Cyber sigurnost (osnove)

Ispit pitanja su također iz materijala o ovim poveznice

Upute za do 6 bodova na ispit (6 +14 na ispitu)

Slijedite upute u dokumentu „Instructions for creating free account on Fortinet Training Institute 2025.pdf" nalazi se na infoeduka pod „Ostali materijali "

Svi studenti **koji imaju** Fortinet certificate od prošle godine trebaju se enrolati u online edukaciju "Introduction to CyberSecurity " na poveznici : https://www.netacad.com/courses/introduction-to-cybersecurity?courseLang=en-US&instance_id=26f8a22f-b38a-4bd3-bb26-da65a3867e3d

Za korisnički račun koristite svoje stvarno ime i prezime

Certifikate pošaljite meni putem maila silvio.papic@algebra.hr i također uploadajte certifikat na infoeduku kao "seminarsk rad"

https://youtu.be/msciBqowPgk?si=hhSgrGnbjs-oLYa6&t=471

CyberSecurity

Ispitno pitanje

- **Sigurnost u kontekstu IT tehnologija možemo definirati kao kontinuirani proces zaštite digitalnih informacija (podataka) i IT resursa (računala, serveri, usmjernici, preklopnici itd…) od unutarnjih i vanjskih zlonamjernih ili slučajnih prijetnji.**
- **Ovaj proces obuhvaća detekciju, prevenciju i odgovor na prijetnje kroz korištenje sigurnosnih politika, programskih alata i IT servisa...**

- **Ranjivosti sustava** su slabosti ili nedostaci u softveru, hardveru ili sigurnosnim politikama koje **napadači** mogu iskoristiti I dobiti neovlašteni pristup sustavu , nanijeti štetu sustavu ili njegovim resursima , izvući osjetljive podatke za osobnu korist.

CyberSecurity

Ispitno pitanje

- Kibernetička sigurnost ključna je u osobnom i poslovnom kontekstu za zaštitu osjetljivih podataka te osiguranje privatnosti, povjerenja u sustava (poslovanje) i neprekinutog rada sustava (poslovanja).
- U današnjem međusobno povezanom svijetu, što više informacija dijelimo online, to smo ranjiviji na kibernetičke prijetnje.
- Kako bismo smanjili te rizike, ključno je usvojiti najbolje prakse, poput ograničavanja količine osobnih podataka koje dijelimo na internetu. Time se smanjuje izloženost prijetnjama i povećava sigurnost.
- Posebnu pažnju treba posvetiti zaštiti osjetljivih podataka/informacija, uključujući:
  - Medicinske podatke, poput zdravstvenih kartona, recepata i povijesti bolesti;
  - Obrazovne podatke, kao što su akademski zapisi, svjedodžbe i detalji o upisu;
  - Podatke o zaposlenju i financijama, uključujući bankovne podatke, informacije o plaćama i profesionalnu povijest;
  - Osobne dokumente, poput osobnih iskaznica, vozačkih dozvola i drugih službenih dokumenata.

Zašto su podaci važni

Ispitno pitanje

U digitalnom dobu podaci su **jedno od najvrjednijih sredstava za pojedince, tvrtke i vlade** .
Osobni podaci, financijska evidencija, intelektualno vlasništvo i informacije o kupcima ključni su za poslovanje i donošenje odluka.

Ekonomska vrijednost:
Podaci pokreću inovacije, marketing i angažman kupaca.
Mnoge se tvrtke oslanjaju na analitiku podataka kako bi optimizirale poslovanje i dobile konkurentsku prednost.

Zaštita privatnosti i identiteta:
Osobni podaci su osjetljive prirode jer sadrže imena, adrese, povijest bolesti i financijski detalji.
Zaštita ovih podataka ključna je za očuvanje privatnosti i sprječavanje krađe identiteta.

Kontinuitet rada:
Organizacije trebaju siguran i pouzdan pristup svojim podacima kako bi učinkovito funkcionirale.
Gubitak podataka ili povrede mogu poremetiti rad, što dovodi do financijske štete i štete po ugled.

Usklađenost sa zakonima i propisima :
Vlade provode stroge propise (npr. GDPR-Opća uredba o zaštiti podataka) za zaštitu podataka.
Neuspjeh u osiguravanju podataka može rezultirati visokim kaznama i pravnim obvezama.

Nacionalna sigurnost:
Vlade ovise o sigurnim podacima za kritičnu infrastrukturu, obranu i obavještajne operacije.
Povrede mogu ugroziti nacionalnu i javnu sigurnost.

Zašto je važna Kibernetička sigurnost

Ispitno pitanje

1.Zaštita od prijetnji:
- Kibernetička sigurnost štiti od raznih prijetnji poput zlonamjernog softvera, krađe identiteta, ransomwarea i hakiranja.
- Bez snažnih mjera kibernetičke sigurnosti, sustavi su osjetljivi na provale i prekide.

2.Održavanje povjerenja:
- Kupci, klijenti i partneri trebaju jamstvo da su njihovi podaci sigurni.
- Povreda može narušiti povjerenje, uzrokujući dugoročnu štetu ugledu.

3.Sprječavanje financijskih gubitaka:
- Kibernetički napadi mogu rezultirati značajnim financijskim gubicima zbog prekida rada, plaćanja otkupnine ili krađe.
- Proaktivna kibernetička sigurnost smanjuje vjerojatnost i učinak takvih gubitaka.

4.Očuvanje inovacija:
- Krađa intelektualnog vlasništva može potkopati godine istraživanja i razvoja.
- Kibernetička sigurnost osigurava da inovacije ostanu zaštićene od konkurenata ili zlonamjernih aktera.

5.Zaštita osobne privatnosti:
- Kibernetička sigurnost štiti osobne podatke pojedinaca od zlouporabe, krađe identiteta i prijevare.
- Neophodno je za održavanje osjećaja sigurnosti u digitalnom svijetu.

6.Ublažavanje rizika novih tehnologija:
- Uz porast IoT-a, AI-a i računalstva u oblaku, kibernetička sigurnost je ključna u zaštiti povezanih uređaja i usluga.
- Osigurava da tehnološki napredak nije ometan sigurnosnim problemima.

7.Usklađenost sa standardima:
- Organizacije se moraju pridržavati standarda i propisa kibernetičke sigurnosti kako bi poslovale zakonito.
- Kibernetička sigurnost osigurava usklađenost i izbjegava kazne.-standardi su rezultat puno negativnih iskustava

Gdje su (naši) podaci, tko ih koristi i u koju svrhu?

1. **Podaci na društvenim mrežama:**
   - Što se događa sa slikama i videozapisima koje postavljamo na Facebook ili druge društvene mreže?
   - Dijele li ih, analiziraju ili unovčavaju treće strane bez našeg izričitog pristanka?
2. **Podaci iz internetskih pretraživanja i kupovnih navika:**
   - Kako se prikupljaju i koriste podaci o našim internetskim pretraživanjima ili kupovnim navikama (npr. korištenje kartice vjernosti)?
   - Prodaje li se oglašivačima ili posrednicima podataka?
3. **Vlasništvo i korištenje podataka:**
   - Kako možemo identificirati tko je vlasnik naših podataka i u koje se svrhe koriste?
   - Postoje li transparentni mehanizmi za praćenje ili kontrolu ove upotrebe?
4. **Utjecaj povrede podataka:**
   - Što se događa ako nam netko "provali" u računalo?
   - Kako bi ukradeni podaci — poput osobnih fotografija, financijskih informacija ili radnih dokumenata — mogli utjecati na naše živote?
5. **Digitalni uređaji kao vektori napada:**
   - Svaki digitalni uređaj, bez obzira na vrstu, može postati potencijalni vektor za napade usmjerene na podatke, usluge ili infrastrukturu.
6. **Rizici operativnog sustava i aplikacija:**
   - Hakerski napadi jednako su opasni na svim operativnim sustavima (Linux, Mac ili Windows).
   - Primarni rizik leži u **broju korisnika** na sustavu i **raznolikosti aplikacija i usluga** koje podržava.
   - Napadači su usredotočeni na **korisnike** , a ne na tehnologiju, jer ljudska pogreška ili ponašanje često predstavljaju najslabiju kariku.

Vrste od napadača

- **Amateri ("Script Kiddies") Tko su:**
  - Neiskusni pojedinci s malo ili nimalo tehničkih vještina.
  - Za izvođenje napada oslanjaju se na već postojeće alate i gotove upute koje mogu pronaći na internetu.

Motivacija:

- Potaknuti znatiželjom ili željom da pokažu svoje "vještine".

utjecaj:

- Unatoč nedostatku stručnosti, još uvijek mogu prouzročiti značajnu štetu neodgovornom uporabom moćnih alata.

Pojedinačni hakeri

Hakerski napadi razlikuju se ovisno o etičkom stavu i namjeri pojedinca. Ovi hakeri imaju za cilj provaliti sustave, često s određenim ciljevima na umu.

White hat hakeri:

- Stručnjaci koji identificiraju ranjivosti sustava kako bi ojačali sigurnost.
  - **Cilj:** Pomoć organizacijama prijavljivanjem nedostataka vlasnicima sustava.
  - **Primjer:** hakiranje automobila radi demonstracije ranjivosti u kibernetičkoj sigurnosti automobila.

Gray hat hakeri:

- Djeluju u sivoj zoni između White I Black hat
- Mogu iskorištavati ranjivosti bez dopuštenja, ali nemaju nužno za cilj nanijeti štetu.

Black hat hakeri:

- Zlonamjerni hakeri čiji je primarni cilj ometanje sustava, krađa podataka ili nanošenje štete.
- Njihovo djelovanje je nezakonito, destruktivno i usmjereno na osobnu ili financijsku korist.

Vrste od napadači

- **Organizirani hakeri:**
  - Visoko kvalificirane i organizirane grupe, koje često financiraju velike organizacije ili vlade.
- **Motivacija:**
  - Ove skupine djeluju s određenim ciljevima kao što su špijunaža, sabotaža ili financijska dobit.
  - **Vrste organiziranih hakera:**
    - **Cyberkriminalci:** Usredotočite se na aktivnosti usmjerene na profit kao što su ransomware, prijevara i krađa podataka.
    - **Cyber teroristi:** Koristite hakiranje kao alat za strah, poremećaje i političke ili ideološke ciljeve.
    - **Cyber Warriors:** Državno sponzorirani hakeri koji se bave špijunažom, sabotažom ili cyber ratovanjem.
  - **utjecaj:**
    - Njihove su operacije često velike, sofisticirane i sposobne izazvati globalne posljedice.

Hacker Profiles

The Yes Men Fix the World

Prikazan u filmu „The Railway Men - The Untold Story Of Bhopal 1984” - Netflix

Kako vas "hakeri" mogu iskoristiti?

Hakeri imaju više načina da dođu do vas, prvenstveno putem vaših uređaja povezanih s internetom kao što su mobilni telefoni, računala, prijenosna računala ili tableti.

- Međutim, nisu svi napadi digitalni ; neki mogu uključivati fizičke, stvarne taktike za ugrožavanje vaših podataka ili sigurnosti.

Čak i ako mislite da niste zanimljivi hakerima, evo nekoliko uobičajenih razloga zašto bi vas mogli ciljati:

1.Koriste vas kao "proxy":

1. Hakeri bi mogli iskoristiti vaš uređaj kao dio botneta za napade kao što je Distributed Denial-of-Service (DDoS).
2. Vaš uređaj može poslužiti kao odskočna daska za maskiranje njihovog identiteta dok ciljaju na druge.

2.Novčana dobit:

1. Jednostavne prijevare poput phishing e-pošte mogu vas prevariti da podijelite financijske podatke (npr. informacije o kreditnoj kartici ili banci).
2. Hakeri ciljaju na lake prilike za financijsku krađu, posebno od korisnika koji nisu svjesni sigurnosnih prijetnji .

3.Iskorištavanje podataka:

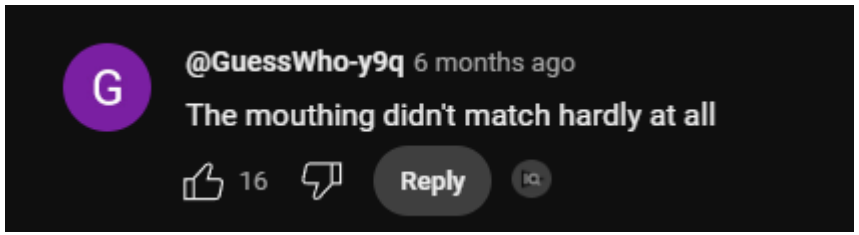
1. Sve što radite na svom računalu ili internetu potencijalno se može iskoristiti protiv vas .
2. Osobni podaci, navike pregledavanja i mrežne aktivnosti dragocjeni su kibernetičkim kriminalcima za prijevaru, krađu identiteta ili ucjenu.

Budućnost nosi još sofisticiranije kibernetičke prijetnje, zbog čega je ključno zaštititi se i online i offline.
Na primjer, izmišljeni scenariji, poput onih prikazanih u traileru za *Unknown Identity* (Liam Neeson, 2011.) , služe kao podsjetnik da su krađa identiteta i manipulacija vrlo stvarne opasnosti.

Kako vas "hakeri" mogu iskoristiti?

Can you spot the deepfake? How AI is threatening elections
https://youtu.be/B4jNttRvbpU?si=o5gUWJffbkm584Pl&t=110

Deepfake example. Original/Deepfake close shot Bill Gates.
https://youtu.be/WzK1MBEpkJ0?si=mgnHGf4NerCGct0O



- Kako tehnologija poput deepfakeova čini da se obmana sve manje može razlikovati od stvarnosti, kritičko razmišljanje postaje bitno.
- Iako alati za otkrivanje mogu pomoći, oni nisu univerzalno dostupni niti su jamstvo.
- Kritičko razmišljanje osnažuje pojedince da ispituju, analiziraju i provjeravaju informacije, štiteći ih od manipulacije i dezinformacija. Potiče otpornost, pomaže u održavanju povjerenja u demokratske procese i osigurava da se pojedinci ne oslanjaju isključivo na “vanjsku obranu” (da će netko razmišljati umjesto vas).
- U digitalnom svijetu koji se brzo razvija, kritičko razmišljanje je najodrživija i najprilagodljivija zaštita od prijevare.

Praktični koraci za sigurnost

1.Zaštitite svoje online račune:
- Koristite jake, jedinstvene lozinke za svaki račun.
- Omogućite provjeru autentičnosti s više faktora (MFA) gdje god je to moguće.

2.Budite oprezni s mrežnim aktivnostima:
- Izbjegavajte klikanje na sumnjive veze ili odgovaranje na neželjenu e-poštu u kojoj se traže osjetljivi podaci.
- Redovito nadzirite svoje račune za neovlaštene aktivnosti.

3.Čuvajte svoj identitet:
- Ograničite osobne podatke koje dijelite na internetu, uključujući društvene medije.
- Prije pružanja osjetljivih podataka provjerite legitimnost bilo koje online platforme ili usluge.

4.Održavajte veze u stvarnom životu:
- Uravnotežite svoj digitalni život s odnosima u stvarnom svijetu kako biste spriječili pretjeranu ovisnost o online interakcijama.

Hacking and how it is not done: The Most Accurate Hacking Scene Ever ☺

Sigurnost podataka: osobna i korporativna dimenzija

I u osobnom iu korporativnom kontekstu, sigurnost podataka vrti se oko tri temeljna načela: **povjerljivosti** , **integriteta** i **dostupnosti** . Bez obzira odnose li se podaci na privatni ili poslovni život, ova su načela ključna za sigurno i pouzdano upravljanje podacima.

Ispitno pitanje

1. Povjerljivost: Zaštita privatnosti

•**Definicija:** Osigurava da osjetljivim podacima pristupaju samo ovlaštene osobe .

•**Važnost:** zaštita osobnih i poslovnih podataka od neovlaštenog pristupa sprječava provale, krađu i zlouporabu.

•**Metode za osiguranje povjerljivosti:**

- **Enkripcija:** Pretvara podatke u siguran format koji mogu dešifrirati samo ovlaštene strane.
- **Mehanizmi provjere autentičnosti:** korištenje korisničkih imena, lozinki i višestruke provjere autentičnosti za kontrolu pristupa.
- **Minimizirana izloženost podataka:** Ograničite dostupnost osjetljivih podataka samo onima kojima su potrebni.
- **Korporativna pravila:** jasne smjernice koje definiraju ograničenja pristupa podacima i sigurnosne protokole.

Sigurnost podataka: osobna i korporativna dimenzija

2. Integritet: osiguranje dosljednosti i pouzdanosti podataka
•**Definicija:** Održava točnost, dosljednost i pouzdanost podataka tijekom njihovog životnog ciklusa.
•**Važnost:** Osigurava da podaci ostanu nepromijenjeni tijekom pohrane, prijenosa i upotrebe.
•**Metode za osiguranje integriteta:**

- **Checksums and Hashing:** Provjerava da podaci nisu izmijenjeni tijekom prijenosa ili pohrane.
- **Kontrola pristupa:** Dozvole za datoteke i mehanizmi kontrole pristupa korisnika sprječavaju neovlaštene promjene.
- **Sigurnosne kopije:** redovite sigurnosne kopije podataka štite od oštećenja ili slučajnih promjena.

Ispitno pitanje

3. Dostupnost: Osiguravanje pouzdanog pristupa
•**Definicija:** Osigurava da su podaci i usluge dostupni kada je potrebno, unatoč potencijalnim prekidima .
•**Važnost:** Podržava besprijekorne osobne i poslovne operacije, čak i u slučaju nesreća ili napada.
•**Metode za osiguranje dostupnosti:**

- **Održavanje i ažuriranja:** Redovita ažuriranja hardvera, operativnih sustava i softvera.
- **Postupci oporavka podataka:** Pripremljeni planovi i sigurnosne kopije za vraćanje podataka u slučaju gubitka zbog ljudske pogreške ili katastrofe.
- **Mehanizmi zaštite:** uređaji poput vatrozida i obrane od DoS napada pomažu u održavanju dostupnosti podataka/usluga.

Prijetnje — unutarnje i vanjski

Unutarnje prijetnje potječu iz organizacije i često proizlaze iz ljudske pogreške, loše prakse upravljanja ili namjernih radnji insajdera. Ključne unutarnje prijetnje uključuju:

1. **Loše upravljanje povjerljivim podacima:**
    1. Neadekvatna zaštita ili loše upravljanje osjetljivim informacijama.
    2. Primjeri: slabe kontrole pristupa, nezaštićena pohrana ili nepropisno odlaganje povjerljivih podataka.
2. **Prijetnje fizičkoj infrastrukturi:**
    1. Fizički rizici poput požara, poplave, nestanka struje ili namjernog oštećenja IT sustava.
    2. Može dovesti do prekida rada sustava, gubitka podataka ili ugroženih operacija.
3. **Pomoć vanjskim napadačima:**
    1. **Namjerna pomoć:** Zlonamjerni insajderi dijele informacije ili pristup s vanjskim napadačima.
    2. **Nenamjerna pomoć:** Zaposlenici koji nesvjesno pomažu napadačima tako što postaju žrtve krađe identiteta ili društvenog inženjeringa (ili su našli USB stick na podu ☺).
4. **Nemarno ponašanje na internetu:**
    1. Zaposlenici koji se bave rizičnim online aktivnostima, kao što su:
        1. Klik na zlonamjerne poveznice.
        2. Preuzimanje zlonamjernog softvera.
        3. Nasjedanje na prijevare društvenog inženjeringa (npr. krađa identiteta ili pretekst).

Prijetnje — unutarnje i vanjski

Vanjske prijetnje potječu od aktera ili izvora izvan kontroliranog okruženja organizacije.

Ove prijetnje uključuju:

- **Pokušaj hakiranja:** Ciljanje ranjivosti u sustavima, aplikacijama ili mrežama.
- **Napadi zlonamjernog softvera:** korištenje zlonamjernog softvera poput ransomwarea, spywarea ili virusa za ugrožavanje sustava.
- **Kampanje krađe identiteta:** obmanjujuća komunikacija usmjerena na krađu osjetljivih podataka.
- **Distribuirani napadi uskraćivanja usluge (DDoS):** preplavljuju sustave prometom koji ometa operacije.
- **Fizički upad:** Neovlašteni pristup vanjskih aktera objektima organizacije.

Posljedice napad

Ispitno pitanje

1. **Financijski gubici:** izravni troškovi od prijevare ili ransomwarea i neizravni gubici zbog prekida rada ili gubitka kupaca.
2. **Reputacijska šteta:** Gubitak povjerenja, negativna medijska pokrivenost i smanjena vjerodostojnost.
3. **Povrede podataka (Data breaches):** Izlaganje osjetljivih podataka, krađa intelektualnog vlasništva i regulatorne kazne.
4. **Operativni prekidi:** Zastoji, nedostupni sustavi i zaustavljeni poslovni poslovi.
5. **Pravna i regulatorna pitanja:** Novčane kazne za nepridržavanje i tužbe pogođenih strana.
6. **Strateški nedostaci:** konkurenti stječu povjerljive informacije (uvide-insights), preusmjeravanje resursa i usporavanje inovacije.
7. **Psihološki učinak:** Stres i smanjeno povjerenje u digitalne sustave.

?

Sigurnosne ranjivosti

Načelno ih možemo podijeliti na;

1. **Software**: Ovaj dio predstavljaju greške u programskom kodu (web browser, mobilne aplikacije, serverske aplikacije…) ili operacijskom sustavu (Windows, Linux, Apple…)-kao prevencija napada je redovito updateanje softwarea ili operacijskog sustava prema preporukama proizvođača
2. **Hardware**: Ovaj dio predstavlja greške u dizajnu hardware komponenata, npr. RAM memorija (RowHammer) ili neke druge komponente…Napadi na fizičke komponente se vrlo rijetko koriste u realnosti osim za mete visokog značaja u kontekstu Cyberwarfare

- Hackers Remotely Kill a Jeep on the Highway—With Me in It
- Hacking the Wi-Fi IoT Coffee Machine
- Hack All The Things: 20 Devices in 45 Minutes ☺

Ovo je bilo prije 9-10 godina!

We Stole a Tesla with this $20 Device

HACKING VEHICLES WITH THIS $20 RADIO!!!

Shocking moment thieves ‘hack car’s HEADLIGHTS’ to break into brand-new motor and speed away in less than 30 seconds
https://www.thescottishsun.co.uk/motors/13648727/shocking-moment-thieves-hack-cars-headlights/

Vrste malwarea

Ispitno pitanje

Virusi

Definicija: Virus je maliciozni kod koji se „prikači” na legitiman program ili datoteku i širi se kada se program pokrene.

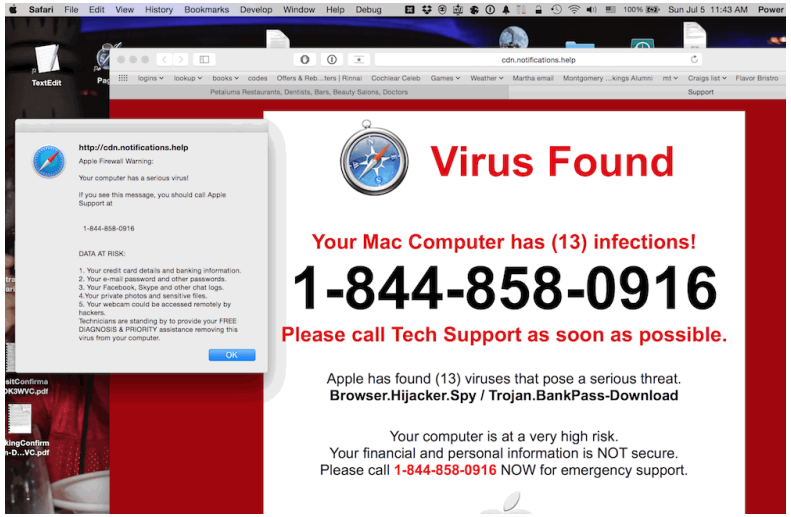
Karakteristike:

- Za širenje je potrebna radnja korisnika (poput otvaranja zaražene datoteke).
- Može mijenjati, pokvariti ili izbrisati datoteke i programe.

Kako radi:

- „Prikači” se izvršnim datotekama.
- Aktivira se kada se pokrene zaražena datoteka.
- Replicira se širenjem na druge datoteke i sustave.

Utjecaj: usporava sustave, briše podatke ili uzrokuje rušenje cijelog sustava.



Vrste malwarea

Ispitno pitanje

Crvi

Definicija: Crvi su samostalni zlćudni programi koji se repliciraju kako bi se širili mrežama bez potrebe za intervencijom korisnika.

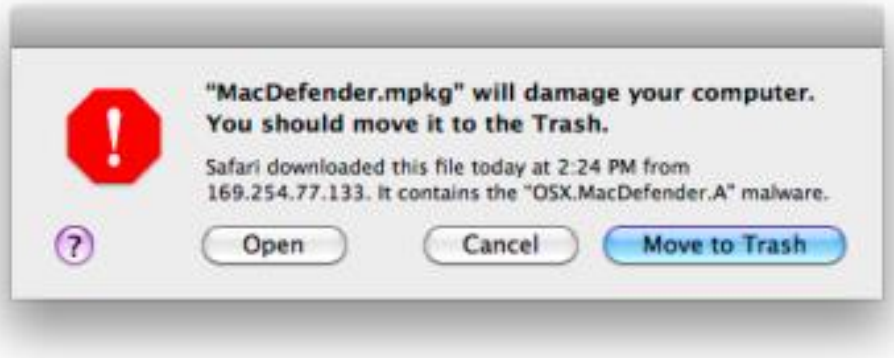
Karakteristike:

- Može se brzo širiti kroz sustave.
- Iskorištava ranjivosti u mrežnim protokolima ili operativnim sustavima.

Kako radi:

- Identificira ranjivost u mreži ili sustavu.
- Replicira se i prenosi na druge uređaje.

Utjecaj: troši propusnost mreže, ruši sustave i širi drugi zlonamjerni softver.



Cyberratovanje - Stuxnet crv

Samo za edukacijske svrhe :

Stuxnet decoder Ralph Langner speaks about Stuxnet

The World's First Cyber Weapon Attack on a Nuclear Plant | Cyberwar
https://www.youtube.com/watch?v=dobTyPKccMA

Vrste malwarea

Ispitno pitanje

Trojanci

Definicija: Trojanac (skraćenica za "trojanski konj") maskira se kao legitiman softver, ali izvodi zlonamjerne aktivnosti nakon što se instalira.

Karakteristike:

- Oslanja se na društveni inženjering kako bi prevario korisnike da instaliraju.
- Često služi kao stražnja vrata za napadače za pristup sustavima.

Kako radi:

- Maskira se kao bezopasna datoteka ili aplikacija.
- Prilikom otvaranja izvršava zlonamjerni kod.

Utjecaj: krađa podataka, ugrožavanje sustava ili isporuka dodatnog zlonamjernog softvera**.**

Vrste malwarea

Ispitno pitanje

Rootkitovi
Definicija: Rootkitovi su programi koji pružaju privilegirani pristup sustavu dok skrivaju svoju prisutnost.
Karakteristike:

- Teško za otkrivanje i uklanjanje.
- Često se koristi za održavanje dugoročnog pristupa ugroženom sustavu.

Kako radi:

- Instalira se na razini kernela ili aplikacije.
- Skriva se od alata za otkrivanje.

Utjecaj: Daje napadačima kontrolu nad sustavom, dopuštajući veliku štetu ili krađu podataka.

Vrste malwarea

Ispitno pitanje

Spyware („špijunski software”)
Definicija: špijunski softver potajno prikuplja informacije o korisniku ili organizaciji, često ih šaljući trećoj strani.
Karakteristike:

- Djeluje tajno kako bi izbjegao otkrivanje.
- Može pratiti navike pregledavanja, uhvatiti pritiske tipki ili ukrasti osjetljive podatke.

Kako radi:

- Instalira se putem zlonamjernih preuzimanja ili softvera.
- Prati i bilježi aktivnost korisnika.

Utjecaj: krađa podataka, krađa identiteta ili ugrožena privatnost.

Vrste malwarea

Ispitno pitanje

Ransomware

Definicija: Ransomware kriptira žrtvine datoteke ili zaključava njihov sustav, zahtijevajući plaćanje (obično u kriptovaluti) za vraćanje pristupa.

Karakteristike:

- Isporučuje se putem phishing e-pošte, zlonamjernih preuzimanja ili ranjivosti softvera.
- Često popraćena porukom o otkupnini s uputama za plaćanje**.**

Kako radi:

- Inficira sustav i kriptira datoteke.
- Prikazuje poruku o otkupnini koja zahtijeva plaćanje.

Utjecaj: Gubitak kritičnih podataka i mogući financijski gubici ako sigurnosne kopije nisu dostupne.

Vrste malwarea

Ispitno pitanje

Botneti

Definicija: Botnet je mreža zaraženih uređaja ("botovi") kojima upravlja napadač (botmaster) radi izvođenja koordiniranih radnji.

Karakteristike:

- Uređaji u botnetu često djeluju bez znanja svojih vlasnika.
- Koristi se za napade distribuiranog uskraćivanja usluge (DDoS), slanje neželjene pošte ili rudarenje kriptovaluta.

Kako radi:

- Inficira uređaje putem ranjivosti ili zlonamjernog softvera.
- Povezuje uređaje s poslužiteljem za upravljanje i kontrolu (C&C-Command and Control)).
- Izvršava koordinirane napade ili zadatke.

Utjecaj: preopterećuje poslužitelje, prekida usluge, ili krade podatke u zlonamjerne svrhe.

Vrste malwarea

Ispitno pitanje

Adware
Definicija: Adware je softver koji automatski prikazuje neželjene reklame, često u paketu s besplatnim softverom.
Karakteristike:
- Generira prihod za napadače putem klikova na oglase.
- Može usporiti sustave i dovesti do daljnjih infekcija zlonamjernim softverom.

Kako radi:
- Instalira se uz legitiman softver.
- Prikazuje nametljive oglase, često preusmjeravajući korisnike na zlonamjerne web stranice.

Utjecaj: Ometa korisničko iskustvo, narušava privatnost i može uvesti drugi zlonamjerni softver**.**

Vrste malwarea-dodatno

15 infamous malware attacks: The first and the worst
https://www.csoonline.com/article/572911/11-infamous-malware-attacks-the-first-and-the-worst.html

The 16 Major Types of Malware – Defined
https://secureops.com/blog/16-types-of-malware/

The 12 Most Common Types of Malware
https://www.crowdstrike.com/en-us/cybersecurity-101/malware/types-of-malware/

FILELESS MALWARE EXPLAINED
https://www.crowdstrike.com/en-us/cybersecurity-101/malware/fileless-malware/

WHAT IS A POLYMORPHIC VIRUS? DETECTION AND BEST PRACTICES
https://www.crowdstrike.com/en-us/cybersecurity-101/malware/polymorphic-virus/

Simptomi malware napada

Ispitno pitanje

Uobičajeni simptomi zaraze zlonamjernim softverom

Bez obzira na vrstu zlonamjernog softvera, sljedeći znakovi mogu ukazivati na zaraženi sustav:

1. **Povećana upotreba CPU-a**: Sustav doživljava neuobičajeno visoku aktivnost procesora, čak i kada je u mirovanju.
2. **Smanjene performanse računala**: Primjetno usporavanje općih operacija ili odziva računala.
3. **Često zamrzavanje ili pad sustava**: Računalo se zamrzava, ruši ili se neočekivano ponovno pokreće.
4. **Sporije pregledavanje weba:** performanse interneta opadaju, a stranice se učitavaju sporije nego inače.
5. **Neobjašnjivi problemi s mrežom**: Prekidi u mrežnoj povezanosti ili neuobičajeni skokovi u korištenju podataka.
6. **Neuobičajene izmjene datoteka:** datoteke su izmijenjene, oštećene ili pokazuju sumnjive promjene.
7. **Neočekivana brisanja datoteka:** Važne datoteke se brišu bez radnje korisnika.
8. Izgled nepoznatih datoteka ili ikona: Pojavljuju se nove, neprepoznate datoteke, programi ili ikone na radnoj površini.
9. **Prisutnost nepoznatih procesa:** Nepoznati procesi rade u pozadini, često trošeći resurse sustava.
10. **Programi se nepravilno ponašaju:** Aplikacije se neočekivano zatvaraju, rekonfiguriraju ili se ponašaju neuobičajeno.
11. **Neovlaštena aktivnost e-pošte:** e-poruke se šalju s vašeg računa bez vašeg znanja ili pristanka.

Antimalware softver

The Best Antivirus Software for 2025
https://www.pcmag.com/picks/the-best-antivirus-protection

Best Virus Protection 2024
https://www.antivirusguide.com/best-virus-protection/

?

Vrste napada

Ispitno pitanje

Category	Types of Attacks	Description
Exploitation of Systems and Applications	• SQL Injection, Code Injection, Command Injection, XML Injection, LDAP Injection • API Exploitation, Cross-Site Scripting (XSS), Application Layer Attacks • Remote Code Execution (RCE), IoT Exploitation, Zero-Day Exploits	Attacks that exploit vulnerabilities in software, applications, APIs, or devices to gain access or manipulate behavior.
Disruption and Resource Overload	• Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS) • Botnet Attacks, Cryptojacking • Logic Bombs	Attacks designed to overwhelm systems, disrupt services, or exploit resources for unauthorized purposes.
Communication Interception and Manipulation	Man-in-the-Middle (MitM), DNS Spoofing (Cache Poisoning), Session Hijacking, Eavesdropping Attack	Attacks targeting communication pathways to intercept, alter, or steal transmitted data.
Social Engineering and Human Exploitation	Phishing, Pretexting, Tailgating, Quid Pro Quo, Social Media Manipulation Attacks, Astroturfing, Watering Hole Attacks, Credential Stuffing, Password Spraying, SIM Swapping	Attacks exploiting human trust and behavior to manipulate victims or gain unauthorized access.
Malware-Based Attacks	Keylogging, Ransomware, Drive-by Download Attacks, Malvertising	Attacks using malicious software, AI, or deceptive technologies to compromise systems or deceive users.
Advanced and Evolving Attacks	• AI-Powered Attacks, Deepfake-Based Attacks, Adversarial AI Attacks • Advanced Persistent Threats (APTs) • Cyber-Physical System Attacks, Supply Chain Attacks, Cloud-Specific Attacks Autonomous System Exploitation • Quantum Cryptography Attacks, Fileless Malware, Synthetic Identity Fraud	Emerging threats leveraging advanced technologies, sophisticated methodologies, or targeting future vulnerabilities like quantum computing

Vrste napada-Exploitation of Systems and Applications

Exam question

SQL Injection

Kako radi:

- •Napadači ubacuju zlonamjerni SQL kod u polje za unos kako bi manipulirali upitima baze podataka (na web stranici).
- •Iskorištava nedovoljnu potvrdu unosa ili sanitaciju
- •Može dovesti do neovlaštenog pristupa, krađe podataka ili oštećenja baze podataka.

Zaštita:

- •Primijeniti validaciju i filtriranje unosa (zabrana određenih znakova ili uzoraka prilikom unosa npr. ‘ ili ” npr. `'; DROP TABLE users; --`), korištenje parametriziranja unosa tako da se unos tretira kao podatak, a ne kao kod i slično..
- •Implementirajte strogu provjeru valjanosti unosa i očistite sve korisničke unose.
- •Redovito ažurirajte i krpajte (patchirajte) sustave za upravljanje bazama podataka.

Vrste napada-Exploitation of Systems and Applications

Ispitno pitanje

API Exploitation

Kako radi:

- Napadači iskorištavaju slabo osigurane API-je slanjem zlonamjernih zahtjeva ili zaobilaženjem mehanizama provjere autentičnosti.
- Može izložiti osjetljive podatke ili dopustiti neovlaštene radnje.

Zaštita:

- Koristite jake mehanizme provjere autentičnosti i autorizacije.
- Slično kao kod SQL injection napada treba osigurati da svi ulazni podaci odgovaraju očekivanom formatu, tipu podataka, i vrijednostima i filtrirati potencijalno opasne upite.
- Redovito provjeravajte ranjivosti API-ja.

Cross-Site Scripting (XSS)

Kako radi:

- Napadač unosi zlonamjerne skripte u dijelove web-aplikacije koje prihvaćaju korisnički unos, poput obrazaca za komentare, tražilica ili URL-ova
- Aplikacija bez odgovarajućih sigurnosnih mjera omogućuje da se unesen kod prikaže na stranicama koje drugi korisnici pregledavaju i na taj način se izvršavaju skripte kada korisnici pregledavaju komentatre.
- Može ukrasti kolačiće, tokene sesije ili preusmjeriti korisnike na zlonamjerne web stranice.

Zaštita:

- Uklonite ili kodirajte opasne znakove (poput `<, >, ', ", &)` iz korisničkih unosa kako bi spriječili njihovo izvršavanje kao koda.Na primjer, unos `<script>` može se kodirati u `&lt;script&gt;`
- Implementirajte CSP (Content Security Policy) kako biste ograničili koje se skripte mogu izvršavati na stranici. CSP omogućuje samo odobrene izvore skripti, čime se smanjuje rizik.
- Nemojte koristiti JavaScript unutar HTML elemenata, poput atributa onclick ili onload

Vrste napada-Exploitation of Systems and Applications

Ispitno pitanje

IoT Exploatation
Kako radi:
•Iskorištava slabe sigurnosne konfiguracije ili ranjivosti u IoT uređajima.
•Napadači mogu preuzeti kontrolu nad uređajima ili ih uključiti u botnete.
•Također mogu počiniti štetu korištenjem samog uređaja (npr. Dizalice, grijalice, ventilatori itd..)
Zaštita:
•Koristite jake lozinke i izbjegavajte predefinirane postavke (primjer preuzimanja kontrole nad kranom s default postavkama).
•Redovito ažurirajte firmware IoT uređaja.
•Izolirajte IoT uređaje na zasebnoj mreži bez vanjskog pristupa i sa strogom kontrolom pristupa unutar mreže.

Zero-Day Exploits
Kako radi:
•Iskorištava ranjivosti nepoznate dobavljaču ili sigurnosnoj zajednici.
•Visok rizik jer nema zakrpa ili obrane u trenutku napada.
Zaštita:
•Koristite sustave za otkrivanje upada (IDS-Intrusion Detecton System) i alate za otkrivanje i odgovor krajnjih uređaja (EDR-Endpoint Detection and Response).
•Primijenite adekvatnu strategiju upravljanja zakrpama.
•Pratiti stanje Zero-Day prijetnji i biti spreman na odgovor (ako niste prvi imate šanse za obranu).

Vrste napada - Disruption and Resource Overload

Ispitno pitanje

Uskraćivanje usluge [Denial-of-Service (DoS)]
Kako radi:
•„Zatrpava” sustav upitima koji opterećuju dostupne resurse do točke kada sustav postaje nedostupan legitimnim korisnicima (npr. Napad na Web server).
•Često uključuje jednog napadača koji cilja na jedan sustav. (primjer suparnička gaming ekipa na Balkanu)
Zaštita:
•Koristite mrežne vatrozide i ograničavanje brzine kako bi filtrirali zlonamjerni promet (npr. 100 zahtjeva po minuti s jedne IP adrese).
•Upotrijebite alate za analizu prometa za otkrivanje abnormalnih skokova (bitno je znati baseline).
•Učinite sustav redundantnim i koristite loadbalancing opterećenja kako biste podnijeli skokove prometa.

Distribuirano uskraćivanje usluge [Distributed Denial-of-Service (DDoS)]
Kako radi:
•Pojačava DoS napade korištenjem više uređaja (često botneta) za simultani napad na cilj.
•Teže ih je ublažiti zbog prometa koji potječe iz različitih izvora (različiti dijelovi svijeta i različiti telekomi).
Zaštita:
•Implementirajte usluge za ublažavanje DDoS napada (npr. Cloudflare, AWS Shield).
•Koristite web application firewalls (WAF) za blokiranje zlonamjernog prometa.
•Uspostavite robusno praćenje prometa kako biste rano otkrili napade i odgovorili na njih (bitno je znati baseline)..

Vrste napada - Disruption and Resource Overload

Ispitno pitanje

Botnet napadi

Kako radi:

- Mreža zaraženih uređaja (botovi) kontrolira se za izvođenje napada velikih razmjera, kao što su DDoS ili spam kampanje.
- Botovi često uključuju kompromitirane IoT uređaje ili loše osigurane sustave.

Zaštita:

- Zaštitite uređaje jakim lozinkama i redovitim ažuriranjima (da ne postanete dio botnet mreže).
- Koristite mrežnu segmentaciju kako biste ograničili širenje bot infekcija.
- Pratite odlazni promet radi sumnjivih aktivnosti.

Dos-Ddos napadi u stvarnom vremenu

Ispitno pitanje

http://www.digitalattackmap.com
https://cybermap.kaspersky.com
https://threatmap.checkpoint.com/ThreatPortal/livemap.html

Ispit pitanje :
DoS napadi ciljaju na dostupnost sustava
Primjer DoS napada je TCP SYN flood - zlorabi mehanizam trosmjernog rukovanja (3-way handshake). Napadač šalje brojne segmente sa postavljenom SYN zastavom (bitom), žrtva odgovara na svaki zahtjev sa SYN/ACK, ali napadač ne odgovara žrtvi sa ACK, već započinje novu vezu i tako sve dok žrtva ne ponestane resursa i legitimni korisnici više ne mogu pristupiti poslužitelju. Napadač obično koristi lažnu IP adresu tako da kada žrtva odgovori na SYN od napadača, zapravo šalje SYN/ACK na uređaj koji uopće nije započeo komunikaciju. Zbog usmjeravanja internetskog prometa, bez obzira što je napadač lažirao IP adresu, odgovor će ići na mrežu na kojoj se ta IP adresa zapravo nalazi.

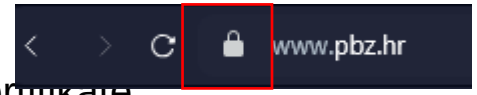
Ispit pitanje :
DDoS napadi

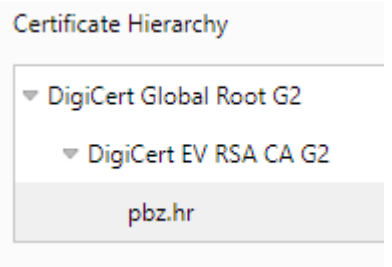
Vrste napada - Communication Interception and Manipulation

Man-in-the-Middle (MitM)
Kako radi:

Ispitno pitanje

•Presreće komunikaciju između dvije strane radi krađe podataka ili ubacivanja zlonamjernog sadržaja.
•Obično se događa na nezaštićenim mrežama (npr. javni Wi-Fi).
•Primjer je DHCP spofing napad gdje se napadač nametne kao DHCP server i korisniku daje lažne DNS odgovore (pošto je sebe postavio kao DNS server)
Zaštita:
•Koristite end-to-end enkripciju (npr. HTTPS, TLS).
•Izbjegavajte javni Wi-Fi ili koristite VPN kada pristupate osjetljivim podacima.
•Implementirajte jake metode provjere autentičnosti npr. multi-factor autentication (MFA), provjerite SSL/TLS certifikate





DNS Spoofing (Cache Poisoning)
Kako radi:
•Mijenja DNS zapise na serveru kako bi preusmjerio korisnika na zlonamjerna web-mjesta.
•Iskorištava slabosti u konfiguracijama DNS poslužitelja.
•Ako DNS poslužitelj koristi zastarjeli softver ili ima sigurnosne propuste (slabe lozinke ili je konfiguriran kao „otvoreni resolver"), napadač može iskoristiti te ranjivosti kako bi dobio pristup i promijenio DNS zapise…ili preko administratorskog računala koje je kompromitirano
Zaštita:
•Koristite DNSSEC (DNS Security Extensions) kako biste osigurali autentičnost DNS odgovora (omogućava provjeru je li odgovor od pouzdanog izvora i je li mijenjan)-Ovo koriste DNS serveri.
•Redovito ažurirajte i osigurajte DNS poslužitelje.
•Pratite DNS zapisnike za sumnjive aktivnosti.

Vrste napada - Communication Interception and Manipulation

Ispitno pitanje

Otmica sesije (Session Hijacking)
Kako radi:
•Krade tokene sesije (jedinstveni identifikatori koje aplikacija ili web-poslužitelj generira kako bi pratila aktivne korisničke sesije. Token omogućuje aplikaciji da zna tko je korisnik tijekom njegovog trajanja na platformi nakon što se uspješno autentificirao (npr. prijavio na račun).) kako bi oponašao korisnike u aktivnim sesijama.
•Često se postiže putem Cross-Site Scripting (XSS) ili „njuškanja" paketa (packet sniffing).
Zaštita:
•Koristite HTTPS za šifriranje podataka sesije u prijenosu.
•Implementirajte sigurno upravljanje sesijom s kratkim vremenima isteka i regeneracijom tokena.
•Uvedite anti-XSS mjere kako biste spriječili krađu tokena.

Napad prisluškivanjem (Eavesdropping Attack)
Kako radi:
•Presreće nešifrirani mrežni promet radi hvatanja osjetljivih informacija.
•Često se događa na javnim ili nezaštićenim mrežama (WiFi).
Zaštita:
•Koristite jake protokole šifriranja kao što su HTTPS ili razne VPN protokole za autentikaciju i enkripciju.
•Izbjegavajte prijenos osjetljivih podataka preko nezaštićenih mreža.
•Educirajte korisnike o osnovama kibernetičke sigurnosti.

Vrste napada - Social Engineering and Human Exploitation

Ispitno pitanje

Phishing (Spear phishing, Whaling, Vishing itd.)

Kako radi:

- Varljive e-poruke ili poruke navedu korisnike da otkriju vjerodajnice ili kliknu zlonamjerne veze.
- Obično lažno predstavlja subjekte od povjerenja (npr. banke, kolege s posla).

Zaštita:

- Educirajte korisnike da prepoznaju pokušaje krađe identiteta.
- Implementirajte alate za filtriranje e-pošte i antiphishing.
- Upotrijebite višefaktorsku autentikaciju (MFA) za zaštitu računa.

1. **Spear Phishing**:
   Ciljani phishing napad usmjeren na pojedince ili specifične skupine, često personaliziran kako bi izgledao uvjerljivije (npr. korištenje imena ili specifičnih informacija).

2. **Whaling**:
   Poseban oblik spear phishinga usmjeren na visoko pozicionirane osobe, poput direktora (CEO) ili financijskih direktora (CFO), koristeći poslovnu terminologiju i izgled legitimnih zahtjeva.

3. **Vishing (Voice Phishing):**
   Napadi putem telefonskih poziva, gdje se napadači predstavljaju kao banke, tehnička podrška ili druge institucije kako bi prevarili žrtve da otkriju osjetljive informacije.

Vrste napada - Social Engineering and Human Exploitation

Ispitno pitanje

Pretexting (priprema terena)
Kako radi:
•Napadači **smišljaju lažne scenarije (kontekst)** koji će žrtva vjerojatno prihvatiti kao vjerodostojan i to da bi manipulirali žrtvama da daju osjetljive informacije (npr. pretvarajući se da su iz IT podrške).
Zaštita:
•Obučite zaposlenike da provjere identitete prije dijeljenja osjetljivih podataka čak i kada se radi o osobama koje su im nadređene.
•Uspostavite stroge protokole za rukovanje osjetljivim informacijama (stroge procedure kojih se pridržavamo).
•Pratite neuobičajene zahtjeve ili ponašanja (npr. Šef prvi puta traži prebacivanje 5000€ na neki račun preko telefona).

Quid Pro Quo (latinski izraz koji znači „nešto za nešto”)
Kako radi:
•Napadači nude nešto (npr. tehničku podršku, dar) u zamjenu za osjetljive podatke.
•Napadači često koriste ovu taktiku na zaposlenicima u tvrtkama:Predstavljaju se kao IT osoblje i nude rješavanje problema s računalom. Traže da zaposlenik preda vjerodajnice ili omogući daljinski pristup sustavu, što im omogućuje neovlašteni pristup.

Zaštita:
•Educirajte zaposlenike da budu oprezni s neželjenim ponudama.
•Provjerite identitet osoba koje nude pomoć.
•Uspostavite pravila za rukovanje osjetljivim informacijama.

Vrste napada - Social Engineering and Human Exploitation

Ispitno pitanje

Tailgating

Kako radi:

•Stjecanje neovlaštenog fizičkog pristupa praćenjem ovlaštene osobe u sigurno područje (obično u gužvi ili s vremenskim odmakom od par sekundi-ulaz na faks).

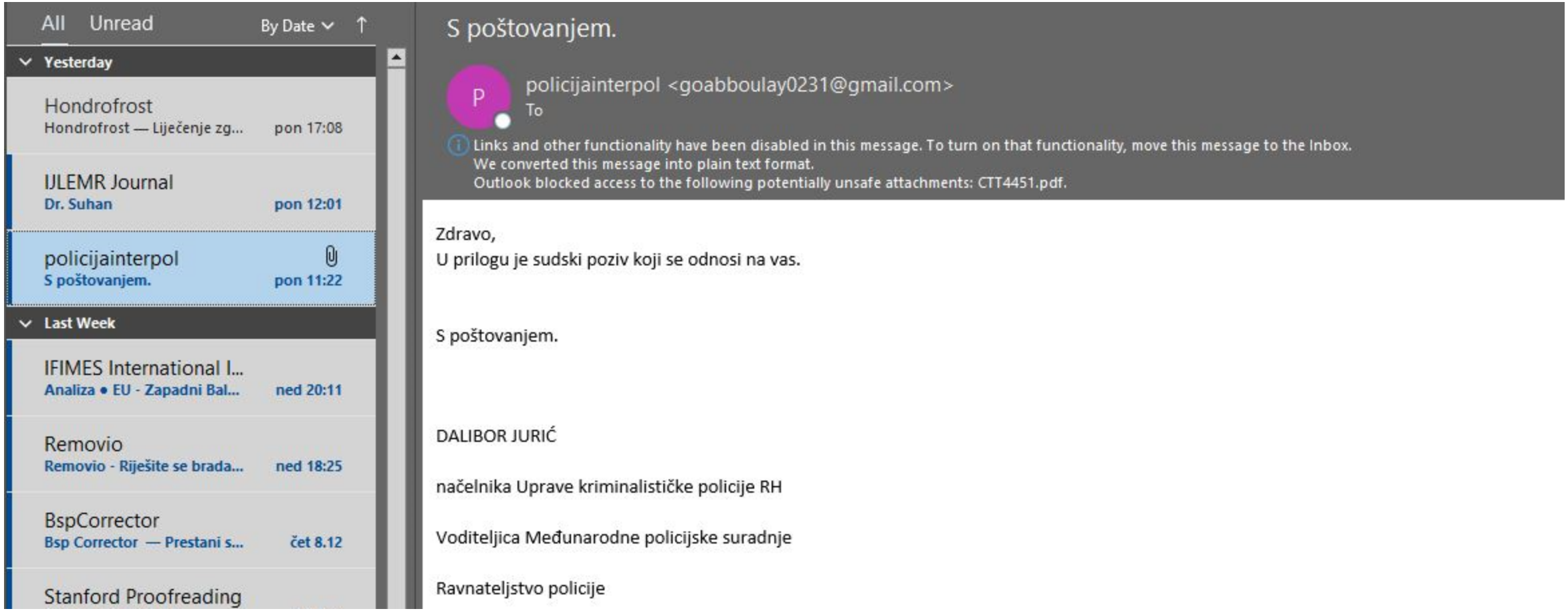
Zaštita:

•Koristite sustave kontrole pristupa poput kartica s ključevima ili biometrijskih skenera.

•Uvježbajte zaposlenike da prepoznaju okolnosti za ovaj napad i da spriječe neovlaštene osobe od ulaska.

•Instalirajte sigurnosne kamere za nadzor ulaznih točaka.

Primjeri - Social Engineering and Human Exploitation



Primjeri - Social Engineering and Human Exploitation

Policija

MM

MAYA MARIA CRĂCIUN <maya.craciun@scoala29mihaiviteazul.ro>
To

Reply | Reply All | Forward

Sun 12/29/2024 5:14 PM

If there are problems with how this message is displayed, click here to view it in a web browser.

Sudski poziv HR.pdf
641 KB

Ne primate često poruke e-pošte pošiljatelja maya.craciun@scoala29mihaiviteazul.ro. Saznajte zašto je to važno

Pravna pritužba protiv vas.

MAYA MARIA CRĂCIUN
Policajac

Primjeri - Social Engineering and Human Exploitation

Izvješće o istrazi :

Podnijeli smo žalbu protiv vas.
Imate 48 sati da odgovorite.

____

Maria Goatti, glasnogovornica
Zagrebačke Policijske uprave

Primjeri - Social Engineering and Human Exploitation

Fwd: : Jedinica za represiju-

Poziv <aristinodar@gmail.com>
To compteinfo.eur@europe.com

Reply | Reply All | Forward

sri 5.4.2023 7:57

If there are problems with how this message is displayed, click here to view it in a web browser.

Translate message to: English | Never translate from: Croatian | Translation preferences

Dobro jutro,
ja sam gospodin Wil ((Juric DALIBOR)), načelnik Uprave kriminalističke policije Republike Hrvatske.
Načelnik Odjela za međunarodnu policijsku suradnju Ravnateljstva policije. Javljam vam se ubrzo nakon zapljene računala Cyber-infiltracije (Posebno u vezi s dječjom pornografijom, pedofilijom, cyber pornografijom) kako bih vas obavijestio da ste predmet nekoliko zakonskih postupaka koji su na snazi: za vašu informaciju, seksualni napadi može biti počinjeno korištenjem interneta, a prekršaje ste počinili nakon što ste bili meta na internetu, zatim tijekom razmjene e-mailova s nekoliko maloljetnika, vaše gole fotografije koje šaljete maloljetnicima su snimljene od strane našeg Cyberžandarma i dokaz su vaših prijestupa. Od vas se traži da se po primitku ove e-pošte javite putem e-pošte tako što ćete nam napisati svoja obrazloženja kako bismo ih ispitali i provjerili kako bismo procijenili sankcije.

NB: Nakon ovog razdoblja, bit ćemo obavezni prenijeti naše izvješće kako bismo uspostavili tjeralicu protiv vas i prijavili vas kao seksualnog prijestupnika, proslijediti vaš dosje na nekoliko nacionalnih televizijskih kanala vijesti za širenje ili vašoj obitelji, vaši voljeni će samo vidjeti što radite ispred svog računala.

Srdačno,
((Jurić DALIBOR))

---------- Forwarded message ---------
Date: mer. 5 avr. 2023 à 05:50
Subject: Automatski odgovor: Jedinica za represiju-

Vrste napada - Malware-Based Attacks

Ispitno pitanje

Keylogging
Kako radi:
•Bilježi pritiske tipki za snimanje osjetljivih informacija poput lozinki ili financijskih detalja.
•Često se instalira putem zlonamjernog softvera ili e-pošte za krađu identiteta.
Zaštita:
•Koristite antivirusni softver za otkrivanje i blokiranje keyloggera.
•Izbjegavajte preuzimanje datoteka iz nepouzdanih izvora.
•Upotrijebite upravitelje zaporki kako biste smanjili izravno upisivanje vjerodajnica.

Na mobilnim uređajima sofisticirani keyloggeri mogu pratiti tipkanje na virtualnoj tipkovnici, bilježeći pritiske na tipke i unose putem ekrana osjetljivog na dodir, pri čemu su posebno ciljani osjetljivi unosi poput lozinki i PIN-ova. Također, mogu analizirati uzorke prstiju i gestikulacije korištenjem senzora mobilnog uređaja, poput akcelerometra ili žiroskopa, kako bi rekonstruirali uzorke unosa, poput PIN-a ili gesti za otključavanje. Ovo je napredniji oblik keyloggera koji ne bilježi izravne dodire, već pokrete uređaja. Osim toga, aplikacije koje traže nepotrebne dozvole, poput pristupa akcelerometru, mogu koristiti te podatke za praćenje korisnikovih unosa ili aktivnosti.

How to Turn OFF All Sensors in Android Phone? Disable All Sensors & Save Battery Life!
https://www.youtube.com/watch?v=3x73bL9D85I

Vrste od napadi - napadi temeljeni na zlonamjernom softveru

Ransomware je vrsta zlonamjernog softvera koji šifrira datoteke ili čitave sustave žrtve, čineći ih nedostupnima dok se ne plati otkupnina (obično u kriptovalutama poput Bitcoina). Ovaj napad je vrlo destruktivan jer može paralizirati organizacije ili pojedince, često uz prijetnju trajnog gubitka podataka ako se otkupnina ne plati.

Ispitno pitanje

Kako radi:

- **Infekcija uređaja:**
  - **Phishing e-pošta:** Napadači šalju lažne e-mailove s privicima ili linkovima koji sadrže zlonamjerni kod. Kada žrtva klikne na link ili otvori privitak, ransomware se instalira na uređaj.
  - **Iskorištavanje ranjivosti:** Napadači koriste sigurnosne propuste u zastarjelom softveru ili operativnim sustavima kako bi instalirali ransomware.
  - **Zlonamjerne web stranice:** Posjet zaraženoj web stranici može automatski pokrenuti preuzimanje ransomwarea (poznato kao "drive-by download").
- **Šifriranje podataka:**
  - Nakon što se instalira, ransomware počinje šifrirati datoteke na uređaju, uključujući dokumente, slike, videozapise i druge kritične podatke.
  - Datoteke postaju neupotrebljive jer su za otključavanje potrebni specifični dešifrirajući ključevi koje posjeduje napadač**.**
- **Zahtjev za otkupninom:**
  - Žrtva dobiva poruku s uputama o uplati otkupnine kako bi dobila dešifrirajući ključ.
  - Napadači često postavljaju vremenski rok, nakon čega prijete trajnim brisanjem ili dodatnim povećanjem otkupnine.
- **Distribucija ransomwarea unutar mreže:**

  U nekim slučajevima, ransomware se širi na druge uređaje unutar iste mreže, brzo šifrirajući sve povezane resurse.

Zaštita:

•Educirajte zaposlenike o prepoznavanju metoda isporuke ransomwarea.
•Održavajte redovite, offline sigurnosne kopije kritičnih podataka.
•Koristite alate za otkrivanje i za blokiranje ransomwarea.

Što učiniti u slučaju ransomware napada?

•**Ne plaćajte otkupninu:**
•Plaćanje ne jamči povrat podataka i potiče napadače na daljnje napade.
•**Izolirajte zaražene sustave:**
•Odspojite zaraženi uređaj od mreže kako biste spriječili širenje.
•**Obratite se stručnjacima:**
•Potražite pomoć stručnjaka za kibernetičku sigurnost ili policije.
•**Koristite dekripcijske alate:**
•Provjerite dostupnost besplatnih alata za dešifriranje putem pouzdanih izvora, poput No More Ransom projekta.

Kako postići sigurno IT okruženje u organizaciji?

Ispitno pitanje

1. Obrazovanje i svijest

Obrazovanje zaposlenika kamen je temeljac kibernetičke sigurnosti . Redovita obuka pomaže korisnicima da prepoznaju prijetnje kao što su krađa identiteta, društveni inženjering i zlonamjerni softver. Promicanje kulture svijesti o kibernetičkoj sigurnosti osigurava da svatko u organizaciji razumije svoju ulogu u održavanju sigurnog IT okruženja.

2. Sigurnosne politike

Uspostavljanje jasnih i smislenih sigurnosnih politika skrojenih prema potrebama organizacije je od vitalnog značaja. Politike bi trebale biti praktične, provedive i učinkovito komunicirane kako bi se osigurala usklađenost. Ova pravila usmjeravaju zaposlenike u rukovanju osjetljivim informacijama i odgovornom korištenju IT resursa.

3. Kontrola pristupa i autentifikacija

Implementacija kontrole pristupa temeljene na ulogama (RBAC- role-based access control) ograničava pristup sustavima i podacima na temelju odgovornosti na poslu, osiguravajući da zaposlenici imaju pristup samo onim resursima koji su im potrebni . Višefaktorska provjera autentičnosti (MFA) dodaje dodatni sloj zaštite, što napadačima otežava kompromitiranje računa.

Kako postići sigurno IT okruženje u organizaciji?

Ispitno pitanje

4. Nadzor sustava i upravljanje incidentima

Uvođenje alata za praćenje omogućuje organizacijama otkrivanje anomalija i potencijalnih prijetnji u stvarnom vremenu . Dobro definiran plan odgovora na incidente osigurava brzu i učinkovitu akciju tijekom proboja sigurnosti, smanjujući štetu i zastoje.

5. Zaštita od zlonamjernog softvera

Zaštita uređaja antimalware softverom je ključna. Ovi alati, u kombinaciji s naprednim sustavima za otkrivanje krajnjih točaka i odgovor (EDR- endpoint detection and response), mogu identificirati i neutralizirati prijetnje prije nego prouzrokuju štetu.

6. Sigurnost mreže

Kategoriziranje i filtriranje mrežnog prometa pomoću vatrozida pomaže u blokiranju neželjenih i zlonamjernih aktivnosti. Sustavi za otkrivanje i sprječavanje upada (IDPS- Intrusion detection and prevention systems) poboljšavaju obranu mreže identificiranjem i zaustavljanjem naprednih prijetnji.

7. Redovita ažuriranja i zakrpe

Održavanje operativnih sustava i softvera ažuriranima je jednostavan, ali učinkovit način za sprječavanje ranjivosti. Redovita zakrpa osigurava da su poznate sigurnosne rupe zatvorene prije nego što ih napadači mogu iskoristiti.

Kako postići sigurno IT okruženje u organizaciji?

Ispitno pitanje

8. Sigurnost bežične mreže
Osiguranje bežičnih mreža jakim protokolima šifriranja kao što je WPA3 je ključno. Organizacije bi također trebale optimizirati snagu bežičnog signala kako bi izbjegle neovlašteni pristup i sakrile SSID-ove kako bi mreže bile manje vidljive vanjskim osobama.

9. Pravila jakih lozinki
Poticanje korištenja jakih, jedinstvenih lozinki za sve račune smanjuje rizik. Upravitelji lozinki (password manager) mogu pomoći zaposlenicima da sigurno pohrane svoje vjerodajnice i upravljaju njima, osiguravajući jednostavnu upotrebu bez narušavanja sigurnosti.

10. Šifriranje podataka
Šifriranjem podataka u stanju pohrane i prijenosa štite se osjetljivi podatci od neovlaštenog pristupa. Enkripcija cijelog diska osigurava da podaci pohranjeni na uređajima ostanu sigurni čak i ako su izgubljeni ili ukradeni.

11. Sigurnosne kopije izvan mjesta i u oblaku
Redovito sigurnosno kopiranje kritičnih podataka kako bi se osigurale lokacije izvan mjesta ili u oblaku štiti od gubitka podataka zbog ransomwarea, kvara hardvera ili drugih incidenata. Periodično testiranje procesa oporavka sigurnosne kopije osigurava da se na sigurnosne kopije možete pouzdati u hitnim slučajevima.

Smjernice za snažne lozinke

https://www.security.org/how-secure-is-my-password/ Ne koristiti !

Umjesto jednostavne lozinke poput "lozinka123," koristite nešto poput: **"9t!Km#Xv*2023"**

- **Izbjegavajte riječi ili imena iz rječnika:**
  Nemojte koristiti uobičajene riječi ili fraze koje se lako mogu pogoditi putem napada rječnikom (*dictionary attack*).
- **Nemojte koristiti uobičajene pravopisne pogreške riječi iz rječnika:**
  Modificirane riječi, poput "p@ssw0rd" umjesto "password," također nisu sigurne jer ih napadači često uključuju u napade.
- **Izbjegavajte imena računala ili računa:**
  Lozinke koje sadrže ime korisnika, računala ili lako dostupne informacije o vama nisu sigurne.
- **Koristite posebne znakove:**
  Dodajte znakove poput **! @ # $ % ^ & *** kako biste povećali složenost lozinke i otežali pogađanje.
- **Duljina je ključna:**
  Preporučuje se korištenje lozinki koje imaju **deset ili više znakova.** Dulje lozinke su sigurnije jer zahtijevaju više vremena za probijanje.
- **Kombinirajte različite tipove znakova:**
  Koristite kombinaciju **velikih i malih slova, brojeva i posebnih znakova** za dodatnu sigurnost.
- **Izbjegavajte očite uzorke:**
  Lozinke poput "12345678," "qwerty" ili "abcdef" nisu sigurne i često su prve na popisu napadača.
- **Nemojte reciklirati lozinke:**
  Koristite jedinstvenu lozinku za svaki račun kako biste spriječili višestruke povrede sigurnosti ako jedna lozinka bude kompromitirana.
- **Razmislite o korištenju upravitelja lozinki:**
  Alati poput LastPass, Dashlane ili Bitwarden pomažu u generiranju i pohranjivanju složenih lozinki, olakšavajući njihovo upravljanje.
- **Redovito mijenjajte lozinke:**
  Iako to više nije univerzalna preporuka, povremena promjena lozinki može biti korisna, osobito ako sumnjate na povredu.

Osigurajte svoj rad u web pregledniku

- Uz korištenje sigurnih lozinki, ključno je osigurati da fizički pristup vašem računalu bude ograničen jer bi neovlaštene osobe mogle pristupiti vašoj povijesti pretraživanja ili podacima za prijavu kako bi ugrozile vaše račune na mreži. Izbjegavajte korištenje tuđih ili javnih, nezaštićenih računala za prijavu na svoje račune jer mogu biti osjetljiva na prijetnje .

- Kako biste poboljšali sigurnost, razmislite o korištenju "glavne" lozinke u pregledniku ili namjenskog upravitelja lozinki za sigurno pohranjivanje vjerodajnica. Prilikom pregledavanja koristite privatne načine pretraživanja kao što su:
  - **Microsoft Internet Explorer:** InPrivate
  - **Google Chrome:** anonimno
  - **Mozilla Firefox:** Privatna kartica / Privatni prozor
  - **Safari:** Privatno pregledavanje

- Za maksimalnu sigurnost, možete koristiti internet s virtualnog računala, koje se nakon korištenja može izbrisati kako bi se uklonili tragovi i potencijalne ranjivosti. Ove prakse pružaju dodatne slojeve zaštite za vaše online aktivnosti i osjetljive informacije.

Kako postići sigurno IT okruženje u organizaciji?

Ispitno pitanje

12. Trajno brisanje podataka

Korištenje sigurnih metoda za trajno brisanje osjetljivih podataka sprječava njihovo vraćanje od strane neovlaštenih osoba. Alati poput softvera za brisanje diska osiguravaju potpuno brisanje podataka.

13. Redovite sigurnosne revizije

Provođenje procjena ranjivosti i testiranja prodora pomaže identificirati slabe točke u obrani organizacije. Ove revizije osiguravaju da su sigurnosne mjere učinkovite i ažurne.

14. Fizička sigurnost

Osiguranje fizičkog pristupa kritičnim sustavima, kao što su poslužitelji i mrežni uređaji, ključno je. Sustavi nadzora, kontrole pristupa i biometrijski skeneri mogu pomoći u zaštiti ove imovine od neovlaštenog pristupa.

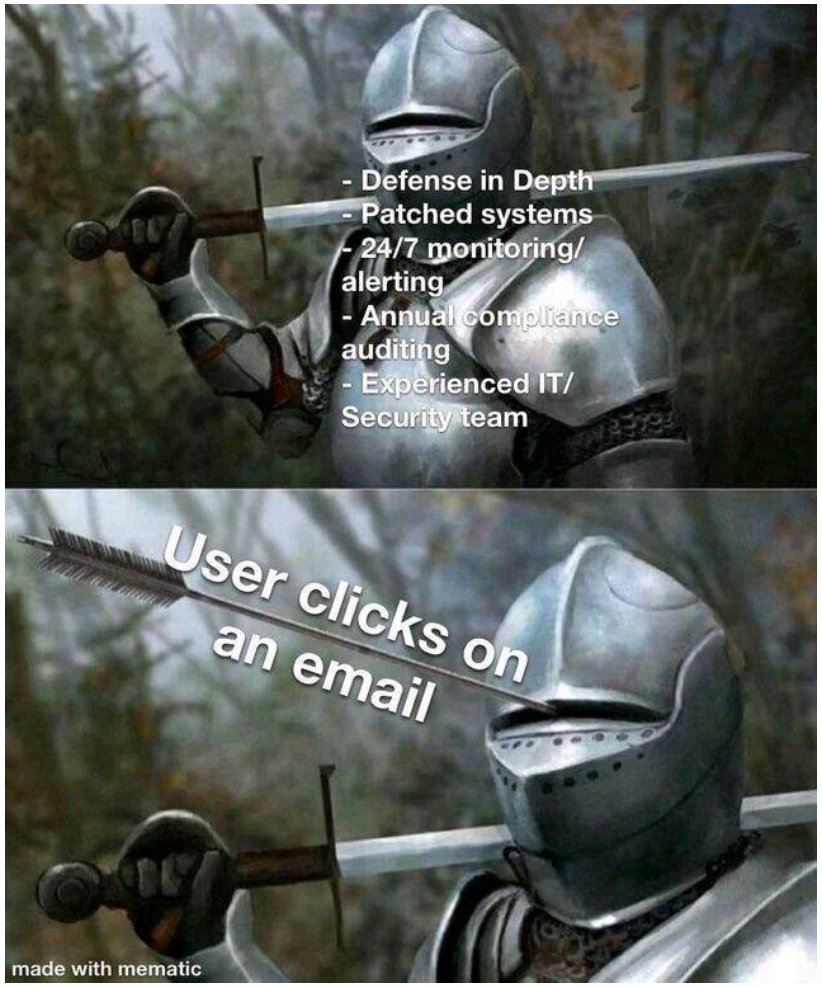
15. Izvještavanje o incidentima i učenje

Poticanje zaposlenika da prijave sumnjive aktivnosti omogućuje organizacijama da brzo odgovore na potencijalne prijetnje. Učenje iz prošlih incidenata pomaže poboljšati sigurnosne mjere i spriječiti buduće povrede.

Kako postići sigurno IT okruženje u organizaciji?

Dodatna poboljšanja:
Za organizacije koje žele dodatno poboljšati svoju sigurnost, usvajanje arhitekture nultog povjerenja (ZTA) osigurava da se svaki zahtjev za pristup provjeri prije odobravanja pristupa. Alati za upravljanje sigurnosnim informacijama i događajima (SIEM) pružaju centralizirano praćenje dnevnika i napredno otkrivanje prijetnji, dok cyber osiguranje može ublažiti financijski učinak sigurnosnih incidenata.

Kako postići sigurno IT okruženje u organizaciji?



?

Vatrozid

Ispitno pitanje

Vatrozid je sigurnosni sustav/uređaj koji prati i kontrolira dolazni i odlazni mrežni promet na temelju unaprijed definiranih sigurnosnih pravila . Njegova primarna svrha je stvoriti barijeru između pouzdane interne mreže i nepouzdanih vanjskih mreža, kao što je Internet, kako bi se zaštitili sustavi i podaci od neovlaštenog pristupa, napada i drugih cyber prijetnji.

Vatrozid – kako radi

Ispitno pitanje

1. **Filtriranje prometa:**
    1. Vatrozidi provjeravaju pakete podataka koji putuju kroz mrežu.
    2. Oni dopuštaju ili blokiraju promet na temelju skupa pravila, kao što su izvorne/odredišne IP adrese, priključci, protokoli i ponašanje aplikacije.
2. **Vrste pravila:**
    1. **Dopusti pravila:** Dopusti promet koji zadovoljava određene kriterije.
    2. **Odbij pravila:** Blokirajte promet koji krši pravila ili se čini sumnjivim.
3. **Praćenje stanja prometa:**
    1. Moderni vatrozidi mogu analizirati stanje veze, osiguravajući da promet pripada legitimnoj sesiji.

Vatrozid - Vrste od Vatrozidi

Ispitno pitanje

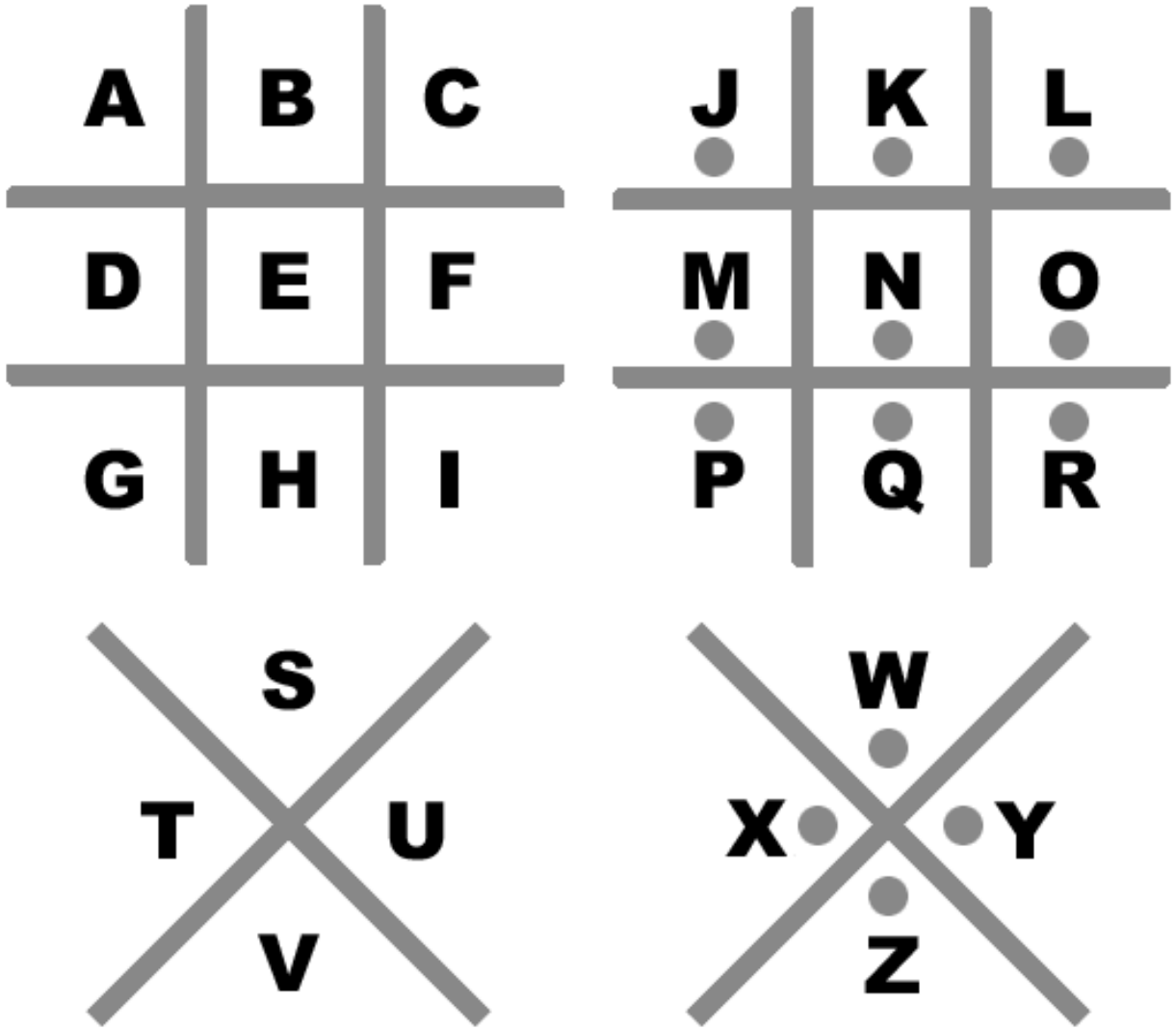
1. **Vatrozidi bez stanja (stateless):**
   - Osnovno filtriranje prometa na temelju statičkih pravila bez razumijevanja konteksta veze.
2. **Vatrozidi s praćenjem stanja (stateful):**
   - Analizirajte i pratite stanje veza, nudeći bolju sigurnost od vatrozida bez stanja.
3. **Aplikacijski vatrozidi (Application aware Firewalls):**
   - Djelujte na aplikacijskom sloju, provjeravajući promet i naredbe specifične za aplikaciju.
4. **Proxy vatrozidi:**
   - Djelujte kao posrednici između korisnika i vanjskih mreža, pružajući dodatnu sigurnost izoliranjem izravnih veza.
5. **Vatrozidi sljedeće generacije (NGFW-Next Generation Firewalls-Unified Threat Management-UTM):**
   - Kombinirajte tradicionalne mogućnosti vatrozida s naprednim značajkama kao što su sprječavanje upada, duboka inspekcija paketa i kontrola aplikacija.

Vatrozid je temeljna komponenta kibernetičke sigurnosti, djeluje kao digitalni vratar koji regulira mrežni promet radi sprječavanja neovlaštenog pristupa i zaštite osjetljivih podataka. U eri rastućih cyber prijetnji, vatrozidi ostaju kritična linija obrane za pojedince i organizacije.

?

Ukratko o šifriranju i VPN-Virtualy Private Networks

„Pig Pen Ciphre”

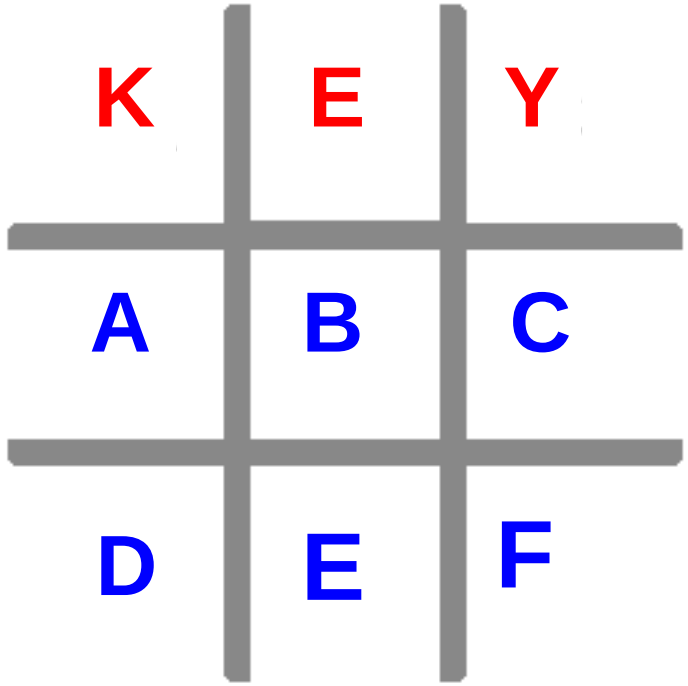


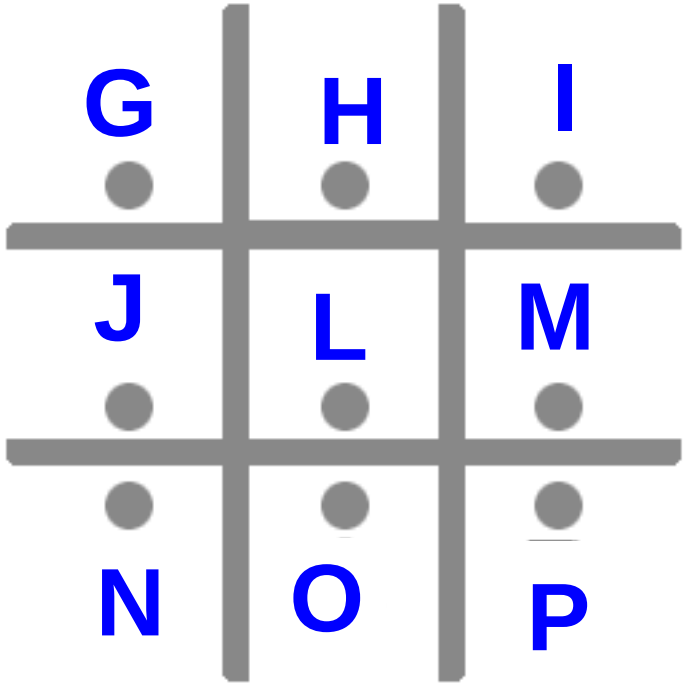
„Pig Pen Ciphre”

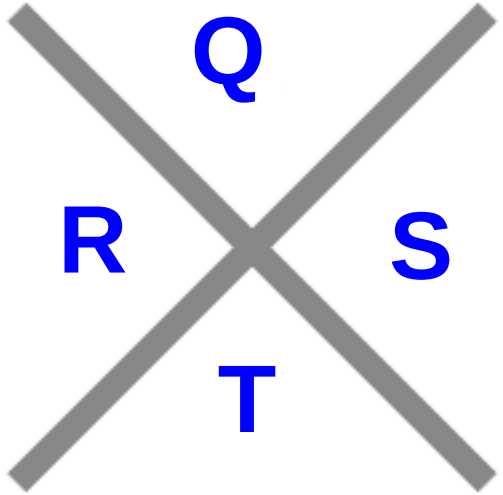
PRAKTIKUM

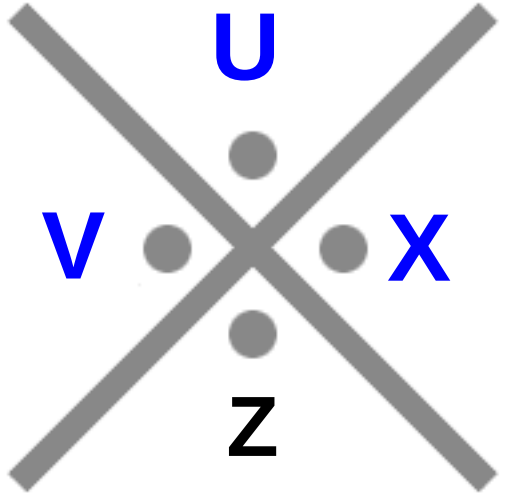
„Pig Pen Ciphre”

KEY









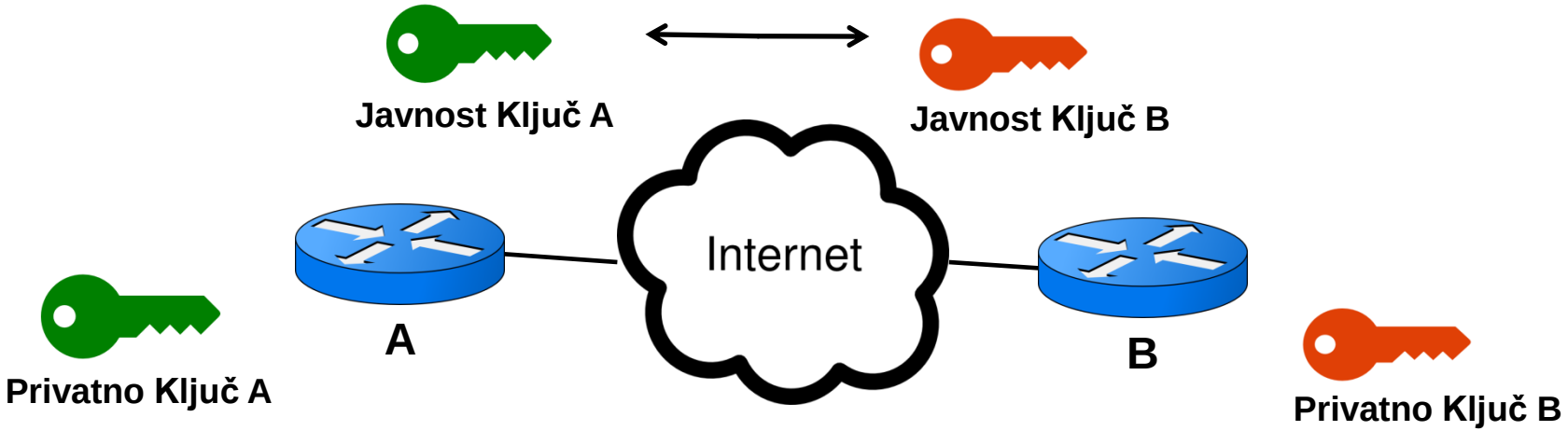
„ *Svinja Olovka Ciphre* ”

Prije

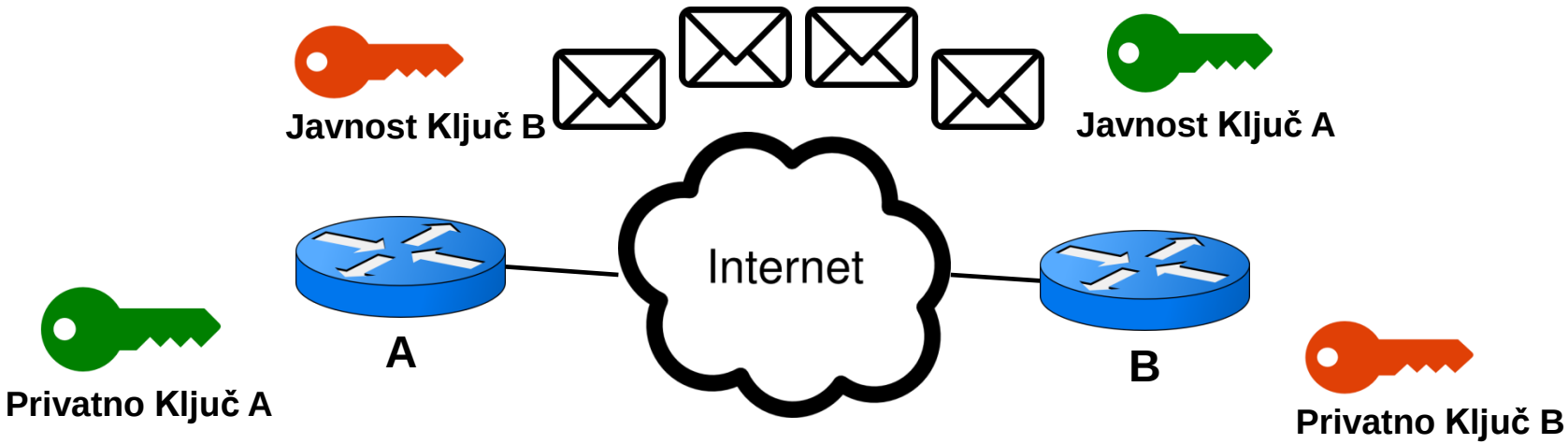
Poslije

PRAKTIKUM

PKI (Public Key infrastructure)- Asimetrična enkripcija



PKI (Public Key infrastructure)- Asimetrična enkripcija

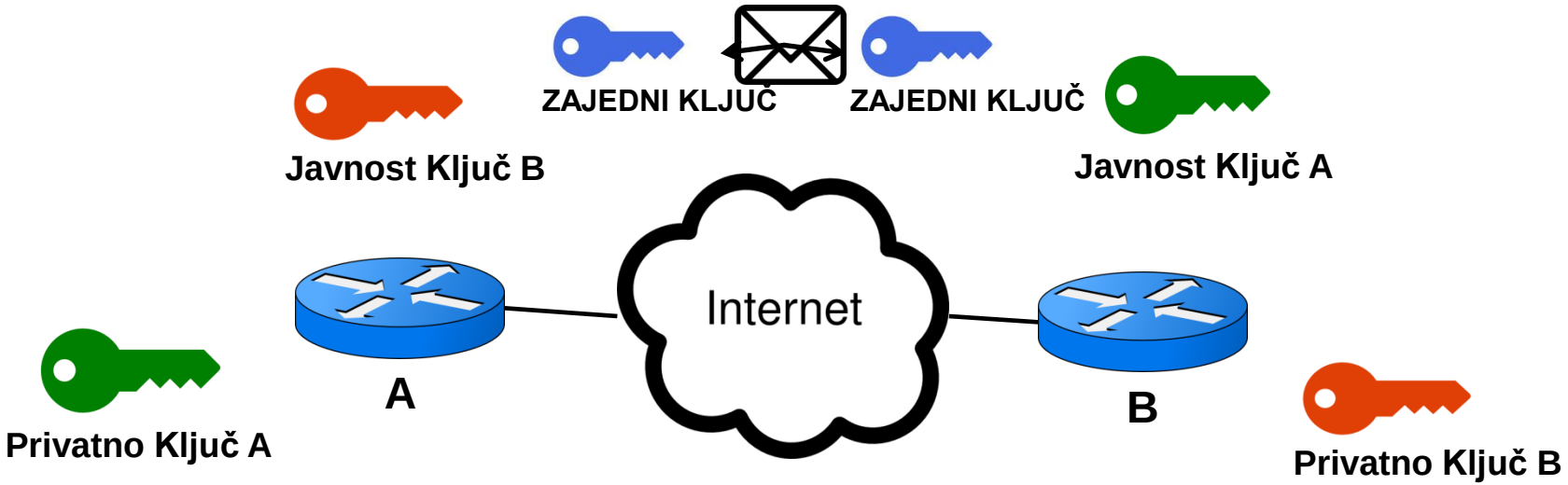


➢Problem je što je uređaj preopterećen i ovo je nepraktičan pristup

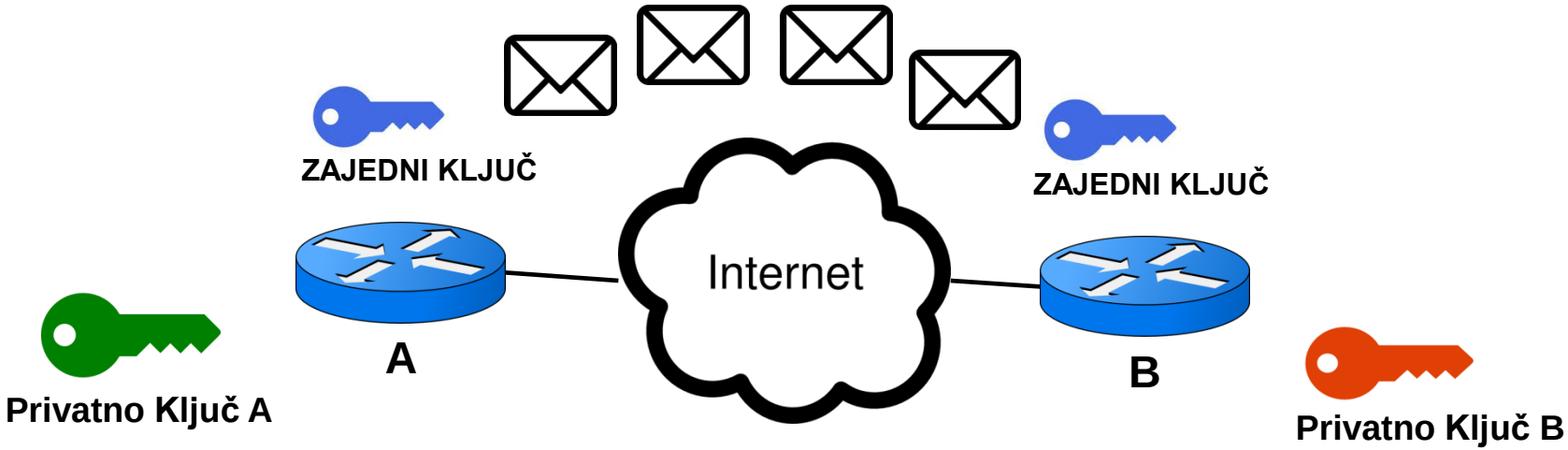
Key exchange:
- Diffie-Hellman (DH)
- Elliptic Curve Diffie-Hellman (ECDH)

Authentication Algorithms:
RSA (Rivest–Shamir–Adleman)
Elliptic Curve Digital Signature Algorithm (ECDSA)-light alternative to RSA for smaller keys

PKI (Public Key infrastructure)- Simetrično šifriranje



PKI (Public Key infrastructure)- Simetrično šifriranje



AES (Advanced Encryption Standard)

- Dobro dovoljno i ne preopterećuje uređaje

?