EUROPEAN UNION AGENCY
FOR CYBERSECURITY

NAJPOGOSTEJŠE KIBERNETSKE GROŽNJE

MAREC 2026

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors, please use OSU MS Support at osu-ms-support@enisa.europa.eu

AUTHORS

ENISA, Telekom Slovenije

ACKNOWLEDGEMENTS

This report has been drafted within the framework of Cybersecurity Support Action Programme under the framework contract No F-OCU-24-C10 LOT 25 with service support provider Telekom Slovenije for the beneficiary entities subject to the ZInfV-1 Act.

LEGAL NOTICE

COPYRIGHT NOTICE

[1] https://www.first.org/tlp/

KAZALO VSEBINE

DDOS NAPADI

1.1 KAJ SO DDOS NAPADI IN ZAKAJ SO NEVARNI

DDoS (Distributed Denial of Service) je napad, pri katerem napadalci z internetnim prometom iz številnih naprav (botnet) preobremenijo spletno storitev, spletno stran, API vmesnik ali omrežje, da postane nedosegljivo ali nedelujoče. Povzročijo lahko popoln izpad storitev, motnje delovanja, finančno škodo in škodo ugleda. Napadalci imajo na voljo veliko število tehnik napada in jih pogosto spreminjajo tudi v teku napada.

Tri glavne vrste DDoS napadov:

- **Volumetrični napadi** z zelo veliko količino Internetnega prometa, cilj je zapolniti pasovno širino.
- **Protokolni napadi** z izkoriščanje slabosti protokolov, cilj je onemogočiti delovanje požarnih pregrad.
- **Aplikativni napadi** ciljajo spletne strežnike, na videz legitimni promet ki pa onemogoči spletne strežnike.

Zakaj je DDoS še vedno pogost tip napada:

- Razširjenost IoT naprav, ki so del botnetov.
- ”DDoS for hire” storitve, dostopne vsakomur za nizko ceno.
- Politično motivirani napadi, hacktivizem.

Posledice za organizacije.

- Izpad Internetnih storitev organizacije.
- Nedostopnost oblačnih storitev in medomrežnih VPN povezav.
- Nedostopnost spletnih strani, API-jev, e-storitve.
- Neposredna in posredna finančna izguba.
- izguba ugleda in zaupanja.

1.2 KAKO SE ZAŠČITIMO PRED DDOS NAPADI

Najbolj učinkovita zaščita vključuje kombinacijo zaščite pri Internetnem ponudniku in zaščite v lastnem omrežju, opcijsko tudi z zaščito v oblaku globalnih ponudnikov (Cloudflare, Akamai, Azure Front Door, AWS Shield ipd.).

1. Zaščita pri ponudniku Internetnega dostopa, ki vključuje samodejno zaznavo DDoS napada in avtomatsko aktiviranje čiščenja DDoS prometa. Ta zaščita je učinkovito za volumetrične in protokolne napade, delno je učinkovita za aplikacijske napade.
2. Zaščita v lastnem omrežju z:
    a. Požarno pregrado ki ščiti pred protokolnimi in aplikativnimi napadi (vključno z SSL dekripcijo)
    b. WAF / L7 DDoS filtering, ki ščiti pred aplikativnimi napadi.
    c. Ustrezno konfiguracijo spletnih strežnikov.
3. Zaščita v oblaku (Cloudflare, Akamai, Azure Front Door, AWS Shield ipd.) za vse vrste napadov.

Priporočeni ukrepi pred DDoS napadom:

- Izdelava načrta odzivanja v primeru DDoS napada.
- Implementacija zaščit pred DDoS napadi.
- Testiranje učinkovitosti delovanja DDoS zaščite na različne tipe napadov.
- Nadzor DDoS dogodkov v SOC

Priporočeni ukrepi ob DDoS napadu:

- Takojšnja, po možnosti avtomatska zaznava in aktivacija DDoS zaščite pri Internetnem ponudniku,
- Spremljanje učinkovitosti delovanja zaščite in po potrebi prilagajanje nastavitev, npr geografsko omejevanje.
- Takojšnje obveščanje SI CERT / SIGOV CERT.

SKENIRANJE IN KIBERNETSKO IZVIDOVANJE

2.3 KAJ JE SKENIRANJE IN KIBERNETSKO IZVIDOVANJE

Kibernetsko izvidovanje (angl. Reconnaissance) je faza kibernetskega napada, v kateri napadalec sistematično in sistematično zbira informacije o tarči z namenom razumevanja njenega okolja, identifikacije ranljivosti ter izbire najučinkovitejšega vektorja napada. V modelu Cyber Kill Chain predstavlja prvo fazo napada, vendar se izvidovanje pogosto izvaja tudi kasneje, po začetni kompromitaciji, v obliki nadaljnje enumeracije in notranjega odkrivanja sistemov.

Dve vrsti izvidovanja:

- Pasivno izvidovanje poteka brez neposrednega stika s sistemi tarče in vključuje zbiranje podatkov iz javno dostopnih virov, kot so spletne strani, družbena omrežja, javni registri, DNS in WHOIS zapisi ter podatki iz preteklih kompromitacij.
- Aktivno izvidovanje vključuje neposredno interakcijo s tarčo na primer skeniranje omrežij in vrat, identifikacijo storitev in verzij ter osnovno testiranje ranljivosti, pri čemer takšne aktivnosti pogosto puščajo sledi v dnevnikih sistemov.

Kakšne podatke zbirajo napadalci:

- Napadalci zbirajo širok nabor tehničnih podatkov o IT infrastrukturi (javni IP naslovi, domene, DNS zapisi, izpostavljene storitve), podatke o uporabljenih operacijskih sistemih, aplikacijah in varnostnih rešitvah,
- Organizacijske podatke (struktura, ključne vloge, partnerji), podatke o zaposlenih ter podatke iz javno dostopnih dokumentov in metapodatkov. Poseben pomen imajo tudi vzorci vedenja (delovni časi, odzivni časi) ter informacije o znanih ranljivostih in napačnih konfiguracijah.

Za izvajanje izvidovanja se uporabljajo številna orodja in tehnike, od OSINT platform (npr. Shodan, Maltego, Censys) in orodij za analizo DNS zapisov (Amass, DNSDumpster) do aktivnih skenerjev, kot so Nmap, Masscan in Nikto. MITRE ATT&CK okvir ločuje dve fazi izvidovanja: izvidovanje pred kompromitacijo (Reconnaissance) in izvidovanje po začetnem dostopu (Discovery), pri čemer je v fazi Discovery registriranih bistveno več tehnik, ki se izvajajo znotraj že kompromitiranega okolja in pogosto z uporabo legitimnih administrativnih orodij, kar je zelo težko zaznati.

2.4 KAKO SE ZAŠČITIMO PRED SKENIRANJEM IN IZVIDOVANJEM

Zaščita pred izvidovanjem temelji na:

- Ozaveščenosti uporabnikov, da ne razkrivajo nepotrebnih službenih informacij.
- Zmanjševanju t.i. napadne površine ki vključuje zapiranje nepotrebnih storitev in vrat (TCP, UDP portov) iz Internet omrežja, odstranjevanje zastarelih domen in DNS zapisov, omejevanje razkrivanja tehničnih informacij.
- Zgodnjem zaznavanju sumljivih aktivnosti preko log zapisov, XDR orodij , vabe (deception).
- Pridobivanju CTI (Cyber Threat Intelligence) informacij, s katero organizacija spremlja ukradene poverilnice, dokumente, domene, zlonamerne aktivnosti usmerjenih proti njim.
- Upravljanju identitet oziroma prijavnih računov (uporaba načela najmanjših pravic, MFA, PAM), omrežni segmentaciji ter nadzoru nad poizvedbami in dostopi znotraj okolja.

VDORI V SISTEME

3.3 KAJ JE KIBERNETSKI VDOR

Kibernetski vdor pomeni nepooblaščen in uspešen dostop do informacijskega sistema ali omrežja, pri katerem napadalec pridobi dejansko prisotnost in možnost delovanja v sistemu. To se lahko zgodi z zlorabo uporabniškega računa, z izvajanjem zlonamerne kode ali z neposrednim dostopom do podatkov in funkcionalnosti sistema. Za pravno opredelitev vdora ni potrebno, da pride do dejanske škode ali kraje podatkov, zadostuje že možnost vpliva na sistem ali podatke.

Kibernetski vdor predstavlja resen varnostni incident, saj lahko ogrozi zaupnost, celovitost ali razpoložljivost informacij, zahteva takojšnje ukrepanje in pogosto zahteva zakonsko obveznost poročanja po ZInfV-1. **Škodo praviloma ne povzroči sam vdor, temveč dejanja po vdoru**, kot so kraja podatkov, šifriranje ali brisanje sistemov, onemogočanje storitev, izsiljevanje.

V praksi je veliko začetnih vdorov nezaznanih. Organizacije pogosto zaznajo vdor šele v kasnejši fazi napada, ko je škoda že povzročena in vidna.

3.4 KAKO SE ZAŠČITIMO PRED KIBERNETSKIM VDOROM

Zaščita pred kibernetskimi vdori temelji na kombinaciji preventive, zaznave in odzivanja na zaznan vdor. Ker imajo napadalci prednost presenečenja, časa in izbire napada, popolne zaščite ni. **Cilj organizacije je zgodnje zaznavanje in hiter učinkovit odziv.**

Najbolj učinkovit (in najcenejši) način zaščite pred vdori je njihovo preprečevanje s preventivnimi ukrepi, kot so:

- Varnostno utrjevanje sistemov.
- Odpravljanje ranljivosti.
- Močna zaščita prijavnih računov in uporaba večfaktorske avtentikacije (MFA) .
- Segmentacija omrežij in omjevanje nepotrebnih komunikacij.
- Zaščita elektronske pošte.
- Zaščita končnih točk (XDR/EDR).
- Izobraževanje uporabnikov.
- Kontrola dobaviteljev.

Zaznavanje poskusov vdorov se v praksi izvaja na več ravneh:

- Zaznava na osnovi podpisov (signature), ki temelji na znanih indikatorjih napadov.
- Z zbiranjem in analizo log zapisov iz vseh sistemov, predvsem omrežja, strežnikov, varnostnih sistemov v SIEM, njihovo analizo in korelacijo kjer se več posameznih dogodkov poveže v celoto ki lahko kaže na napad.
- Vedenjska ali statistična zaznava, ki prepoznava odstopanja od običajnega delovanja (UEBA, EDR) kot so neobičajne prijave, neobičajne spremembe pravic uporabnikov itd.
- Uporaba CTI virov informacij

Ko je vdor zaznan, je ključno strukturirano odzivanje na incidente. Uveljavljeni kibernetsko-varnostni ogrodji (framework), kot sta NIST CSF 2.0 in SANS Incident Management Framework, poudarjajo sledeče faze odzivanja:

- Načrtovanje odzivanja na incidente.
- Hitro identifikacijo incidenta.
- Zajezitev vdora.
- Odstranitev grožnje.
- Obnovo sistemov.
- Učenje iz incidenta.

Namen procesa odzivanja na incidente ni le odprava posameznega incidenta, temveč stalno izboljševanje varnostne zrelosti organizacije.

SOCIALNI INŽENIRING

4.3 KAJ JE SOCIALNI INŽENIRING

Socialni inženiring je nabor manipulacij, s katerimi napadalci izkoriščajo človeško psihologijo, da žrtve prepričajo v razkritje občutljivih informacij, izvedbo finančnih transakcij in izvedbo drugih škodljivih dejanj. Napadalci uporabljajo pristop, ki temelji na zaupanju, nujnosti, psihološkem pritisku in lažnem predstavljanju.
Obstaja več oblik socialnega inženiringa, najpogostejša so: **Phishing (e-pošta), smishing (SMS), vishing (glasovni klic), quishing (QR kode)**.

Tipičen phishing napad poteka v več stopnjah:

- Iskanje priložnostne žrte ali ciljanje na določeno osebo (sphear phishing)
- Zbiranje informacij o žrtvi z izvidovanjem, razumevanje organizacije, izbira metode napada.
- Vzpostavitev kontakta, ustvarjanje prepričljive zgodbe, vzpostavitev zaupanja.
- Pridobitev željenih informacij, prijavnih podatkov in nadaljevanje vdora, prevaranje uporabnika da izvede plačilo itd.

Direktorska prevara je oblika prevare preko elektronske pošte ali klica, pri katerem napadalci:

- V sporočilu, ki je poslano iz lažne domene ali kompromitiranega email računa, posnemajo direktorja.
- V sporočilu ciljajo na osebe v finančnem oddelku ki so odgovorni za plačila.
- Zahtevajo npr. nujno plačilo zaradi nekega razloga ali sporočajo spremembo TRR dobavitelja.
- Uporabljajo kratka, prepričljiva sporočila brez zlonamernih priponk, včasih kombinirana z lažnimi telefonskimi klici (vishing).

4.4 KAKO SE ZAŠČITIMO PRED SOCIALNIM INŽENIRINGOM

Učinkovita zaščita temelji na kombinaciji tehničnih ukrepov, organizacijskih pravil in ozaveščenosti zaposlenih.

Tehnični zaščitni ukrepi:

- Obvezna dvofaktorska avtentikacija (2FA) za e-pošto in kritične aplikacije.
- Spremljanje in opozarjanje na sumljive prijave pri dostopu do e-poštnih računov.
- Filtri proti lažnim domenam, preverjanje SPF/DKIM/DMARC.
- Orodja za zaznavanje phishing e-pošte in preverjanje URL-jev, vključno z zaščito pred QR-kodami.

Organizacijski postopki:

- Dosledni postopki za potrjevanje finančnih transakcij, preverjanje sprememb zlasti sprememb TRR.
- Nikoli ne izvesti plačila samo na podlagi e-pošte ampak preveriti preko telefonskega klica.
- Ob sumu na prevaro to takoj prijaviti interno vodstvu in IT ter vaši banki pa tudi policiji.

Ozaveščenost uporabnikov:

- Redna usposabljanja o socialnem inženiringu in prepoznavanju pasti
- Izvajanje phishing testiranja.
- Krepitev pazljivosti in kritične presoje uporabnikov:
    - preveriti pošiljatelja,
    - preveriti URL,
    - ne odpiraj prilog iz nenavadnih sporočil,
    - preveri slovnične napake, nenavadne zahteve, nujnost.
- Prepoznavanje znakov direktorske prevare:
    - nenavadne zahteve za izplačila,
    - nenadna sprememba TRR,
    - zahteva po zaupnosti,
    - nujnost.

RANSOMWARE

5.3 KAJ JE RANSOMWARE

Izsiljevalska programska oprema je zlonamerna koda, namenjena šifriranju podatkov, kraji informacij ter izsiljevanju organizacij za plačilo odkupnine. Najpogosteje se izvaja dvofazni napad, najpej se izvede kraja ali eksfiltracija podatkov in nato šifriranje podatkov, t. i. »double extortion«.

Napad se začne z izvidovanjem, ter pogosto nadaljuje s socialnim inženiringom. Sledi faza **vdora in premikanja v notranjem omrežju** (lateralno gibanje), pri čemer napadalci iščejo ključne sisteme ter pridobivajo nadzor nad napravami in strežniki.
Za napredovanje v omrežju izrabljajo ranljivosti in napačne konfiguracije, ukradene poverilnice uporabnikov in dvig njihovih pravic z določenimi tehnikami ali ukradene poverilnice privilegiranih računov.

Končna akcija je namestitev ransomware kode in šifriranje datotek. Ko koda zašifrira podatke, napadalci zahtevajo plačilo odkupnine, pogosto prek anonimiziranih kanalov (Tor, posebni portali). Napadalci uporabljajo napredne šifrirne algoritme in šifrirajo različne tipe datotek na različnih sistemih.

Posledice za organizacije so lahko hude:

- Motnje in izpad delovanja IT sistemov in posledično procesov v organizaciji.
- Izgubo in uničenje podatkov.
- Finančne izgube (izpad poslovanja, okrevanje, odkupnina, sankcije).
- Izguba ugleda.
- Zakonske/regulatorne posledice, zlasti ob kompromitaciji osebnih podatkov.

5.4 KAKO SE ZAŠČITIMO PRED RANSOMWAROM

Zaščita pred ransomware napadi zahteva kombinacijo specifičnih tehničnih in procesnih ukrepov.

Tehnični zaščitni ukrepi:

- Varnostno utrjevanje sistemov, odpravljanje ranljivosti in redno nameščanje varnostnih popravkov.
- Uporaba EDR rešitev za zaščito računalnikov in strežnikov.
- Omrežna segmentacija in načelo najmanjših pravic s čemer otežujemo premikanje po omrežju.
- Redno varnostno kopiranje podatkov in preverjanje obnovitvenih postopkov.
- Uporaba obveščevalnih informacij (CTI), npr. spremljanje razkritih poverilnic.

Načrt za odzivanje na ransomware napad:

- Potrebno je imeti načrt odzivanja za scenarij izsiljevalskega napada (zaznava, zaustavitev, odstranitev, povrnitev).
- Definirati je potrebno protokole komuniciranja (interno in eksterno) tudi za primer da IT storitve ne delujejo.
- Ob napadu izvesti digitalno forenziko za določitev vzroka in poti napada ter odstranitev vseh artefaktov.

Krepitev odpornosti organizacije:

- Redno izobraževanje zaposlenih o prepoznavanju groženj ki lahko vodijo do ransomware napada, prijava sumljivih opažanj.

ZLONAMERNA PROGRAMSKA OPREMA

6.3 KAJ JE ZLONAMERNA PROGRAMSKA OPREMA

Zlonamerna programska oprema (ang. malware) je programska koda, namenoma ustvarjena za škodovanje informacijskim sistemom, krajo podatkov, nepooblaščen dostop, povzročanje motenj v delovanju in finančne škode. Večina sodobnih kibernetskih incidentov vključuje eno ali več oblik zlonamerne kode.

Kako zlonamerna koda pride v IT sistem
Najpogostejši vstopni mehanizmi so:

- Phishing in socialni inženiring (zlonamerna e-pošta, priponke, povezave).
- Zlonamerne ali kompromitirane spletne strani, prenos okuženih datotek in aplikacij.
- Izkoriščanje ranljivosti, tudi t.i. 0-day.
- Slabo zaščitene naprave, VPN dostopi, požarne pregrade in strežniki.

Zlonamerna koda je uspešna metoda za napadalce zaradi

- Previsokih pravic običajnih uporabnikov, admin pravice.
- Zakasnjenega nameščanja varnostnih popravkov.
- Kompleksnih in slabo segmentiranih omežij.
- Nezadostnega zaznavanje in blokiranje zlonamernih programov, uporaba zgolj klasičnega antivirusa, brez napredneha EDR/XDR.

Najpogostejše vrste zlonamerne programske opreme

- **spyware in keylogger**, kraja poverilnic in podatkov,
- **adware**, sledenje in zloraba podatkov
- **trojanci in črvi,** oddaljen nadzor, širjenje po omrežju,
- **rootkit**, prikrivanje in vztrajnost,
- **botnet,** DDoS,
- **wiper** , uničenje podatkov,
- **ransomware**, šifriranje in izsiljevanje.

6.4 KAKO SE ZAŠČITIMO PRED ZLONAMERNO PROGRAMSKO OPREMO

Učinkovita zaščita temelji na kombinaciji tehnoloških in procesno-organizacijskih ukrepov.

Tehnični ukrepi

- Uvedba EDR/XDR/NDR za zaznavanje naprednih napadov z zlonamerno programsko opremo na končnih točkah in v omrežju.
- Redno posodabljanje kritičnih sistemov (VPN, firewall, e-pošta).
- Segmentacija omrežja in čim večja izolacija IoT/OT naprav.
- Minimalni privilegiji uporabniških računov, onemogočanje nepotrebnih skript (PowerShell, makroji).

Organizacijski ukrepi

- Jasne politike kaj je dovoljeno nameščati in kaj ne.
- Izobraževanje uporabnikov o kibernetskih grožnjah s poudarkom na zlonamerni programski opremi.
- Izdelan in redno preverjan načrt odziva na napad z zlonamerno programsko opremo.
- Zagotovljeni viri, kadri, za utrjevanje sistemov, zaznavanje napadov in odzivanje nanje.

XX-00-00-000-XX-X

ABOUT ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN 000-00-0000-000-0
doi: 0000.0000/000000