Sajber bezbjednost

Računarski sistemi i mreže

- **Svrha korišćenja** je različita: za komunikaciju, bankarstvo, kupovina, zabava, društveni život
- Organizacije često obrađuju **osjetljive podatke** o klijentima i partnerima, kao i finansijske informacije i intelektualno vlasništvo
- **Rizici**: sajber napadi, krađa ličnih podataka, kontrola uređaja/sistema

Računarski sistemi i mreže

- Organizacije svakodnevno upravljaju velikim brojem zaposlenih, koji imaju pristup velikom broju **internih resursa**
- U interne resurse svrstavamo od **poslovnih naloga elektronske pošte** do **povjerljivih finansijskih podataka i ugovora**
- Bez **odgovarajuće zaštite**, ovi **resursi** mogu biti **kompromitovani**, a **podaci izloženi krađi ili zloupotrebi**
- Na ovaj način, može doći do **nepoželjnih posljedica**:

Računarski sistemi i mreže

1) **Reputacionoj šteti** po kompaniji u očima klijenata i strateških partnera;
2) **Finansijskoj šteti** u vidu plaćanja zakonskih kazni zbog gubitka osjetljivih i povjerljivih informacija;
3) **Finansijskom trošku** saniranja posljedica sajber incidenta;
4) **Potencijalnim tužbama** vlasnika ukradenih podataka

Računarski sistemi i mreže

Zato je neophodno preduzeti **preventivne mjere**: upotrebu **jake lozinke**, **redovno ažuriranje softvera**, **instaliranje antivirusa** i ostalih **bezbjednosnih alata**, kao i pridržavanje najboljih **praksi za zaštitu ličnih i poslovnih informacija**

Definicija sajber bezbjednosti

- Predstavlja **zaštitu** računarskih sistema, mreža i podataka od neovlašćenog pristupa, oštećenja ili krađe
- Primjenom **tehnologije, procesa i politika** obezbjeđuje **integritet, povjerljivost i dostupnost** informacija i resursa, koji su kritični za poslovanje organizacije ili pojedinca
- Različite tehnologije i procesi: **šifrovanje**, **firewall**, **antivirusni programi**, **softverske zakrpe**, **autentifikacija i autorizaciju korisnika**, **sigurnosne politike i procedure**

Definicija sajber bezbjednosti

- Važna je i **edukacija o bezbjednom korišćenju** računarskih sistema i mreža (**podizanje svijesti** korisnika računarskih sistema)
- Najbolji način da se zaštitite od prijetnji: **temeljno razumijevanje i usvajanje pravila ponašanja** za prepoznavanje i reagovanje na sajber napade

Definicija sajber bezbjednosti

- *"Sajber bezbjednost jedne organizacije je snažna onoliko koliko i njena najslabija karika. Potrebna je samo jedna slaba tačka da se izazove domino efekat koji napadačima daje pristup osjetljivim internim resursima."*
- *"Sajber bezbjednost je štit čiji je zadatak da odgovori na različite vrste prijetnji koje mogu doći iz virtuelnog svijeta, kao što su razni zlonamjerni softveri (malware), phishing, ransomware, kao i neovlašćeni pristupi i krađe podataka."*
- *"Cilj plana je da pomaže poslovnoj organizaciji da identifikuje svoje ranjivosti i uspostavi protokole za rješavanje bilo kakvih problema u vezi sa sajber bezbjednošću."*

Sajber kriminal

- **Antagonisti sajber bezbjednosti**, koriste tehnologiju u negativne svrhe
- Različitim tehnikama i alatima izvršavaju **hakovanje računara, krađu podataka, izradu zlonamjernih softvera**
- **Razlog**: finansijski, lični, politički, ideološki
- Rade **samostalno** ili u **grupama/organizacijama**

Sajber kriminal

- *"Kada su sajber prijetnje u pitanju, važno je razlikovati "način dostave" od "paketa". Prvo se odnosi na metode koje sajber kriminalci koriste kako bi infiltrirali maliciozne softvere na računarske sisteme, dok "paket" predstavlja različite vrste malicioznih softvera."*
- *"Napadači mogu da prisluškuju i ukradu privatne informacije, kao što su lozinke, finansijski i lični podaci. Takođe, napadači mogu da iskoriste nezaštićene rutere kako bi preusmjerili korisnike na lažne veb-sajtove koje izgledaju autentično, čime korisnici mogu biti prevareni i dovedeni u opasnost od malvera."*

Sajber kriminal

Uobičajene zablude vezane za sajber kriminal:

1. Sajber kriminalce ne zanimaju moji podaci
2. Čak i da ukradu moje podatke, oni su beskorisni
3. Sajber kriminalci su nemoćni, ako imam antivirus
4. Sajber kriminalac je isto što i haker

Zabluda #1: Sajber kriminalce ne zanimaju moji podaci

- Iako izgleda da može biti tačno, ovo Vas **ne čini bezbjednim - naprotiv**
- Sajber kriminal počiva na **krađi i preprodaji** ogromnih količina osjetljivih, ličnih i drugih tipova **podataka**
- Ovi procesi su zadnjih godina postali **automatizovani**, pa se tako angažuju "**botovi**"
- Bot - program sa jasnim instrukcijama da pretražuje Internet u potrazi za propustima, a zatim infiltriraju malver ili kradu dostupne podatke

Zabluda #2: Čak i da ukradu moje podatke, oni su beskorisni

- Naši lični podaci = vrata drugim, osjetljivijim informacijama i sistemima
- **Koristeći jednu istu lozinku** za svaki Vaš nalog, napadačima **omogućava pristup** vaše elektronske pošte i drugih podataka
- Ukoliko su podaci kompromitovani, mogu **prouzrokovati** štetu Vama, i drugima oko Vas u digitalnoj sferi

Zabluda #3: Sajber kriminalci su nemoćni, ako imam antivirus

- Koristan je, ali **nije univerzalno rješenje** za svaku prijetnju
- Kao što postoje antivirusi, tako postoje alati i programi za **neutralizovanje** njihovih zaštitnih kapaciteta i mogućnost **infiltriranja** u računarske sisteme
- Sajber kriminalci često koriste **naivnost svojih meta** (spuštaju “gard svog računara” i instaliraju zlonamjerne softvere)
- Ne postoji stopostotno rješenje koje garantuje apsolutnu bezbjednost

Zabluda #4: Sajber kriminalac je isto što i haker

- Koriste se kao sinonimi, iako zapravo nisu isti
- Hakeri - stručnjaci za sajber bezbjednost koji **koriste svoje znanje u etičke svrhe** (white hat)
- Sajber kriminalci - **koriste svoje tehničko znanje isključivo u nezakonite svrhe**, kao što su krađa podataka, iznuda novca ili sabotiranje sistema (black hat)

Dark Web – Mračna strana interneta

- **Centar zbivanja, obavljanja ilegalnih radnji** anonimno i sa bezbjedne distance
- Dio Interneta koji **nije indeksiran** od strane pretraživača („sakriven“ ili „nevidljiv“)
- U ovom virtuelnom prostoru se izvršava **prodaja** i/ili **razmjena hakerskih usluga**, **koordinacija sajber napada**, kao i **razmjena informacija o ranjivostima** u sistemima
- **Nije preporučljivo** posjećivati ove zabačene uglove Interneta

Dark Web – Mračna strana interneta

- Njenim funkcionisanjem su: ilegalne radnje postale **svakodnevnica**, **primopredaja** ukradenih podataka **omogućena**, usluge **pristupačne**
- Ovakva rasprostanjenost je doprinijela ogromnim ulaganjima **u borbu protiv sajber kriminala**
- **Kazne variraju od novčanih do zatvorskih**, a odnose se kako na pružaoce, tako i primaoce usluga
- Vodeće svjetske agencije za borbu protiv kriminala: **Interpol, FBI**

Dark Web – Mračna strana interneta

PONUDA/USLUGA NA DARK

Socijalni inženjering

- **Manipulisanje žrtvom** da preuzme i aktivira malver, ili da oda osjetljive informacije
- Napadač se predstavlja kao **osoba od povjerenja** (poput službenika tehničke podrške)
- Može se lažno predstaviti preko e-mejla, SMS-a, društvenih mreža
- Upotrebljava se i sa ostalim tehnikama: **phishing**, **deepfake**

Socijalni inženjering

- **“Socijalni kameleoni” -** uvijek nađu način da iskoriste nadolazeće tehnologije u zlonamjerne svrhe
- **Stara taktika** za manipulisanje ljudi i prikupljanja osjetljivih informacija i podataka
- “Vaše ponašanje je ono što sajber kriminalci pokušavaju da eksploatišu”
- **Na prepad ili sofisticiran način mogu doći do svog cilja**

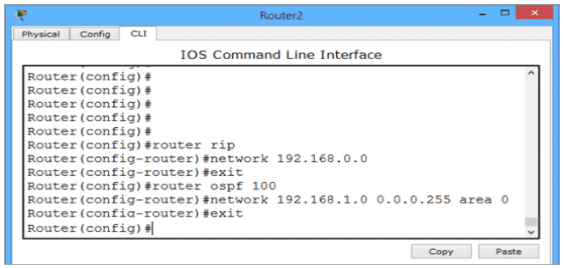
Kako se zaštititi od socijalnog inženjeringa

Par uputstava koje bi bilo poželjno primjenjivati, da biste izbjegli ovakve situacije:

1) **Edukujte se** (o taktikama socijalnog inženjeringa)
2) **Aktivirajte dvofaktornu autentifikaciju** na svim nalozima
3) **Koristite jake lozinke**
4) **Ograničite pristup informacijama na društvenim mrežama** (samo na ljude koje lično poznajete)
5) **Podaci koji ne treba da budu javno dostupni** - broj telefona, škola koju ste pohađali, radno mjesto, pozicija, adresa
6) **Ne odajte lične podatke strancima** (onlajn i/ili uživo)

Kako zaštititi svoju Wi-Fi mrežu

- **Wi-Fi** - tehnologija koja omogućuje uređajima, poput računara i drugih, bežično komuniciranje jednih s drugima
- **Fabrička podešavanja** rutera **sadrže propuste** koje sajber kriminalci mogu iskoristiti
- Treba **izvršiti dodatna podešavanja** rutera
- Nekoliko preporučenih postupaka kojima ćete učiniti vašu konekciju na Internet znatno bezbjednijom:



Kako zaštititi svoju Wi-Fi mrežu

1. Promijenite šifru za Wi-Fi mreže
2. Isključite WPS
3. Isključite SSID emitovanje
4. Aktivirajte WPA3 enkripciju
5. Aktivirajte mrežu za goste i za IoT uređaje
6. Koristite Firewall
7. Ažurirajte softver rutera barem jednom godišnje
8. Koristite VPN

Savjeti za bezbjedno surfovanje i onlajn kupovinu

Da biste se zaštitili od raznih prevara i malvera onlajn, morate:

1. Uvijek provjeriti da li sajt koji posjećujete ima HTTPS sertifikat koji garantuje enkripciju podataka.
2. Koristite sigurne Internet konekcije i zaštićene sajtove za onlajn kupovinu.
3. Ako koristite Apple uređaj, aktivirajte opciju “sakrij moju e-adresu” (hide my email).
4. Ako koristite Mozilla pretraživač, ova funkcija se zove Firefox Relay.
5. Ako je moguće, koristite alternativne načine plaćanja, poput PayPal-a.