"Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them."

WBnet

Co-funded by the European Union

Internet i računarska bezbednost

dr Bojana Milosavljević

AASKM

ATYCC

UNIVERSITY OF LJUBLJANA
Faculty of Electrical Engineering

POLITÉCNICA

University of Pristina
Kosovska Mitrovica

Co-funded by the European Union

Internet, osnovni pojmovi-kratka istorija razvoja

- Istorija Interneta počinjee 1961. godine sa teorijom paketnog prebacivanja(packed switching), MIT-a (*Massatchuseetts Institute of Tehnology)*
- Godine 1965. prvi put su povezana dva računara, Masačusets /Kalifornija, korišćenjem spore telefonske linije.
- Rad na stvaranju mreže ARPANET*(Advanced Research Projects Agency Network)* je počeo 1966. godine. DARPA (*Defense Advanced Research Projects Administration*)
- Prvi čvor - računar Univerziteta Kalifornija iz Los Anđelesa (*University of California Los Angeles/UCLA*), drugi čvor - računar u Istraživačkom institutu Stratford (*Stanford Research Institute/SRI*).

Internet, osnovni pojmovi - evolucija

- Originalni ARPANET je vremenom prerastao u Internet.
- Internet se zasniva na novoj ideji o postojanju više nezavisnih mreža od kojih je svaka proizvoljno dizajnirana, dok je ARPANET predviđao postojanje jedne mreže.
- Ključna ideja na kojoj se zasniva Internet je *otvorena arhitektura umrežavanja*,
- U Evropi je 1984. godine počela izgradnja EARN mreže (*European Academic and Research Network*) koja je sledila koncept povezivanja mreža.
- Jugoslavija se uključila u mrežu EARN praktično 1989 godine. Prvi računar koji je uključen u mrežu bio je računar Republičkog zavoda za statistiku.

Co-funded by the European Union

Internet, osnovni pojmovi

- Računarska mreža - skup više računara, perifernih jedinica i drugih uređaja koji su međusobno povezani sa ciljem razemne informacije i deobe mrežnih resursa.
- Komunikacija između čvorova koji su u mreži vrši se na osnovu protokola.
- Postoji više klasifikacija mreža:
- prema dometu: LAN (*Local Area Network*), WAN (*Wide Area Network*), MAN (*Metropolean Area Network*), CAN, PAN,
- prema odnosu između čvorova: *peer-to- peer* i serverske mreže; i
- klasifikacija prema topologiji: magistrala (*Bus*), prsten (*Ring*) i zvezda (*Star*).

Co-funded by the European Union

Internet, osnovni pojmovi

- **Protokoli**
- Protokol označava skup pravila koja određuju kako dva programa mogu da komuniciraju. Računari komuniciraju tako što razmenjuju određeni set poruka, a protokol određuje formate tih poruka.
- TCP/IP (*Transmission Control Protocol/Internet Protocol*) protokol, koji omogućava komunikaciju između dva ili više računara.
- Protokoli za svaku od internet usluga i to npr.:
- HTTP (*Hyper-Text Transfer Protocol*) za *Worl Wide Web*,
- FTP (*File Transfer Protocol*) je servis za distribuciju datoteka na Internetu,
- SMTP (*Small Mail Transfer Protocol*) za prenos *e-mail* poruka,
- NNT (*Network News Transfer Protocol*) za prenos *news* poruka, i
- Telnet - za rad na udaljenim serverima / računarima

Co-funded by the European Union

Internet, osnovni pojmovi

- **Portovi**
- Svaki internet protokol (www, ftp, smtp...) ima svoj odgovarajući port (broj)..
- **Internet adrese**
- Da bi računari mogli međusobno da se prepoznaju, svaki pojedinačni računar mora da ima svoju unikatnu adresu. Uspešno korišćenje Interneta podrazumeva razumevanje nekoliko različitih vrsta adresa.
- IP adrese su jednostavne brojčane adrese računara spojenih na Internet.
- Simboličke adrese – domeni. Kako bi lakše pamtili adrese serverima se dodeljuju simboličke adrese tipa www. kpa.edu.. Podela se vrši na sledeći način : ime servisa + ime servera + ime domena + ime root domena,
- *URL (Uniform Resource Locator*) je veb adresa određenog resursa na Internetu. Resurs na koji pokazuje URL adresa može biti HTML dokument (veb stranica), slika, ili bilo koja datoteka koja se nalazi na određenom veb serveru.

Co-funded by
the European Union

Internet, osnovni pojmovi

Internet

Co-funded by the European Union

Osnove Internet i računarske bezbednosti

- Internet i kompjuterska tehnologija se mogu zloupotrebljavati na razne načine, a sama zloupotreba koji se realizuje pomoću kompjutera može imati oblik bilo kog od tradicionalnih vidova kriminaliteta.
- Pojavni oblici **kompjuterskog kriminaliteta** su: protivpravno korišćenje usluga i neovlašćeno pribavljanje informacija, kompjuterske krađe, prevare, sabotaže, i kompjuterski terorizam i kriminal vezan za kompjuterske mreže.

Co-funded by the European Union

Osnove Internet i računarske bezbednosti

- **Kriminal vezan za kompjuterske mreže** je oblik kriminalnog ponašanja kod koga se *cyberspace*- okruženje u kome su kompjuterske mreže, pojavljuju u trostrukoj ulozi:
- *Kompjuterske mreže kao cilj napada* – napadaju se servisi, funkcije i sadržaji koji se nalaze na mreži. Kradu se usluge i podaci, oštećuju se ili uništavaju delovi ili cela mreža i kompjuterski sistemi, ili se ometaju funkcije njihovog rad.
- *Kompjuterske mreže kao sredstvo ili alat* - Danas moderni kriminalci koriste sve više kompjuterske mreže kao oruđa za realizaciju svojih namera.
- *Kompjuterske mreže kao okruženje u kome se napadi realizuju*, najčešće se kompjuterske mreže koriste za prikrivanje kriminalnih radnji. Postoje i druge uloge, kao što je npr. korišćenje mreže kao simbola zastrašivanja.

Osnove Internet i računarske bezbednosti

- Deseti kongresa UN (april 2000. godine), dokument Kriminal vezan za kompjuterske mreže (*Crime related to computer networks*), Konvenciji o sajber kriminalu (*Convention on Cybecrime*) :
- *„Pod ovim kriminalom podrazumeva "kriminal koji se odnosi na bilo koji oblik kriminala koji se može izvršavati sa kompjuterskim sistemima i mrežama, u kompjuterskim sistemima i mrežama ili protiv kompjuterskih sistema i mreža". To je, u suštini, kriminal koji se odvija u elektronskom okruženju. Ako se pod kompjuterskim sistemom podrazumeva "svaki uređaj ili grupa međusobno povezanih uređaja kojima se vrši automatska obrada podataka (ili bilo kojih drugih funkcija)" kako je to definisano."*

Co-funded by the European Union

Osnove Internet i računarske bezbednosti

- *Cyberspace*(sajber prostor) je termin za nefizički prostor koji stvaraju kompjuterski sistemi. Sajber prostor je veštačka tvorevina koja zahteva visoku tehničku opremljenost, dobru informacionu infrastrukturu i koji je ničija i svačija svojina, u kome paralelno koegzistiraju virtuelno i realno i kod koga je komunikacija kolektivna. U takvom okruženju izuzetno je teško govoriti o nacionalnim razmerama kriminala i društvenoj opasnosti, bar ne u konvencionalnom smislu reči

Co-funded by the European Union

Osnove Internet i računarske bezbednosti

Zavisno od tipa počinjenih dela sajber kriminal može biti:

- *politički*: sajber špijunaža; haking; sajber sabotaža; sajber terorizam; sajber ratovanje.
- *ekonomski*: sajber prevare; haking; krađa Internet usluga i vremena; piraterija softvera, mikročipova i baza podataka; sajber industrijska špijunaža; lažne Internet aukcije
- *proizvodnja i distribucija nedozvoljenih i štetnih sadržaja*: verske sekte; širenje rasističkih, nacističkih i sličnih ideja i stavova; zloupotreba žena i dece; manipulacija zabranjenim proizvodima, robama i supstancama, drogom, ljudskim organima i oružjem.
- *povrede sajber privatnosti*: nadgledanje e-pošte, spam, *phiching*, prisluškivanje, snimanje “pričaonica”, praćenje e-konferencija, *cookies*…

Co-funded by the European Union

Osnove Internet i računarske bezbednosti

- **Računarska sigurnost** (**cybersecurity**) odnosi se na zaštitu računarskih sistema, mreža i podataka od neovlašćenog pristupa, napada, oštećenja, ili krađe.

- **Cilj**: očuvanje poverljivosti, integriteta i dostupnosti podataka i resursa u informacionim sistemima.

- Tri principa -**CIA trijada** predstavljaju osnovu svih strategija zaštite informacionih sistema i osnovne smernice u razvoju sigurnosnih politika i sistema.

Osnove Internet i računarske bezbednosti

- CIA trijada:

- **Poverljivost** (Confidentiality) se odnosi na obezbeđivanje da informacije budu dostupne samo onima koji imaju odgovarajući autorizovani pristup. Ovo uključuje zaštitu podataka od neovlašćenog pristupa, curenja ili otkrivanja. Postupci koji omogućavaju poverljivost su npr. šifrovanje podataka i kontrola pristupa

- **Integritet** (Integrity) se odnosi na očuvanje tačnosti i doslednosti podataka. To znači da podaci ne smeju biti menjani ili oštećeni bez odgovarajuće autorizacije. Verifikacija integriteta podataka može se ostvariti pomoću tehnika poput heširanja ili digitalnih potpisa, koji osiguravaju da podaci nisu neovlašćeno izmenjeni.

- **Dostupnost** (Availability) označava sposobnost sistema da bude dostupan korisnicima i resursima kada su im potrebni. Ovo podrazumeva da infrastruktura, mreže i podaci moraju uvek da budu dostupni i operativni.jedna od pretnj su **DDoS napadi** (Distributed Denial of Service) koji imaju za cilj da onemoguće pristup podacima.

Osnove Internet i računarske bezbednosti

CIA trijada

Sajber pretnje i ranjivosti

- Sajber pretnje i ranjivosti su dva ključna problema u oblasti računarske bezbednosti, odnose se na različite načine na koje računarske mreže i sistemi mogu biti ugroženi.

- **Sajber pretnje** predstavljaju potencijalne opasnosti koje mogu negativno uticati na računarske sisteme i mreže. To su pokušaji ili akcije koje uključuju neovlašćen pristup, manipulaciju, uništavanje podataka ili ometanje rada sistema.

- Primeri sajber pretnji**:hakovanje**, **malver** (maliciozni softver), **phishing** napadi (prevara putem lažnih e-mailova ili web stranica) ili **ransomware** (otmica podataka), takodje i tzv. nenamerne greške (ljudska greška, konfiguracijska greška)

- **Sajber ranjivosti predstavljaju** slabosti u računarskim mrežama ili sistemima koje omogućavaju napadačima maliciozne aktivnosti.

- Primeri ranjivosti: programerske greške u kodu, loša zaštita lozinkama, nesigurni protokoli komunikacije ili neadekvatna zaštita od malvera.

Sajber pretnje i ranjivosti

- Maliciozni softver (**malware)** je svaki tip softverskog koda dizajniran da naškodi računarima, mrežama ili korisnicima s različitim ciljevima.

- Primeri malicioznog softvera: virusi i trojanaci, ransomware, spyware…

- **Virus** je softver koji se zakači za datoteke ili programime i širi se kopiranjem u druge fajlove, čineći da računar postane „zaražen“. Virusi obično imaju sposobnost da unište podatke i sistemske datoteke.

- **Trojanac (Trojan Horse)** je maliciozni program koji se maskira kao koristan ili neškodljiv softver, ali zapravo omogućava napadaču da pristupi i kontroliše računar. Za razliku od virusa, trojanci se ne repliciraju

- **Ransomware,** ovaj softver otima šifrovanjem podatke na računaru ili uređaju i traži otkupninu od žrtve u zamenu za dešifrovanje podataka. Ransomware može imati ozbiljne posledice jer može potpuno uništiti podatke korisnika.

Sajber pretnje i ranjivosti

- **Spyware** je softver koji prikuplja informacije o korisnicima bez njihovog znanja. To može uključivati lozinke, bankovne podatke ili druge lične informacije. Spyware obično prati aktivnosti korisnika na Internetu.

- **Adware** - Ovaj softver automatski prikazuje ili preuzima reklame na računaru. Iako nije nužno destruktivan kao neki drugi maliciozni softver, može biti vrlo iritantan i usporiti rad računara.

- **Rootkit** je softver dizajniran da sakrije prisustvo drugih malicioznih programa na računaru. Rootkit daje napadaču "root" ili administrativni pristup računaru, što omogućava kontrolu nad njim bez otkrivanja.

- **Worm** su samostalni maliciozni programi koji se repliciraju i šire putem mreža, najčešće preko e-pošte ili ranjivih tačaka u softveru. Mogu izazvati mrežne i računarske probleme.

Kriptografija i zaštita podataka

- **Kriptografija** je nauka koja u praksi obezbedjuje zaštitu informacija pomoću matematičkih algoritama,cilj je osiguravanje privatnosti, integriteta i autentifikacija podataka.

- Zaključujemo da su sigurnost podataka i kriptografija tesno povezane, čak se može reći da se bez kriptografije ne bi mogla realizovati zaštita informacija.

- Četiri osnovne funkcije Kriptografije su:
- povjerljivost (confidentiality),
- integritet podataka (data integrity),
- potvrdivanje identiteta (authentication) i
- neporicanje(non-repudiation).

Kriptografija i zaštita podataka

- **Povjerljivost,** obezbjedivanje da sadržaj informacija nije dostupan nikome drugom od onoga kome su informacije namijenjene. Ovo je najstarija namjena kriptografije. Ponekad se za ovu namjenu koriste termini privatnost ili tajnost.

- **Integritet podataka** je osiguravanje nepromjenjivosti podataka,tj. otkrivanje bilo kakve promene podataka. Pod promenama podataka se podrazumijevaju radnje kao ˇsto su dodavanje, uklanjanje ili zamena.

- **Potvrdivanje identiteta** je vezano za razmenu informacija. Njegova namena je identifikacija subjekata pri razmjeni informacija i same informacije. Elementi autentićnosti informacije su njeno poreklo, vreme nastajanja i vrijeme slanja. Ponekad se potvrdivanje identiteta deli na dvije klase: potvrdivanje identiteta entiteta i potvrdivanje porekla podataka.

- **Neporicanje** onemogućava negiranje prethodno učinjenih dela od strane bilo kog učesnika u njima. Sa aspekta razmene informacija ovo znači da ni jedna strana u toj razmeni ne može poreći svoje učešće u razmjeni i sadržaj razmenjenih informacija.

Co-funded by the European Union

Kriptografija i zaštita podataka

- **Simetrična kriptografija,** isti ključ se koristi za **šifrovanje** i **dešifrovanje** podataka. Ovaj ključ mora biti poznat i poverljiv između pošiljaoca i primaoca podataka. Zbog toga se simetrična kriptografija naziva i **"kriptovanjem sa zajedničkim ključem„**

- Simetrična kriptografija zahteva manje računarskih resursa, što je čini bržom i efikasnijom, naročito kada je potrebno šifrovati velike količine podataka. Nedostatak je prvenstveno izazov kako bezbedno preneti tajni ključ između pošiljaoca i primaoca.

- Algoritmi simetrične kriptografije:
- **AES (Advanced Encryption Standard)**: jedan od najpopularnijih i najsigurnijih simetričnih algoritama. Koristi ključeve različite dužine (128, 192, 256 bitova). Koristi se u industriji, bankarstvu itd.
- **DES (Data Encryption Standard)**: stariji algoritam koji se sada smatra nesigurnim zbog relativno kratkog ključa (56 bita).
- **3DES (Triple DES)**:Povećava sigurnost DES-a tako što šifruje podatke tri puta, koristeći tri različita ključa.
- **RC4 (Rivest Cipher 4)**: Stream cipher (strim šifra) koja se koristi za šifrovanje podataka u strimovima, poput HTTPS protokola.

Kriptografija i zaštita podataka

- **Asimetrična kriptografija** (**kriptografija sa javnim ključem**) je vrsta kriptografije u kojoj se koriste **dva različita ključa**: jedan za šifrovanje (**javni ključ**) i drugi za dešifrovanje (**privatni ključ**). Ovaj princip omogućava sigurnu komunikaciju, jer ne zahteva da dve strane dele tajne ključeve unapred.

- Javni ključ, slobodno se deli za šifrovanje podataka i verifikaciju digitalnog potpisa.
- Privatni ključ, tajni i koristi se samo pri dešifrovanju podataka.

- Primalac koristiti svoj **privatni ključ** za digitalno potpisivanje poruke, dok pošiljalac može koristiti javni ključ da verifikuje autentičnost potpisane poruke.

Kriptografija i zaštita podataka

- Algoritmi asimetrične kriptografije:

- **RSA** (Rivest-Shamir-Adleman):koristi se za šifrovanje podataka i digitalne potpise. RSA se temelji na matematičkom problemu faktorizacije velikih brojeva, obično se koriste ključevi od 2048 bita ili duži. RSA je široko korišćen u protokolima kao što su HTTPS i PGP.

- **ECC** (Elliptic Curve Cryptography): koristi eliptične krivulje za generisanje ključeva i omogućava viši nivo sigurnosti sa kraćim ključevima, koristi se u mobilnim uređajima i u novim sigurnosnim protokolima.

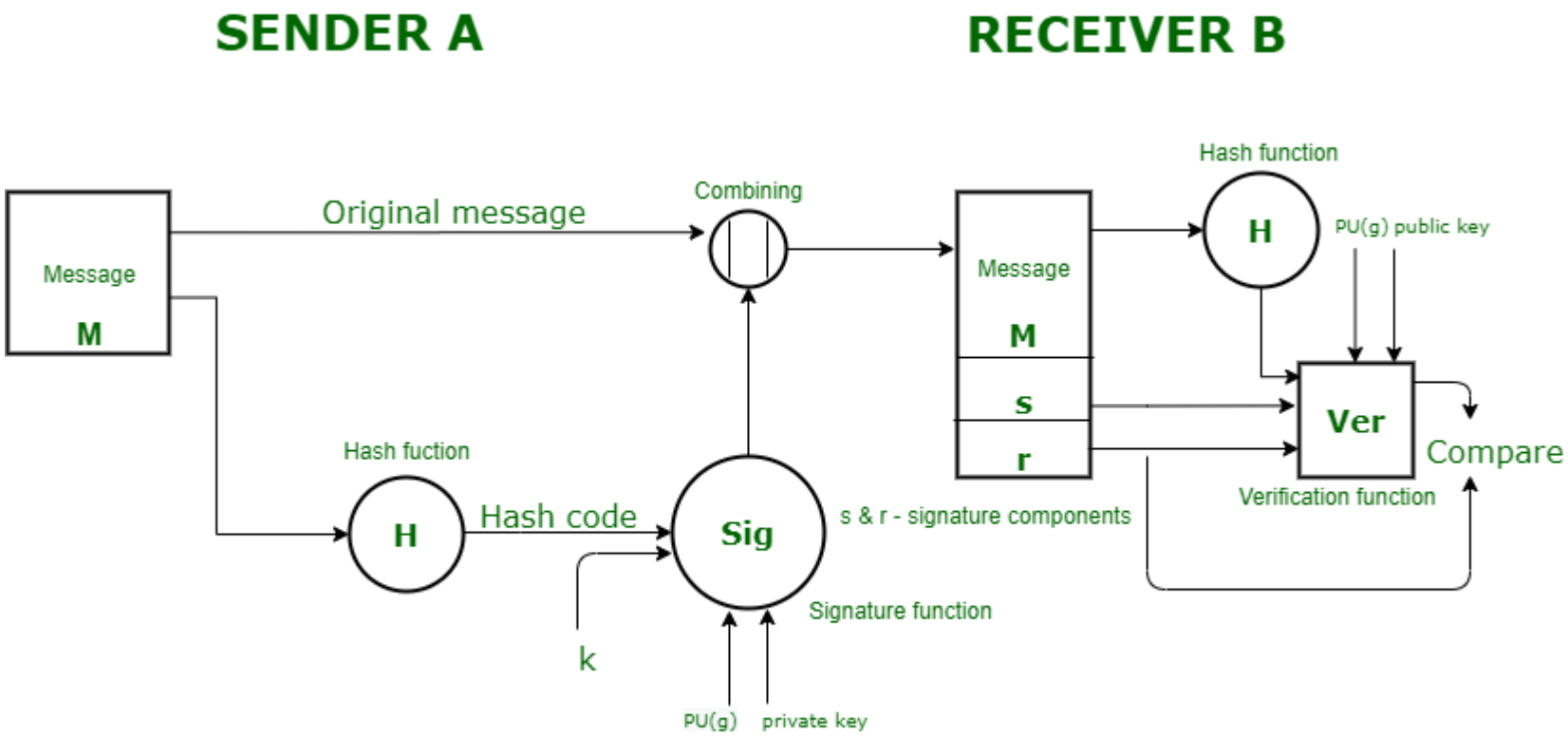
- **DSA** (Digital Signature Algorithm): koristi se za digitalne potpise, iako se danas uglavnom koristi u kombinaciji sa **SHA (Secure Hash Algorithm)** za kreiranje sigurnih potpisa. DSA je deo šireg sistema **Digital Signature Standard** (DSS).

Kriptografija i zaštita podataka

- Digitalni potpis (Digital Signature Standard-DSS)
- **Digitalni potpis** je matematički baziran na asimetričnoj kriptografiji i omogućava korisnicima da potvrde autentičnost poruka ili dokumenata. Koristi se kao softverski potpis(garantuje da softver nije izmenjen) i u E-mail komunikaciji.

- Pošiljalac koristi svoj **privatni ključ** da potpiše podatke (poruku, dokument, fajl, itd.), pomoću **hash funkcije** (koja generiše jedinstveni identifikator podataka), a zatim se taj hash potpisuje privatnim ključem.

- Primalac izračunava hash vrednost primljene poruke, zatim koristi javni ključ da dešifruje potpis i dobije originalnu hash vrednost. Ako se hash vrednosti podudaraju, to znači da podaci nisu izmenjeni i da su potpisani od strane pošiljaoca.


SENDER A
RECEIVER B
Message
M
Original message
Combining
Hash fuction
H
Hash code
Sig
k
PU(g)
private key
Signature function
s & r - signature components
Message
M
s
r
Hash function
H
PU(g) public key
Ver
Compare
Verification function

DSS

Kriptografija i zaštita podataka

- **Digitalni sertifikat** je elektronski dokument koji služi za verifikaciju identiteta pošiljaoca i omogućava korišćenje javnog ključa u kriptografskim operacijama.

- Sertifikat sadrži informacije o vlasniku, kao i njegov javni ključ, a sve je potpisano od strane pouzdane treće strane, zvane **sertifikacioni autoritet** (CA – Certification Authority). (CA) izdaje sertifikat vlasniku javnog ključa nakon što verifikuje identitet korisnika.

- **Sadržaj sertifikata**:
- **Javni ključ** korisnika
- **Podaci o korisniku**: ime, organizacija, e-mail adresa.
- **Podaci o sertifikaciji**: informacija o sertifikacionom autoritetu, datum izdavanja i isteka sertifikata.
- **Digitalni potpis CA**: Sertifikat je potpisan od strane CA kako bi se garantovalo da su informacije u njemu verifikovane i tačne.

Autentifikacija i autorizacija

- **Autentifikacija** i **autorizacija** su komponente u oblasti sigurnosti računarskih sistema i mreža. Iako se često koriste zajedno, predstavljaju različite faze u procesu obezbeđivanja pristupa resursima.

- **Autentifikacija** se odnosi na proces potvrde identiteta korisnika ili sistema.
- Mehanizama za autentifikaciju: korisničke lozinke, biometrija i dvofaktorska autentifikacija

- **Autorizacija** se odnosi na proces odlučivanja šta korisnik ili sistem može da uradi, odnosno koji su njegove mogućnosti za manipulaciju sadržajem.

-

Autentifikacija i autorizacija

- Korisnička lozinka predstavlja tajni niz znakova koji korisnicima omogućuje pristup datotekama, programima ili računarima. Ujedno, onemogućuje pristup neovlašćenim osobama tj.lozinka se koristi za autentikaciju i dokazivanje identiteta korisnika koji žele pristupiti određenim podacima ili mrežnim resursuma.
- Prednost-jednostavna implementacija
- Nedostatak-mogu biti slabe ili se otkriti phising napadima, ponavljanje lozinke povećava rizik

- Korištenje jednokratnih lozinki (eng. single-use password) Ovom metodom se smanjuju mogućnosti neovlaštenog pristupa (korisnička imena, lozinke, brojevi kreditnih kartica, itd.), informacijama i/ili datotekama. Istu lozinku je moguće koristiti jednom a za svaku sledeću prijavu je potrebno oblikovati novu lozinku. Primer korišćenja su jednokratne lozinke primljene SMS porukom koje se koriste za pristup pojedinim web usluga.

- Ova metoda za identifikaciju korisnika uglavnom se koristi u Internet bankarstvu. Vrlo je slična jednokratnim lozinkama, s tim što korisnici dobijaju posebne uređaje koje koriste kako bi dokazali svoj identitet.

Co-funded by
the European Union

Autentifikacija i autorizacija

- Biometrijske metode
- Biometrija je tehnika za proveru identiteta koja koristi jedinstvene fiziološke osobine svakog čoveka (otisak prsta, skeniranje rožnjače oka, DNK, itd).
-
- Biometrijski podaci se prikupljaju pomoću senzora i šalju na analizu, a pomoću njih se stvara biometrijski uzorak koji se uporedjuje sa ranije dobijenim uzorkom.

- Radi se o metodu koja je sigurniji od lozinki jer se temelji na specifičnostima svakog pojedinca.
- Nedostaci: cena (koja zavisi o tipu biometrijske provere) i činjenica da se korisnički podaci ne mogu promieniti ukoliko dođe do njihove kompromitacije.

Autentifikacija i autorizacija

- Dvofaktorska autentifikacija (2FA)

- Pojam dvofaktorska autentikacija (T-FA ili 2FA) je termin koji se koristi za opisivanje mehanizma za identifikaciju korišćenjem dva parametra.
-
- Dva osnovna faktora koja se pritom uzimaju u obzir su:

- nešto što je poznato korisniku ,to može biti npr. PIN broj i
- nešto što korisnik posjeduje, npr. mobilni uređaj sa kodom ili tokenom

- Primer takvih uređaja su token i/ili pametna kartica.
- Prednosti: povećava sigurnost u poređenju sa jednostavnom lozinkom, jer napadači moraju da poseduju oba faktora.

Autentifikacija i autorizacija

- **Protokoli za autentifikaciju**, omogućavaju sigurnu razmenu podataka o identitetu između klijenata i servera.

- **Kerberos** je protokol zasnovan na principu simetrične kriptografije koji omogućava autentifikaciju između klijenata i servera u distribuiranim mrežama. Kerberos koristi **Ticket Granting Ticket (TGT)** da bi omogućio pristup resursima u mreži.

- **OAuth (Open Authorization)** protokol za autorizaciju koji omogućava korisnicima da dele određene resurse sa trećim stranama, bez potrebe da dele svoje korisničke lozinke. U OAuth-u, korisnik odobrava aplikaciji pristup svom resursu putem "tokena".

- **OAuth 2.0** je verzija koja je vrlo popularna za autentifikaciju na web sajtovima i mobilnim aplikacijama.

Co-funded by the European Union

Bezbednost Web aplikacija

- Zbog svoje distupnosti putem Interneta Web aplikacije su često meta napada.

- S obzirom na sve veću upotrebu web aplikacija u poslovanju i svakodnevnom životu njihova bezbednost postaje bitan deo Internet i računarske bezbednosti.

- Web aplikacije su često izložene različitim vrstama napada. Neki od najčešćih i najopasnijih napada su:
- SQL Injection (SQLi)
- XSS (Cross-Site Scripting)
- CSRF (Cross-Site Request Forgery)

Co-funded by the European Union

Bezbednost Web aplikacija

- SQL Injection (SQLi)
- U standardnoj softverskoj praksi, SQL upit je zahtev koji se šalje bazi podataka za neku vrstu aktivnosti ili funkcije kao što je upit podataka ili izvršavanje SQL koda.

- Obično je ova vrsta web obrasca dizajnirana tako da prihvata samo vrlo specifične vrste podataka kao što su ime i/ili lozinka. Kada se ta informacija unese, provjerava se u bazi podataka, a ako se podudara, korisniku se dopušta ulaz u istu.

- Hakeri mogu iskoristiti ovu slabost i koristiti okvire za unos na obrascu za slanje vlastitih zahteva bazi podataka. Zbog rasprostranjenosti web stranica i servera koji koriste baze podataka, metoda napada SQL injekcije jedna je od najstarijih i najraširenijih vrsta napada.

- Zaštita: **parametrizovani upiti**: (odvajaju podatke od SQL koda, kako bi se sprečilo ubacivanje malicioznog koda), Upotreba ORM (Object-Relational Mapping) alata…

Bezbednost Web aplikacija

- XSS (Cross-Site Scripting) je napad u kojem napadač unosi zlonamerni JavaScript kod u web stranicu korisnika tj.napadač ubacuje JavaScript kod u formu ili URL parametar, što mu omogućava, da kada korisnik otvori stranicu, njihov browser izvršava napad.

- CSRF (Cross-Site Request Forgery) Napadač može poslati link koji, kada korisnik klikne na njega, automatski izvrši neovlašćenu radnju u aplikaciji, poput promena lozinke ili izvršavanja transfera novca.

Bezbednost Web aplikacija

- Opšti principi zaštite:
- **Princip najmanjih privilegija**: Korisnici i procesi treba da imaju minimalne privilegije koje su im potrebne za obavljanje svojih zadataka.
- **Redovno testiranje koda**: Korišćenje alata za statičku analizu koda kako bi se otkrile ranjivosti.
- **Ažuriranje**: Redovno ažuriranje biblioteka, framework-a i svih softverskih komponenti na poslednje sigurnosne verzije
- **Šifrovanje podataka**: Korišćenje jakih šifarskih algoritama za zaštitu podataka tokom prenosa (npr. SSL/TLS)
- **Sigurna pohrana lozinki**: Lozinke treba čuvati u šifrovanom formatu koristeći sigurnu tehniku kao što je **bcrypt** ili **Argon2**

Bezbednosni incidenti

- **Posledice incidenta**:
- Kompromitacija sistema, preuzimanje kontrole nad serverimai uredjajima
- Prekid usluga: DDoS napadi uzrokuju uskraćivanje usluga, posledica su finansijski gubici
- Narušavanje ugleda: napadi narušavaju poverenje korisnika i reputaciju preduzeća

- **Reakciju na sigurnosne incidente**:
- Detektovanje incidenta što je pre moguće, putem alata za nadzor i analizu logova
- Izolovanje pogođenih sistema kako bi se sprečilo dalje širenje napada. Na primer, isključivanje servera ili ograničavanje pristupa mreži
- Analiziranje incidenta pomoću forenzičkih tehnika kako bi se shvatilo šta se tačno dogodilo. To može uključivati analizu logova, mrežnog saobraćaja, sistemskih resursa i drugih podataka.
- Obnavljanje sistema i podataka sa sigurnih kopija. Takođe, proveriti da li su svi sistemi ispravni i sigurni pre nego što se ponovo omogući pristup korisnicima.
- Dokumentovanje svih koraka u odgovoru na incident, uključujući uzroke, posledice i strategije za sprečavanje ponovnih napada, izveštavanje nadležnih vlasti ako je to potrebno prema zakonodavstvu (npr. GDPR).

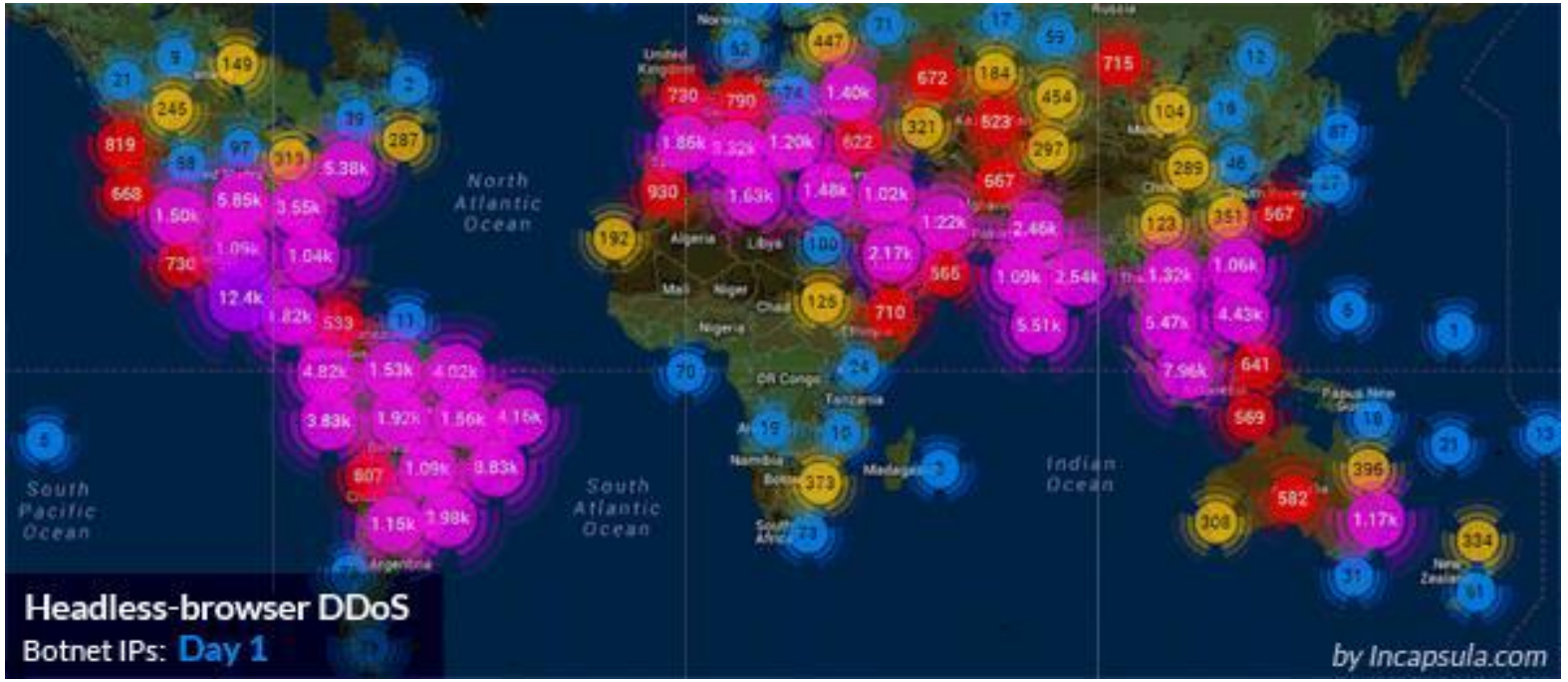
Bezbednosni incidenti

- Incidenti:
- **Distribuirani napad uskraćivanja usluge (DDoS)** nastoji da iscrpiti resurse sistema. DDoS napad inicira veliki broj host mašina zaraženih zlonamernim softverom koje kontroliše napadač.

- DDoS napai imaju tri oblika:

1. Napadi temeljeni na volumenu: Uključuje UDP poplave, ICMP poplave i druge poplave lažnih paketa. Cilj napada je zasićenje propusnosti napadnutog mesta, a veličina se meri u bitovima u sekundi (Bps).
2. Napadi protokola: Uključuje SYN poplave, fragmentirane paketne napade, Ping of Death, Smurf DDoS i još mnogo toga. Ova vrsta napada troši stvarne serverske resurse ili one posredne komunikacijske opreme, a mjeri se u paketima u sekundi (Pps).
3. Napadi na aplikacijski sloj: Uključuje niske i spore napade, GET/POST poplave, napade koji ciljaju ranjivosti Apachea, Windowsa i još mnogo toga. Sastoje se od naizgled legitimnih i nevinih zahteva, cilj ovih napada je rušenje web servera, a veličina se meri u zahtevima po sekundi (Rps).

Bezbednosni incidenti



DDoS napad

Bezbednosni incidenti

- Incidenti:
- **MITM napadi (čovek u sredini)**
- MITM napadi odnose se na kršenjea sajber sigurnosti, gde se napadaču omogućava da prisluškuje podatke koji se šalju napred-nazad između dve osobe, mreža ili računara. Napadač se pozicionira u “sredini” ili između dve strane koje komuniciraju, tj.napadač špijunira interakciju između dve strana. Napadačda nezakonito modifikuje poruku ili joj pristupa pre nego što stigne na odredište.

- **Phishing napad**
- Phishing napad ili napad krađe identiteta događa se kada zlonamerni akter šalje e-poruke za koje se čini da dolaze iz proverenih, legitimnih izvora u pokušaju da otkrije osetljive informacije od žrtve. Napadi krađe identiteta kombiniraju društveni inženjering i tehnologiju, a takozvani su zato što napadač zapravo "lovi" pristup zabranjenom području koristeći "mamac" naizgled pouzdanog pošiljatelja.
- Pored elektronske pošte, fišeri koriste i druge servise na Internetu kao što su Windows Messenger, Skype, Google Talk, društvene mreže (Facebook, Twitter, Pinterest) i dr.

Bezbednosni incidenti

- Incidenti:
- **Brute force napad**
- Brute Force Attack dobio je ime po "brutalnoj" ili jednostavnoj metodologiji koju koristi napadač. Metod se sastoji od sledećih koraka:

1. Napadač jednostavno pokušava pogoditi akreditaciju za prijavu nekoga ko ima pristup ciljnom sistemu. Iako ovo može izgledati dugotrajno i teško, napadači često koriste botove za probijanje akreditacija
2. Napadač daje botu popis akreditacija za koje misle da im mogu omogućiti pristup sigurnom području. Bot zatim pokušava svaki od njih sve dok ne pogodi.

- **Botnet napad**
- Izraz "botnet" nastao je od riječi "robot" i "mreža". Sastavljanje botneta obično je faza infiltracije višeslojne šeme. Botovi služe kao alat za automatizaciju masovnih napada, kao što su krađa podataka, rušenje servera i distribucija zlonamernog softvera. Botovi koriste vaše uređaje i ubrzaju sposobnost hakera za izvođenje većih napada.

Co-funded by the European Union

Zaštita mreža

- Mreže su često meta napada jer omogućavaju komunikaciju i prenos podataka među uređajima, ukoliko nisu pravilno zaštićene, može doći do ozbiljnih sigurnosnih incidenata. Zaštita mreža obuhvata različite tehnologije i strategije za sprečavanje, otkrivanje i odgovaranje na napade.

- **Vrste mrežnih topologija:**
- **Zvjezdasta topologija**: Svi uređaji su povezani sa centralnim uređajem (switch ili router). Iako je efikasna u smislu kontrole,takodje je i ranjiv ako je centralni uredjaj kompromitovan.
- **Bus topologija**: Svi uređaji su povezani na jedan kabel (bus). Ova topologija je sklonija napadima poput **sniffing-a** (presretanje saobraćaja).
- **Ring topologija**: Uređaji su povezani u kružni lanac. U ovoj topologiji, napadi mogu uticati na celu mrežu ako je jedan uređaj preuzet ili oštećen.
- **Mesh topologija**: Svi uređaji su povezani sa svim drugim uređajima. Ova topologija je najotpornija na napade, ali i najkompleksnija.

Zaštita mreža

- Alati zaštite:

- **Firewall** je osnovni sigurnosni alat koji štiti mrežu od neovlašćenog pristupa filtrirajući dolazni i odlazni saobraćaj prema definisanim sigurnosnim pravilima.
- **Packet-filtering firewall**: analizuje svaki paket podataka koji ulazi ili izlazi iz mreže i odlučuje hoće li ga propustiti ili blokirati na osnovu unapred definisanih pravil
- **Stateful inspection firewall**: prati stanje svih otvorenih konekcija i omogućava/proverava pakete samo ako su deo legitimne sesije
- **Proxy firewall**: zamenjuje pravu mrežnu adresu sa sopstvenom, čime skrivaju mrežnu infrastrukturu i sprečavaju direktnu interakciju sa spoljnim svetom.

- Namena Firewalla:
- Ograničavanje pristupa određenim uslugama ili portovima
- Blokiranje neovlašćenog saobraćaja

Zaštita mreža

- Alati zaštite:

- IDS/IPS (Intrusion Detection/Prevention)
- **Intrusion Detection System (IDS)** je alat koji otkriva sumnjive aktivnosti u mreži i upozorava administratore na potencijalnu pretnju. IDS ne blokira napad, već pruža obaveštenje o incidentu.
- **Intrusion Prevention System (IPS)**, je preventivni alat koji ne samo da otkriva napad, već i blokira ili sprečava napad u realnom vremenu.

- Namena IDS/IPS alata:
- Detekcija zlonamernog saobraćaja
- Upozorenja na pokušaje neovlašćenog ulaska u mrežu
- Skenira potencijalne ranjivosti

Zaštita mreža

- Alati zaštite:

- Virtualne privatne mreže (VPN)
- **VPN** (Virtual Private Network) omogućava bezbednu i šifrovanu komunikaciju između uređaja u javnoj mreži, kao što je Internet.

- VPN obezbedjuje:
- Maskiranje IP adrese: obezbedjuje anonimnost na Internetu.
- Šifrovanje saobraćaja: koristi šifrovane tunel-protokole (npr. **IPSec**, **SSL**, **OpenVPN**) da zaštiti podatke koji putuju od korisnika ka cilju
- Pristup udaljenim mrežama: omogućava korisnicima da pristupe internoj mreži organizacije, kao da su fizički prisutni u toj mreži, što je korisno za rad na daljinu ili pristupanje osetljivim podacima.

Trendovi u računarskoj bezbednosti

- **Sigurnost IoT (Internet of Things) uredjaja:**

- **IoT** uređaji su postali sve prisutniji u domaćinstvima i poslovnim okruženjima
- **Sigurnost IoT uređaja** predstavlja izazov zbog broja uređaja povezanih na Internet i specifičnih ranjivosti samih uredjaja. IoT uređaji su prisutni u različitim oblastima, uključujući domove, industriju, zdravstvo, transport...
- IoT uređaji nude velike prednosti u smislu automatizacije, efikasnosti i povezanosti,ali i značajan sigurnosni rizik.

- Slabosti IoT:
- Koriste se slabe lozinke ili nemaju autentifikaciju
- Najčešće ne koriste šifrovanje
- Neredovno ažuriranje
- Prekomerna pravapristupa
- Fizička ranjivost samih uređaja
- Nedostatak sigurnosnih standarda

Trendovi u računarskoj bezbednosti

- Sigurnost IoT (Internet of Things) uredjaja se može poboljšati:
- Enkripcija komunikacije: Protokoli poput TLS (Transport Layer Security) ili SSL (Secure Sockets Layer) mogu biti korišćeni za osiguranje komunikacije.
- OAuth i OpenID Connect i Dvostruka autentifikacija
- Segmentacija mreže: IoT uređaji bi trebalo da budu povezani na odvojene mreže od drugih kritičnih sistema. VLAN (Virtual Local Area Networks) i segmentacija sa firewall-om mogu pomoći u postizanju ove zaštite.
- Fizička zaštita
- Upotreba sigurnosnih protokola kao što su DTLS (Datagram Transport Layer Security) i MQTT (Message Queuing Telemetry Transport)

Trendovi u računarskoj bezbednosti

- **Korišćenje veštačke inteligencije (AI) u bezbednosti**
- AI i mašinsko učenje (ML) mogu značajno poboljšati sigurnost, omogućavajući brže prepoznavanje napada, automatske odgovore na incidente, predviđanje pretnji i analizu velikih količina podataka u realnom vremenu.

- Primena AI u bezbednosti:
- Automatska detekcija pretnji
- Prediktivna analitika: AI analizira prethodne napade i pravi model koji predviđa vrste napada u budućnosti.
- Automatizovani odgovori na pretnje (SOAR- Security Orchestration, Automation, and Response) : izolacija kompromitovanih sistema, blokiranje IP adresa napadača, ili automatsko obaveštavanje administratora.
- Prepoznavanje socijalnog inženjeringa (phishing, vishing): AI analizira e-mailove, SMS poruke, pozive, mogu se analizirati tekstovi, prepoznavati sumnjive fraze, linkovi, lažno predstavljanje. **Natural Language Processing (NLP)** tehnike omogućavaju analizu jezika i stilova pisanja
- Korišćenje AI za analizu sigurnosnih logova

Trendovi u računarskoj bezbednosti

- **Blockchain tehnologija**
- **Blockchain** je tehnologija distribuirane baze podataka. Ovaj princip omogućava sigurno i transparentno beleženje podataka u "blokovima", koji su povezani u linijsku, nepromenljivu i **decentralizovanu** strukturu.
- Svaki blok u blockchainu sadrži podatke (transakcije, informacije ili druge vrste zapisa), **vremensku oznaku** i jedinstveni **hash** prethodnog bloka. Kroz ovu strukturu, blockchain omogućava **transparentno** i **sigurno čuvanje podataka**, bez potrebe za centralizovanim posrednikom ili autoritetom.
- Upotreba blockchaina:
- Kriptovalute: primena blockchain tehnologije je u **kriptovalutama** (npr. Bitcoin), decentralizovane transakcije bez potrebe za tradicionalnim bankama ili posrednicima.
- Pametni ugovori (Smart Contracts) omogućavaju automatizaciju i izvršenje ugovornih obaveza bez potrebe za posrednicima, kada su uslovi ispunjeni, pametni ugovor se automatski izvršava.
- Supply Chain Management (Upravljanje lancem snabdevanja)
- Digitalni identitet: smanjuje rizik od krađe identiteta.
- Zdravstvo:sigurnost i efikasnost u deljenju medicinskih podataka, omogućavajući siguran pristup i kontrolu podataka od strane pacijenata i lekara.

Propisi iz oblasti sajber bezbednosto

- Savet Evrope (engl. CoE) okuplja 47 zemalja članica. Njegova Konvencija o sajber kriminalu (poznata kao **'Budimpeštanska konvencija'**) smatra se, za sada, najrelevantnijim međunarodnim pravnim instrumentom koji daje pravni okvir za borbu protiv sajber kriminala.

- Budimpeštanska konvencija pruža državama i spisak napada koji se smatraju prekršajima, a počinjeni su preko kompjutera, i proceduralne pravne alate za sprovođenje istraga o sajber kriminalu, kao i efektivno čuvanje elektronskih dokaza počinjenim prekršajima, a omogućava i međunarodnu policijsku i sudsku saradnju po pitanju sajber krminala i razmene e-dokaza.

- CoE je sastavio Konvenciju o zaštiti pojedinaca i automatske obrade ličnih podataka (**konvencija pod brojem CETS 108**),koja ima za cilj da 'zaštiti svakog pojedinca, bez obzira na njegovu nacionalnost ili mesto prebivališta, kao i obradu njihovih ličnih
- podataka i na taj način doprinese poštovanju njihovih ljudskih prava i fundamentalni sloboda, a posebno prava na privatnost'.

Propisi iz oblasti sajber bezbednosto

- Organizacija za evropsku bezbednost i saradnju (engl. OSCE) bavi se sajber/IKT bezbednosnim problemima, a posebno u svetlu borbe protiv terorizma i sajber kriminala. OEBS je 2013.godine usvojio mere izgradnje poverenja (engl. CBMs) za sajber proctor putem Odluke Stalnog saveta broj 1106, 3.decembra 2013. godine. Ove mere imaju za cilj da smanje sukobe koji se javljaju kao posledica korišćenja informacionokomunikacionih tehnologija.
- Organizacija američkih država (engl. OAS) je osnovala Radnu grupu za sajber criminal već 1999. godine kao osnovni forum za ’jačanje međunarodne saradnje na temu prevencije, istraga i gonjenja sajber krminala, kao i omogućavanje razmene informacija i iskustava između njenih članova i davanja neophodnih preporuka za unapređivanje i obezbeđivanje aktivnosti u cilju borbe protiv ove vrste prestupa.
- Šangajska organizacija za saradnju (engl. SCO), međunarodna organizacija koja okuplja šest država članica (Kinu, Kazahstan, Kirgistan, Rusiju, Tadžikistan i Uzbekistan), usvojila je 2009.godine Sporazum između vlada zemalja članica SCO-a o saradnji na polju obezbeđivanja međunarodne informacione bezbednosti.

Propisi iz oblasti sajber bezbednosto

- EU je 2013. godine objavila svoj prvi sveobuhvatni dokument, svoju Strategiju sajber bezbednosti, koja se odnosi na široki spektar sajber pretnji. EU je 2016. godine usvojila Direktivu o bezbednosti mreža i informacionih sistema (engl. NIS Directive).

- Prva politika sajber odbrane Severno-alantskog saveza (engl. NATO) je izašla 2008. godine. Na Lisabonskom samitu 2010. godine sajber odbrana je ušla u Strateški concept NATO-a i deklaracija koja je usvojena na samitu predvidela je neophodnost ažuriranj Politike sajber bezbednosti iz 2011. godine i izradu pratećeg Akcionog plana iz 2012. godine.

Propisi iz oblasti sajber bezbednosto

- Države širom sveta razvijaju i usvajaju strategije kako bi mogle da reaguju na ove sve veće bezbednosne pretnje, što uključuje usvajanje novih ili izmenu i dopunu postojećih nacionalnih politika bezbednosti. Nacionalne politike bezbednosti koje se bave pretnjama u sajber prostoru nazivaju se nacionalne strategije sajber bezbednosti (engl. NCSS).

- Međunarodna telekomunikaciona unija (engl. ITU) definiše nacionalnu strategiju sajber bezbednosti (NCSS) kao:
- izraz vizije najvažnijih ciljeva, principa i prioriteta kojima se jedna zemlja rukovodi u borbi protiv sajber pretnji;
- pregled interesnih strana koje imaju zadatak da poboljšaju sajber bezbednost države i njihove odgovarajuće uloge i odgovornosti;
- opis koraka, programa i inicijativa koje će zemlja da preduzme kako bi zaštitila svoju nacionalnu sajber infrastrukturu, i na taj način povećala bezbednost i prilagodljivost.

Propisi iz oblasti sajber bezbednosto

- Zvanična statistika ukazuje na trend porasta broja sajber napada i slučajeva sajber kriminala u Srbiji. Tokom 2020. godine dogodilo se oko 26 miliona sajber napada na sisteme informacionih i komunikacionih tehnologija (IKT) – od kojih su najčeši bili pokušaji upada u IKT sisteme i neovlašeno prikupljanje podataka.
- Oblast informacione bezbednosti u Srbiji regulisana je Zakonom o informacionoj bezbednosti iz 2016. godine, kojim se definišu prava, dužnosti i odgovornosti svih pravnih lica i državnih organa koji upravljaju i koriste IKT sisteme.
- U ovom zakonu detaljno se opisuju mere zaštite od izazova, rizika i pretnji u vezi sa IKT sistemima. Takođe se navode organi nadležni za zaštitu ovih sistema, oblici koordinacije između ovih aktera i sprovođenje propisanih mera
- Tri godine nakon usvajanja, ovaj zakon je izmenjen i dopunjen kako bi se poboljšala njegova primena i rešili problemi koji su identifikovani u praksi.
- .

Propisi iz oblasti sajber bezbednosto

- Akteri u sektoru informacione bezbednosti:

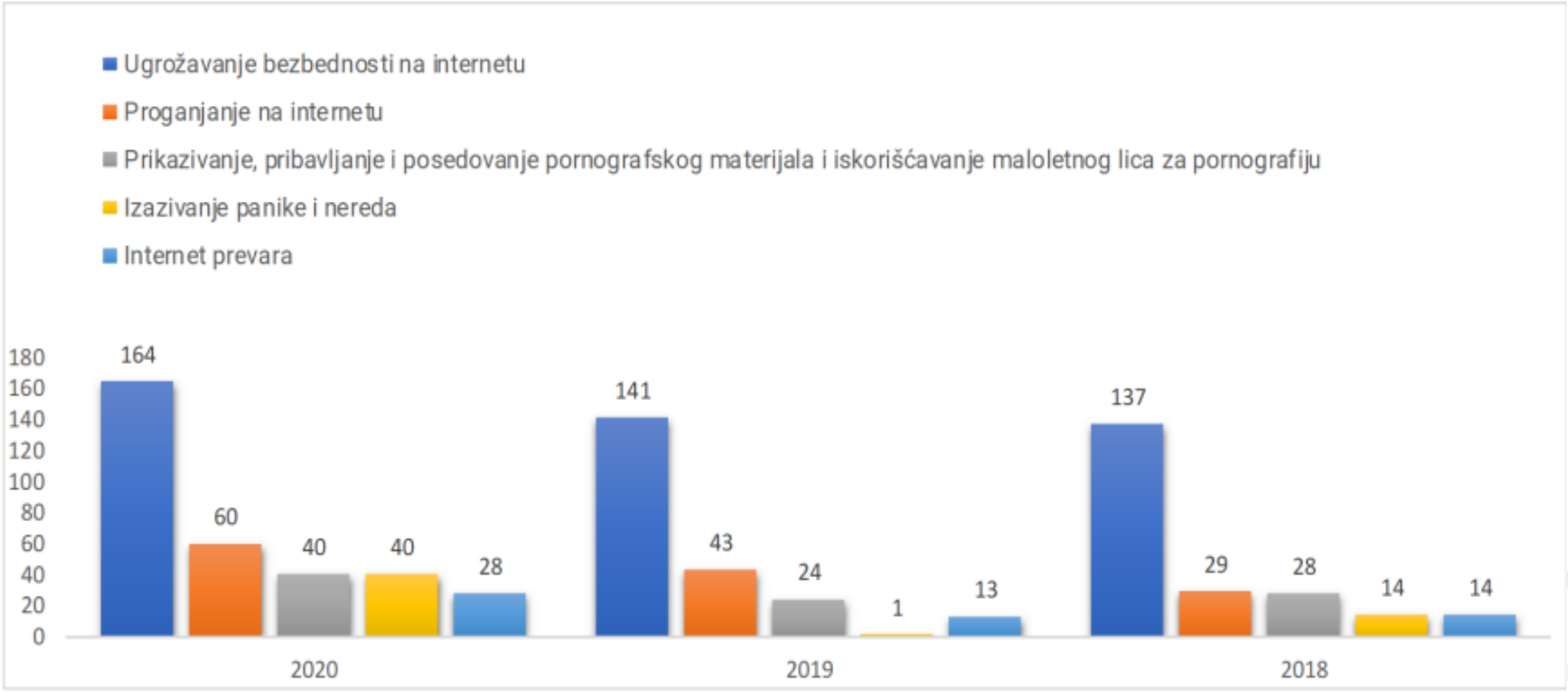
- Glavne državne institucije u oblasti informacione bezbednosti su MTTT, Regulatorna agencija za elektronske komunikacije i poštanske usluge (RATEL) i njen računarski tim za hitne slučajeve (CERT), kao i Telo za koordinaciju poslova informacione bezbednosti.

- Pravo na privatnost je regulisano sistemskim Zakonom o zaštiti podataka o ličnosti iz 2018. godine, koji je usklađen sa Opštom uredbom EU o zaštiti podataka o ličnosti (GDPR)

- **GDPR (General Data Protection Regulation)** je **regulativa Evropske unije (EU)** koja je usvojena 2016. godine i postala obavezna 2018. godine. Cilj GDPR-a je da zaštiti privatnost i lične podatke građana EU i da im obezbedi veću kontrolu nad tim podacima.

- **PCI-DSS (Payment Card Industry Data Security Standard)** je set sigurnosnih standarda koji je razvijen od strane **Payment Card Industry Security Standards Council (PCI SSC)**, a odnosi se na zaštitu podataka o kreditnim karticama. PCI-DSS ima za cilj da poboljša sigurnost transakcija i zaštiti korisnike od **krađe identiteta** i **prevara**.

Propisi iz oblasti sajber bezbednosto



Najčešće vrste sajber kriminala u Srbiji, izvor: Republičko javno tužilaštvo

WBnet

Co-funded by the European Union

Questions & Answers

"Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them."

Network of centers for regional short study programs in the countries of the Western Balkans

Call: ERASMUS-EDU-2023-CBHE

Project number: 101128813

ATYCC

UNIVERSITY OF L]UBL]ANA
Faculty of Electrical Engineering

POLITÉCNICA

University of Pristina
Kosovska Mitrovica