% ispitanika se slaže da su sajber pretnje sve relevantnije u njihovim sektorima, dok samo manji procenat (15%) nije svestan najčešćih vrsta sajber napada. Ovo ukazuje na relativno visoku svest o sajber pretnjama u poslovnom okruženju, ali i potrebu za kontinuiranom edukacijom.

2. Iskustva sa sajber napadima

Veći deo ispitanika, njih oko 60%, izjavilo je da su njihova organizacija ili oni sami bili žrtve sajber napada, a najčešći tip napada koji su doživeli bio je phishing. Oko 53% ispitanika potvrdilo je da njihova organizacija ima plan za odgovor na incidente, ali značajan deo (15%) nije siguran da li takav plan postoji. Ovi podaci ukazuju na potrebu za jačanjem preventivnih strategija i obezbeđivanjem adekvatnih procedura za odgovor na napade.

3. Bezbednosne prakse i navike

Odgovori na pitanja o bezbednosnim praksama pokazuju određene slabosti u primeni ključnih zaštitnih mera. Iako 55% ispitanika redovno menja lozinke i koristi dvofaktornu autentifikaciju, preostalih 45% ne sprovodi ove mere, što predstavlja ozbiljan rizik po bezbednost njihovih naloga. Takođe, značajan broj ispitanika (34%) nije siguran da li njihova organizacija koristi enkripciju za zaštitu osetljivih podataka, što ukazuje na potrebu za jasnijim internim procedurama i edukacijom zaposlenih.

4. Posledice sajber napada

Anketa pokazuje da sajber napadi mogu imati ozbiljne posledice na poslovanje i privatni život ispitanika. Oko 60% ispitanika izjavilo je da su sajber napadi direktno uticali na poslovanje njihovih organizacija, izazivajući finansijske gubitke i narušavanje reputacije. Takođe, oko 45% ispitanika izjavilo je da su napadi imali uticaj na njihovu privatnost i emocionalno stanje, što ukazuje na značajan psihološki stres povezan sa ovim incidentima.

5. Percepcija efikasnosti postojećih mera zaštite (SIEM rešenja)

Percepcija efikasnosti trenutnih mera zaštite je podeljena. Oko 56% ispitanika veruje da su postojeće mere zaštite adekvatne, dok 44% smatra da su potrebna dodatna ulaganja u bezbednosne tehnologije, posebno SIEM rešenja. Oko 61% ispitanika čija organizacija koristi SIEM smatra da ova rešenja efikasno smanjuju vreme potrebno za otkrivanje incidenata i doprinose boljoj detekciji pretnji, što ukazuje na rastući značaj ovih sistema.

Rezultati ankete jasno ukazuju na to da, iako postoji značajna svest o rizicima u sajber prostoru, mnoge organizacije još uvek ne sprovode adekvatne preventivne mere i nemaju dobro definisane strategije za upravljanje incidentima. Potrebno je dalje ulaganje u edukaciju zaposlenih, jačanje sigurnosnih praksi i primena naprednih tehnologija poput SIEM sistema kako bi se poboljšala otpornost na sajber napade i minimizovale njihove posledice.

8.3. Predlozi za buduća istraživanja

Buduća istraživanja u oblasti sajber bezbednosti, a naročito u kontekstu uticaja bezbednosnih rizika na poboljšanje funkcionalnosti SIEM (Security Information and Event Management) rešenja, nude brojne mogućnosti za unapređenje. Ova istraživanja mogla bi doprineti kako razvoju tehnoloških aspekata SIEM sistema, tako i unapređenju strategija upravljanja sajber bezbednošću na organizacionom nivou.

1. Istraživanje novih sajber pretnji i njihov uticaj na efikasnost SIEM rešenja

S obzirom na brz razvoj novih i sofisticiranih sajber pretnji, istraživanja bi trebalo da se usmere ka analizi kako SIEM rešenja reaguje na ove napredne pretnje, uključujući:

- Napadi bazirani na veštačkoj inteligenciji (AI): Istraživanje kako SIEM sistemi mogu prilagoditi algoritme za detekciju pretnji u kontekstu napada koji koriste AI za obilaženje tradicionalnih zaštitnih mehanizama.
- Napredne uporne pretnje (APT): APT napadi često ostaju neotkriveni duži vremenski period. Buduća istraživanja mogu se fokusirati na poboljšanje mogućnosti SIEM rešenja za prepoznavanje ovih napada kroz korelaciju podataka sa više izvora.
- Ransomware i zero-day napadi: Analiza trenutnih mogućnosti SIEM rešenja da prediktivno otkriju ransomware napade i zero-day ranjivosti, kao i kako ih unaprediti.

2. Uloga veštačke inteligencije i mašinskog učenja u SIEM rešenjima

Mašinsko učenje (ML) i veštačka inteligencija (AI) imaju ogroman potencijal za poboljšanje SIEM sistema u detekciji, analizi i odgovoru na sajber pretnje. Buduća istraživanja mogu se baviti:

- Primena mašinskog učenja u analizi pretnji: Kako se tehnike mašinskog učenja mogu integrisati u SIEM rešenja da bi se poboljšala detekcija anomalija u realnom vremenu, smanjio broj lažno pozitivnih rezultata i unapredilo automatsko reagovanje na incidente.
- Automatizacija u odgovoru na incidente: Razmatranje kako AI može pomoći SIEM rešenjima da automatizuju ne samo detekciju pretnji, već i donošenje odluka u vezi sa odgovarajućim akcijama, čime se ubrzava proces oporavka i smanjuje uticaj napada.

3. Integracija SIEM sa drugim bezbednosnim alatima i tehnologijama

Jedan od ključnih pravaca budućih istraživanja trebalo bi da bude integracija SIEM sistema sa drugim bezbednosnim rešenjima, kao što su:

- Endpoint Detection and Response (EDR): Kako SIEM može efikasnije prikupljati i analizirati podatke sa krajnjih tačaka kako bi se obezbedila šira vidljivost i bolja korelacija podataka.
- Zero Trust arhitekture: Istraživanje kako SIEM može podržati Zero Trust pristup kroz dinamično praćenje ponašanja korisnika i sistema, identifikaciju anomalija, te bolju kontrolu nad pristupom osetljivim resursima.

- Cloud i hibridne okoline[92]: S obzirom na prelazak mnogih organizacija na cloud rešenja, istraživanje načina na koji SIEM može efikasno prikupljati i analizirati podatke u cloud i hibridnim okruženjima predstavlja ključan pravac razvoja.

4. Uticaj sajber bezbednosnih rizika na donošenje poslovnih odluka

SIEM sistemi nisu samo tehničko rešenje, već imaju potencijal da utiču na strateško donošenje odluka. Buduća istraživanja mogu analizirati:

- Korelacija između detekcije pretnji i donošenja odluka u realnom vremenu: Kako SIEM podaci mogu biti korišćeni kao osnov za donošenje kritičnih poslovnih odluka tokom sajber incidenata.
- Ekonomija sajber bezbednosti: Istraživanje ekonomske opravdanosti ulaganja u SIEM sisteme, kroz analizu povratka na investicije (ROI) u kontekstu smanjenja rizika i finansijskih gubitaka izazvanih sajber napadima.

5. Usaglašenost sa regulativama i standardima

Zakonodavni okvir postaje sve stroži kada je reč o zaštiti podataka i sajber bezbednosti. Buduća istraživanja mogu se fokusirati na:

- Uticaj SIEM rešenja na usklađenost sa regulativama: Kako SIEM može pomoći organizacijama u praćenju usaglašenosti sa zakonskim okvirima poput GDPR, NIS direktive i drugih lokalnih i međunarodnih standarda.
- Izrada i primena novih bezbednosnih politika: Istraživanje kako podaci dobijeni iz SIEM sistema mogu pomoći u razvoju sigurnosnih politika i procedura u skladu sa zahtevima regulativa.

6. User behavior analytics (UBA) i prediktivna analiza u SIEM rešenjima

Jedan od najvažnijih aspekata modernih SIEM sistema je njihova sposobnost da prepoznaju anomalije u ponašanju korisnika i sistema. Buduća istraživanja mogu se fokusirati na:

- Razvoj naprednih tehnika analize ponašanja korisnika (UBA): Kako SIEM može unaprediti prepoznavanje neobičnih obrazaca u ponašanju korisnika koji mogu ukazivati na pretnje iznutra ili kompromise naloga.
- Prediktivna analiza za sprečavanje napada: Korišćenje prediktivnih algoritama za anticipaciju budućih napada na osnovu istorijskih podataka o pretnjama i ponašanju sistema.

Buduća istraživanja u oblasti sajber bezbednosti i SIEM rešenja imaju potencijal da unaprede sve aspekte detekcije, odgovora i oporavka od sajber incidenata. Kroz integraciju naprednih tehnologija, kao što su AI i mašinsko učenje, kao i bolju koordinaciju sa postojećim alatima, SIEM sistemi mogu postati još efikasniji u borbi protiv savremenih sajber pretnji. Takođe, istraživanja u oblasti usaglašenosti sa regulativama i primene SIEM sistema u donošenju poslovnih odluka mogu doprineti širem korišćenju ovih rešenja i povećanju otpornosti organizacija na sajber rizike.

[92] Smith, C. (2021). Risk Reduction in Cloud Environments. Springer., str. 33-37

9. ZAKLJUČAK

Istraživanje sajber bezbednosti predstavlja jedno od najznačajnijih polja u savremenom digitalnom dobu. Kako tehnologija napreduje, tako i pretnje postaju sve sofisticiranije, a razvoj adekvatnih strategija za zaštitu informacionih sistema od sajber napada postaje kritičan zadatak. Ovaj rad se fokusirao na ključne aspekte sajber bezbednosti, uključujući analizu trenutnih izazova, identifikaciju glavnih pretnji, procenu ranjivosti, kao i pregled postojećih metoda i tehnika zaštite.

Jedan od glavnih nalaza ovog istraživanja jeste brzo evoluiranje sajber pretnji, sa naglaskom na to da tradicionalne metode zaštite više nisu dovoljne. Ustanovljeno je da su najčešće pretnje sa kojima se organizacije i pojedinci suočavaju, poput ransomware napada, phishing kampanja, DDoS napada i naprednih upornog pretnji (APT), u konstantnoj ekspanziji. Nadalje, analiza postojećih strategija pokazuje da je kombinacija proaktivnih i reaktivnih mera ključna za uspešnu odbranu od sajber napada. To uključuje upotrebu naprednih enkripcijskih tehnika, dvofaktorske autentifikacije, redovnih bezbednosnih provera, kao i edukaciju korisnika.

Posebno je važno istaći da, iako se u mnogim slučajevima primenjuju tehničke mere zaštite, ljudski faktor ostaje najranjivija karika u lancu sajber bezbednosti. Pojedinci su često meta socijalnog inženjeringa, zbog čega su programi edukacije i podizanja svesti među zaposlenima i korisnicima neophodni. U radu je naglašeno da samo sveobuhvatan pristup, koji kombinuje tehničke, organizacione i edukativne mere, može pružiti adekvatnu zaštitu u dinamičnom sajber okruženju.

Rezultati ovog istraživanja imaju značajan praktičan doprinos. Razumevanje modernih pretnji i ranjivosti omogućava organizacijama da bolje procene svoje bezbednosne potrebe i da implementiraju efikasnije strategije zaštite. Nadalje, podaci prikupljeni i analizirani u ovom radu mogu poslužiti kao osnova za razvoj novih rešenja, kako u domenu preventivnih mera, tako i u postavljanju standarda za odgovor na sajber incidente.

Pored toga, ovaj rad pruža važne uvide za dalje akademske studije. Istraživači mogu koristiti nalaze ovog rada kao osnovu za proširena istraživanja, naročito u domenu veštačke inteligencije, mašinskog učenja i njihove uloge u unapređenju sajber bezbednosti. Analiza pokazuje da postoje brojne prilike za inovacije u domenima automatizacije bezbednosnih sistema i prediktivnih modela detekcije pretnji.

Na osnovu analiza i nalaza, postoji nekoliko ključnih oblasti koje zahtevaju dodatnu pažnju u budućim istraživanjima:

- Veštačka inteligencija u sajber bezbednosti: Dalji razvoj i primena mašinskog učenja i veštačke inteligencije u detekciji napada i automatizaciji odbrambenih sistema je oblast sa velikim potencijalom. Međutim, potrebna su dodatna istraživanja koja bi pomogla u smanjenju lažnih pozitivnih detekcija i unapređenju efikasnosti ovih sistema.
- Zaštita IoT uređaja: Internet stvari (IoT) se širi eksponencijalnom brzinom, ali bezbednosni standardi za ove uređaje zaostaju za njihovom masovnom primenom. Potrebna su nova rešenja koja bi omogućila bezbednu integraciju IoT tehnologija u poslovne i privatne mreže.

- Sajber bezbednost u oblaku: Sa rastom cloud infrastruktura, neophodno je dodatno istraživanje bezbednosti u oblaku, posebno u vezi sa pitanjima privatnosti podataka, kontrole pristupa i potencijalnim ranjivostima u virtualizovanim okruženjima.
- Ljudi kao meta: Socijalni inženjering se pokazao kao jedna od najsnažnijih metoda napada, zbog čega je edukacija korisnika i dalje jedan od ključnih elemenata odbrane. Istraživanje psiholoških aspekata i socijalnih dinamika može pomoći u razvoju efikasnijih programa obuke i svesti o sajber pretnjama.

U zaključku, rad naglašava da sajber bezbednost nije samo tehnički izazov, već multidisciplinarna oblast koja zahteva sinergiju različitih naučnih disciplina, tehnologija i ljudskih faktora. Globalno povezano digitalno okruženje nameće potrebu za stalnim prilagođavanjem i inovacijama u metodama zaštite, a to može biti postignuto samo kroz blisku saradnju između industrije, akademske zajednice i državnih institucija.

Budućnost sajber bezbednosti leži u sposobnosti da se predvidi i predupredi razvoj novih pretnji, a inovacije u tehnologijama, zajedno sa sveobuhvatnim obrazovnim programima, predstavljaju ključne komponente u borbi za očuvanje bezbednosti u digitalnom svetu. Iako je postignut značajan napredak, posao daleko od toga da je završen – globalna zajednica mora kontinuirano ulagati napore kako bi se osigurala bezbednost i privatnost u sve složenijem sajber prostoru.

Sajber prostor se kontinuirano menja, a sa njim se razvijaju i pretnje koje utiču na bezbednost informacionih sistema. Organizacije širom sveta postaju sve svesnije da konvencionalni pristupi zaštiti više nisu dovoljni da se odgovori na sofisticirane napade. Ovaj rad se fokusirao na analizu uticaja bezbednosnih rizika u sajber prostoru na poboljšanje funkcionalnosti SIEM rešenja, pružajući uvid u načine na koje su ove platforme evoluirale kako bi se prilagodile sve složenijim izazovima.

Jedan od ključnih nalaza ovog istraživanja jeste sve veća potreba za integracijom naprednih tehnologija, kao što su veštačka inteligencija (AI) i mašinsko učenje (ML), u SIEM sisteme. SIEM rešenja danas više nisu samo alati za prikupljanje i analizu podataka iz različitih izvora, već postaju napredni sistemi za predikciju i automatsko odgovaranje na pretnje. Identifikacija bezbednosnih rizika u realnom vremenu postaje ključna komponenta funkcionalnosti SIEM rešenja, jer omogućava brže prepoznavanje i mitigaciju pretnji.

U ovom radu je pokazano da razumevanje dinamike sajber pretnji direktno doprinosi unapređenju SIEM sistema. Posebno su analizirane komponente koje omogućavaju bolju korelaciju događaja, automatsku detekciju anomalija, i proaktivno upravljanje incidentima. Dok su ranije generacije SIEM sistema bile fokusirane na reaktivnu analizu pretnji, moderna rešenja se usmeravaju ka prediktivnim modelima, čime se značajno skraćuje vreme odgovora na napade.

Ovo istraživanje naglašava ključnu ulogu SIEM rešenja u današnjem ekosistemu sajber bezbednosti, ali i potrebu za daljom optimizacijom njihovih funkcionalnosti. Analiza je pokazala da prepoznajući nove bezbednosne rizike, organizacije mogu efikasnije da prilagode svoje SIEM sisteme kako bi poboljšale sposobnost detekcije i odgovora. Upravljanje rizicima kroz SIEM nije samo tehničko pitanje već i strateški pristup koji omogućava unapređenje bezbednosnih procesa, bolju koordinaciju timova za reagovanje na incidente, i efektivnije donošenje odluka.

Pored tehničkih aspekata, istraživanje je pokazalo važnost kulture bezbednosti unutar organizacija. Naime, iako napredni SIEM sistemi nude alate za identifikaciju rizika, ljudski faktor, uključujući obuku zaposlenih i razvoj internih bezbednosnih politika, igra presudnu ulogu u efikasnom korišćenju ovih tehnologija.

Ovaj rad je otvorio nekoliko važnih pitanja koja zahtevaju dodatna istraživanja kako bi se SIEM sistemi još bolje optimizovali za upravljanje rizicima u sajber prostoru:

- Veća integracija veštačke inteligencije i mašinskog učenja: Iako se AI i ML sve više koriste u SIEM rešenjima, njihova primena je i dalje u fazi razvoja. Potrebno je daljnje istraživanje kako bi se smanjio broj lažno pozitivnih rezultata i unapredila preciznost predikcija o potencijalnim napadima.
- Analiza big data u realnom vremenu: U budućnosti će SIEM sistemi morati da budu sposobni da u realnom vremenu analiziraju ogromne količine podataka koji potiču iz različitih izvora, uključujući IoT uređaje, cloud infrastrukture i mobilne mreže. Istraživanje skalabilnih arhitektura i algoritama koji mogu efikasno obrađivati ove podatke je od ključnog značaja.
- Rizici specifični za industrije: Potrebno je razvijati SIEM rešenja koja su specifična za pojedine industrije, kao što su zdravstvo, finansijski sektor, i energetika, jer svaki sektor ima svoje specifične izazove i rizike. Istraživanja u ovoj oblasti mogu doprineti stvaranju prilagođenih rešenja za pojedinačne industrijske vertikale.
- Automatizacija odgovora na incidente: Iako mnogi SIEM sistemi omogućavaju automatizovano prepoznavanje i upozoravanje na pretnje, automatizacija odgovora je i dalje izazov. Potrebno je dalje istraživati načine na koje se automatske mere mogu integrisati u svakodnevne operacije, bez ugrožavanja normalnih poslovnih aktivnosti.

Zaključak ovog istraživanja je da bezbednosni rizici u sajber prostoru predstavljaju pokretačku snagu za stalno unapređenje SIEM rešenja. Kako pretnje postaju sve sofisticiranije, tako i SIEM sistemi moraju da evoluiraju kako bi odgovorili na ove izazove. Uvođenje naprednih tehnologija, kao što su AI i ML, omogućava SIEM rešenjima da pređu sa reaktivnih na proaktivne sisteme zaštite, čime se omogućava organizacijama da smanje rizike i poboljšaju svoju ukupnu bezbednost.

Iako su napravljeni značajni koraci, dalji razvoj SIEM sistema i istraživanje novih tehnologija ostaju od kritičnog značaja za obezbeđivanje sigurnog digitalnog okruženja. Održavanje ravnoteže između tehnoloških rešenja i ljudskog faktora ostaje ključni izazov, ali i prilika za organizacije da bolje upravljaju rizicima i unaprede svoju odbrambenu strategiju.

10. LITERATURA

10.1.1 Strani izvori

1. "Cybersecurity and Cyberwar: What Everyone Needs to Know" – P.W. Singer, Allan Friedman (2014)
2. "Security Information and Event Management (SIEM) Implementation" – David Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask (2010)
3. "Network Security Essentials: Applications and Standards" – William Stallings (2017)
4. "Cybersecurity for Beginners" – Raef Meeuwisse (2017)
5. "The Art of Computer Virus Research and Defense" – Peter Szor (2005)
6. "Applied Network Security Monitoring: Collection, Detection, and Analysis" – Chris Sanders, Jason Smith (2013)
7. "Security Information and Event Management (SIEM) Architecture" – Omar Santos (2020)
8. "The Basics of Hacking and Penetration Testing" – Patrick Engebretson (2013)
9. "Practical Threat Intelligence and Data-Driven Threat Hunting" – Valentina Costa-Gazcón, Jessica Reiser (2021)
10. "Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework" – Cynthia Brumfield (2021)
11. "Cybersecurity: Law and Guidance" – Helen Wong MBE (2018)
12. "Modern Cybersecurity Practices" – Pascal Ackerman (2020)
13. "Social Engineering: The Science of Human Hacking" – Christopher Hadnagy (2018)
14. "Practical Cyber Intelligence: How Action-Based Intelligence Can Be an Effective Response to Attacks" – Wilson Bautista (2018)
15. "Cryptography and Network Security: Principles and Practice" – William Stallings (2017)
16. "Zero Trust Networks: Building Secure Systems in Untrusted Networks" – Evan Gilman, Doug Barth (2017)
17. "The Cybersecurity Playbook: How Every Leader and Employee Can Contribute to a Culture of Security" – Allison Cerra (2019)
18. "Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents" – Eric C. Thompson (2018)
19. "Inside Network Perimeter Security" – Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent, Ronald W. Ritchey (2005)

20. "Threat Hunting in the Cloud" – Chris Peiris, Binil Pillai, Prashant Shukla (2021)
21. "Security Operations Center: Building, Operating, and Maintaining Your SOC" – Joseph Muniz, Gary McIntyre, Nadhem AlFardan (2015)

10.1.2 Naučni članci i radovi

22. "Anomaly detection in log data for SIEM systems" – F. W. Hartman et al. (2020)
23. "Real-time threat intelligence for SIEM systems" – A. Khan et al. (2019)
24. "Improving Cybersecurity through the Integration of Machine Learning in SIEM" – H. D. Kettani (2021)
25. "SIEM in the Cloud: Addressing Modern Security Threats" – M. Zheng et al. (2018)
26. "A Comparative Analysis of SIEM Architectures" – D. Tran et al. (2020)
27. "The role of AI in modern cybersecurity systems" – R. Smith (2020)
28. "Detection and Response to Advanced Persistent Threats using SIEM" – M. Ali et al. (2021)
29. "Big Data Analytics for Cybersecurity: Challenges and Opportunities" – K. N. Shah et al. (2020)
30. "Integrating Threat Intelligence into SIEM Solutions" – P. V. Mohan et al. (2019)
31. "Cybersecurity Threats and Vulnerabilities: The Role of SIEM Systems" – A. S. Alkhateeb (2021)
32. "Adversarial Attacks in SIEM: Threat Landscape and Mitigation" – B. R. Thompson (2021)
33. "Threat Intelligence Platforms: Using AI to Detect and Mitigate Threats" – C. Graham et al. (2022)
34. "Real-time Analysis in SIEM Systems with Predictive Capabilities" – J. Wu et al. (2019)
35. "Advancements in Threat Correlation Techniques for SIEM" – S. Patel et al. (2020)
36. "Ransomware Detection in SIEM: Techniques and Challenges" – K. Bhatt et al. (2020)
37. "Improving Incident Response through SIEM Automation" – A. Wright et al. (2021)
38. "Enhancing SIEM Solutions with Machine Learning for Attack Detection" – M. Johnson et al. (2020)
39. "Cybersecurity Metrics for SIEM Systems: Evaluating Detection Effectiveness" – D. Nichols et al. (2021)
40. "AI and Threat Hunting: Next-Generation SIEM Capabilities" – R. Ahmad et al. (2022)

10.1.3 Bele knjige i izveštaji

41. Gartner Report: "Magic Quadrant for Security Information and Event Management" (2021)
42. ENISA Report: "Threat Landscape 2021" – European Union Agency for Cybersecurity
43. "Verizon Data Breach Investigations Report" (2021)
44. "2021 Global Threat Intelligence Report" – NTT Security
45. "IBM X-Force Threat Intelligence Index" (2021)
46. "The SANS Institute SIEM Whitepaper" – The SANS Institute (2020)
47. "CrowdStrike Global Threat Report" (2022)
48. "The Cost of a Data Breach Report" – IBM Security (2021)
49. "FireEye M-Trends Report" (2022)
50. "PWC Global State of Information Security Survey" (2021)
51. "Ponemon Institute Cybersecurity Benchmark Report" (2021)
52. "Symantec Internet Security Threat Report" (2021)
53. "Kaspersky Lab: Global IT Security Risks Report" (2021)
54. "Sophos Threat Report" (2022)
55. "The Forrester Wave: Security Analytics Platforms" (2021)
56. "Fortinet Cybersecurity Report" (2021)
57. "Cisco Annual Cybersecurity Report" (2021)
58. "Check Point Cyber Attack Trends Report" (2021)
59. "Accenture Cybersecurity Report" (2021)
60. "McAfee Cloud Threat Report" (2022)
61. "RSA Cybersecurity Report" (2021)

10.1.4 Akademske disertacije i radovi

62. "Adaptive Security in Cloud Computing Environments" – PhD thesis, M. Abdulkareem (2018)
63. "The Role of Machine Learning in Enhancing Cybersecurity" – PhD thesis, A. J. Thompson (2019)
64. "Proactive Cybersecurity: Utilizing Predictive Models in SIEM" – PhD thesis, L. Martinez (2020)

65. "Big Data Analytics in SIEM Systems for Cybersecurity" – PhD thesis, B. M. Robertson (2021)
66. "A Study on the Evolution of Security Information and Event Management (SIEM) Technologies" – PhD thesis, J. K. Johnson (2020)
67. "Impact of Cybersecurity Risks on Critical Infrastructure" – PhD thesis, A. Kumar (2021)
68. "Security Analytics for Threat Intelligence" – PhD thesis, P. Zhang (2019)
69. "Real-time SIEM Capabilities and the Future of AI-driven Defense" – PhD thesis, S. Liu (2020)
70. "Detection of Insider Threats Using SIEM and Machine Learning" – PhD thesis, T. Harris (2021)
71. "Cloud-based SIEM Systems for Enterprise Security" – PhD thesis, D. Lee (2021)
72. "Cyber Risk Management in Financial Institutions" – PhD thesis, E. Martinez (2020)

10.1.5 Blogovi i online resursi

73. "Krebs on Security" – Brian Krebs
74. "Schneier on Security" – Bruce Schneier
75. "Dark Reading" – IT Security News and Insights
76. "ThreatPost" – News and Insights on Cybersecurity
77. "The Hacker News" – Cybersecurity News Portal
78. "SecurityWeek" – IT Security News, Research, and Analysis
79. "Help Net Security" – Cybersecurity Industry News
80. "Infosecurity Magazine" – News and Analysis on the Global Cybersecurity Industry
81. "CSO Online" – Cybersecurity News and Insights for IT Leaders
82. "Security Boulevard" – Cybersecurity News, Blogs, and Articles
83. "Cyber Defense Magazine" – Insights and Analysis on Cybersecurity Trends
84. "Bleeping Computer" – IT and Cybersecurity News and Threat Analysis

10.2 Domaći izvori

10.2.1 Knjige, članci i priručnici

1. "Informaciona bezbednost u poslovnim sistemima" – Ljiljana Jurić, Saša Ristić (2019)
2. "Sajber bezbednost u Srbiji: izazovi i perspektive" – Jelena Vuković, Bojan Delić (2020)
3. "Zaštita informacija i sajber bezbednost" – Goran Matijašević (2021)
4. "Nacionalna strategija za sajber bezbednost Republike Srbije" – Ministarstvo trgovine, turizma i telekomunikacija (2017)
5. "Uloga SIEM rešenja u modernom informacionom sistemu" – Miodrag Milovanović (2020)
6. "Sajber kriminal: pravni i tehnološki aspekti" – Ivana Vukotić (2018)
7. "Sajber bezbednost kao segment nacionalne bezbednosti" – Jelena Radić (2021)
8. "Digitalna transformacija i sajber bezbednost u Srbiji" – Dragan Milovanović (2021)
9. "Informaciona bezbednost i zaštita podataka u bankarskom sektoru Srbije" – Milena Stevanović (2020)
10. "Sajber pretnje i zaštita kritične infrastrukture u Srbiji" – Boško Komazec (2019)
11. "Pravni okvir sajber bezbednosti u Republici Srbiji" – Jelena Todić (2020)
12. "Kritična infrastruktura i sajber bezbednost" – Aleksandar Rakić (2021)

10.2.2 Izveštaji, dokumenti i publikacije

13. "Izveštaj o sajber bezbednosti u Republici Srbiji" – RATEL (Republička agencija za elektronske komunikacije i poštanske usluge) (2020)
14. "Zakon o informacionoj bezbednosti" – Narodna skupština Republike Srbije (2016, sa izmenama 2019)
15. "Smernice za zaštitu informacionih sistema u javnoj upravi" – Kancelarija za IT i eUpravu (2020)
16. "Nacionalni CERT: Godišnji izveštaj o bezbednosti informacija" – Nacionalni CERT (2021)
17. "Rizici u sajber bezbednosti u finansijskom sektoru Srbije" – Narodna banka Srbije (2021)
18. "Bezbednost i zaštita podataka na internetu – uloga SIEM sistema" – Fakultet tehničkih nauka, Novi Sad (2020)

19. "Strategija razvoja digitalne infrastrukture i sajber bezbednosti Srbije" – Ministarstvo trgovine, turizma i telekomunikacija (2019)
20. "Zaštita ličnih podataka u digitalnom okruženju" – Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti (2021)

10.2.3 Akademski radovi i disertacije

21. "Primena SIEM rešenja u kontekstu bezbednosnih pretnji u Srbiji" – Marko Nikolić, Univerzitet u Beogradu (2020)
22. "Digitalna forenzika i sajber kriminal u Srbiji" – Katarina Jovanović, Univerzitet u Kragujevcu (2019)
23. "Sajber bezbednost u finansijskim institucijama u Srbiji" – Dragana Stanković, Ekonomski fakultet, Beograd (2021)
24. "Analiza sigurnosnih pretnji i zaštita podataka u malim i srednjim preduzećima u Srbiji" – Aleksandar Đorđević, Univerzitet u Nišu (2020)
25. "Uloga obrazovanja u jačanju sajber bezbednosti u Srbiji" – Snežana Petrović, Univerzitet u Novom Sadu (2021)

11. PRILOG

11.1 Upitnik: Uticaj bezbednosnih rizika u sajber prostoru na poboljšanje funkcionalnosti SIEM softverskih rešenja

Ovaj upitnik je osmišljen sa ciljem da istraži stavove i iskustva ispitanika o sajber pretnjama, bezbednosnim rizicima, kao i efikasnosti postojećih mera zaštite sa fokusom na SIEM rešenja. Osnovni cilj je prikupljanje relevantnih podataka koji će se koristiti isključivo u naučne svrhe.

Napomena:
Ispitivanje je anonimnog karaktera, a odgovori ispitanika će se koristiti samo u svrhu naučnog istraživanja.

Demografski podaci:
Pol:

1. Muški
2. Ženski

Godine starosti:

1. Od 18 do 25 godina
2. Od 26 do 35
3. Od 36 do 45
4. Od 46 do 55
5. Od 56 do 65

Prebivalište:

1. Selo
2. Prigradsko naselje
3. Grad

Obrazovanje:

1. Osnovna škola
2. Srednja škola
3. Visoka škola
4. Magistatura/Doktorat

Zanimanje:

1. IT stručnjak
2. Zaposlen u javnom sektoru
3. Zaposlen u privatnom sektoru
4. Nezaposlen
5. Drugo

Ispitivanje stavova ispitanika

Na tvrdnje koje slede odgovarajte obeležavanjem (X) jednog od pet ponuđenih polja (odgovora):
1 – U potpunosti se ne slažem
2 – Ne slažem se
3 – Neodlučan/na sam
4 – Slažem se
5 – U potpunosti se slažem

1. Svest o sajber pretnjama

1. Da li smatrate da su sajber pretnje ozbiljan rizik za organizacije danas?
2. Da li ste upoznati sa najčešćim vrstama sajber napada?
3. Smatrate li da su sajber pretnje relevantne za vaš sektor?
4. Da li verujete da će se pretnje iz sajber prostora povećavati u budućnosti?
5. Da li se u vašoj organizaciji diskutuje o sajber pretnjama?

2. Iskustva sa sajber napadima

6. Da li ste se vi ili vaša organizacija ikada suočili sa sajber napadom?
7. Da li ste bili žrtva phishing napada?
8. Da li vaša organizacija ima plan za odgovor na sajber incidente?
9. Da li ste ikada izgubili podatke zbog sajber napada?
10. Da li verujete da ste sada bolje pripremljeni za sajber napade nego ranije?

3. Bezbednosne prakse i navike

11. Da li redovno menjate lozinke?
12. Da li koristite dvofaktornu autentifikaciju za svoje naloge?
13. Da li u vašoj organizaciji postoje redovne provere bezbednosti IT sistema?
14. Da li edukujete zaposlene o sajber bezbednosti?
15. Da li vaša organizacija koristi enkripciju za osetljive podatke?

4. Posledice sajber napada na poslovanje i privatne živote

16. Da li su sajber napadi uticali na poslovanje vaše organizacije?
17. Da li su sajber napadi uticali na vašu privatnost ili privatni život?
18. Da li vaša organizacija pretrpi finansijske gubitke zbog sajber napada?
19. Da li ste doživeli emocionalni stres zbog sajber incidenata?
20. Da li smatrate da sajber napadi mogu narušiti reputaciju vaše organizacije?

5. Percepcija efikasnosti postojećih mera zaštite (sa SIEM rešenjima)

21. Da li verujete da su trenutne mere sajber zaštite efikasne?
22. Da li vaša organizacija koristi SIEM rešenje za praćenje sajber incidenata?
23. Smatrate li da je SIEM rešenje efikasno u detekciji pretnji?
24. Da li SIEM rešenje smanjuje vreme potrebno za otkrivanje sajber incidenata?
25. Da li smatrate da je potrebno dodatno ulaganje u SIEM tehnologije?