Cyber Security osnove

Ispitna pitanja materijala na linkovima:

Upute za do max. 6 bodova na ispitu (6+14 na ispitu)

Svi koji nemaju Fortinet Certifikat od prošle godine (NSE1 i NSE2) slijedite upute u dokumentu „Instructions for creating free account on Fortinet Training Institute 2024.pdf" koji se nalazi na infoeduci pod „Ostali dokumenti kolegija"

Svi koji imaju certifikat Fortinet od prošle godine (oni koji su mi ga poslali) neka se uključe u Cisco „Introduction to CyberSecurity" putem linka https://www.netacad.com/portal/web/self-enroll/m/course-2196763

Za bodove na ispitu trebate položiti sve „chapter examove" i „Final exam" i poslati mi certifikat putem maila na silvio.papic@algebra.hr i taj certifikat uplodati na infoeduku pod „seminarski radovi"

https://www.youtube.com/watch?v=msciBqowPgk

CyberSecurity *(ovo je jedna moguća definicija)*

Ispitno pitanje:

- **Sigurnost u kontekstu IT tehnologija možemo definirati kao kontinuirani proces zaštite digitalnih informacija 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...**

- Sigurnost je važna u osobnom životu, ali i u životu poslovnog okruženja (tvrtka)
- Što smo više prisutni na Internetu to je naša sigurnost više ugrožena (ne stavljati sve informacije o sebi na Internet)
- Posebno trebamo paziti na osjetljive podatke kao što su medicinski podaci, podaci o obrazovanju (detalji) ili podaci o zaposlenju i financijama, detalji o zaposlenju kao i podaci na ispravama (osobna, vozačka, kartice itd…)
- Ranjivosti sustava (Vulnerabilities) su mane u softwareu, hardwareu ili sigurnosnim politikama koje napadač može iskoristiti za pristup sustavu kako bi načinio nekakvu štetu za sustav i/ili korist za sebe

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

- Što se dogodi sa slikama i video sadržajem koji uplodamo na Facebook ili neku drugu društvenu mrežu?
- Što se dogodi s podacima o internetskim pretragama ili našim navikama prilikom kupovine u trgovini (korištenje loyalty kartica)?
- Kako možemo znati tko sve posjeduje naše podatke i u koju svrhu ih koristi?
- Što ako netko „upadne” u naše računalo…kako se to može reflektirati na naš život?
- Bilo koji digitalni uređaj može biti potencijalni vektor za napad naše podatke, usluge/servise i infrastrukturu
- Neovisno o operativnom sustavu (Linux, Mac ili windows) hakerski napadi su u principu jednako opasni, najveća razlika je u brojnosti pojedinog operativnog sustava i raznovrsnosti/brojnosti aplikacija i servisa koji se koriste (jer se uglavnom koristi princip prijevare korisnika, a ne napada na tehnologiju)

Vrste napada(ča)

- **Amaterski-** još se nazivaju „Script Kiddies”, jer su to „Hakeri” s vrlo malo ili ništa znanja i vještina koji koriste postojeće jednostavne alate i gotove upute. Obično su samo znatiželjni i žele pokazati svoje „vještine”…međutim ovi napadi također mogu biti devastirajući
- **Hakerski-** ovim napadima je za cilj upasti u sustav i dobiti kontrolu nad što više elemenata IT sustava. Ove napade možemo još podijeliti na
  - „White Hat”-cilj ovih hakera je otkriti slabosti sustavu kako bi ga osnažili tako što ranjivosti komuniciraju prema vlasniku (primejr hakiranja automobila)
  - „Grey Hat” – Ovo je na pola puta između White i Black
  - „Black Hat”-ovo su zlonamjerni hakeri koji upadaju u sustave kako bi ih onesposobili u bilo kojem smislu
- **Organizirani hakerski (Cyber teroristi, cybercriminals, cyberwariors) -** ovo su skupine hakera koje financiraju velike organizacije…obično države u svrhu špijunaže, sabotaže i slično…

Hacker Profiles

The Yes Men Fix the World

Kako vas „hakeri” mogu iskoristiti?

- Hakeri do vas mogu kroz bilo koju vezu koju ostvarujete prema internetu (mobitel, PC, laptop…), ali nekad mogu i drugačije (direktno kroz stvarni svijet)..
- Zašto bi vi uopće bili zanimljivi hakerima? Vjerojatno niste nikome zanimljivi, osim ako vas ili vaše računalo ne žele koristiti kao „proxy” (npr. za DDoS napade) ili ako bi mogli lako do novca (npr..odgovorite na mail u kojem vas traže podatke o kartici…)
- Sve što radite na računalu, a posebno na internetu može se iskoristiti protiv vas
- Ono što bi nas moglo čekati u budućnosti, je nešto slično ovome (zato je vrlo važno imati prijatelje u stvarnom životu! ☺)

Unknown Identity (Liam Neeson) - Trailer HD 2011

- Trebamo biti vrlo oprezni sa svojim online računima, lozinkama i uopće aktivnosti na internetu

Kako se hakiranje ne radi: The Most Accurate Hacking Scene Ever
:D

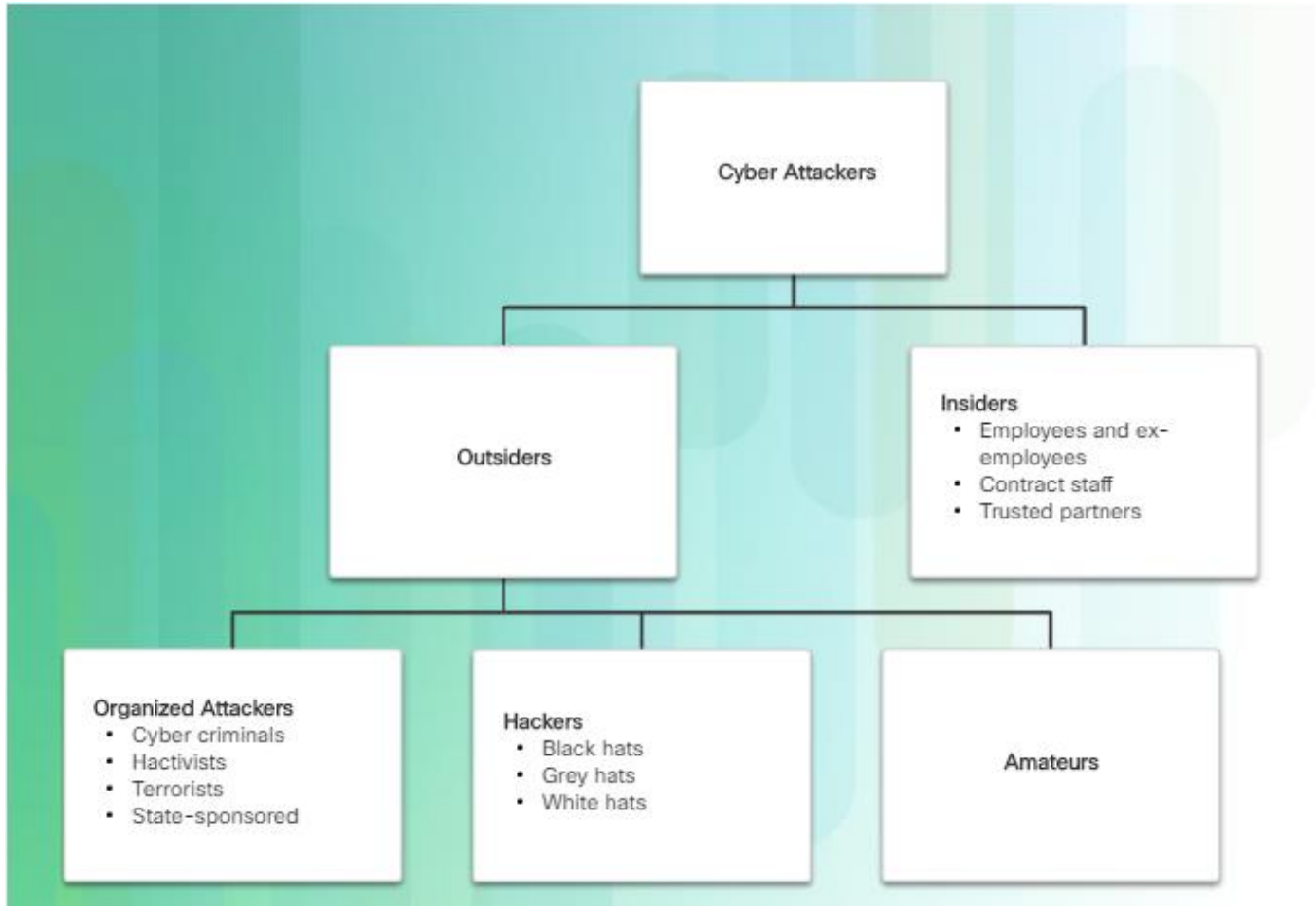
Vrste podataka i što je važno

Osobni i **korporativni** zato što načelno imamo privatni i poslovni život
Bez obzira o kojim podacima se radi tri stvari su važne:

1. Povjerljivost (engl. Confidentiality)-privatnost podataka
   Povjerljivost podataka bi trebala biti zajamčena propisanim korporativnim politikama koje ograničavaju pristup podacima neovlaštenim osobama. Povjerljivost osiguravamo kriptiranjem, Username/password, višestrukom autentikacijom i minimiziranjem dostupnosti osjetljivih podataka
1. Integritet (engl. Integrity)- Ovo bi bila konzistentnost podataka i vjerodostojnost podatak tiejkom životnog ciklusa podataka. Podaci se ne smiju mijenjati prilikom prijenosa. Checksum (hash) se koristi za provjeru integriteta podatka, a za zaštitu se koriste File permissions i user access control mehanizmi uz svakako osiguran backup podataka
2. Dostupnost (engl. Availability)- održavanje opreme, operativnih sustava i softwarea up-to-date kao i izrada backupa osigurava dostupnost podataka u slučaju njihovog gubitka uzrokovanog ljudskim faktorom ili višom silom. Za povrat podataka moraju postojati pripremljene procedure. Uređaji poput Firewalla, ali i razni drugi mehanizmi mogu štititi od napada poput DoS napada koji imaju za cilj učiniti podatke/uslugu nedostupnom

Ispitno pitanje:

Prijetnje-unutarnje i vanjske



Unutarnje ugroze:

- Loše upravljanje povjerljivim podacima
- Prijetnje fizičkoj infrastrukturi (požar, poplava, napajanje, oštećenje…)
- Pomoć vanjskim napadačima (namjerno ili nenamjerno)
- Neoprezno ponašanje na internetu (social engineering, malware…)

Vanjske ugroze podrazumijevaju sve pokušaje napada na IT sustav koji dolaze izvan kontroliranog okruženja

Posljedice napada

Ispitno pitanje:

- Reputation loss
- Data loss
- Loss of sales and revenue
- Loss of intelectual properties
- …

- Vaša tvrtka se smatra nesigurnom/nepouzdanom i manje ljudi želi s vama poslovati
- Možete imati veliku štetu zbog izgubljenih podataka (web trgovina koja nema proizvode). Napad samo radi uništavanja (Zašto? Zato što mogu!)
- Krađa podataka vaših korisnika, email adrese, kreditne kartice itd…(šteta za sve)
- Zbog krađe podataka, gubitka ugleda imat ćete manje prihode ili čak propasti u poslovnom smislu.
- Ako vam netko ukrade ideju za npr. „antigravitacijski stroj” to je sigurno velika šteta za tvrtku, ali i za ljude koji rade na tome…

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 VEHICLES WITH THIS $20 RADIO!!!

Cyberwarfare

Stuxnet decoder Ralph Langner speaks about Stuxnet

Vrste malwarea

- **Bot-malware** dizajniran da učini vaše računalo dijelom veće mreže botova (**botnet**) kako bi bili iskorišteni obično za DDoS napad
- **Ransomware-** malware koji ima za cilj držati naše računalo kao taoca kriptiranjem podataka na disku dok napadaču ne uplatimo novac
- **Scareware-** malware koji natjera korisnika koji je uplašen da napravi određene radnje…obično pop-up prozor gdje piše da radite nelegalne stvari i da trebate platiti kaznu ili nešto drugo

Vrste malwarea

Rootkit- malware dizajniran da modificira operacijski sustav kako bi omogućio napadaču „backdoor”-obično si kroz neke druge slabosti u programima poveća privilegije i onemogući računalo da ga prepozna
Virus- malware koji se zakači na druge .exe programe (legitimne) kako ga ne bi detektirali..svrha mu je od bezopasnih do brisanja podataka ili gore. Većina virusa zahtjeva korisničku aktivaciju za rad i korisnici ga šire po IT sustavu obično preko USB-a, mrežne veze, emailom itd..
Trojan horse- malware koji se predstavlja kao legitimna aplikacija, ali u pozadini radi zlonamjerne stvari. Obično se nalaze u video i audio datotekama, slikama, igrama…razlika u odnosu na virus je što se veže za datoteke koje nisu .exe

Worms- malware koji se sam replicira i iskorištava ranjivosti u IT sustavu. Nakon što ih korisnik ubaci u sustav dalje se sami repliciraju

Vrste malwarea

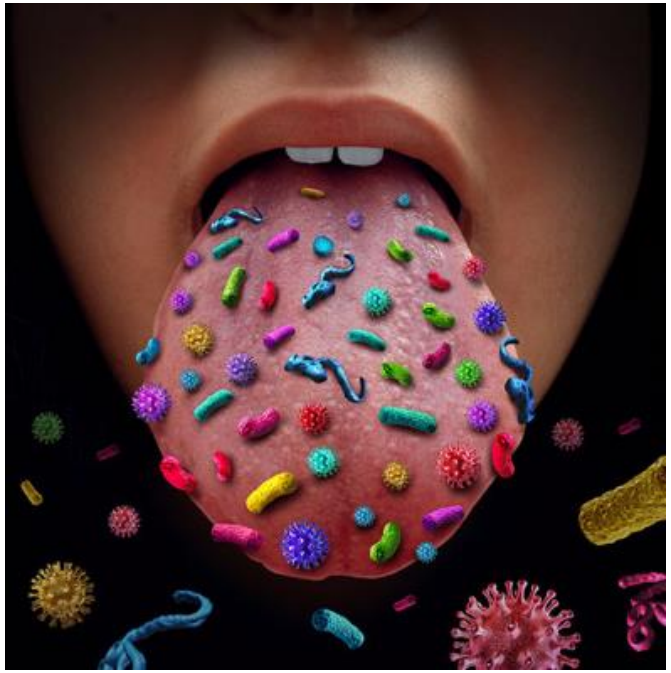
- **Spyware-** malware koji je dizajniran da prati ponašanje korisnika i skuplja zanimljive podatke (keystrokes, browsing history, dana capture…) često isključuje sigurnosne mjere na računalu
- **Adware-** programi koji automatski bez znanja korisnika prikazuju reklamni sadržaj

Simptomi napada malwarea

Ispitno pitanje:

Neovisno o vrsti malwarea ovo su uobičajeni simptomi :

- There is an increase in CPU usage.
- There is a decrease in computer speed.
- The computer freezes or crashes often.
- There is a decrease in Web browsing speed.
- There are unexplainable problems with network connections.
- Files are modified.
- Files are deleted.
- There is a presence of unknown files, programs, or desktop icons.
- There are unknown processes running.
- Programs are turning off or reconfiguring themselves.
- Email is being sent without the user’s knowledge or consent.

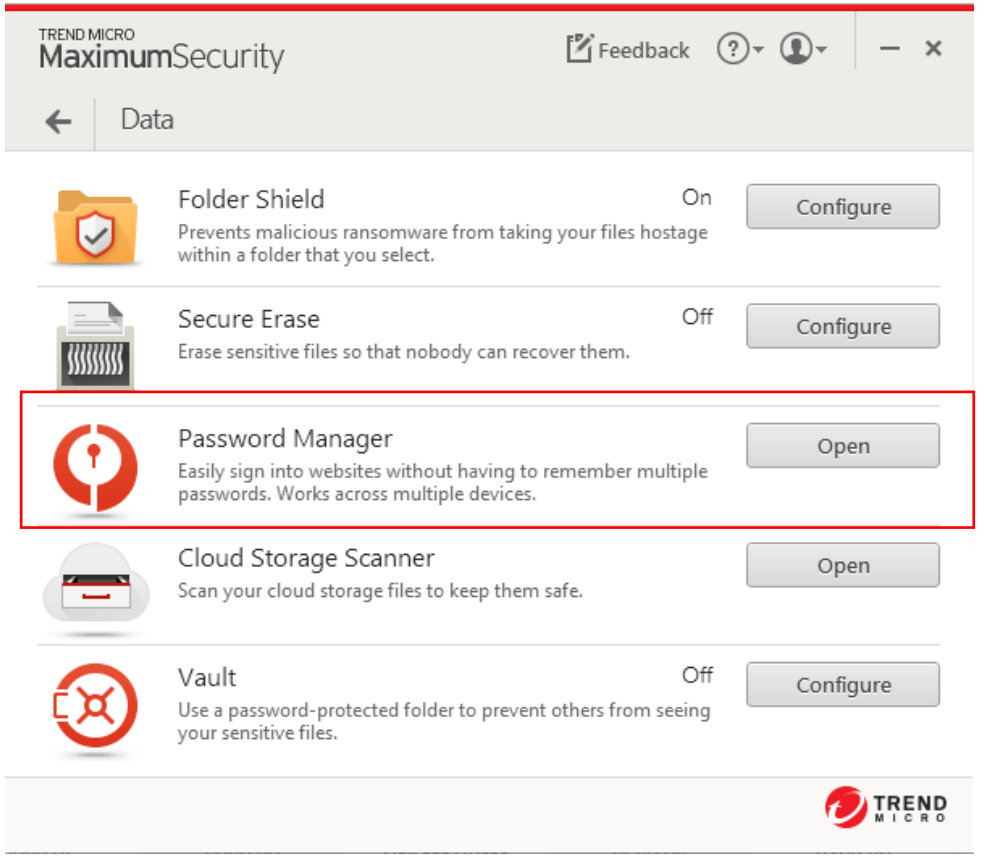


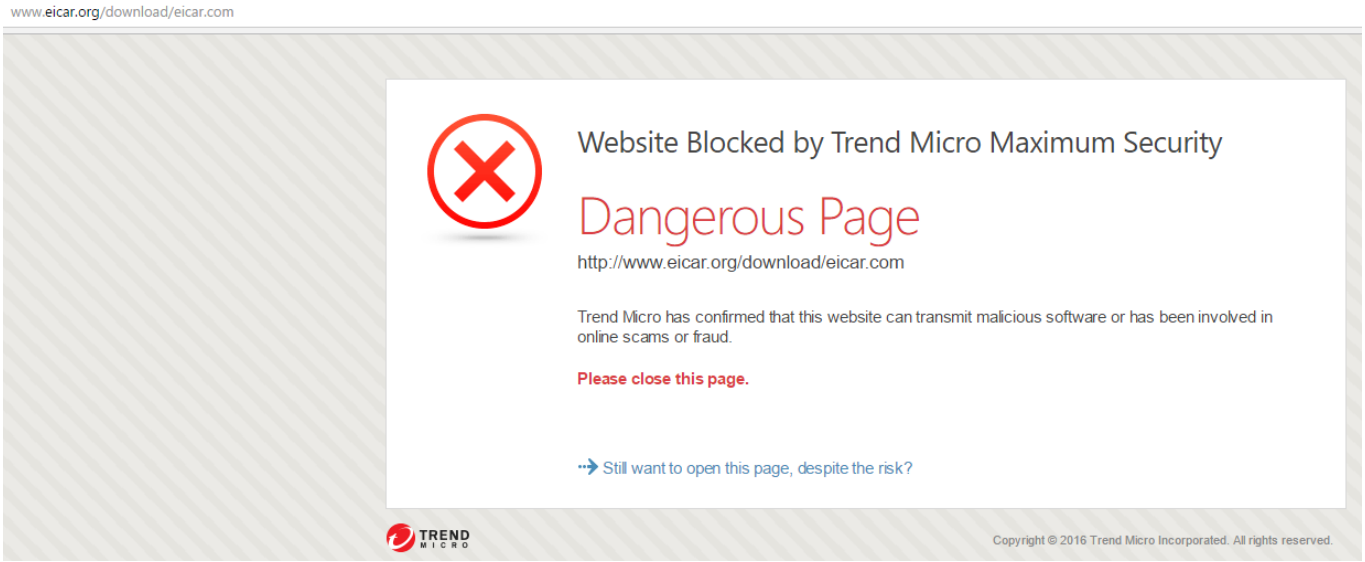
Antivirus

http://www.toptenreviews.com/software/security/best-small-business-antivirus

https://www.pcmag.com/article2/0,2817,2372364,00.asp

http://www.eicar.org





Vrste napada

Ispitno pitanje

1. **Reconnaissance attack-** ovo je zapravo priprema za napad..npr skeniranje portova ili traženje ranjivih osoba (za social engineering)… https://www.youtube.com/watch?v=1e6tBAaykg4
2. **DOS napad-** napada kojim se želi neka usluga učiniti nedostupnom, obično se radi velikim količinama prometa prema ciljanom servisu, ali može se koristiti i posebno dizajniran promet za specifičan servis (koji ga onda sruši)
3. **DDoS-isto kao DoS**, ali s više lokacija odjednom
4. **Man in the middle-** napad koji za cilj ima presretanje komunikacije bez znanja sudionika u komunikaciji s ciljem dobivanja osjetljivih informacija (lozinke, username,…)
5. **Wi-fi password cracking-** hakiranje wireless AP-a u svrhu pristupa mreži (može se koristiti social engineering, brute force napad, network sniffing)
6. **Social engineering-** vrsta napada u kojoj napadač pokušava manipulirati žrtvom kako bi napravila radnje kojima će otkriti povjerljive informacije
   - **Phishing-** napadač šalje email u kojem se predstavlja kao netko drugi kako bi zadobio povjerenje žrtve
   - **Pretexting** –laganje u svrhu dobivanja osjetljivih informacija (npr. lažno se predstavljamo da zovemo iz banke)
   - **Tailgating-** Napadač prati osobu koja ima pravo pristupa sigurnoj lokaciji
   - **Something for something-** napadač traži osobne podatke u zamjenu za poklon

Dos-Ddos napadi u „realnom vremenu”

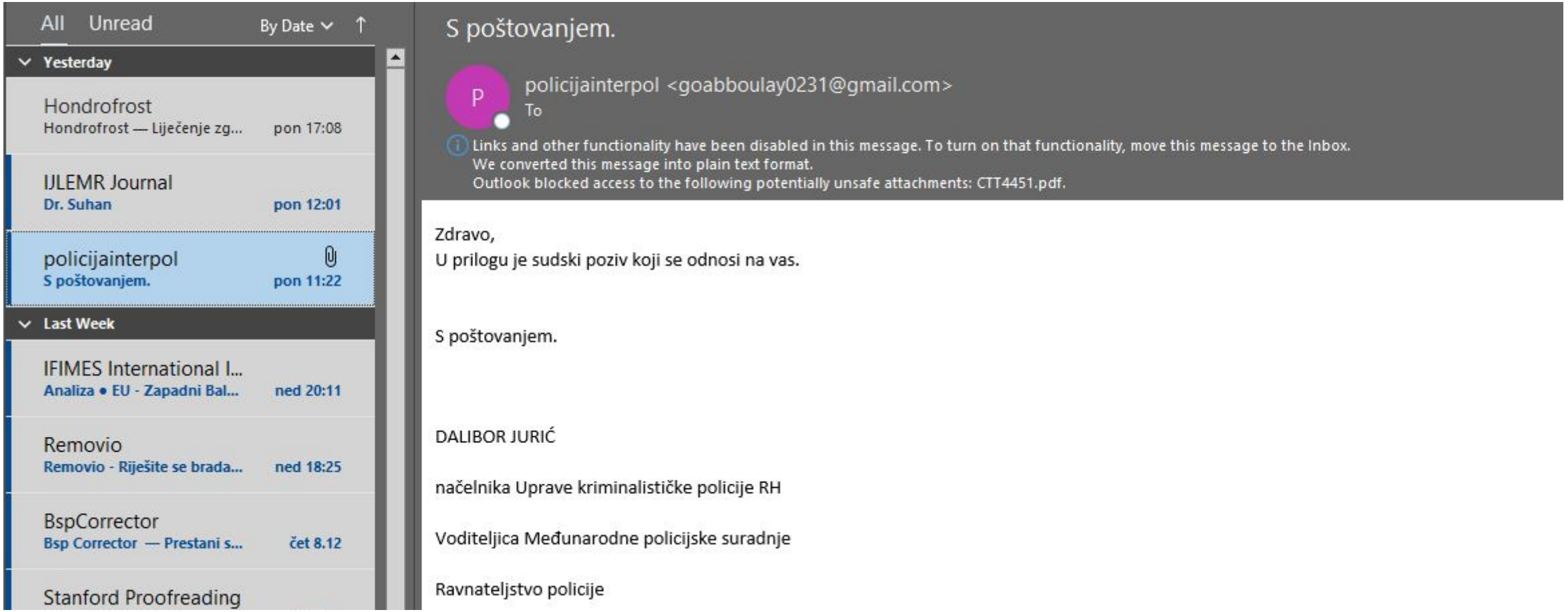
http://www.digitalattackmap.com
https://cybermap.kaspersky.com
https://threatmap.checkpoint.com/ThreatPortal/livemap.html

Ispitno pitanje:
DoS napadi ciljaju na dostupnost (Availability) sustava
Primjer DoS napada je TCP SYN Flood –zloupotrebljava 3-way handshake mehanizam tako što napadač šalje brojne segmente s postavljenom SYN zastavicom (bitom), žrtva na svaki upit odgovara sa SYN/ACK, ali napadač ne odgovori žrtvi s ACK, već započinje nove konekciju i tako dok žrtva ostane bez resursa i legitimni korisnici više ne mogu pristupiti serveru. Napadač obično koristi lažnu IP adresu tako da kada žrtva odgovara na SYN od napadača, zapravo šalje SYN/ACK na IP adresu koja uopće nije inicirala komunikaciju. Zbog usmjeravanja prometa na internetu bez obzira što napadač lažira IP adresu odgovor će otići prema mreži u kojoj se ta IP adresa zaista nalazi.

Ispitno pitanje:
DDoS napadi

Kako postići sigurno IT okruženje u organizaciji?

- Edukacija i osvješćivanje korisnika/zaposlenika
- Smislene sigurnosne politike unutar organizacije (nešto što će se zaista koristiti kako je očekivano)
- Kontrola pristupa IT sustavu (mreža, serveri…višestruka autentikacija)
- Smislen nadzor IT sustava i upravljanje incidentima
- Zaštititi sve uređaje u organizaciji s antimalware zaštitom
- Kategorizacija i filtriranje nepoželjnog prometa (Firewall za organizaciju)
- Držati operativne sustave i software up-to-date
- Osigurati primjereno wireless mrežu (enkripcija, primjerena snaga signala, skriveni SSID)
- Koristiti primjerene lozinke
- Kriptirati svoje podatke i komunikaciju
- Raditi backup (offsite-cloud)
- Trajno brisanje podataka


All
Unread
By Date
Yesterday
Hondrofrost
Hondrofrost — Liječenje zg...
pon 17:08
IJLEMR Journal
Dr. Suhan
pon 12:01
policijainterpol
S poštovanjem.
pon 11:22
Last Week
IFIMES International I...
Analiza • EU - Zapadni Bal...
ned 20:11
Removio
Removio - Riješite se brada...
ned 18:25
BspCorrector
Bsp Corrector — Prestani s...
čet 8.12
Stanford Proofreading
S poštovanjem.
P
policijainterpol <goabboulay0231@gmail.com>
To
Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.
We converted this message into plain text format.
Outlook blocked access to the following potentially unsafe attachments: CTT4451.pdf.
Zdravo,
U prilogu je sudski poziv koji se odnosi na vas.
S poštovanjem.
DALIBOR JURIĆ
načelnika Uprave kriminalističke policije RH
Voditeljica Međunarodne policijske suradnje
Ravnateljstvo policije

Re: Slučaj prekršaja

ZP

ZAGREBACKA POLICIJA <coie@plasencia.uned.es>
To

Reply | Reply All | Forward

čet 20.4.2023 23:19

Slučaj_prekršaja _2304221685-1.pdf
147 KB

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

Izvješće o istrazi :

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

___

Maria Goatti, glasnogovornica
Zagrebačke Policijske uprave

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-

Kako postići sigurno osobno IT okruženje?

- Kontrola pristupa svojim računima (višestruka autentikacija)
- Antimalware zaštita na svim uređajima koje koristimo
- Firewall-na računalu ga ne isključivati
- Držati operativne sustave i software up-to-date prema preporukama proizvođača (automatic update)
- Osigurati primjereno wireless mrežu (enkripcija i skriveni SSID)
- Koristiti primjerene lozinke (Passphrases)
- **Kriptirati** svoje podatke i raditi backup (offsite-cloud)
- Ne izlagati se u velikoj mjeri na internetu
- U mailovima ne klikati na linkove bez provjere („mouse over” to confirm legitemate sources)
- Ne koristiti istu lozinku za sve korisničke račune (Use password manager software)
- Zaključavati računalo ako niste kraj računala  + L
- Slijediti preporuke i smjernice organizacije u kojoj radite
- …

Ispitno pitanje

Primjer lozinki

https://howsecureismypassword.net Ne koristiti!

OK	Good	Better
allwhitecat	a11whitecat	A11whi7ec@t
Fblogin	1FBLogin	1.FB.L0gin$
amazonpass	AmazonPa55	Am@z0nPa55
ilikemyschool	ILikeMySchool	!Lik3MySch00l
Hightidenow	HighTideNow	H1gh7id3Now

Ispitno pitanje

Tips for choosing a good password:

- Do not use dictionary words or names in any languages
- Do not use common misspellings of dictionary words
- Do not use computer names or account names
- If possible use special characters, such as ! @ # $ % ^ & * ( )
- Use a ten or more character password

Bolje je koristiti „passphrases”

OK	Thisismypassphrase.
Good	Acatthatlovesdogs.
Better	Acat th@tlov3sd0gs.

Ispitno pitanje

Tips in choosing a good passphrase:
Choose a meaningful statement to you
Add special characters, such as ! @ # $ % ^ & * ( )
The longer the better
Avoid common or famous statements, for example, lyrics from a popular song

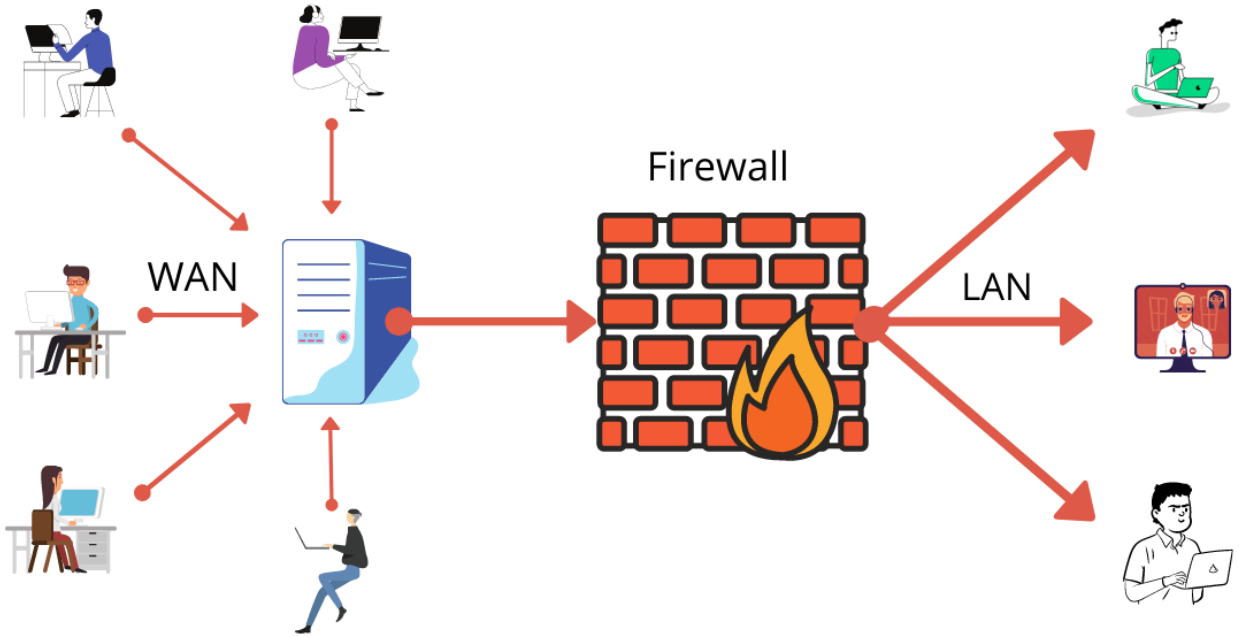
Osigurati svoj rad u web browseru

- Bilo tko ako ima fizički pristup vašem računalu (što svakako treba spriječiti) može saznati vašu povijest pretraživanja i koristiti vaše login podatke za upasti u vaše online račune
- Ne koristiti tuđa/javna neosigurana računala za logiranje u svoje accounte
- Zato trebamo koristiti „master” lozinku u browseru (ili neki drugi alat za čuvanje lozinki) i privatni mod pretraživanja

  Microsoft Internet Explorer: InPrivate
  Google Chrome: Incognito
  Mozilla Firefox: Private tab / private window
  Safari: Private: Private browsing
  …
  Ili surfati iz virtualke koju kada završimo obrišemo.

Firewall-vatrozid

- Ovi uređaji služe kako bi zaštitili jednu mrežu od druge…uglavnom mrežu tvrtke od napada s interneta



Postoje

- Rubni mrežni vatrozidi (engl. network perimeter firewalls)
- Vatrozidi na računalima (engl. host-based firewalls)

Vatrozidi mogu biti implementirani u hardwareau, softwareu ili i jedno i drugo istovremeno

Firewall-vatrozid

- Prvi vatrozidi su bili **Liste za kontrolu pristupa** na temelju IP adrese bez praćenja konekcije (engl. Stateless)

- Kasnije su vatrozidi počeli raditi i provjere konekcije i stanja tih konekcija (engl. **Statefull**) gdje su pratili IP adrese izvora i odredišta, portove izvora i odredišta kao i stanje konekcije

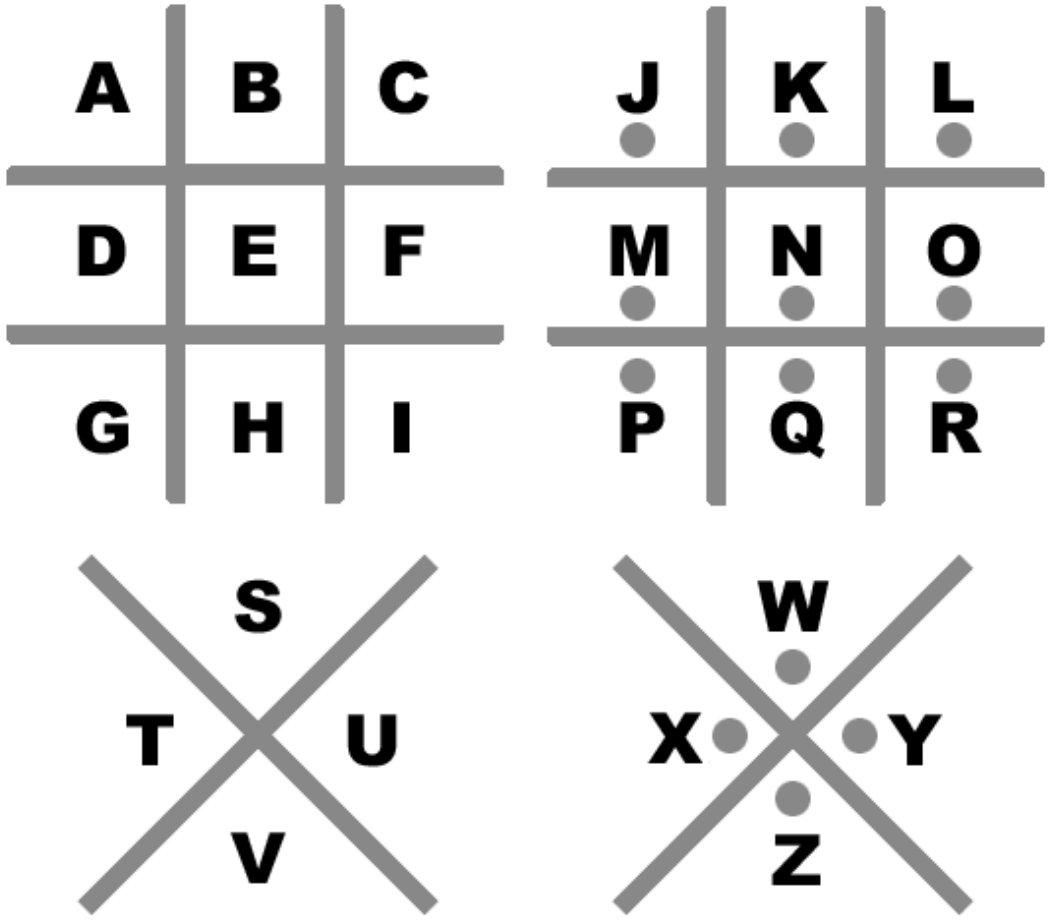
- Nakon toga su se razvili **aplikacijski vatrozidi** (engl. Application Firewall) koji su mogli osim IP adresa portova i stanja veze prepoznati i aplikaciju koja se koristi i blokirati samo neke elemente aplikacije (poput naredbi) ili cijelu aplikaciju. To su mogli raditi i na temelju prepoznavanja odstupanja aplikacije od uobičajenog rada.

- **Aplikacijski-Proxy firewall-** uređaj koji se postavlja između klijenta i ostatka mreže (Internet), ali osim svega što može raditi application firewall ovaj može još i autenticirati korisnika i zapravo posreduje u komunikaciji..tako da svaka veza klijenta prema serveru na internetu ima dvije konekcije, jedna prema proxy firewallu, a druga od proxy firewalla prema serveru na internetu (nešto je sporiji od čistog aplikacijskog firewalla)

- **UTM** (engl. Unified Threat management).najnovija vrsta vatrozida (još ih zovemo i Next-Gen Firewall)-ideja je da se više funkcionalnosti integrira u jedan uređaj (web security, mail security, network security…)

?

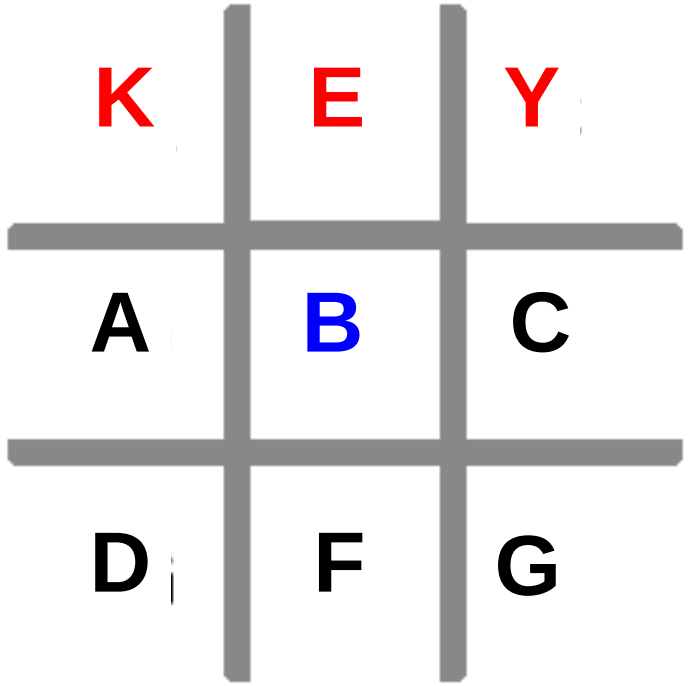
„Pig Pen Ciphre”

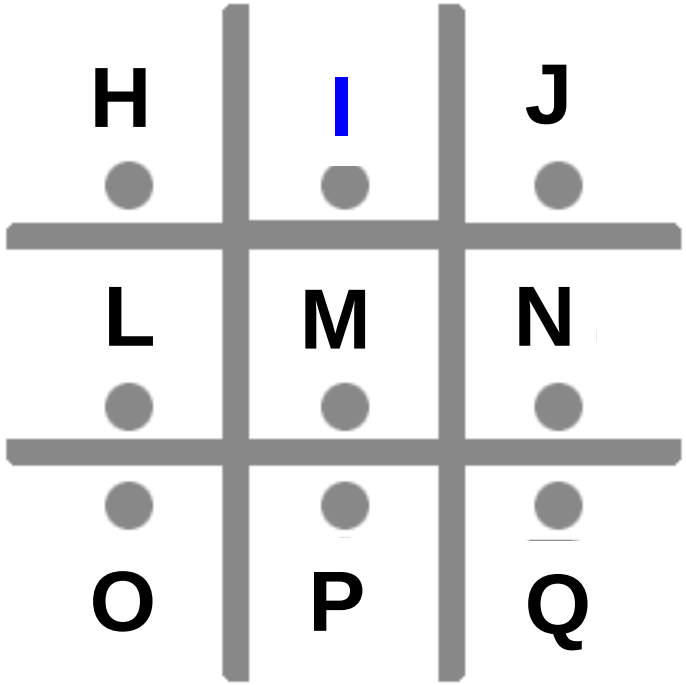


„Pig Pen Ciphre”

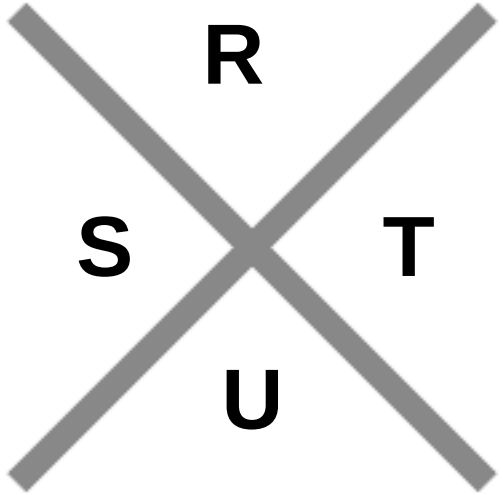
PRAKTIKUM

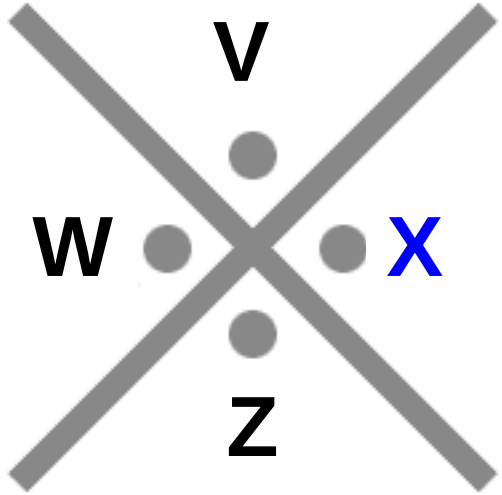
„Pig Pen Ciphre”





KEY



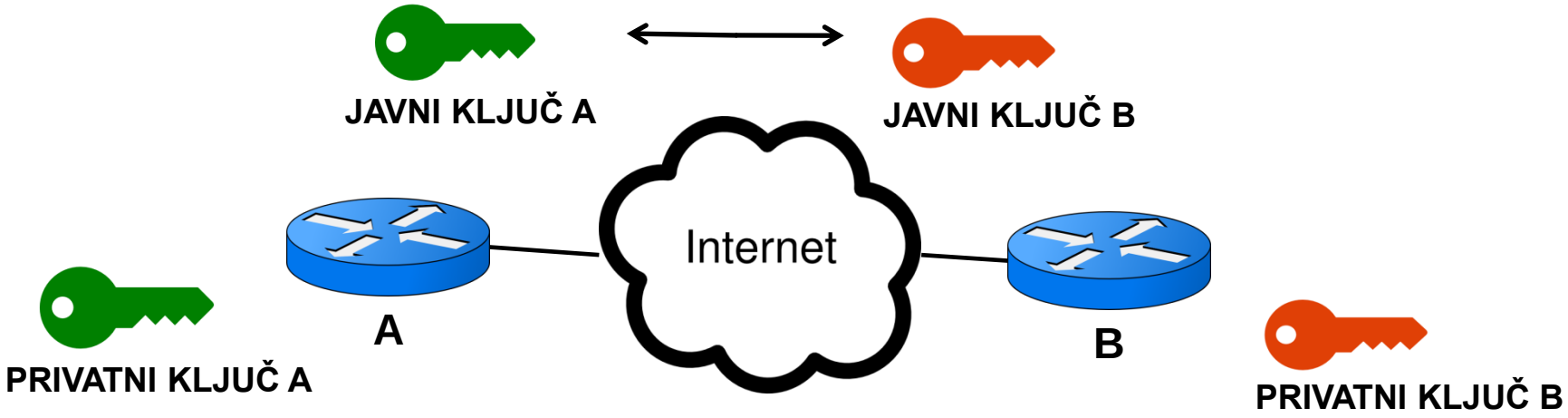


„Pig Pen Ciphre”

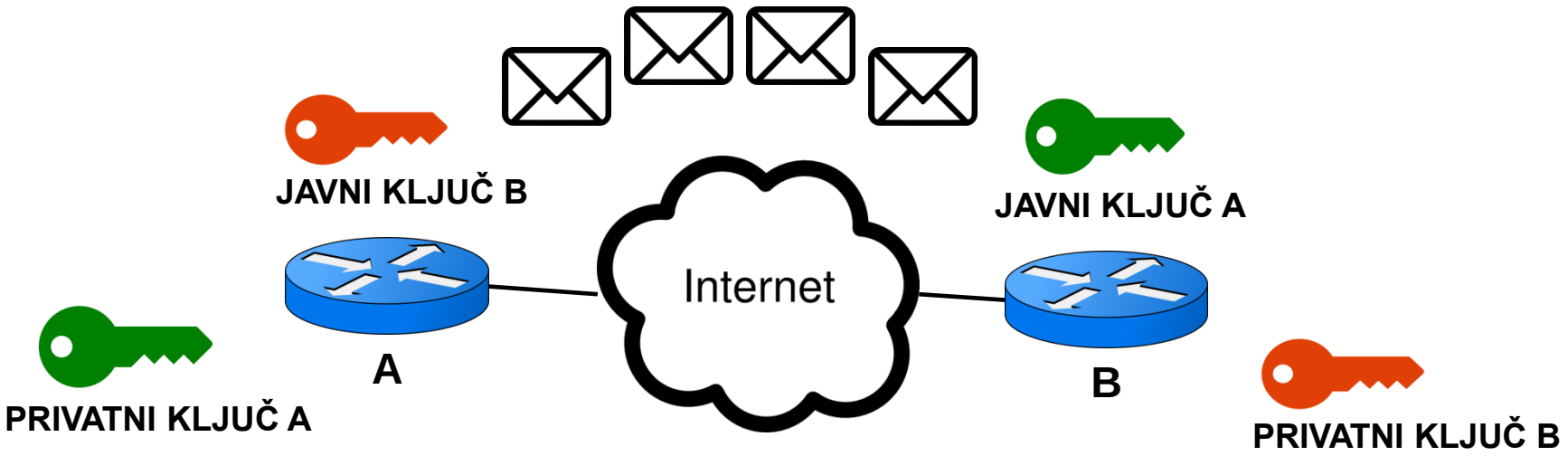
PRIJE

P R A K T I K U M

Enkripcija komunikacije ključem danas- Asimetrična enkripcija

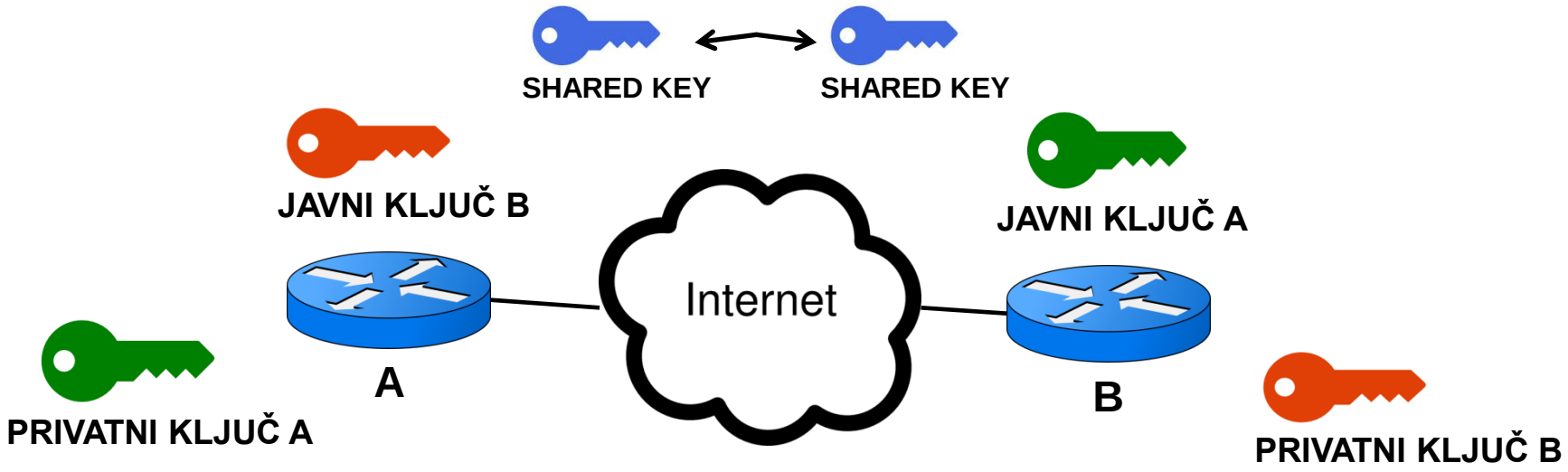


Enkripcija komunikacije ključem danas- Asimetrična enkripcija

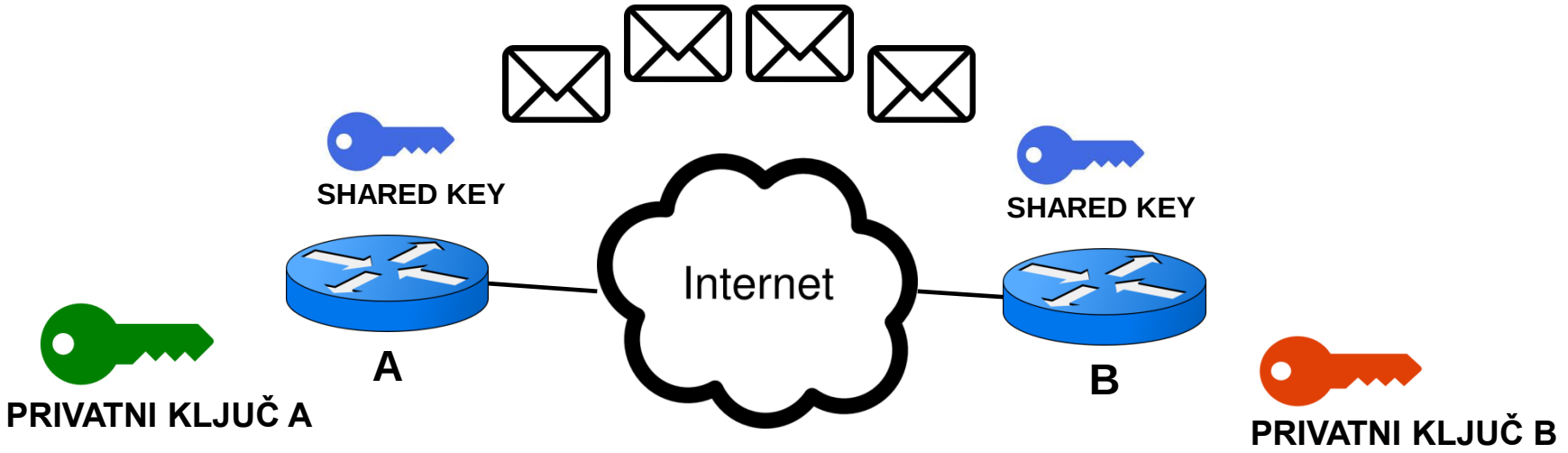


- Problem je preveliko opterećenje uređaja koje nije potrebno

Enkripcija komunikacije ključem danas- Simetrična enkripcija



Enkripcija komunikacije ključem danas- Simetrična enkripcija



- Dovoljno sigurno a ne opterećuje uređaj kao asimetrično kriptiranje

?