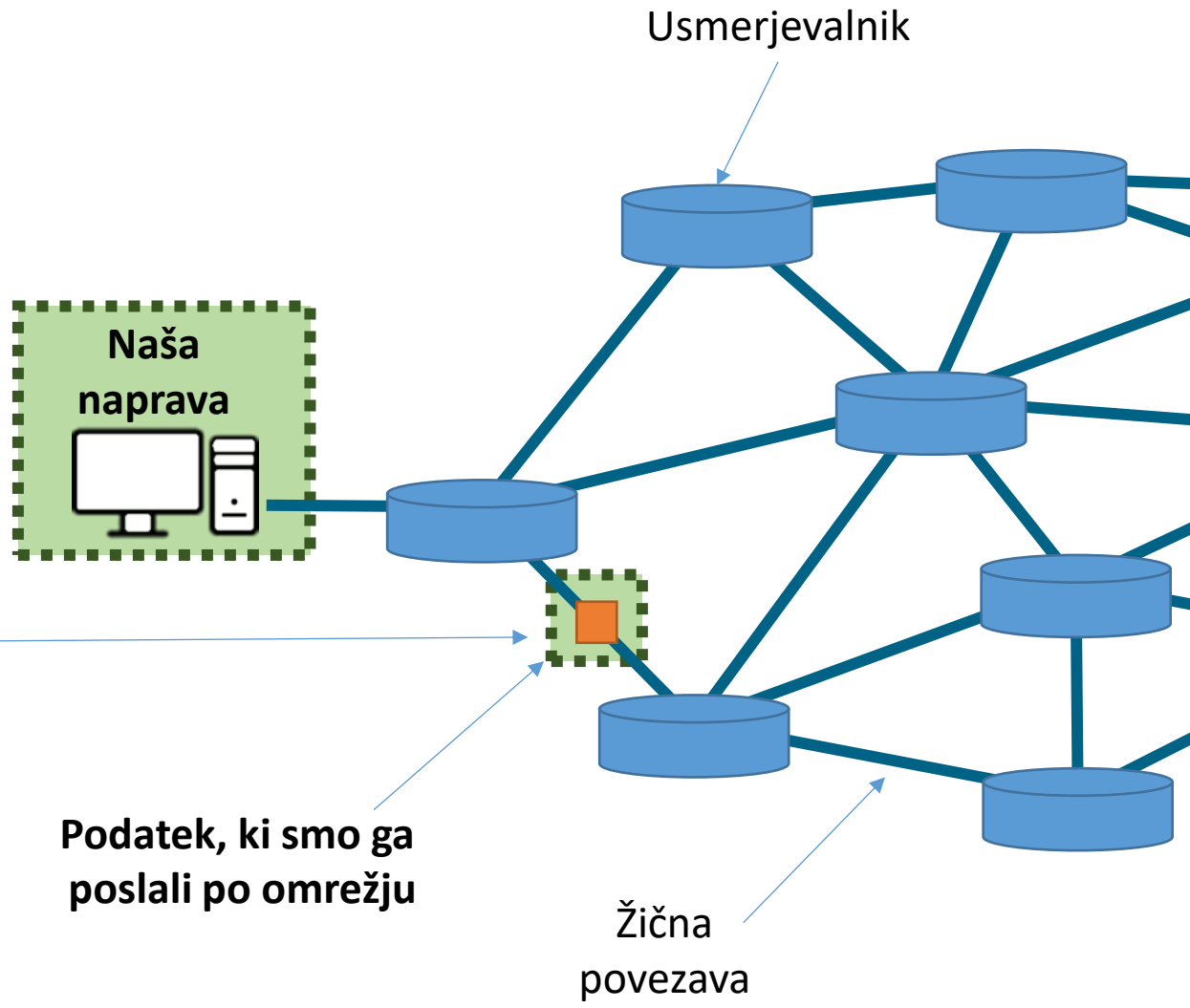
Računalniška varnost

Ranljivost na internetu

- Na računalniškem omrežju smo ranljivi na več nivojih:
  - Ranljivi so **viri na napravah** – dostop le avtoriziranim uporabnikom. S tem se ukvarja področje **računalniške varnosti**.
  - Ranljivi so **podatki, ki se prenašajo po omrežju** – dostop le pošiljateljem in naslovnikom. S tem se ukvarja področje **zasebnosti**.



Varnost podatkov in virov

- **Računalniška varnost** (angl. *cyber security*) združuje tehnike, ki skrbijo, da ni **neavtorizirane interakcije** s shranjenimi podatki in viri na naših napravah in omrežjih.
  - Viri: naprave priključene na računalnik ali omrežje: tiskalnik, zvočniki, ekran, televizor, mobilni telefon.
  - Način interakcije: uporaba, branje, spreminjanje, odtujitev, brisanje.

- Več nivojev varnosti:
  - Varnost na sami **napravi**, ker so shranjeni podatki.
  - Varnost na **lokalnem omrežju** (ne še internetu) v katerega je naprava priključena.

Hekerji

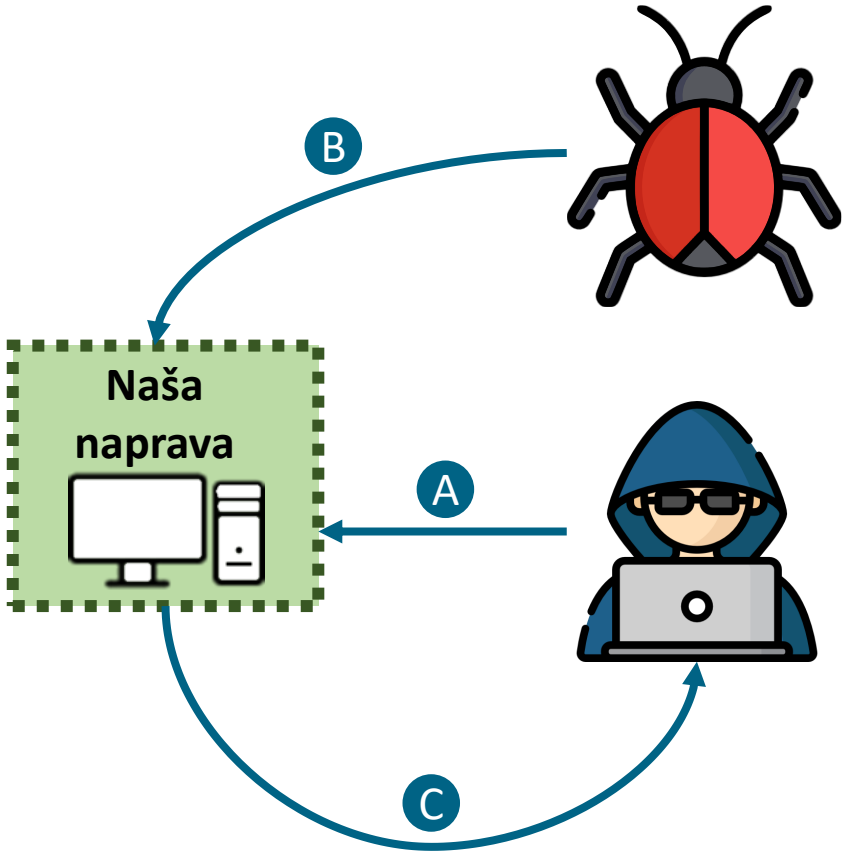
- Nepridipravi, ki izkoriščajo varnostne pomanjkljivosti za svoj dobrobit so **hekerji** (angl. *hackers*).
  - Včasih hekerji le odkrivajo pomanjkljivosti, jih pa ne izkoriščajo. Najdene pomanjkljivosti se prodajajo na spletu za milijone.

- Hekerji so bodisi posamezniki ali pa dobro organizirane skupine visoko izobraženih in odlično plačanih zaposlenih.
  - Hekerske skupine ima vsaka večja velesila.

Znane državne hekerske skupine

- **Etični hekerji** (angl. *ethical hackers* ali *white-hat hackers*) delajo to kot službo in pomanjkljivosti sporočajo naročniku (in jih ne izkoriščajo za svoj dobrobit).

Kako pride do neavtorizirane interakcije



A. Hekerji izkoriščajo **neprimerne nastavitev** ali **varnostne pomankljivosti**, da sami izvedejo neavtorizirano interakcijo.

B. Zlonamerna programska oprema za hekerje izvede neavtorizirano interakcijo.

C. Hekerji s **socialnim inženiringom** prepričajo lastnika naprave, da samovoljno za njih izvede neavtorizirano interakcijo.

Varnostne pomankljivosti

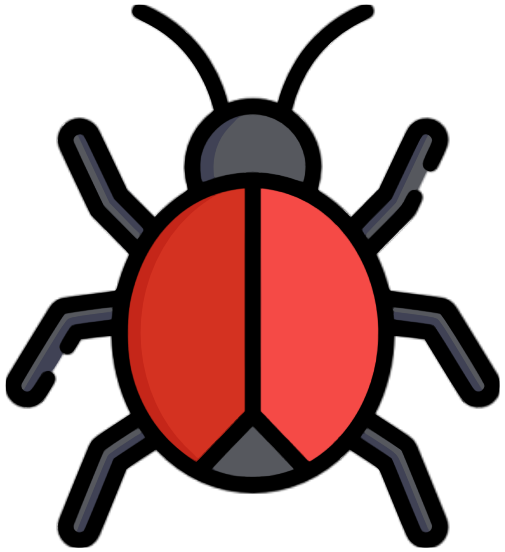
- Naše naprave in programska oprema na napravi so narejene pomanjkljivo. Obstajajo napake, ki so posledica napak pri kreaciji naprav in programov ali interakcij med napravami in programi.

- **Varnostne pomanjkljivosti** (angl. *security vulnerability*) so take napake, ki omogočajo neavtorizirane interakcije s shranjenimi podatki in viri na naših napravah in omrežjih.
  - Prav zato posodabljamo naše programe/aplikacije in operacijske sisteme!

- Pomanjkljivosti, ki so že najdene, ampak javno še niso znane (se pa že prodajajo nepridipravom) so **zero-day varnostne pomanjkljivosti**.
  - Cena dobrih zero-day pomanjkljivosti se giblje v milijonih evrov.

Zlonamerna programska oprema

- **Zlonamerna programska oprema** (angl. *malicious software* ali *malware*) je program katerega namen je motnja delovanja naprave (npr. računalnik ali mobilni telefon) in neavtorizirana interakcija z viri in datotekami na napravi.

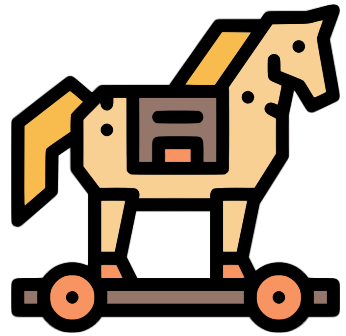


- Način okužbe:
  1. preko **omrežja** (interneta ali lokalnih omrežij)
  2. preko drugih **vhodov v napravo** (USB ključki, zunanji diski, DVDji, Blu-ray…)

Malware glede na način širjenja

- **Virus** – program, ki ga mi namestimo na naš računalnik brez naše vednosti (npr. odpiranje datoteke). Za širjenje rabijo gostitelja – datoteko na katero se “prilepijo”.

- **Trojanski konj** – program, kateri na prvi pogled zgleda koristno, ampak skriva zlonamerno delovanje. Namestimo ga sami in se tega zavedamo.



- **Črv** – program, ki se namesti samodejno brez našega posredovanja. Ne rabijo gostitelja, so samostojni programi.

Malware glede na zle namene

- **Adware** – prikazuje nam nezaželene reklame, bodisi kar kot svoje programe ali nam jih vtakne v spletne strani.
- **Spyware** – prisluškuje naši interakciji na napravi in z omrežjem. Npr. keylogger spremlja naše tipkanje.
  - Informacije o nas pošlje lastniku največkrat za krajo identitete.
- **Ransomware** – z različnimi tehnikami (izbris ali okvara datotek in naprav; prisluškovanjem) od nas zahteva denar.
- **Zombie** – naredi naš računalnik v posrednika med (zlonamernim) lastnikom in njegovimi drugimi zli delovanji.

Antivirusni program

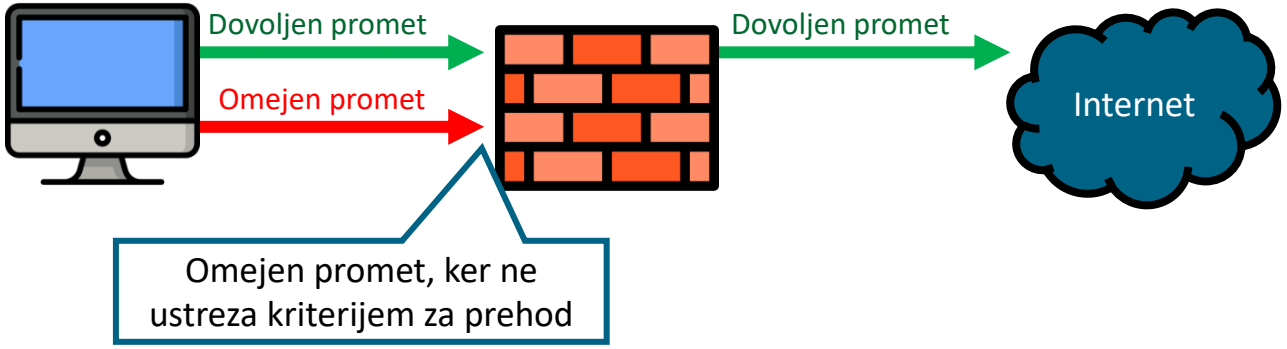
- Je programska oprema, ki išče in prepreči zlonamerno programsko opremo. Pregleduje **že nameščeno** zlonamerno programsko opremo in **tako, ki se šele preizkuša namestiti** na našo napravo.
  - Najdene že nameščeno zlonamerne programe preizkuša odstraniti, okužene datoteke pa “pozdraviti” – odstraniti virus od drugače normalnih datotek.
  - Delovanje antivirusnih programov je lahko **pasivno** (ves čas pregleduje internetni promet, ter programe in datoteke na napravi), ali **aktivno** (ob uporabnikovi želji zažene pregled programov in datotek).
  - Pregleduje bodisi **vsebino datotek**, ali pa **opazuje obnašanje delovanja** programov/datotek.

Požarni zid (angl. *firewall*)

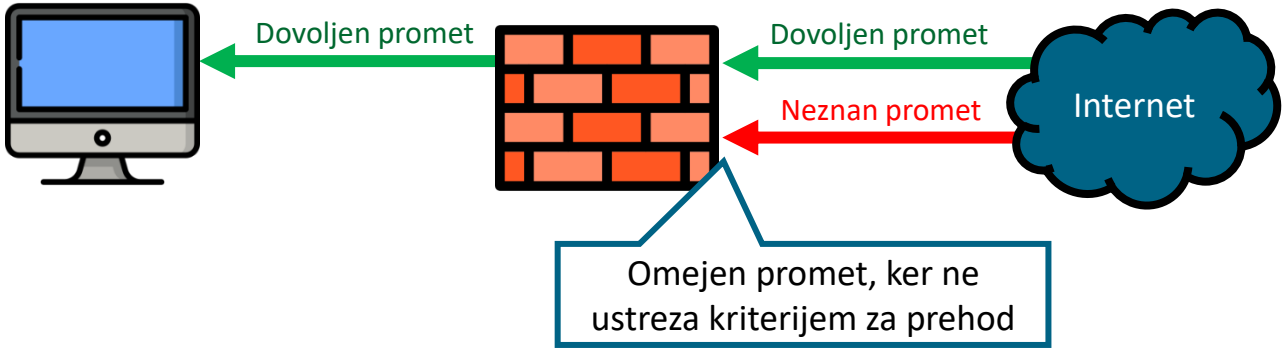
- Onemogoča prehod potencialno nevarnih vsebin (požar) z interneta v privatno omrežje ali posamezno napravo.
  - S tem prepreči širjenje nevarnih vsebin oz. prepreči širjenje požara.

- Deluje tako, da pregleda ves promet (v obe smeri), ki poteka skozi njega. Če promet vsebuje vsebino, ki jo oceni za škodljivo, prepreči prehod.

Prepreči promet iz lokalnega omrežja v internet.



Prepreči promet iz interneta v lokalno omrežje.



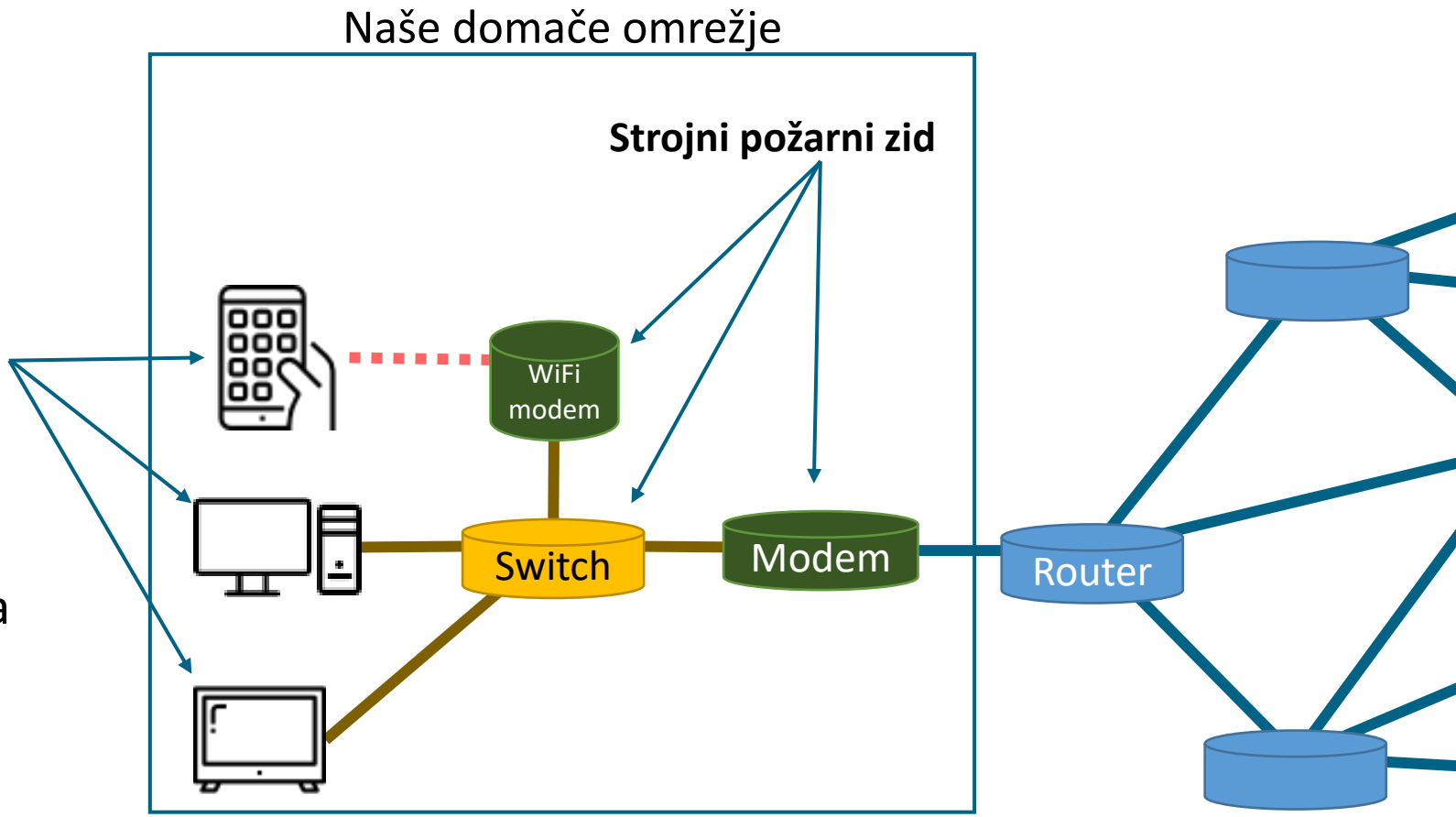
Pravila prepuščanja požarnega zida

- Pravila prepusta določimo na dva načina:
  - **Izrecno dovolimo določen promet**, vse kar pravilom ne ustreza, ne gre skozi.
  - **Izrecno prepovemo določen promet**, vse kar pravilom ne ustreza gre skozi.

- Pravila so lahko preprosta: prepuščamo ali blokiramo promet iz/na določen IP ali domeno, skozi določena vrata, na določenih protokolov….
  - Primeri: blokiramo promet k/iz facebook.com; blokiramo Torrent protokol v obe smeri; blokiramo vrata FTP protokola v naši smeri…
- Pravila so lahko tudi kompleksna: pregledamo ves promet in glede na vsebino določimo, če gre skozi ali ne.
  - Primeri: blokiramo promet, če ima ta vsebino podobno prenosu glasbe; blokiramo promet v naši smeri, če se prenašajo programske datoteke…

Dva tipa požarnih zidov

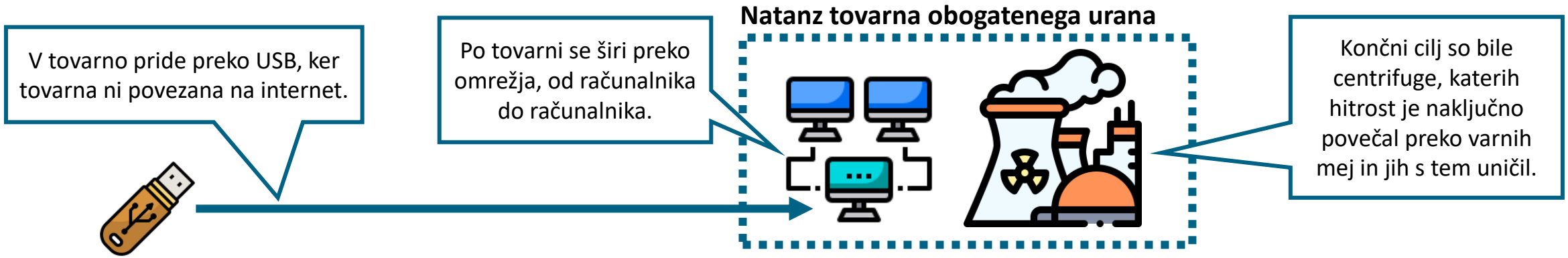
- **Strojni požarni zid** je del naprave.
  - Na omrežnih napravah.
- **Programski požarni zid** je program na napravi.
  - Kot samostojni program (Comodo Firewall).
  - Kot del operacijske sistema (v Windows in Linux).
  - Kot del antivirusnega paketa (Avast Firewall).



Stuxnet – orožje kibervojne

Več o tem v dokumentarcu Zero Days

- Črv, ki se je širil preko omrežja in preko USB ključkov po računalnikih z Microsoft Windows operacijskim sistemom.
- Odkrili so ga julija 2010, ampak njegovega namena niso poznali.
  - Odkril ga je beloruski znanstvenik – ob pisanju opisa je doživel kibernapad.
- Namen Stuxneta je bil sabotaža Iranskih centrifuge za proizvodnjo obogatenega urana (kateri se lahko nameni za nuklearno orožje).



Motnja virov z DDoS napadi

- Zombiji tvorijo **botnet omrežja**, ki mirujejo, dokler jih lastnik tega omrežja pokliče, da izvedejo DDoS napad na izbran strežnika.
  - Lastniki so kriminalne družbe (ali tudi države?).

- V **DDoS napadu** pošljejo vsi zombiji povpraševanje za spletno stranjo na njen strežnik tolikokrat v sekundi, da za strežnik napada preneha delovati.
  - Napadi se vrstijo na privatna podjetja in državne institucije.
  - Manjši napad (ki onesposobi slabši strežnik) se lahko kupi že za nekaj 100€.

Kateri DDoS napadi se vršijo danes

Avtorizacija in avtentikacija

- Osebe ali naprave katerim dovolimo interakcijo s shranjenimi podatki in viri na naših napravah in omrežjih so **avtorizirane** – imajo dovoljenje za interakcijo.

- Izziv: kako se prepričamo, da je oseba ali naprava, ki zahteva interakcijo res ta za katero se izdaja?

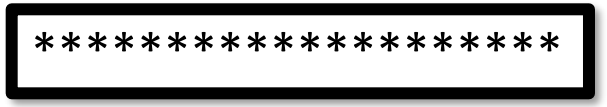
- **Avtentikacija** je postopek dokazovanja, da smo oseba ali naprava, ki ima dovoljenje za interakcijo s shranjenimi podatki in viri na naših napravah in omrežjih.

Pristopi avtentikacije

- Tirje pristopi avtentikacije:
  - **Kaj veš**: geslo, PIN, odgovor na varnostno vprašanje…
  - **Kaj imaš**: kartico s kodo, telefon kamor dobiš SMS, USB ključ s kodo…
  - **Kaj si**: prstni odtis, sken roženice ali obraza…

- Stopnja varnosti je odvisna od števila uporabljenih pristopov:
  - Najmanjša stopnja varnosti zahteva le en pristop in se imenuje **enofaktorska** (angl. *one-factor*) avtentikacija.
  - **Dvofaktorska** (angl. *two-factor*) avtentikacija zahteva dva pristopa.
    - Primer: ob vpisu gesla, se na telefon pošlje SMS s kodo.
  - **Večfaktorska** (angl. *multi-factor*) pa več pristopov.

Gesla



- **Gesla** so najpogostejši pristop „*kaj veš*“ avtentikacije. Praviloma bi geslo naj poznal le njen lastnik.

- Izziv: kako si izbrati geslo, ki si ga hkrati **enostavno zapomnimo** in ga je **težko uganiti**.
  - Če imamo prelahka gesla, jih je enostavno uganiti. To postaja vedno lažje z vse hitrejšimi računalniki.
  - Današnji računalniki lahko preizkusijo okoli milijon gesel v eni sekundi!

Kako enostavno je odkriti tvoje geslo

- Tudi, če imamo dobro geslo, pa različne storitve ne skrbijo primerno za naša gesla.
  - Z vdori v strežnike je neprimerno shranjena gesla (ki niso primerno kriptirana) enostavno ukrasti.
  - Zato redno menjujmo gesla in jih ne imejmo vedno enaka (ali po enakem vzorcu).

Preverite, če je tvoje geslo bilo ukradeno

Gesla – zakaj in kako izbrati primerno

Primer

- Če je geslo sestavljeno izključno iz majhnih črk slovenske abecede, je to 25 možnih znakov. Če je tako geslo dolgo le 5 znakov, obstaja

  $25*25*25*25*25 = 25^5 =$
  $= 9.765.625$ možnih gesel

- Koliko največ časa rabimo za ugotovitev gesla, če računalnik lahko preizkusi milijon gesel v 1 sekundi?

  $9.765.625/1.000.000 =$
  $= 9,77$ sekund

Kako izbrati primerno geslo?

- Kaj pa če dodamo še velike črke, presledke, številke in posebne znake ()!?.,:;_-+/*

  $74^5 = 2.219.006.624$ gesel

  2.219 sekund ali 37 min

- Kaj pa, če ostanejo male črke in bo geslo dolgo 15 znakov?

  $25^{15} = 931.322.574.615.478.515.625$ gesel

  29.942.212 let!

Spoofing

- **Spoofing** je zlonamerna akcija, kjer napadalec **prevzame identiteto** žrtve (se pretvarja, da je žrtev) in s tem dobi dovoljenje za interakcijo z viri in podatki.
  - Izvede se z **lažno avtentikacijo**, da smo nekdo, ki ima pravice za opravljanje določenih akcij.

- Vrste spoofingov: login spoofing, IP spoofing, email spoofing, spoofing telefonskih številk, DNS spoofing…
  - Največ škode povzroči DNS spoofing, kjer se napadalec pretvarja, da je DNS strežnik in kliente pošilja na napačne naslove. Npr. ko nekdo želi na facebook.com, ga pošlje na spletno stran, ki zgleda kot Facebook in je namenjena zbiranju uporabniških imen in gesel.

Socialni inženiring

- Danes je tehnologija že tako napredovala, da je tehnološko težko kaj “ušpičiti”. V celotni verigi pošiljanja podatkov, ni več najšibkejši člen tehnologija, temveč človek!

- Termin **socialni inženiring** (angl. *social engineering*) združuje tehnike prevare kako s pomočjo zavajanja človeka pridobimo podatke zaupne narave (gesla, številke kreditne kartice, osebne podatke…).

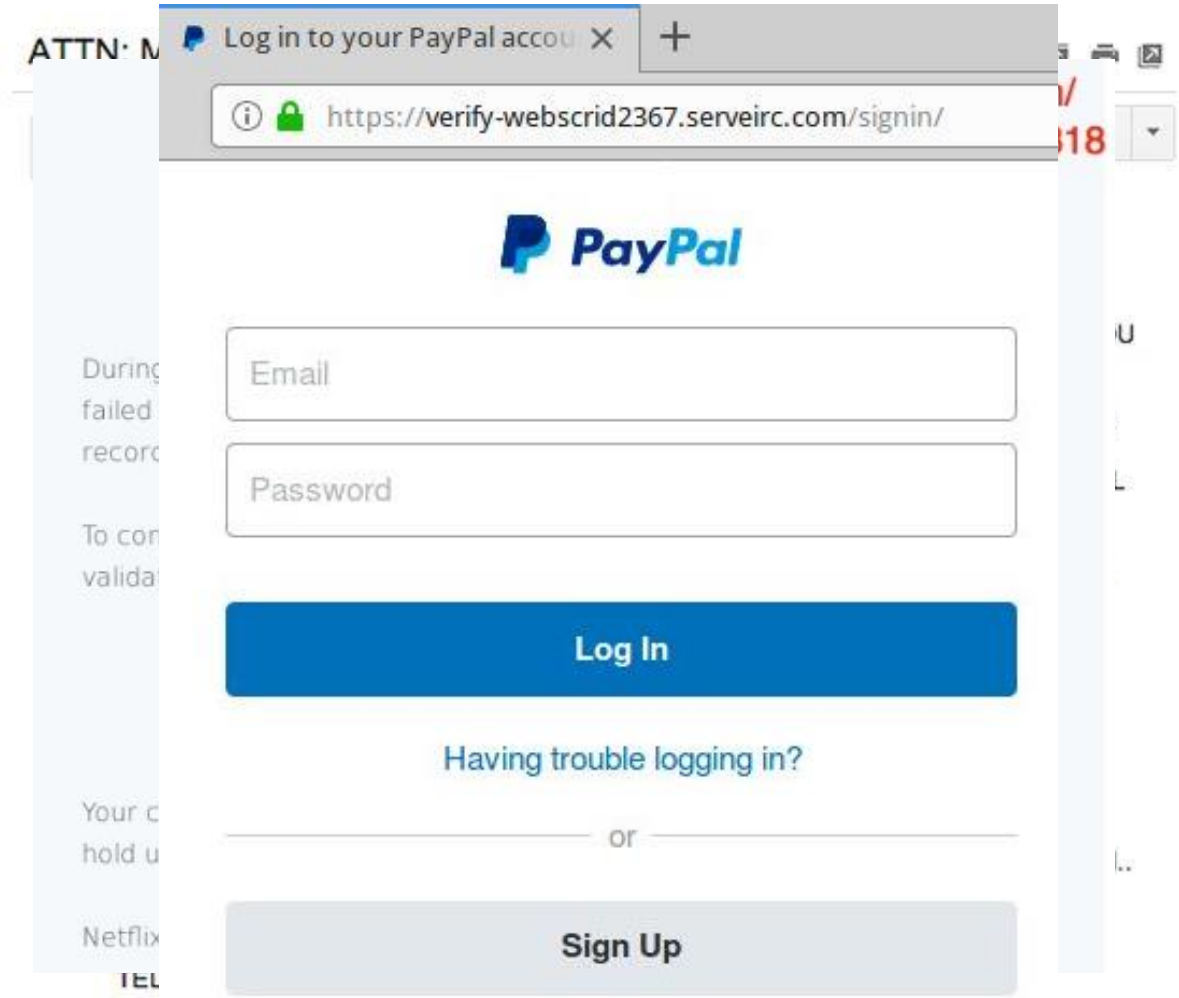
- Moderni napadi se redkokdaj izvedejo le ob izkoriščanju tehnoloških pomanjkljivosti – skorajda vedno je prisoten socialni inženiring.

Primer

Primer kombinacije spoofinga, socialnega inženiringa in malware-a

Vrste socialnega inženiringa

- **Phishing** – je goljufiv poskus pridobitve podatkov preko elektronske komunikacije z žrtvijo.
  - Email, lažne kopije strani…
- **Vishing** – phishing preko telefona.
  - Iz “banke” kličejo glede večjega nakazila, rabijo vašo davčno številko…
- **Smishing** – phishing preko SMS sporočil.
  - Dobite lažni two-factor SMS od napadalca.
- **Lažna predstavitev v živo** – ko se z izdajamo za nekoga drugega v živo.
  - S pomočjo kopij ključev in dovolilnih kartic, ter lažno predstavitvijo zaposlenim se vdira v gospodarska ali državna poslopja.



Kako se zavarovati? 1/2

- **Posodabljajte** svoje naprave.
  - Ne preskakujte pozivov za namestitev posodobitev na telefonih.
  - Če računalniki samodejno ne posodablja programov/aplikacij, jih posodabljajte sami ročno.
  - Če naprave več ne ponujajo posodobitev, je čas za menjavo naprave.

- **Ne nasedajte** emailom, klicem ali SMS/sporočilom.
  - Pazljivo z emaili, klici ali sporočili neznanih pošiljateljev.
  - Pazljivo tudi pri znanih pošiljateljih (se spomnite spoofing!).
  - V emailih ne klikajte linkov (pojdite na storitev in tam najdite obvestilo).
  - Če vas nekdo pokliče s prošnjo po informacijah, vrnite klic tako da pokličete na uradno številko.
  - Če po nesreči nasedete phishingu, je čas za menjavo gesla na storitvi za katero se je nepridiprav izdajal in na vseh storitvah, kjer imate enako geslo.

Kako se zavarovati? 2/2

- Uporabljajte **antivirusne** programe in **požarne zide** (dovolj so vgrajeni).

- Poskrbite, da so **gesla dovolj močna** ali še boljše – rabite **programe za hranjenje gesel**.
  - Gesla naj se ne ponavljajo (vsaj ne na pomembnih storitvah).
  - Gesla na pomembnih storitvah obnovite, ko so ta ukradena (ni potrebe po periodični obnovi gesel).

- Poskrbite za **varnostne kopije** pomembnih datotek (3-2-1 sistem).
  - 3 kopije, od tega ena originalna in dve kopiji.
  - 2 različna medija (npr. en na disku na našem računalniku, drugi na spletu/USB/zunanjem disku).
  - 1 kopija mora biti na drugi lokaciji (splet je ok).

- Pomembne informacije/datoteke **zakodirajte z gesli**.

Vdor v Sony

- Leta 2014 se na internetu pojavijo številni zaupni podatki podjetja Sony Pictures in steče DDoS napad na PlayStation Network, kar je povzročilo nezmožnost igranja.

- Varnostni pregled je pokazal, da je vdor v Sony stekel z uporabo ukradenih gesel preko phishing email-a o Apple ID. Z uporabo teh gesel, so napadalci v Sonyev sistem namestili viruse in ukradli podatke.

Zakaj pa je prišlo do tega napada?

- Leta 2014 so se pri Sony Pictures pripravljali na izid filma *The Interview* – komedijo o voditelju Severne Koreje. Voditelj Severne Koreje ni imel smisla za humor, zato je sprožil napad.