KIBERNETIČKA SIGURNOST / CYBER SECURITY

Mejra Hidić[1];
[1]Internacionalni univerzitet Travnik u Travniku
e-mail: mejra.899@gmail.com

Prelgedni članak
UDK / UDC 004.056.5

Sažetak

Kibernetička sigurnost postaje sve značajnija u savremenom digitalnom okruženju, gdje zaštita podataka, sistema i korisnika od različitih prijetnji ima ključnu ulogu. Pojave poput phishinga, ransomwarea i cyber špijunaže predstavljaju ozbiljne izazove, kako za pojedince tako i za organizacije. Ovaj rad istražuje ključne aspekte kibernetičke sigurnosti, uključujući prepoznavanje prijetnji, primjenu preventivnih mjera i uvođenje inovativnih tehnologija u zaštitu sistema. Posebna pažnja posvećena je važnosti edukacije i podizanja svijesti o sigurnosnim rizicima, kao i potrebi za međunarodnom saradnjom u razmjeni znanja i resursa. U zaključku, naglašava se da kibernetička sigurnost nije samo tehnički izazov već i društvena odgovornost koja zahtijeva proaktivan pristup svih uključenih strana.

Ključne riječi: kibernetička sigurnost, prijetnje, zaštita podataka, edukacija, tehnologija, prevencija.
JEL klasifikacija: K240

Abstract

Cybersecurity is increasingly important in today's digital environment, where protecting data, systems, and users from various threats is essential. Challenges such as phishing, ransomware, and cyber espionage pose significant risks for individuals and organizations alike. This paper examines the key aspects of cybersecurity, including threat detection, preventive measures, and the integration of innovative technologies into system protection. Special attention is given to the importance of education and raising awareness about security risks, as well as the necessity of international cooperation in sharing knowledge and resources. In conclusion, cybersecurity is highlighted as not just a technical challenge but a societal responsibility requiring a proactive approach from all stakeholders.

Keywords: cybersecurity, threats, data protection, education, technology, prevention.
JEL classification: K240

UVOD

U današnjem digitalnom dobu, kibernetička sigurnost postala je jedan od najvažnijih aspekata u očuvanju integriteta, privatnosti i sigurnosti podataka. Kako se tehnologija brzo razvija, tako raste i broj prijetnji koje ugrožavaju ne samo pojedince, već i organizacije, vlade, pa i čitave nacije.

Kibernetički napadi, poput phishinga, ransomwarea i cyber špijunaže, postali su svakodnevna stvarnost, čineći zaštitu podataka i informacija vitalnim za opstanak u digitalnom okruženju. Kibernetička sigurnost obuhvata strategije, tehnologije i prakse koje se koriste za zaštitu računarskih sistema, mreža i podataka od različitih oblika kibernetičkih prijetnji. Zadatak je očuvanje povjerljivosti, integriteta i dostupnosti informacija, kako bi se spriječile finansijske gubitke, oštećenje reputacije i druge ozbiljne posljedice. S obzirom na brzinu napredovanja tehnologije i kompleksnost prijetnji, kibernetička sigurnost zahtijeva stalnu prilagodbu i inovaciju.

U kontekstu globalizacije i digitalizacije, zaštita informacija je postala zajednička odgovornost. Kibernetički napadi ne poznaju granice, zbog čega je međunarodna saradnja ključna u stvaranju zajedničkog fronta za borbu protiv ovih prijetnji. Kroz ovu konferenciju, cilj nam je podići svijest o važnosti kibernetičke sigurnosti, podijeliti znanja i iskustva te predstaviti nove tehnologije koje omogućavaju efikasniju zaštitu u dinamičnom digitalnom okruženju.

1.ZNAČAJ KIBERNETIČKE SIGURNOSTI U SAVREMENOM DIGITALNOM DOBU

Kibernetička sigurnost obuhvaća skup procesa, mjera i standarda kojima se jamči određena razina pouzdanosti pri korištenju proizvoda i usluga u kibernetičkom prostoru, pri čemu sustavna zaštita računala i računalnih mreža, informatičke i informacijske infrastrukture, mobilnih uređaja i podataka od malicioznih napada tome značajno pridonosi.[229] Kibernetičke prijetnje, poput cyber napada, krađe identiteta, hakiranja i malicioznih softverskih prijetnji, predstavljaju ozbiljan rizik za pojedince, organizacije, a čak i države.

[229] https://rdd.gov.hr/kiberneticka-sigurnost/1436 (datum pristupa, 03.12.2024)

Organizacije sve više zavise od digitalnih rješenja, poput cloud usluga, Interneta stvari (IoT) i mobilnih aplikacija, što znači da su ovi sistemi stalno podložni napadima. Kibernetički napadi mogu paralizirati poslovanje, oštetiti imidž firme, a često i ugroziti ljudske živote, kao što je slučaj u zdravstvenim institucijama.

Slika 1, Kibernetička sigurnost

Izvor; https://poduzetnik.biz/tehnologija/kiberneticka-sigurnost/

Zaštita privatnosti i podataka: S povećanjem količine podataka koji se svakodnevno prikupljaju putem interneta, postaje ključna zaštita tih podataka. Privatne informacije, financijski podaci, medicinski zapisi i intelektualna svojina mogu biti izloženi krađi ili zloupotrebi. Kibernetička sigurnost pomaže u očuvanju povjerljivosti i integriteta tih informacija, osiguravajući da ih ne iskoriste zlonamjerni akteri. Globalna povezanost i međunarodni aspekti: Digitalna povezanost omogućava međunarodnu razmjenu podataka, ali također stvara i globalne prijetnje. Kibernetički napadi mogu prelaziti nacionalne granice, čime se stvara potreba za međunarodnom saradnjom u borbi protiv kibernetičkog kriminala. Djelotvorni zakoni i strategije borbe protiv cyber prijetnji moraju biti koordinirani na globalnom nivou

1.1.CILJEVI SKUPA: PODIZANJE SVIJESTI O PRIJETNJAMA, RAZMJENA ISKUSTAVA I IMPLEMENTACIJA SAVREMENIH RJEŠENJA U KIBERNETIČKOJ SIGURNOSTI

1.1.1.Ciljevi Kibernetička sigurnost

Podizanje svijesti o kibernetičkim prijetnjama, Informisanje učesnika o najnovijim prijetnjama u oblasti kibernetičke sigurnosti., Razumijevanje važnosti zaštite podataka i sistema u privatnom i poslovnom sektoru. Edukacija o osnovnim metodama prevencije i zaštite od kibernetičkih napada. Povećanje svijesti o društvenoj odgovornosti u zaštiti privatnosti i digitalne imovine. Od zvijezda do digitalnih prijetnji. Dr. Leila Powell svojedobno je proučavala formiranje galaksija, a danas je vodeća znanstvenica za podatke u tvrtki Panaseer. "Proučavanje svemira je važno, ali željela sam

raditi nešto što više utječe na svakodnevni život ljudi," objašnjava Powell, dodajući kako je promjena karijere donijela i bolje uvjete rada.[230]

1.1.2.Razmjena znanja među stručnjacima i organizacijama

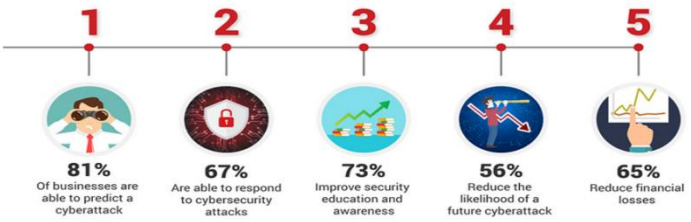
Stvaranje platforme za dijalog i saradnju među stručnjacima iz oblasti IT sigurnosti, biznisa i obrazovanja. Razmjena iskustava u rješavanju kibernetičkih incidenata i izazova u različitim sektorima. Prezentacija istraživanja, novih studija i izvještaja o globalnim trendovima u kibernetičkoj sigurnosti. Stvaranje mreže profesionalaca koji mogu pružiti podršku i savjete u slučaju kibernetičkih prijetnji.

1.1.3.Prezentacija novih tehnologija u zaštiti podataka

Upoznavanje učesnika sa najnovijim tehnološkim rješenjima u oblasti kibernetičke sigurnosti. Prikazivanje inovacija u primjeni umjetne inteligencije, blockchain tehnologije, enkripcije i drugih alata za zaštitu. Demonstracija naprednih alata i softverskih rješenja za prevenciju i otkrivanje prijetnji. Razmatranje budućnosti kibernetičke sigurnosti u kontekstu novim tehnologija, poput kvantnog računarstva i 5G mreža.

2. TRENUTNO STANJE KIBERNETIČKE SIGURNOSTI

Kibernetička sigurnost je postala jedan od najvažnijih izazova u modernom digitalnom društvu, jer sve više organizacija, vlada, ali i pojedinaca postaju ciljevi sofisticiranih kibernetičkih napada. Digitalizacija poslovanja, prijenos podataka u oblak, te masovna upotreba interneta stvari (IoT) stvorili su nove prilike za napadače. Dok su napadi na digitalne sisteme sve češći i složeniji, organizacije, pa čak i države, često ne uspijevaju da se adekvatno pripreme i zaštite.



Slika 2, Upravljanje kibernetičkom sigurnošću

[230] https://forbes.n1info.hr/ljudi/nova-karijera-u-kibernetickoj-sigurnosti-put-promjene/ (datum pristupa, 03.12,2024)

Izvor: https://zih.hr/konzalting/informacijska-sigurnost-i-kontinuitet-poslovanja/upravljanje-kibernetickom-sigurnoscu/

Globalni trendovi u kibernetičkim prijetnjama

Povećanje broja napada: Prema statistikama, broj cyber napada raste svake godine. Na globalnom nivou, kibernetički napadi su porasli za više od 50% u posljednje tri godine, uz značajan porast napada zasnovanih na ransomware-u, koji su se udvostručili u posljednjih nekoliko godina. Ransomware i phishing: Najveći broj prijetnji dolazi od ransomware napada, gdje napadači šifriraju podatke i zahtijevaju otkupninu za otključavanje. Phishing napadi, koji se koriste za krađu osjetljivih podataka poput korisničkih imena, lozinki i brojeva kreditnih kartica, također su među najrasprostranjenijim prijetnjama.

Ažuriranje zakonodavnih okvira: Zaštita podataka postaje ključna u kontekstu globalne povezanosti. Zakonodavstvo poput GDPR-a (Opća uredba o zaštiti podataka) na evropskom nivou postavlja jasne zahtjeve za zaštitu podataka i jačanje kibernetičke sigurnosti.

2.1. PREGLED GLOBALNIH TRENDOVA U KIBERNETIČKIM PRIJETNJAMA.

Kibernetičke prijetnje stalno evoluiraju i postaju sofisticiranije, a globalni trendovi u kibernetičkoj sigurnosti ukazuju na rastući broj napada, različite taktike napadača i izazove s kojima se organizacije suočavaju. Neki od ključnih trendova u kibernetičkim prijetnjama uključuju.
Povećanje ransomware napada
Ransomware napadi, u kojima napadači šifruju podatke i zahtijevaju otkupninu za dešifriranje, postaju sve češći i raznovrsniji. Zločinci koriste sofisticirane tehnike, poput tzv. „double extortion" metoda, gdje ne samo da blokiraju pristup podacima, već i prijete njihovim objavljivanjem ukoliko otkupnina nije plaćena[231]. Ovi napadi su ciljano usmjereni na organizacije s visokim vrijednostima podataka, poput bolnica, financijskih institucija i vladinih agencija.

Phishing napadi i social engineering
Phishing napadi su među najpopularnijim prijetnjama, jer napadači koriste socijalni inžinjering kako bi manipulisali korisnicima da otkriju osjetljive podatke. Te napade često prate napadi koji

[231] https://hrcak.srce.hr/file/378328 (datum pristupa, 03.12.2024)

koriste lažne e-mailove, web stranice i telefonske pozive kako bi prevarili korisnike da instaliraju maliciozne softvere ili predaju privatne informacije.

Povećana upotreba AI i automatizacije od strane napadača
Napadači sve više koriste umjetnu inteligenciju (AI) i mašinsko učenje (ML) kako bi unaprijedili svoje napade. Korištenje AI omogućava napadačima da brzo analiziraju velike količine podataka, prilagođavaju napade u stvarnom vremenu i automatski skeniraju ranjivosti u sistemima. Ova tehnologija omogućava napade u većem obimu i uz manji ljudski angažman.

Napadi na Internet of Things (IoT)
S porastom IoT uređaja, napadi na ove uređaje postaju sve češći. IoT uređaji, poput pametnih termostata, kamera i zdravstvenih aparata, često nemaju odgovarajuću zaštitu, čineći ih idealnim ciljevima za napadače. Kroz ove uređaje, napadači mogu dobiti pristup širem mrežnom okruženju ili čak izvršiti napade tipa DDoS (Distributed Denial of Service).

3. GLAVNE PRIJETNJE KIBERNETIČKOJ SIGURNOSTI

Phishing je jedan od najčešćih oblika kibernetičkog napada, gdje napadači koriste lažne e-mailove, poruke ili web stranice kako bi prevarili korisnike i ukrali njihove osobne podatke poput lozinki, brojeva kreditnih kartica ili drugih osjetljivih informacija. Ovi napadi često koriste socijalni inženjering kako bi izgledali uvjerljivo.

Ransomware je zlonamjerni softver koji zarazi računar ili mrežu, šifruje podatke i zahtijeva otkupninu za njihovo dešifrovanje. Ovi napadi mogu paralizirati poslovanje organizacija i izazvati ogromne finansijske gubitke. Napadači obično zahtijevaju plaćanje u kriptovalutama, što otežava praćenje i identifikaciju.[232] Malware uključuje razne vrste štetnog softvera kao što su virusi, trojanski konji, spyware i adware, koji mogu uzrokovati ozbiljna oštećenja na računarima, ukrasti podatke ili omogućiti napadačima pristup sistemima i mrežama. Malware se često širi putem zaraženih datoteka ili neosigurane internetske povezanosti. DDoS napadi (Distributed Denial of Service) ciljanjem velikih brojeva uređaja stvore ogromnu količinu prometa prema određenom serveru ili mreži, što uzrokuje prekid usluga. Ovi napadi mogu značajno utjecati na dostupnost

[232] https://chatgpt.com/c/674f3024-e7ac-8012-80ae-cc54dbd30418 (datum pristupa, 03.12.2024)

online usluga i uzrokovati veliki ekonomski gubitak za organizacije[233]. Cyber špijunaža uključuje krađu osjetljivih podataka, poslovnih informacija ili državnih tajni uz pomoć sofisticiranih hakera. Hakeri mogu provaliti u mreže organizacija ili vlada, krađom povjerljivih podataka ili instaliranjem špijunskih programa koji omogućuju neovlašteni pristup. Unutrašnje prijetnje dolaze od samih zaposlenika ili bivših radnika koji imaju pristup poslovnim podacima ili mrežama. Ove prijetnje mogu biti namjerne, kao što je krađa podataka, ili nenamjerne, poput nesvjesnih grešaka u rukovanju podacima. Interni napadi mogu biti teži za otkriti i spriječiti jer su napadači već legitimni korisnici sistema.

Zero-day napadi koriste ranjivosti u softveru koje proizvođači nisu otkrili ili zakrpili. Budući da su ove ranjivosti nepoznate, napadači ih mogu iskoristiti prije nego što se postigne popravak, čineći ih posebno opasnima i teškima za odbranu.

4. STRATEGIJE ZA ZAŠTITU

Kibernetička sigurnost zahtijeva sveobuhvatan pristup koji uključuje tehničke, organizacijske i ljudske aspekte. Preventivne mjere poput enkripcije podataka i višefaktorske autentifikacije (MFA) ključne su za zaštitu povjerljivih informacija. Enkripcija osigurava da podaci ostanu nečitljivi i zaštićeni, čak i ako dođe do njihovog neovlaštenog pristupa, dok MFA dodaje dodatni sloj sigurnosti, čineći pristup podacima sigurnijim. Redovno ažuriranje softverskih sistema, uključujući zakrpe za sigurnosne rupe, pomaže u sprječavanju napada koji iskorištavaju zastarjele tehnologije.

Tehnološka rješenja također igraju ključnu ulogu u zaštiti kibernetičkih sistema. Vatrozidi filtriraju mrežni promet i blokiraju potencijalne prijetnje, dok antivirusni softver omogućava detekciju i uklanjanje malicioznog softvera prije nego što prouzrokuje ozbiljnu štetu. Sistemi za detekciju i prevenciju upada (IDS/IPS) prepoznaju neovlaštene aktivnosti i automatski blokiraju prijetnje. Edukacija i obuka zaposlenika također su ključni za prevenciju napada, jer nepažnja ljudi često predstavlja najveći sigurnosni rizik.[234] Organizacije bi trebale redovno organizirati obuke koje uključuju prepoznavanje phishing napada i drugih malicioznih prijetnji. Također, simulacije

[233] Kibernetička sigurnost: Tehnologija, procesi i ljudi" – Autor: Ivica Pavić
[234] "Sigurnost informacija: Praktični vodič" – Autor: Davor Strugar

kibernetičkih napada pomažu u pripremi zaposlenika za stvarne situacije. Za odgovor na napade, svaka organizacija treba imati razvijen plan koji uključuje brzo prepoznavanje prijetnji, minimiziranje štete i oporavak od napada. Takvi planovi trebaju biti testirani kroz redovne sigurnosne vježbe kako bi se osigurala njihova učinkovitost.

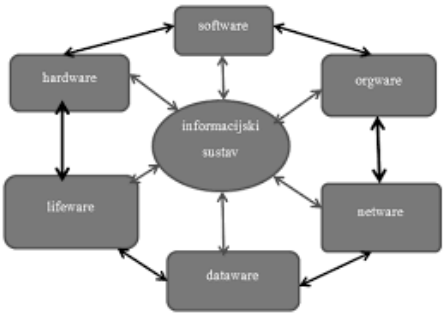
Uvođenje inovativnih tehnologija poput umjetne inteligencije i mašinskog učenja može pomoći u prepoznavanju novih prijetnji u stvarnom vremenu i omogućiti bržu reakciju. Također, sigurno pohranjivanje podataka u oblaku, uz odgovarajuće sigurnosne mjere, smanjuje rizik od gubitka ili krađe podataka. Kibernetička sigurnost mora biti višeslojna i stalno se prilagođavati novim prijetnjama, jer nijedna zaštita nije apsolutna.[235]

5.MEĐUNARODNA SARADNJA I ZAKONODAVNI OKVIR U BORBI PROTIV KIBERNETIČKOG KRIMINALA

5.1.VAŽNOST MEĐUNARODNOG PARTNERSTVA U BORBI PROTIV KIBERNETIČKOG KRIMINALA

Kibernetički kriminal nema granica, što znači da napadi mogu poticati iz bilo kojeg dijela svijeta i uticati na države i organizacije širom planeta. Zbog toga je međunarodna saradnja ključna u borbi protiv ovog globalnog problema. Ujedinjeni pristup omogućava efikasnu razmjenu informacija, resursa i tehnoloških rješenja za prevenciju, otkrivanje i suzbijanje kibernetičkog kriminala. Ključne prednosti međunarodne saradnje uključuju: Razmjena informacija i podataka: Zajednički rad omogućava brže otkrivanje prijetnji i napada, jer zemljama koje se suočavaju sa sličnim prijetnjama često može pomoći razmjena iskustava. Koordinirani odgovor na napade: Kada se napad širi preko više jurisdikcija, međunarodne organizacije mogu koordinirati odgovore i suradnju između različitih zemalja i agencija. Standardizacija sigurnosnih procedura: Zajednička primjena sigurnosnih protokola i tehnoloških rješenja omogućava usklađivanje napora na globalnom nivou

[235] https://chatgpt.com/c/674f3024-e7ac-8012-80ae-cc54dbd30418 (datum pristupa, 03.12.2024)



Slika 4, Važnosti kibernetičke sigurnosti

Izvor: https://repozitorij.bak.hr/islandora/object/bak%3A732/datastream/PDF/view

5..PREGLED ZAKONODAVNIH RJEŠENJA: GDPR, CYBERSECURITY ACT

GDPR (Opća uredba o zaštiti podataka)

GDPR je regulativa Evropske unije koja je uvedena kako bi zaštitila privatnost korisnika i poboljšala sigurnost podataka u digitalnom okruženju. Njegova primjena ne samo da štiti korisničke podatke, već i stvara pravnu osnovu za suočavanje s kibernetičkim napadima, posebno u pogledu obveza organizacija u slučaju povrede podataka. Kibernetički napadi koji ugrožavaju lične podatke mogu dovesti do ozbiljnih sankcija, uključujući visoke kazne za nepoštivanje sigurnosnih mjera.[236]

Slika 5, GDPR

Izvor: https://cybersecurity.ba/gdpr-zastita-podataka-u-evropi-i-svijetu-s-fokusom-na-bih-i-zapadni-balkan/

[236] Cybersecurity Law" – Autor: Jeff Kosseff

5.3.CYBERSECURITY ACT

Europski zakon o kibernetičkoj sigurnosti, poznat kao Cybersecurity Act, postavlja standarde za sigurnost mreža i informacijskih sistema unutar EU. Ovaj zakon osigurava jaču saradnju između država članica u borbi protiv kibernetičkih prijetnji i omogućava usklađivanje nacionalnih politika kibernetičke sigurnosti. Također, ustanovljava Europol's European Cybercrime Centre (EC3), koje pomaže u istraživanju i prevenciji kibernetičkog kriminala u EU.

Slika 6, Cybersecurity Act

Izvor: https://www.pinterest.com/pin/875598352547830498/

5.4.CERT (COMPUTER EMERGENCY RESPONSE TEAM)

CERT-ovi su timovi odgovorni za pružanje tehničke i strateške podrške u incidentima kibernetičke sigurnosti. Ovi timovi rade u saradnji s vladama, privatnim sektorom i organizacijama za analizu prijetnji, razvijanje odgovora na napade i poduzimanje preventivnih mjera. CERT-ovi pomažu u koordinaciji odgovora na velike kibernetičke incidente i pružaju obuku i savjete o sigurnosnim praksama.

Slika 7, CERT

Izvor: https://www.pinterest.com/search/pins/?q=Sony%20Pictures%20Entertainment%20(2014)&rs=typed

6.STUDIJE SLUČAJA: KIBERNETIČKI NAPADI

6.1. Napad na Sony Pictures Entertainment (2014)

Opis napada: U 2014. godini, Sony Pictures Entertainment bio je meta sofisticiranog cyber napada, za koji je odgovornost preuzela hakerska grupa "Guardians of Peace". Napadači su uspjeli dobiti pristup velikoj količini osjetljivih podataka, uključujući interne e-mailove, osobne podatke zaposlenih i neobjavljene filmove. Osim toga, grupa je prijetila da će objaviti još veću količinu podataka, što je izazvalo ozbiljnu štetu uglednom brendu.

Pouke:

Značaj proaktivne zaštite podataka: U trenutku napada, organizacija nije imala adekvatne mehanizme zaštite podataka, što je omogućilo napadačima da lako dođu do povjerljivih informacija. Interna sigurnost: Napad je pokazao kako su interna e-mail komunikacija i informacije o zaposlenima postale ključne mete za hakerima. Brza reakcija: Sony je bio prisiljen brzo reagirati, ali šteta po ugled kompanije bila je neminovna.

Preporuke za prevenciju: Implementacija višefaktorske autentifikacije i naprednih sistema za detekciju prijetnji. Redovno obrazovanje zaposlenih o sigurnosnim prijetnjama (npr. prepoznavanje phishing e-mailova). Razvijanje jasnih kriznih planova i procedura za brzo djelovanje u slučaju napada.[237]

6.2. NAPAD NA EQUIFAX (2017)

Opis napada: Jedan od najvećih napada na kompaniju za kreditnu analizu, Equifax, dogodio se 2017. godine, kada su hakeri iskoristili sigurnosnu ranjivost u softverskom sistemu. Napad je rezultirao kompromitacijom osobnih podataka više od 147 miliona ljudi, uključujući socijalne brojeve, datume rođenja i druge osjetljive informacije.

Pouke:

Zastareli sistemi: Iako su ranjivosti bile poznate, Equifax nije pravovremeno implementirao zakrpe, što je omogućilo napadačima da iskoriste ovu sigurnosnu rupu.

[237] https://chatgpt.com/c/674f3024-e7ac-8012-80ae-cc54dbd30418

Procjena rizika: Ovaj napad pokazuje koliko je važno kontinuirano procjenjivati i ažurirati sigurnosne protokole, posebno kada je u pitanju pohrana osjetljivih podataka. Preporuke za prevenciju: Redovno ažuriranje sistema i softverskih zakrpa. Implementacija enkripcije za pohranu osjetljivih podataka. Redovno testiranje sigurnosnih sistema i izvođenje simulacija napada.

Slika 8, Equifax

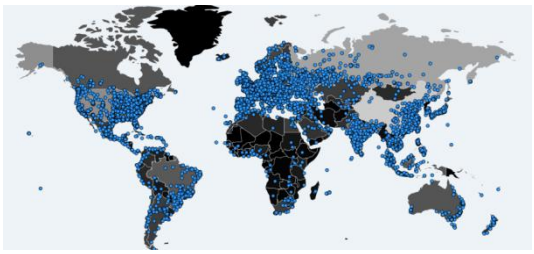
Izvor: https://www.theguardian.com/us-news/2019/jul/22/equifax-data-breach-security-ftc-settlement

6.3. NAPAD NA WANNACRY RANSOMWARE (2017)

Opis napada: WannaCry je globalni ransomware napad koji je pogodio tisuće organizacija u 150 zemalja. Koristio je ranjivost u Microsoftovom operativnom sistemu, a nakon infekcije, napadači su šifrirali podatke i tražili otkupninu za njihovu dešifriranje.

Pouke:

Zastareli sistemi i neprimijenjeni zakrpe: WannaCry je iskoristio ranjivost koja je već bila zakrpljena u novim verzijama operativnog sistema, ali mnoge organizacije nisu izvršile ažuriranje. Nedostatak svijesti: Ovaj napad pokazuje koliko je važno imati svijest o prijetnjama i pravilno upravljati sistemima kako bi se izbjegle slične situacije.



Slika 9, WannaCry Ransomware

Izvor: https://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday

7.KIBERNETIČKA SIGURNOST U BUDUĆNOSTI

U budućnosti, kibernetička sigurnost suočit će se s novim izazovima i prijetnjama koje će se razvijati zajedno s napretkom tehnologije. Predviđa se da će cyber prijetnje postati sofisticiranije, s većim kapacitetima za automatizaciju i umjetnu inteligenciju, što će otežati njihovu detekciju i prevenciju. Također, očekuje se porast napada na Internet stvari (IoT) i povezane uređaje, budući da će sve više uređaja biti povezano na internet, čime se otvara veliki prostor za potencijalne napade.

Jedan od ključnih trendova u budućnosti bit će utjecaj novih tehnologija, kao što su blockchain i kvantno računarstvo, na kibernetičku sigurnos[238]t. Blockchain, kao decentralizirana tehnologija, nudi potencijalnu zaštitu od cyber prijetnji, posebno u sektorima poput finansija i logistike, gdje omogućava sigurnu i transparentnu razmjenu podataka. Međutim, blockchain tehnologija također može postati meta napada, a nova rješenja za sigurnost morat će se razviti kako bi se u potpunosti iskoristili njezini potencijali. [239]Kvantno računarstvo, s obzirom na svoju sposobnost obraditi ogromne količine podataka u vrlo kratkom vremenu, može stvoriti nove izazove u pogledu enkripcije podataka. Kvantni računari potencijalno bi mogli dešifrirati trenutne sigurnosne protokole, što bi zahtijevalo razvoj novih, kvantno-sigurnih algoritama koji bi zaštitili podatke na još sigurniji način. Stalna prilagodba i inovacija bit će ključne za održavanje visokog nivoa sigurnosti. Kako se prijetnje razvijaju, tako će i strategije zaštite morati biti u stalnom razvoju.

To uključuje integraciju novih tehnologija u zaštitu podataka, kontinuiranu edukaciju korisnika, te međunarodnu saradnju u borbi protiv globalnih cyber prijetnji. Ove promjene neće biti samo tehnički izazov, već i društvena odgovornost koja zahtijeva sinergiju između tehnoloških stručnjaka, zakonodavaca i krajnjih korisnika.

[238] Cybersecurity for Beginners" – Autor: Raef Meeuwisse
[239] https://zir.nsk.hr/islandora/object/ffos%3A5571/datastream/PDF/view (datum pristupa, 03.12.2024)

ZAKLJUČAK

Kibernetička sigurnost predstavlja temeljnu komponentu zaštite modernog digitalnog društva, jer prijetnje koje dolaze sa strane cyber kriminala mogu imati ozbiljne posljedice po privatne i poslovne korisnike. Ova konferencija je istakla važnost proaktivnog pristupa u identifikaciji i prevenciji prijetnji, kao i nužnost stalnog usavršavanja tehnoloških rješenja koja pomažu u zaštiti podataka i infrastrukture. Naglašena je ključna uloga edukacije i svijesti, jer ljudski faktor često predstavlja najranjiviju tačku sigurnosnih sistema. Također, jasno je da kibernetička sigurnost nije samo tehnički izazov, već i društvena odgovornost koja zahtijeva aktivnu saradnju između vladinih tijela, međunarodnih organizacija, poslovnog sektora i krajnjih korisnika. Internacionalna saradnja i razvoj zajedničkih zakonskih okvira i sigurnosnih protokola od ključne su važnosti za jačanje globalne sigurnosti. U zaključku, kibernetička sigurnost mora biti kontinuirani proces, u kojem je prevencija, edukacija i inovacija ključ za izgradnju otpornog digitalnog svijeta. Potrebno je neprestano pratiti nove tehnologije, prijetnje i pristupe u zaštiti, kako bi se osigurao siguran digitalni prostor za sve.

LITERATURA

(1) Kibernetička sigurnost: Tehnologija, procesi i ljudi" – Autor: Ivica Pavić

(2) "Sigurnost informacija: Praktični vodič" – Autor: Davor Strugar

(3) Cybersecurity and Cyberwar: What Everyone Needs to Know

(4) Hacking: The Art of Exploitation" – Autor: Jon Erickson

(5) Cybersecurity for Beginners" – Autor: Raef Meeuwisse

(6) Cybersecurity Law" – Autor: Jeff Kosseff

(7) Applied Cryptography" – Autor: Bruce Schneier

(8) https://rdd.gov.hr/kiberneticka-sigurnost/1436 (datum pristupa, 03.12.2024)

(9) https://www.consilium.europa.eu/hr/policies/cybersecurity/ (datum pristupa, 03.12.2024)

(10) https://poduzetnik.biz/tehnologija/kiberneticka-sigurnost/ (datum pristupa, 03.12.2024)

(11) https://courses.minnalearn.com/hr/courses/cybersecurity/what-is-cybersecurity/ (datum pristupa, 03.12.2024)

(12) https://chatgpt.com/c/674f3024-e7ac-8012-80ae-cc54dbd30418(datum pristupa, 03.12.2024)

(13) https://www.theguardian.com/us-news/2019/jul/22/equifax-data-breach-security-ftc- (datum pristupa, 03.12.2024)settlement

(14) https://repozitorij.bak.hr/islandora/object/bak%3A732/datastream/PDF/view (datum pristupa, 03.12.2024)

(15) https://unija.com/hr/kiberneticka-sigurnost-sve-sto-trebate-znati-o-cyber-sigurnosti/ (datum pristupa, 03.12.2024)