KIBERNETSKI CUNAMI

Ko val napadov postane realnost

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

V živo – ali smo varni

Milan Gabor
direktor, Viris d.o.o.

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

dr. Uroš Svete

direktor,
Urad Republike Slovenije
za Informacijsko Varnost

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

Igor Zorko

predsednik,
Združenje za informatiko
in telekomunikacije

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

Značilnosti kibernetskih incidentov v 2025, zaznava, odzivanje in kaj lahko izboljšamo

Gorazd Božič, vodja nacionalnega odzivnega centra za kibernetsko varnost SI-CERT

si·cert

- nacionalna kontaktna točka
- javni zavod ARNES
- preiskovanje, svetovanje, koordinacija
- ozaveščanje (Varni na internetu)
- pričetek delovanja: 1995
- Zakon o informacijski varnosti, 28. člen
- član FI-ISAC, FIRST, EU CSIRT Network, Global Cyber Alliance

EU OKVIR

- direktiva NIS2 (Network and Information Security)
- direktiva RCE (Resilience of Critical Entities)
- DORA (Digital Operational Resilience Act)
- CRA (Cyber Resilience Act)
- CSoA (Cyber Solidarity Act)
- DSA (Digital Services Act)
- DMA (Digital Markets Act)

VLOGA CSIRT SKUPIN

- pomoč pri preiskovanju incidenta
- laboratorij za preiskovanje zlonamerne kode
- situacijsko zavedanje in pregled nad ranljivostmi
- vpetost v mednarodno okolje
  - EU CSIRTs Network, FIRST, Trusted Introducer, FI-ISAC, Global Cyber Alliance, Microsoft CTIP, Shadowserver Foundation, Cyber Balkans, WB3C
- deljenje informacij v skupnostih
- “first-responder” profil

KDAJ PRIJAVITI INCIDENT?

Primer incidenta	Pričakovane dejavnosti centra SI-CERT
Okužba računalnika (izsiljevalski virusi, bančni trojanski konji, ciljani napadi, agenti za pošiljanje neželene elektronske pošte)	Pomoč pri odstranjevanju okužbe in njenih posledic, analiza vzorca in korelacija z do zdaj znanimi grožnjami. Svetovanje o ukrepih za sanacijo stanja.
Opažen vdor v strežnik (razobličenje, zloraba podatkovnih zbirk, namestitev prikritih orodij storilca)	Iskanje izrabljene varnostne luknje ali ranljivosti, pomoč pri opredeljevanju posledic in vira vdora, analiza sledi na zlorabljenih sistemih, nasveti za odstranjevanje škode in zaščito.
Phishing elektronska sporočila (potvorjena elektronska sporočila, ki vas napeljujejo, da podatke vpišete na lažni spletni strani)	Odstranjevanje in označevanje lažnih spletnih mest. Prepoznava širših in ciljanih napadov, obveščanje medijev in javnosti, sodelovanje z bančnim sektorjem in ponudniki storitev.
Napad onemogočanja (poplava s prometom, napad na storitev ali spletno aplikacijo z namenom njenega onemogočanja)	Ocena o uporabljenih sredstvih za napad, opredelitev mogočih zaščitnih ukrepov, poskus onemogočanja botneta ter obveščanje ponudnikov o zlorabljeni infrastrukturi in njeni zaščiti.
Ranljive ali izpostavljene storitve (vmesniki za upravljanje spletnih storitev, upravljanje naprav ali industrijskih procesov, spletnih kamer ipd., ranljiva omrežna infrastruktura, ki omogoča napade onemogočanja)	Obveščanje skrbnikov, svetovanje pri nastavitvah in omejevanju dostopa, preiskovanje zlorabe storitve.
Izguba gesel ali kraja omrežne identitete (zloraba prek phishing napada ali okužbe računalnika)	Svetovanje pri ponovnem prevzemu računov, dodatnih zaščitnih ukrepih in možni identifikaciji storilca.

NOVICE / 15. 3. 2024

SI-CERT TZ015 / Analiza bančnega trojanca Anatsa za Android mobilne naprave

Povzetek

Na SI-CERT smo v analizo prejeli dve aplikaciji za mobilne naprave sistema Android, za kateri je obstajal sum, da sta bili vzrok finančnega oškodovanja večih slovenskih državljanov. V analizi smo ugotovili, da obe vzorca sodita v skupino škodljive programske opreme iz družine Anatsa (tudi TeaBot, Toddler in ReBot). Ugotovili smo, da so bili prenašalci škodljivih aplikacij na voljo za prenos s tržnice Google Play pod pretvezo bralnikov PDF dokumentov in čistilcev telefona. Aplikacije so bile na voljo za prenos le v ciljanih državah, med katerimi je tudi Slovenija. Po poročanju Bleeping Computer je škodljive aplikacije preneselo približno 150 tisoč uporabnikov.

Bančni trojanec Anatsa

Glavni cilj škodljive aplikacije iz družine Anatsa je pridobitev uporabniških podatkov, med katere sodijo tudi podatki za prijavo v bančne aplikacije in zagotavljanje oddaljenega dostopa napadalcu. Aplikacija napadalcu posreduje vse potrebne podatke za oddaljen dostop do žrtvine naprave, prijavo v spletno banko in izvedbo finančnih transakcij. Po podatkih, ki smo jih prejeli, napadalec finančno oškodovanje izvede po več dneh od inicialne okužbe, ukraden denar pa nakaže na bančni račun v tujini, od koder v nadaljevanju potuje na menjalnice s kriptovalutami.

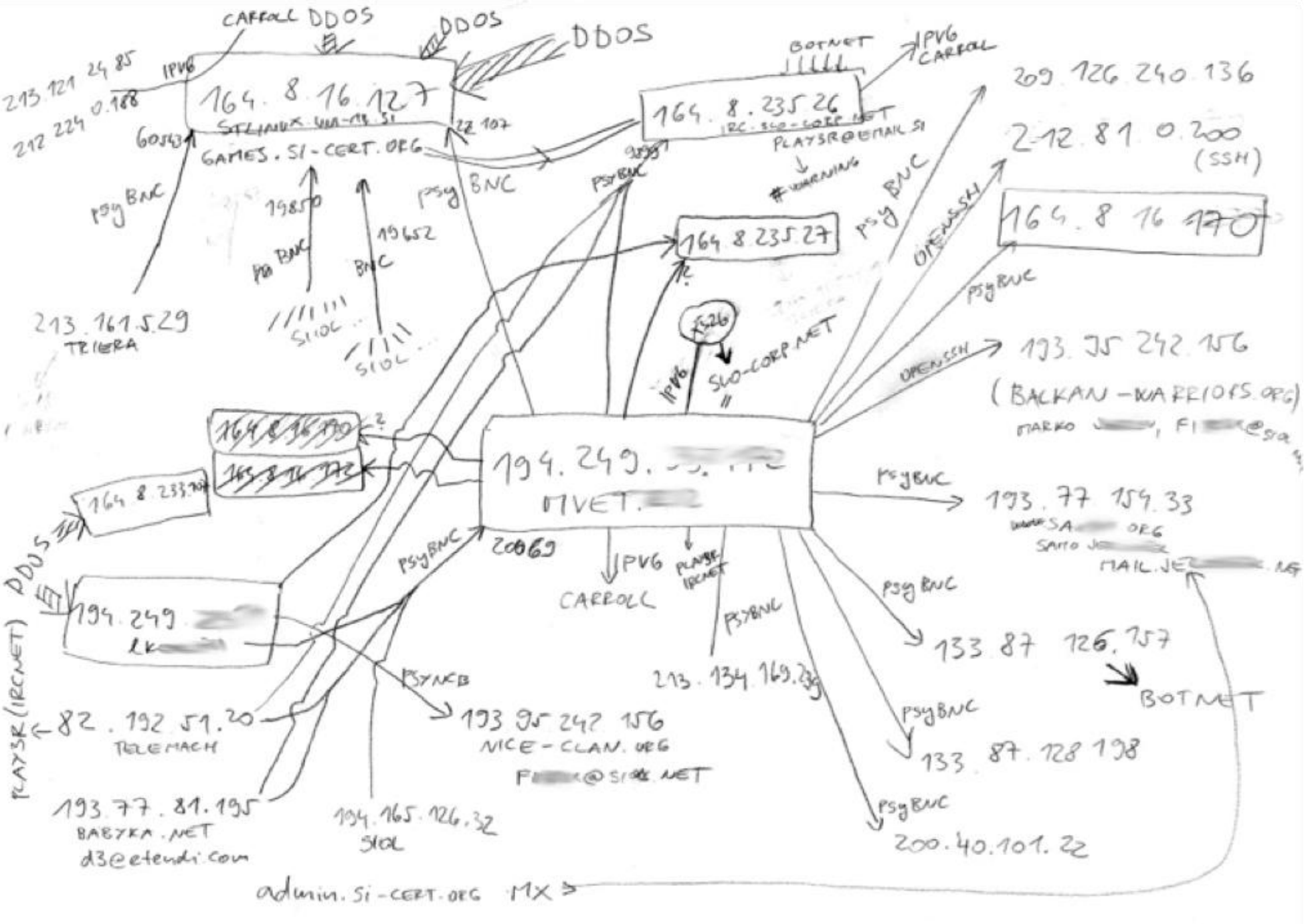
Tehnični zapis se navezuje na varnostno obvestilo o okužbah mobilnih naprav: https://www.cert.si/si-cert-2024-03/.

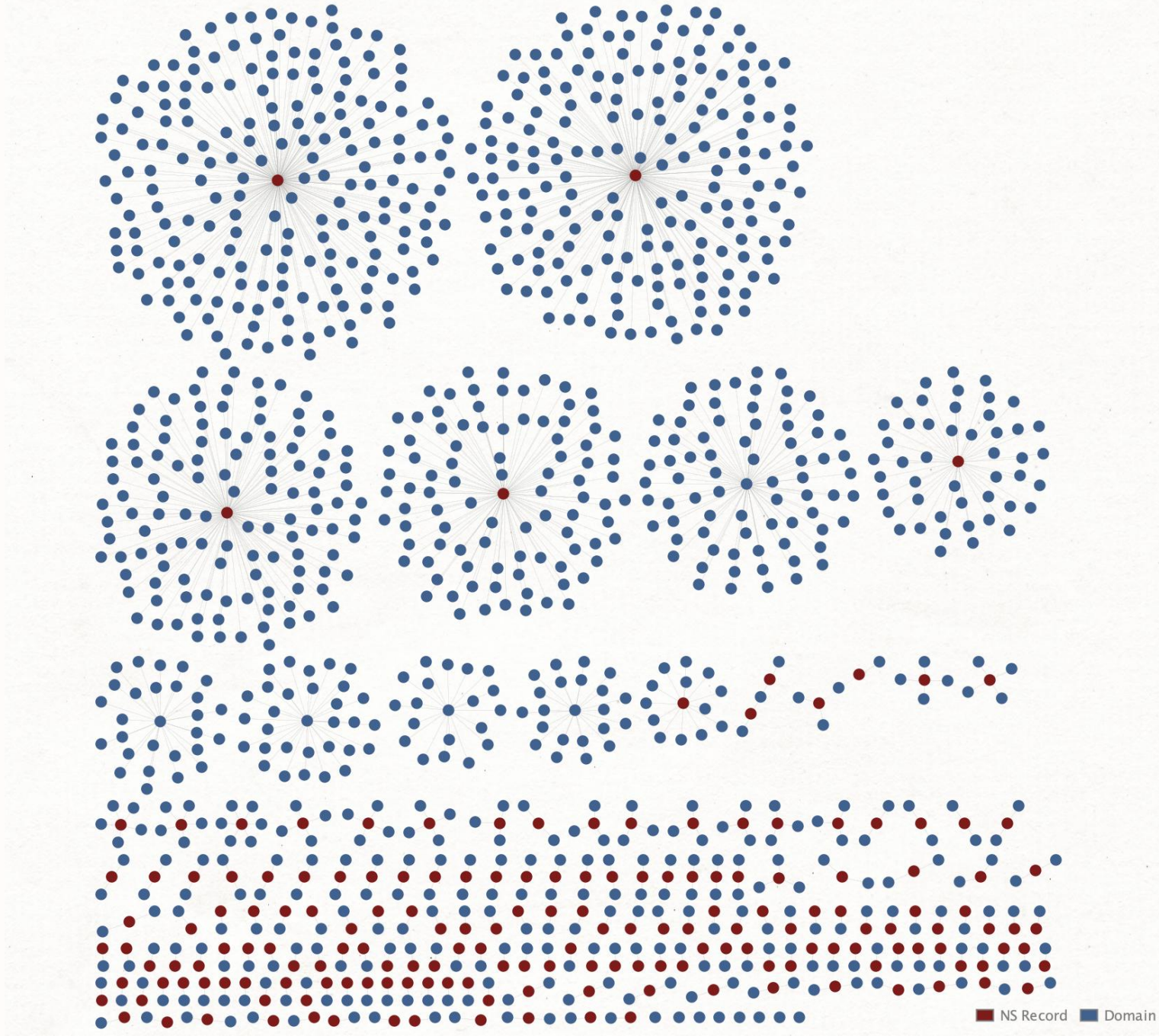
Glavna odšifrirna logika razreda se nahaja v metodi mw_decryptionLogic, ki prebere šifriran tovor, odšifrira njegovo vsebino in dobljen rezultat zapiše v novo datoteko. Pri postopku odšifriranja uporablja množico operacij ARX algoritma, ki ga sestavljajo operacije seštevanja in rotacije elementov tabel ter šifriranja s funkcijo XOR.

```
private static void mw_decryptionLogic(InputStream inputStream, OutputStream outputStream) throws Exception {
    // razširjanje šifrirnega ključa
    int[] mw_key = mw_keyExpansionARX();

    byte[] buffer = new byte[0x2000];
    int bytesRead;

    while ((bytesRead = inputStream.read(buffer)) > 0) {
        // Posodabljanje ključa na 8 bajtov
        if (bytesRead % 8 == 0) {
            mw_keyUpdateARX(mw_key);
        }

        // XOR šifriranje
        for (int i = 0; i < bytesRead; ++i) {
            buffer[i] = (byte) (buffer[i] ^ (mw_key[i % 8 / 4] >> (i % 4) * 8));
        }

        // Zapis odšifriranega tovora
        outputStream.write(buffer, 0, bytesRead);
    }
}
```

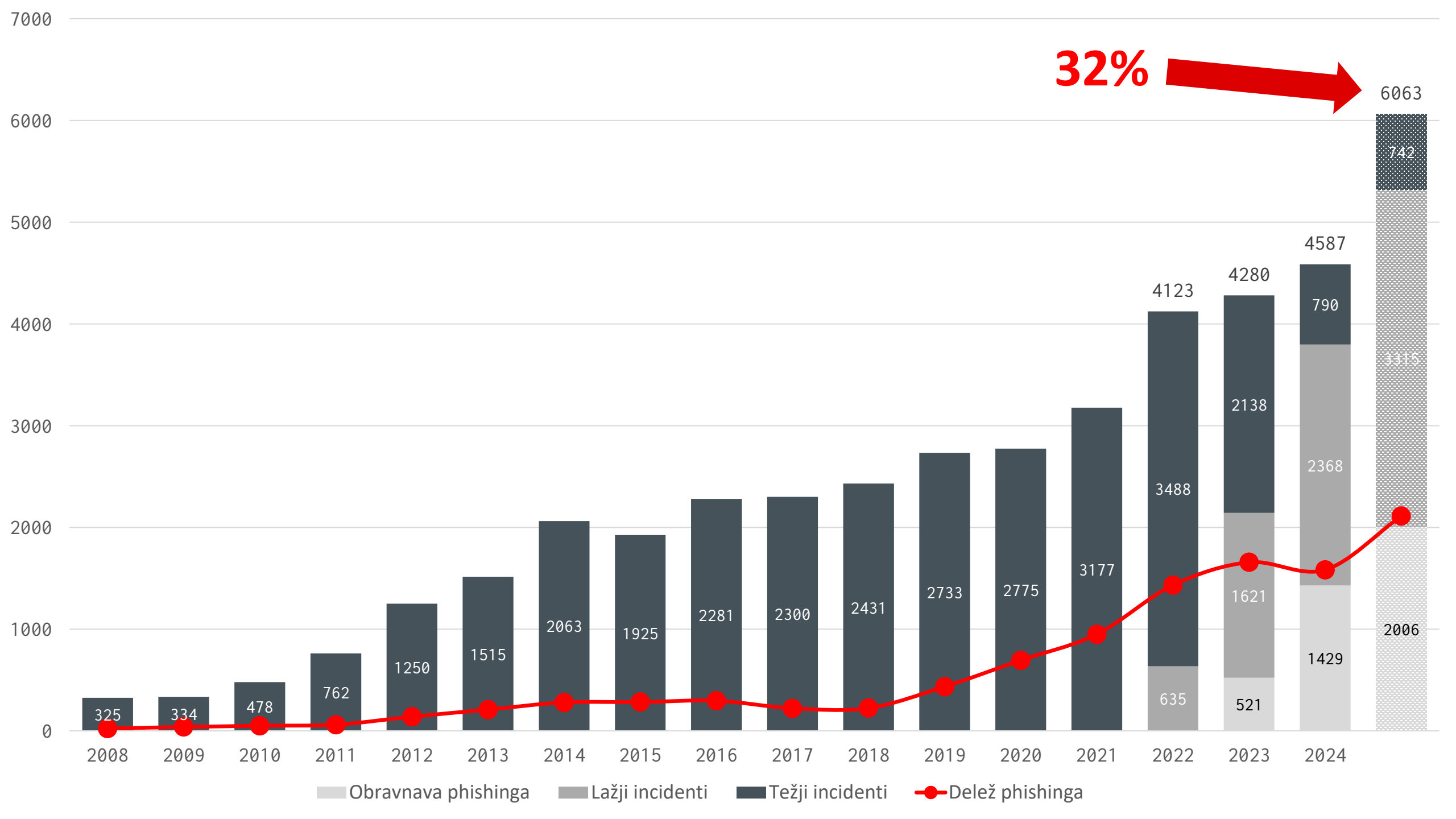
Aplikacija med svojim izvajanjem razširi in dinamično spreminja šifrirni ključ, za kar skrbi metoda mw_keyExpansionARX(). Njena koda razširi originalen šifrirni ključ na dolžino 27 (27 * 4B), kar predstavlja 108 bajtov.

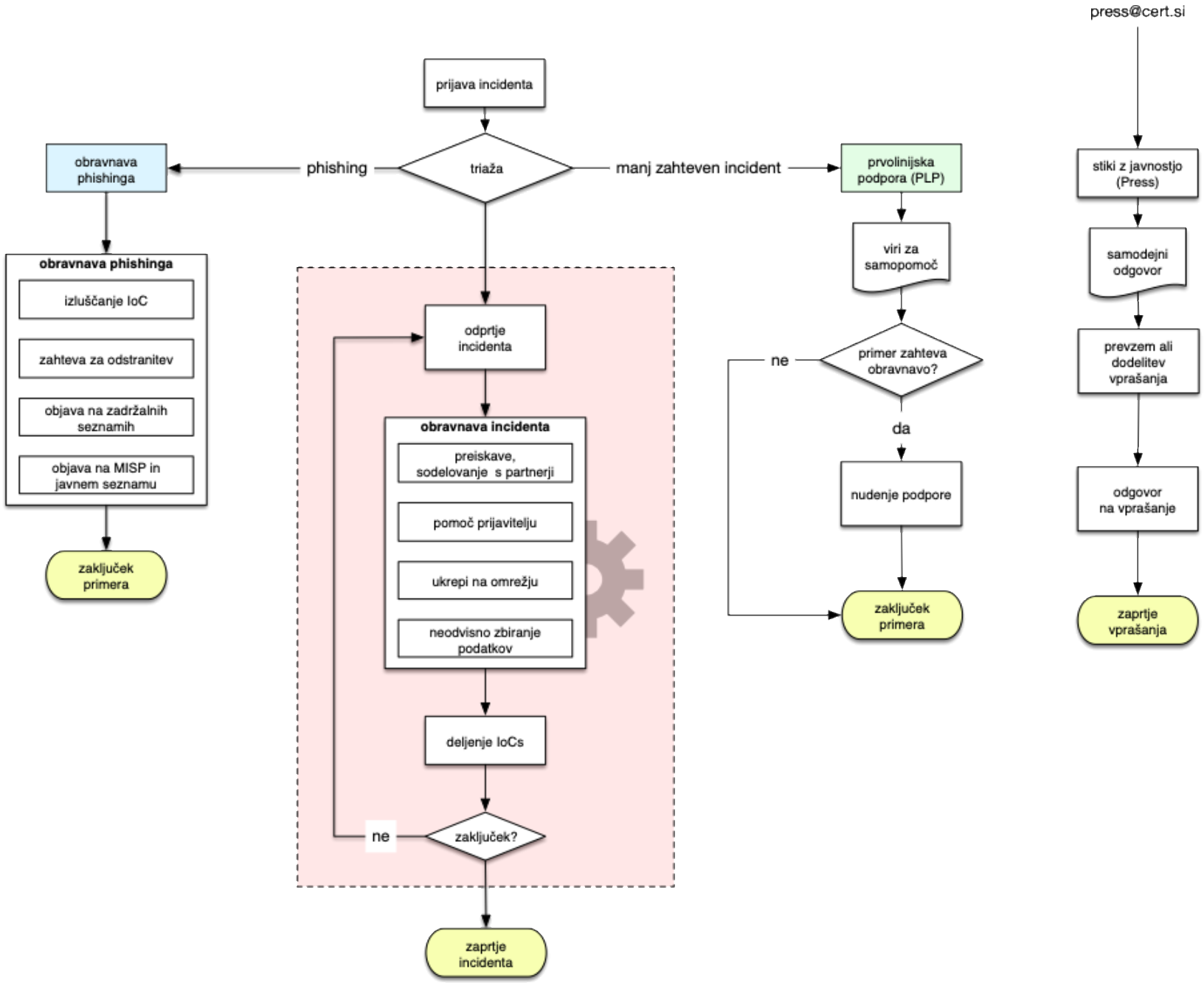
SITUACIJSKO ZAVEDANJE




NS Record
Domain


phishing
facebook
vdor
kriptovalute
lažno izsiljevanje
lažna spletna trgovina
sporočilo policije
izsiljevanje
infostealer
direktorska prevara
investicijska prevara
domnevna okužba računalnika
prevara
lažni kredit
keylogger
spam
malware
email
kripto
priponka
investiranje
subscription trap
whatsapp
booking
sms
scam
subscription renewal
okužba
policija
ddos
instagram
delo od doma
verifikacijski sms
false positive
meta
google
bec
prodaja
kreditna kartica
bitcoin
ce24
419
agent tesla
blockchain
izplačilo valute
malspam
powershell
sextortion
klic
kraja identitete
spletno nakupovanje
obnova naročnine
microsoft
marketplace
oškodovanje
nlb
telegram
downloader
paypal
gls
pošta
romance scam
sms klub
guloader
povrnitev stroškov
preverba
telefonski klic
cc phishing
ljubezenska prevara
brez skrbi
.net
kitajska
virus
smtp
tiktok
ranljivost
gmail
ceo fraud
copyright
dropbox
bolha
mali oglasi
oglasi
smishing
spletna trgovina
lažna trgovina
iban
dpd
ransomware
remcos
čudežni pripomočki
lažni klic tehnične pomoči
osebna izkaznica
spletni nakup
lažni profil
trojan
formbook
skrita naročnina
anydesh
extortion
rat
vprašanje
kredit
fake extortion
mcafee
obvestilo
android
crypto
testiranje
fb marketplace
vdor v račun
facebook marketplace
intimni posnetki
fake sextortion
elektronska pošta
spletna stran
nakazilo


7000
6000
5000
4000
3000
2000
1000
0
32%
6063
4587
4280
4123
325
334
478
762
1250
1515
2063
1925
2281
2300
2431
2733
2775
3177
3488
635
2138
521
790
2368
1621
1429
742
3315
2006
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
Obravnava phishinga
Lažji incidenti
Težji incidenti
Delež phishinga


prijava incidenta
triaža
phishing
obravnava phishinga
manj zahteven incident
prvolinijska podpora (PLP)
press@cert.si
stiki z javnostjo (Press)
obravnava phishinga
izluščanje IoC
zahteva za odstranitev
objava na zadržalnih seznamih
objava na MISP in javnem seznamu
zaključek primera
odprtje incidenta
obravnava incidenta
preiskave, sodelovanje s partnerji
pomoč prijavitelju
ukrepi na omrežju
neodvisno zbiranje podatkov
deljenje IoCs
ne
zaključek?
zaprtje incidenta
viri za samopomoč
ne
primer zahteva obravnavo?
da
nudenje podpore
zaključek primera
samodejni odgovor
prevzem ali dodelitev vprašanja
odgovor na vprašanje
zaprtje vprašanja

OZNAKA “POMEMBNO”

zelo razširjena zloraba ali ranljivost
velik vpliv na žrtev
strateško pomemben akter
velika javna izpostavljenost

OZNAKA “KRITIČNO”

dejanske posledice se vrstijo,
potreba po takojšnji zamejitvi
ogroženost življenja

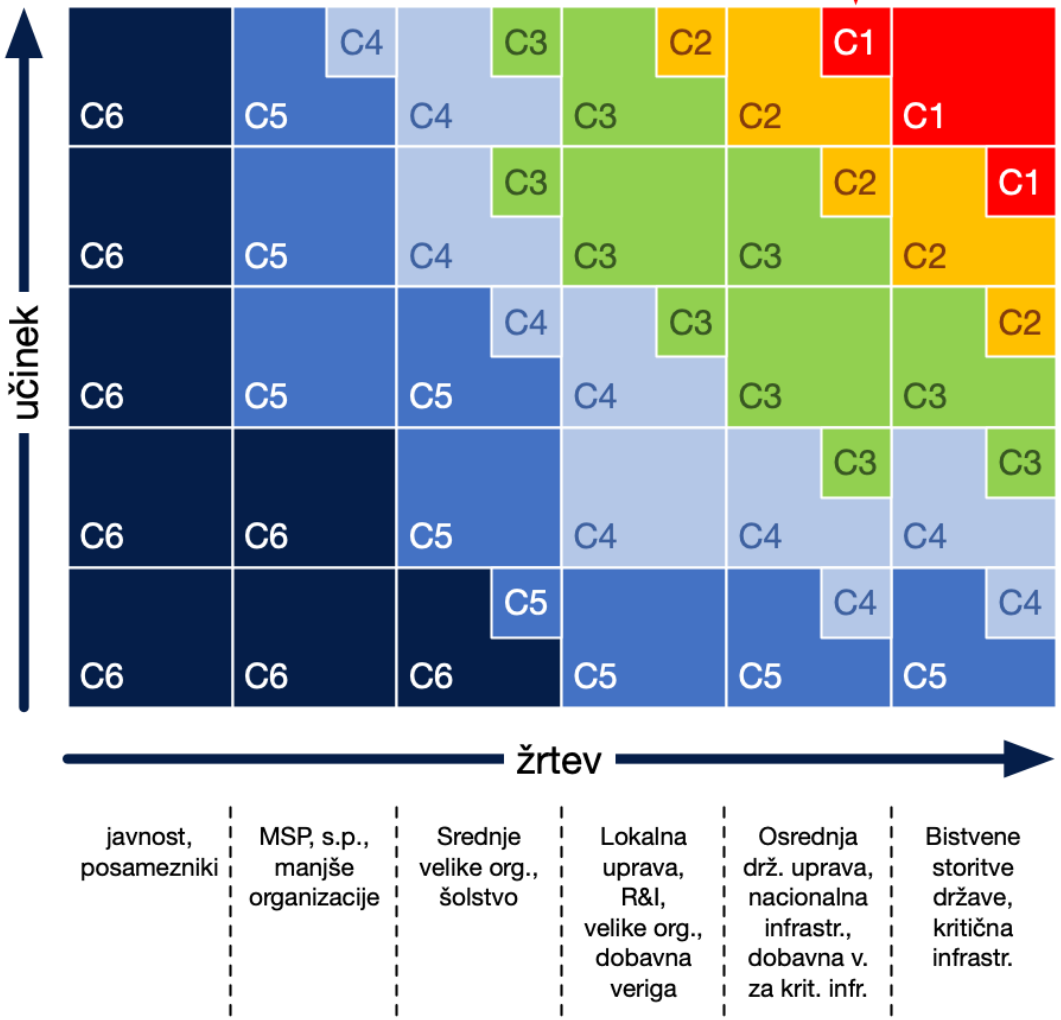
dlje trajajoče motnje bistvenih storitev in povezanih sistemov

eksfiltracija, poškodovanje ali izguba ključnih in občutljivih podatkov in intelektualne lastnine

zlonamerna koda, C2 komunikacija, aktivni vdor preko omrežja, zač. motnja storitev in sistemov

zlonameren napad nižje pomem., ciljano skeniranje, phishing, izguba manj občutljivih podatkov

skeniranje in pregledovanje, identifikacija možnih tarč ali žrtev, goljufije



C1: Kritičen incident: povzročanje resne motnje delovanja osrednjih državnih storitev, motnja stabilnosti države.
C2: Zelo pomemben incident: zaznan ali zelo možen vpliv na občutljive podatke in delovanje državne in kritične infrastrukture.
C3: Pomemben incident: zaznan ali možen vpliv na gospodarstvo, dele državne infrastrukture in dobavno verigo za kritično infrastr.
C4: Incident višje stopnje: zaznan ali možen vpliv na srednja pod. ali nižji vpliv na gospodarstvo in dele državne uprave ali dobav. verigo.
C5: Incident srednje stopnje: zaznan ali možen vpliv na mala pod., nizek vpliv na srednja, priprave na napad na gosp. ali drž. inf.
C6: Rutinski incident: vpliv na javnost ali priprave in poskusi, ki bi vplivali na posameznike in MSP

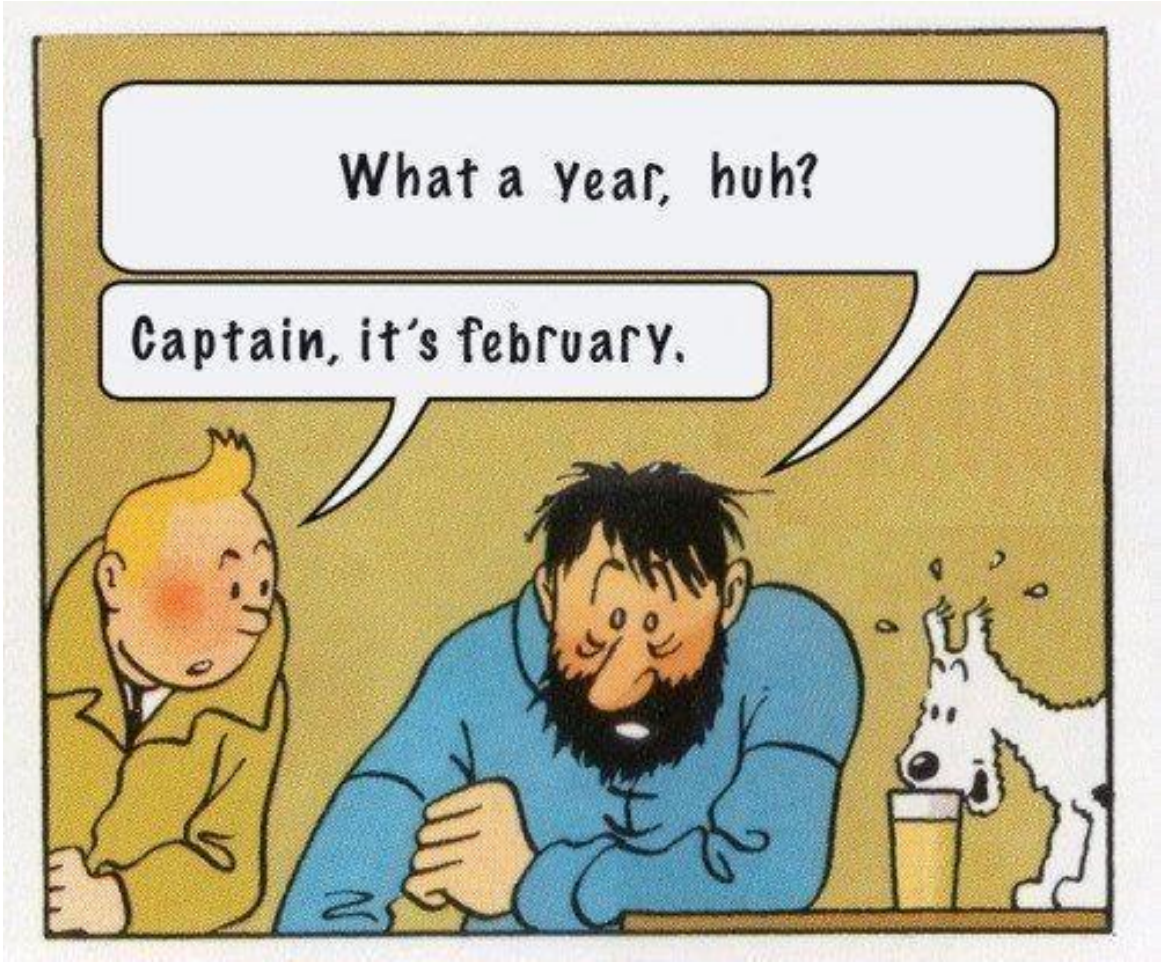
SI-CERT
Nacionalni odzivni center za kibernetsko varnost

LEKCIJE IZ 2024

MOBILNE NAPRAVE

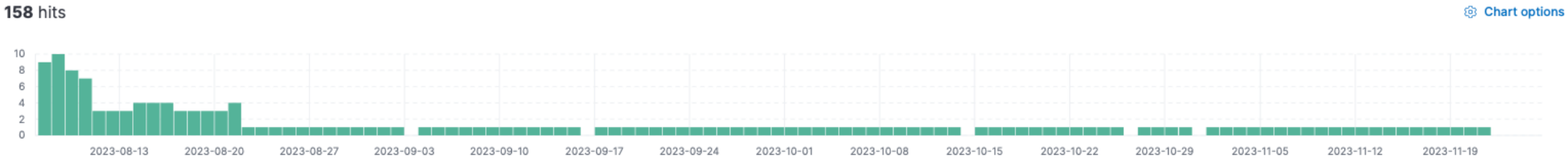
RANLJIVOSTI INFRASTRUKTURE

DRUŽBENI INŽENIRING NA NOVEM NIVOJU



OBRAVNAVA RANLJIVOSTI

- NIS2 in CVD (koordinirano razkrivanje ranljivosti)
- obveščanje skrbnikov
- težave pri iskanju kontaktov

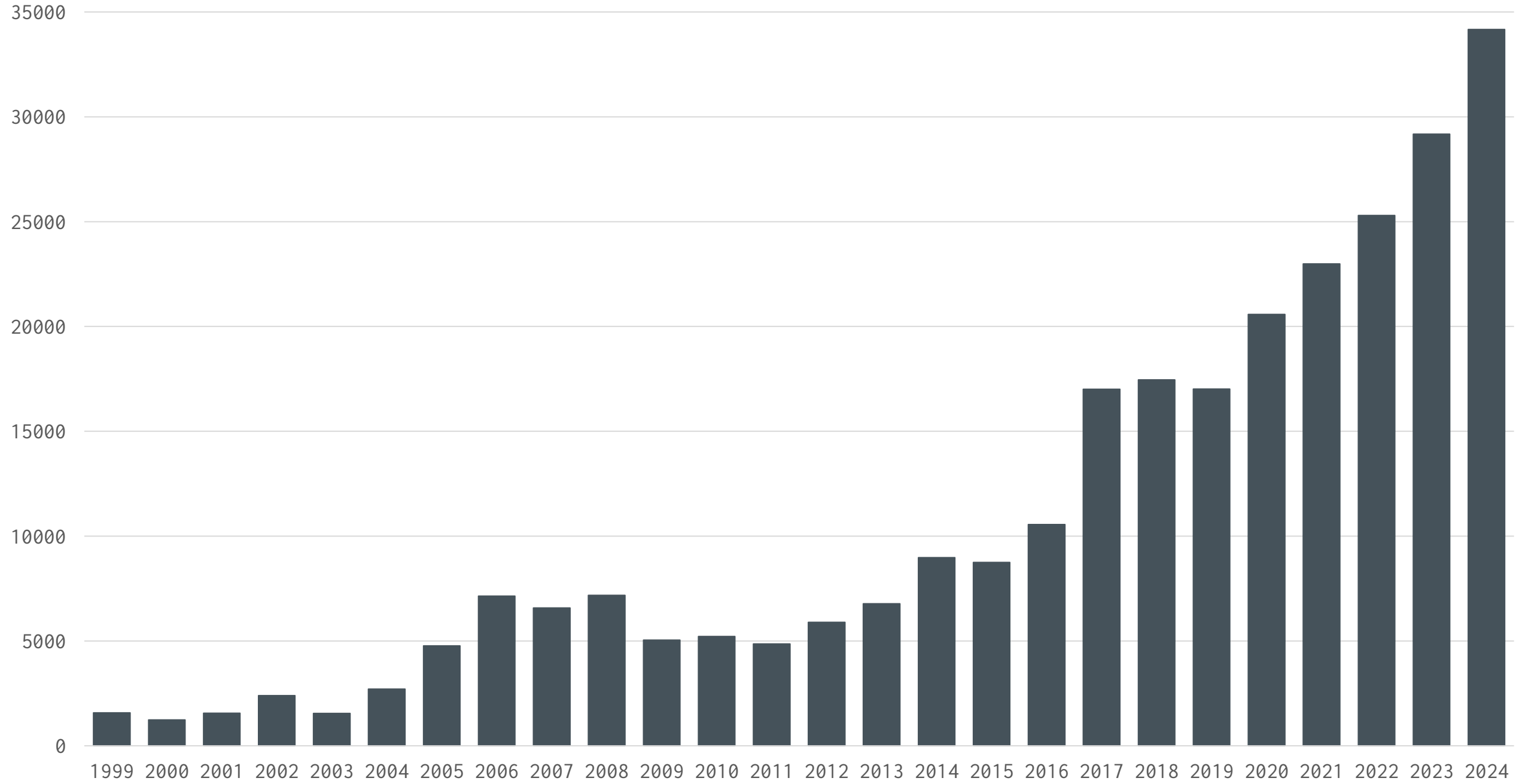


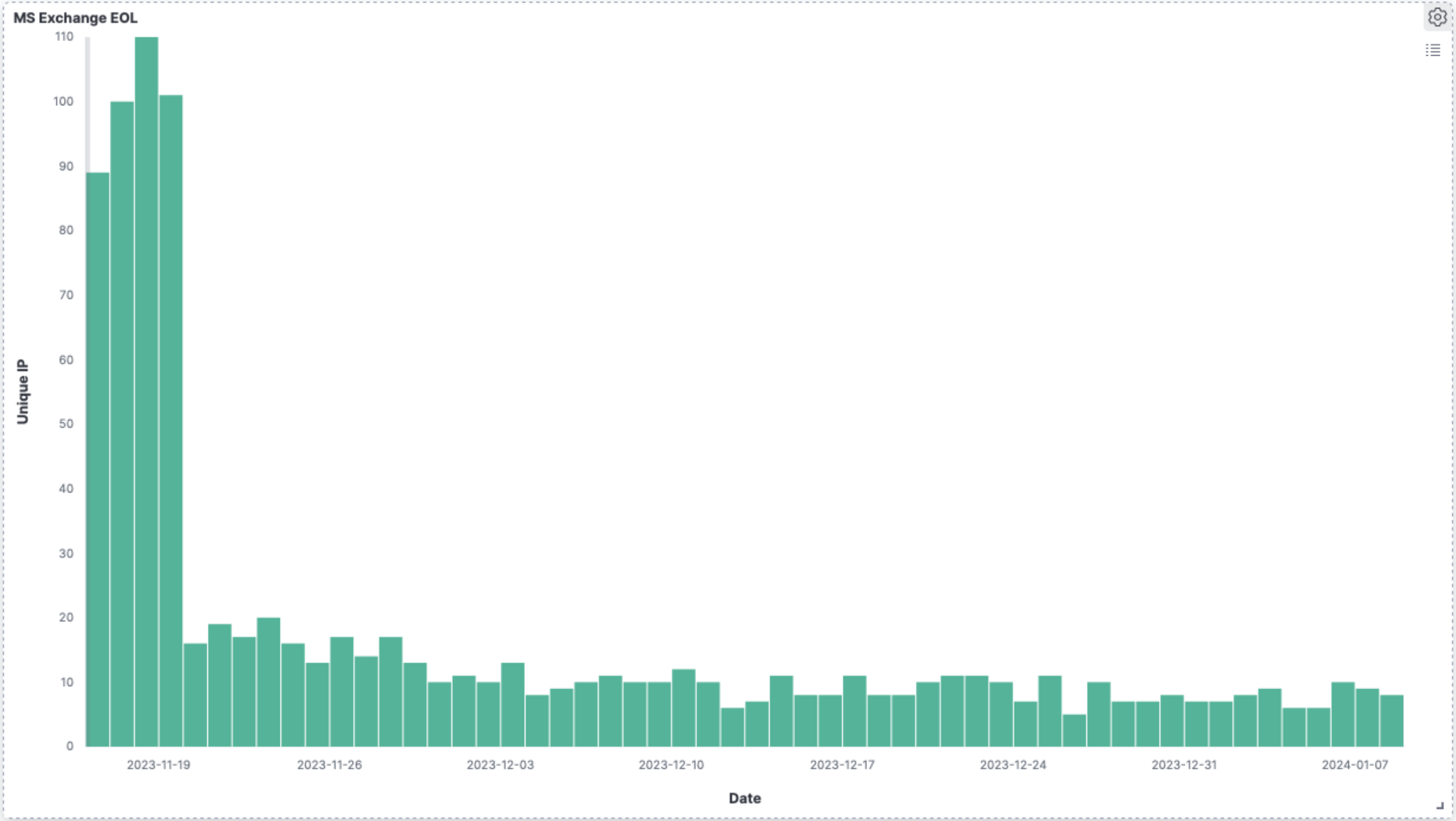
Koordinirano razkrivanje ranljivosti

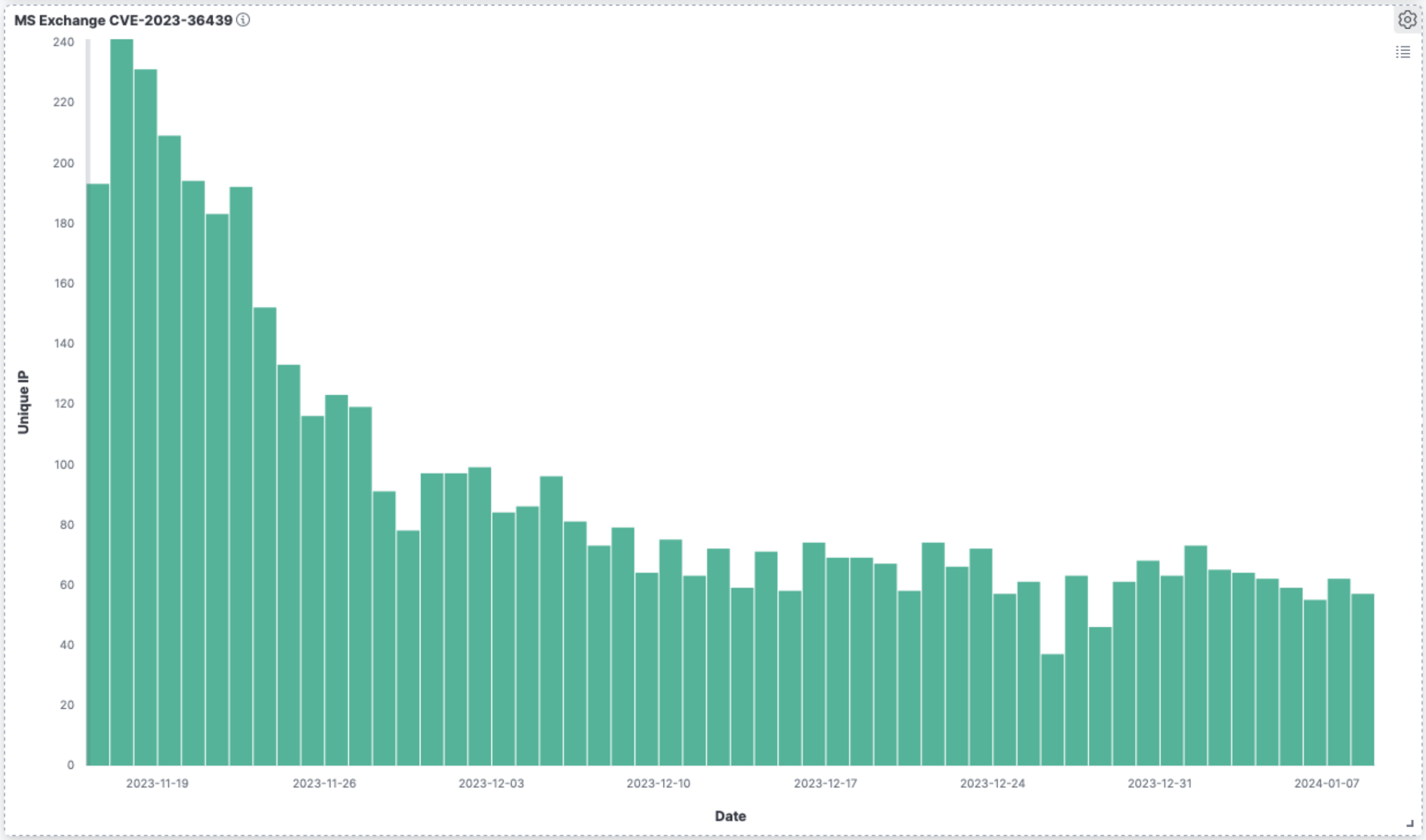
Če ste odkrili tehnično ranljivost v spletni aplikaciji, kakšnem drugem programskem produktu ali omrežni napravi in ta pomeni varnostno tveganje, potem o tem **obvestite Nacionalni odzivni center za kibernetsko varnost (SI-CERT)**. V tem primeru bo SI-CERT opravljal vlogo koordinatorja in predal potrebne informacije upravljalcem sistema ali razvijalcem, pri čemer **ne bo razkril identitete prijavitelja**. Neposredno razkritje ranljivosti še preden proizvajalec da na voljo popravke, lahko povzroči škodo uporabnikom produkta ali naprave.

https://www.cert.si/koordinirano-razkrivanje-ranljivosti/

Ranljivosti (CVE)




MS Exchange EOL
110
100
90
80
70
60
50
40
30
20
10
0
Unique IP
2023-11-19
2023-11-26
2023-12-03
2023-12-10
2023-12-17
2023-12-24
2023-12-31
2024-01-07
Date


MS Exchange CVE-2023-36439
Unique IP
240
220
200
180
160
140
120
100
80
60
40
20
0
2023-11-19
2023-11-26
2023-12-03
2023-12-10
2023-12-17
2023-12-24
2023-12-31
2024-01-07
Date

https://www.cert.si/koordinirano-razkrivanje-ranljivosti/

Kaj je ranljivost?

Ranljivost je niz različnih pogojev, ki omogočajo kršitev varnostne politike. Ranljivost lahko povzročijo napake programske opreme, napačna konfiguracija ali nepričakovane interakcije med sistemi. Uspešno izkoriščanje ranljivosti ima lahko za posledico tehnična tveganja kot tudi tveganja, ki lahko ogrozijo celoten sistem. V sistemih za obdelavo informacij se lahko ranljivosti pokažejo v fazi načrtovanja, kot tudi kasneje v fazi produkcije.

NIST opredeljuje med drugim naslednje razlage pojma ranljivost:

1. Slabost v informacijskem sistemu, varnostnih postopkih sistema, notranjem nadzoru ali izvajanju, ki bi ga lahko izkoristil ali sprožil kdorkoli.
2. Slabost v sistemu, aplikacijah ali omrežju, ki je lahko predmet izkoriščanja ali zlorabe.

Ranljivost se razume neželena in ponavadi nenamerna značilnost programske ali strojne opreme, ki se lahko izkoristi in napadalcu omogoča izvaje dejanj izven načrtovanega namena. Vpliv takih ranljivosti je lahko različen: od nepooblaščenega dostopa do storitve ali sistema, do povzročanja izpada delovanja sistema in s tem povzročenih posledic.

Ladies and Gentlemen,

Siemens ProductCERT is going to publish the attached security advisories on 2025-01-14. The advisories are classified with TLP:AMBER+STRICT and recipients may share this on a need-to-know basis only within their own organization.

Please do not publish corresponding advisories before we notified you about our publication.

Siemens supports the CSAF standard [0,1].
Therefore, we also include the CSAF versions of our advisories to this partner notification. By the use of CSAF parsers this may allow you to automate the creation of your respective derived advisories.

Broken Code: Inside Facebook and the fight to expose its toxic secrets
Jeff Horwitz, 2023, p. 27

… bonuses and promotions were doled out to employees based on how many features they "shipped" … reviews [incentivised] employees to complete products within six months … even if it meant the finished product was only ***minimally viable and poorly documented****.*

Building things is way more fun than making things secure and safe … until there's a regulatory or press fire, ***you don't deal with it****.*

SKRB ZA EKOSISTEM

- vpeljava obveščanja operaterjev
- obveščanje IBS
- širitev mreže MISP na zavezance
- objava škodljivih spletnih mest
- skladnost z NIS2: pregledovanje omrežij, povečanje števila zavezancev, CVD, napredovanje po zrelostni lestvici SIM3

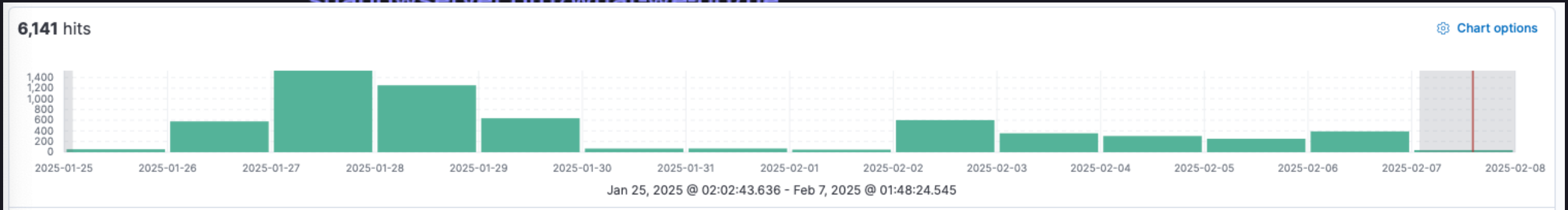
jaKa Močnik @jkmcnk@mastodon.social 20h

~16k italian IPs involved in a brief attempt at credential stuffing us yesterday, but giving up in an hour. a random sample tested shows port 22 open on every one of them and a random open port (2222, 6699 etc) every so often. all the tested ssh servers run the same openssh server version. IPs come mostly from vodafone italia AS and a few from Windtre AS. my guess is compromised home routers of vodafone italia. #infosec

2

The Shadowserver Foundation
@shadowserver@infosec.exchange

Large increase in web login brute forcing attacks against edge devices seen last few weeks in our honeypots, with up to 2.8M IPs per day seen with attempts (especially Palo Alto Networks, Ivanti, SonicWall etc). Over 1M from Brazil. Source IPs shared in shadowserver.org/what-we-do/ne



HTTP attacks by src device. Only in cases where we can map src IP to a device. Note it may be a device behind the identified device that is involved:
dashboard.shadowserver.org/sta...

If you receive an alert from us about an IP in your constituency seen attacking please investigate and reach out to us with your findings

Domov › Novice ›

Ministrstvo za zunanje in evrops
zadeve tarča kibernetskega nap

7. 4. 2023 Ministrstvo z

Ministrstvo za zunanje in evropske zadeve je bilo tarča kibernetskih akti
izvajanja varnostnih ukrepov.

Trenutno smo v fazi ocenjevanja razsežnosti in posledic aktivnosti, vendar delovanje ministrstva ni moteno. Aktivnosti smo odkrili sami v sodelovanju s partnerji. Vzporedno s temeljito preiskavo smo sprožili vse ustrezne ukrepe. Pri upravljanju z incidentom sodelujemo z uradom vlade za informacijsko varnost.

Znane so nove podrobnosti kibernetskega napada na skupino HSE

Avtor: Sa. B.

Generalni direktor HSE je zagotovil, da večjih posledic z vidika varnostnega sistema in ekonomskega vpliva ne bo. Foto: STA

Znane so nove podrobnosti obsežnega kibernetskega napada na skupino Holding Slovenske elektrarne (HSE), ki se je zgodil v noči s petka na soboto, prvič pa je bil zaznan že v noči s srede na četrtek. Nove informacije sta v skupni izjavi za medije podala generalni direktor skupine HSE Tomaž Štokelj in direktor Urada vlade RS za informacijsko varnost Uroš Svete, ki je povedal, da je "situacija v tem trenutku pod nadzorom".

robnosti o kibernetskem napadu kažejo na
nost URSZR

2022 15.15 |

S BRANJA: **6 min**

narič KOMENTARJI 46

o je na Upravi za zaščito in reševanje prišlo do kibernetskega napada z virusom. Po naših neuradnih informacijah je kasnejši pregled dnevnikov in podatkov o omrežju pokazal številne ranljivosti, teh naj bi bilo več kot 950. Med drugim naj bi uporabljali zelo šibka gesla, kljub temu da je sistem omogočal dvostopenjsko avtentikacijo, pa te možnosti niso uporabljali. Do okužbe je najverjetneje prišlo prek računalnika enega od zaposlenih, ki je delal na daljavo.

Nacionalni odzivni center za kibernetsko varnost (SI-CERT) je že pripravil poročilo v zvezi s kibernetskim napadom na informacijski sistem Uprave za zaščito in reševanje (URSZR). Po naših neuradnih informacijah naj bi pregled podatkov o dostopnih storitvah in morebitnih ranljivostih na naslovnem prostoru URSZR kazal na zelo razširjen nabor ranljivosti. Teh naj bi bilo kar 954, tri od njih pa naj bi imele glede na skupni sistem točkovanja ranljivosti (CVSS) najvišjo oceno: 10.

Port of Seattle hit by Rhysida ransomware in August attack

By **Sergiu Gatlan**

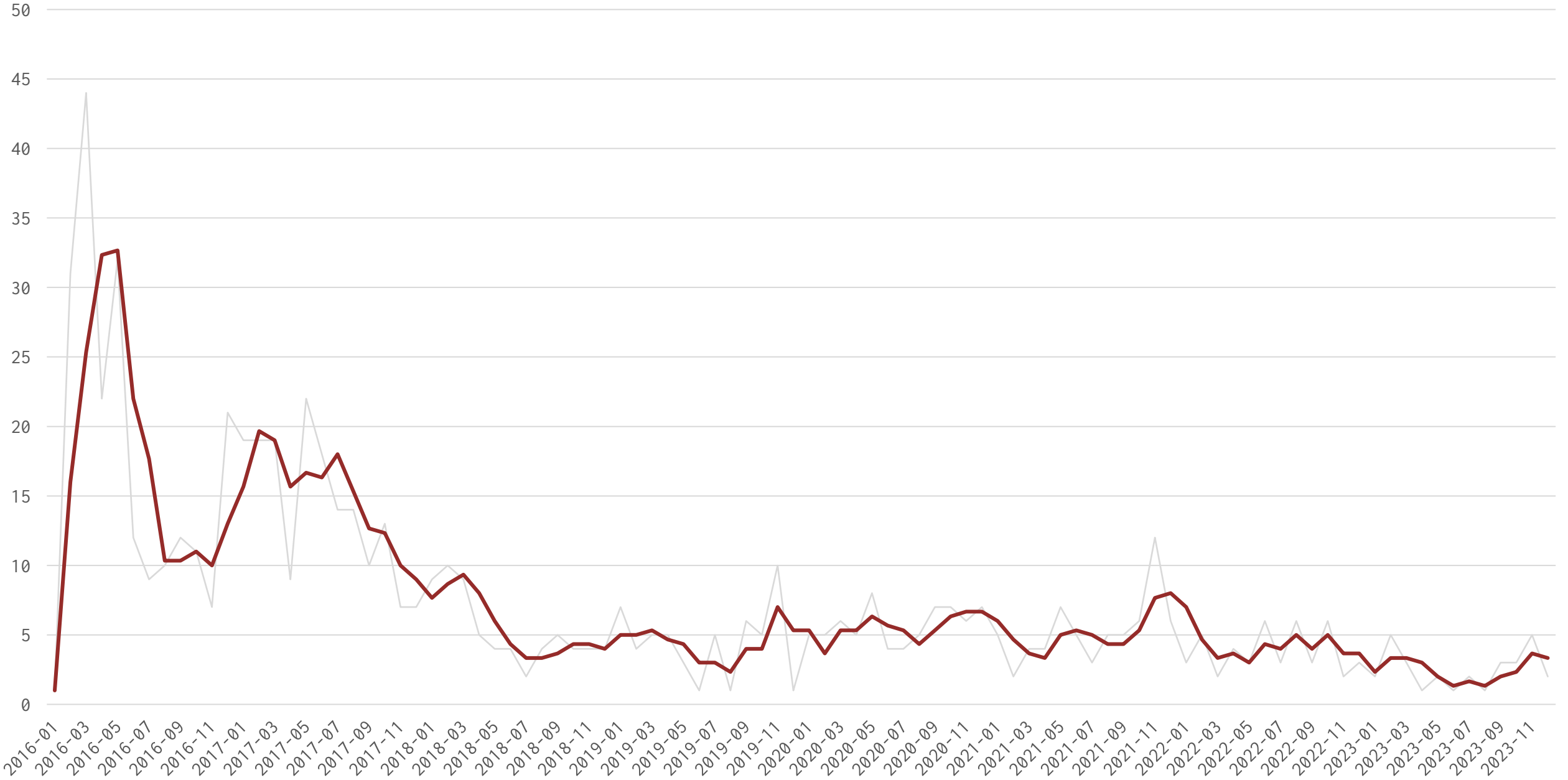
September 13, 2024 06:54 PM 0

Image: Midjourney

Port of Seattle, the United States government agency overseeing Seattle's seaport and airport, confirmed on Friday that the Rhysida ransomware operation was behind a cyberattack impacting its systems over the last three weeks.

Slika je simbolična. CC-BY Chesapeake Bay Program @ flickr.com

Mesečno število prijavljenih incidentov z izsiljevalskimi virusi - ransomware
(s 3-mesečnim gibljivim povprečjem)

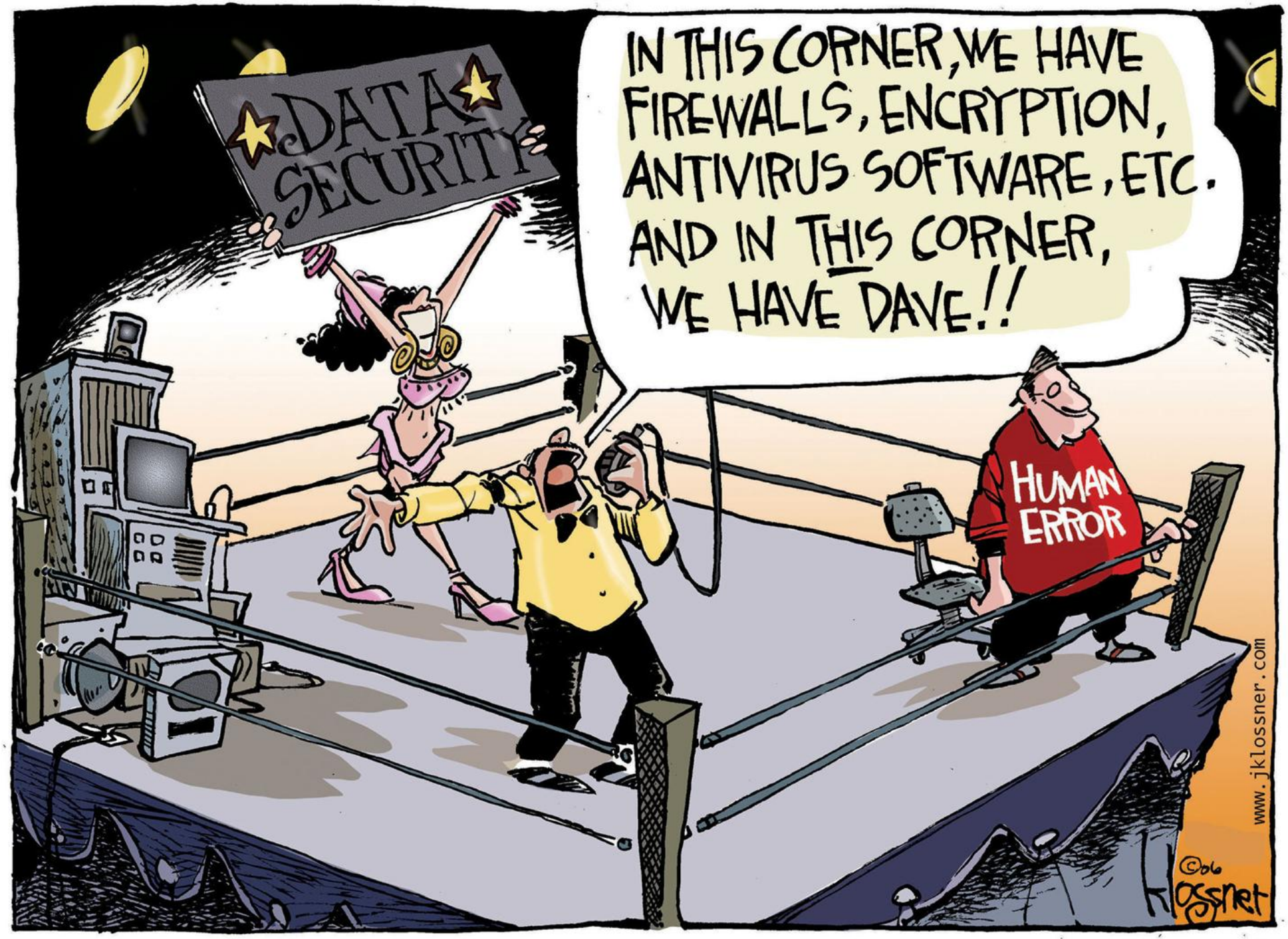


VARNOSTNA OBVESTILA / 16. 1. 2025

SI-CERT 2025-01 / Prevzemi in kreiranje Telegram računov brez vednosti uporabnikov telefonskih številk

Povzetek

Od sredine leta 2024 na SI-CERT beležimo primere kreiranja uporabniških računov na platformi Telegram s slovenskimi telefonskimi številkami, pri čemer računov niso kreirali uporabniki teh številk. Prav tako na podoben način prihaja do prevzema obstoječih Telegram računov, ki niso zaščiteni z dodatnim geslom. Zaenkrat na SI-CERT ne vemo, na kakšen način prihaja do teh zlorab, vemo pa, da ne gre za težavo, na katero bi uporabniki lahko vplivali. Trenutno zbrane informacije kažejo, da ne gre za ciljane napade. Računi so najverjetneje kreirani z namenom kasnejše preprodaje le-teh in se ne uporabljajo z namenom povzročanja neposredne škode uporabnikom telefonskih številk.



Video namigi Archives - Varni na

varninainternetu.si/knjiznjice/video-namigi/

Brez beleženja zgodovine (2)

VARNI NA INTERNETU
Od mene je odvisno vse.

PREVARE NASVETI NOVICE ZA PODJETJA GRADIVA

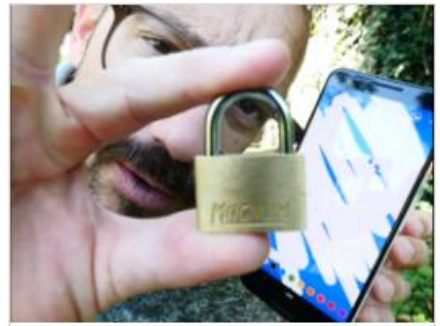
VIDEO NAMIGI

HITRA FINTA #13: POSTAL SEM ŽRTEV SPLETNE PREVARE – KAJ ZDAJ?

→ POGLEJ

HITRA FINTA #12: KAKO PREPOZNAŠ PREVARO Z LAŽNIM KREDITOM?

→ POGLEJ



HITRA FINTA #11: KAKO VARNO IZBRIŠEŠ PODATKE NA TELEFONU?

→ POGLEJ

HITRA FINTA #10: KAKO PREPOZNAŠ LAŽNI OGLAS ZA STANOVANJE?

HITRA FINTA #9: KAKO ZAŠČITIŠ FACEBOOK RAČUN?

HITRA FINTA #8: KAKO NASTAVIŠ GESLO ZA WI-FI?

NAJPOGOSTEJŠE TEŽAVE, S KATERIMI SE SOOČAJO SPLETNI UPORABNIKI.

Odgovor na vašo težavo se verjetno nahaja med zbranimi članki.

PREJELI STE IZSILJEVALSKI EMAIL, DA SO VAM VDRLI V RAČUNALNIK

→ KAJ LAHKO NAREDITE

PREVARA, KI CILJA PRODAJALCE NA SPLETNIH OGLASNIKIH

→ KAJ LAHKO NAREDITE

NEOBIČAJNI TELEFONSKI KLICI IZ TUJINE

→ KAJ LAHKO NAREDITE

ALI LAHKO ZAUPAM SPLETNI TRGOVINI?

→ KAJ LAHKO NAREDITE

INVESTICIJSKE PREVARE S KRIPTOVALUTAMI

→ KAJ LAHKO NAREDITE

PREVARE S SKRITO NAROČNINO (SUBSCRIPTION TRAP)

→ KAJ LAHKO NAREDITE

IMAM DRUGO TEŽAVO

Varni v pisarni

https://www.varnivpisarni.si

Guest

VARNI v pisarni

Učni moduli

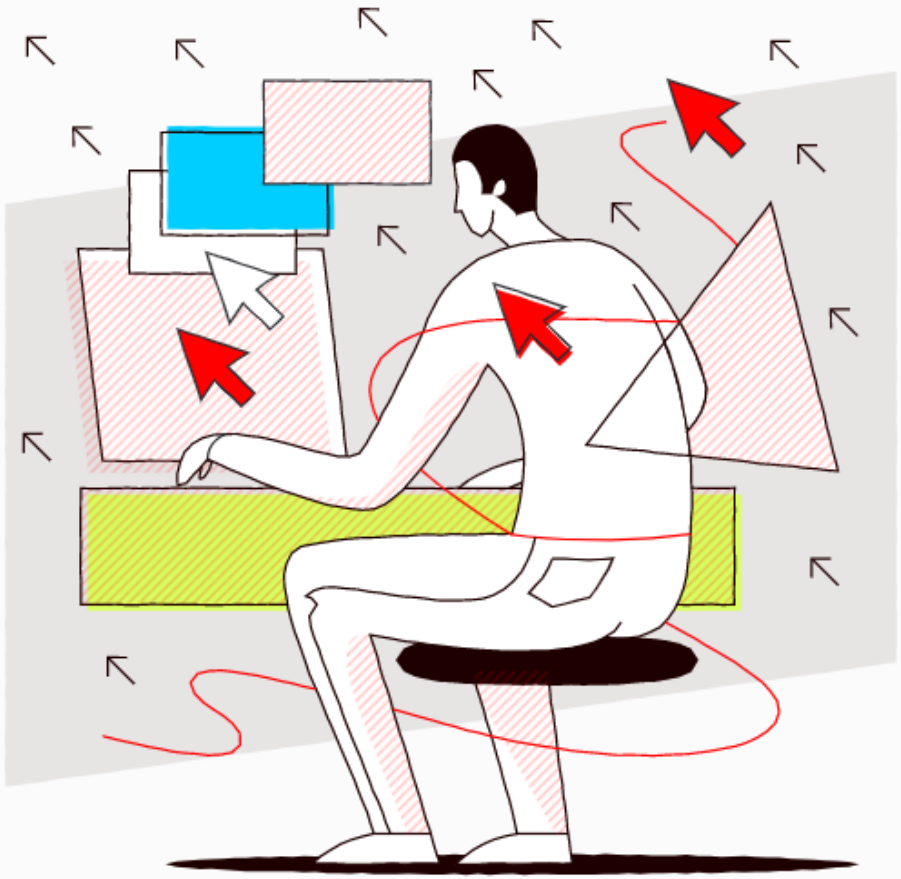
Moj račun

BREZPLAČNI SPLETNI TEČAJ ZA ZAPOSLENE

30 minut za informacijsko varnost na delovnem mestu

En sam napačen klik lahko pomeni neznansko škodo za podjetje. Z brezplačnim tečajem boste pridobili novo znanje, kako ostati varni v pisarni. Tečaj opravite kadarkoli, vsebine prilagodite svojim delovnim nalogam.

Učni moduli



OPRAVLJEN

Osnove informacijske varnosti

Odprite

100% Opravljeno

OPRAVLJEN

Računovodstvo, tajništvo, finance

Odprite

100% Opravljeno

VPISAN

Marketing, prodaja, nabava, logistika

Odprite

85% Opravljeno

OPRAVLJEN

IT oddelek – informatiki, zunanji vzdrževalci

Odprite

100% Opravljeno

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

Osnove (ne)varnosti

Matjaž Breskvar, CEO,
Beyond Semiconductor d.o.o.

(Ne)Varnost

Matjaz Breskvar (Beyond Semiconductor)

„Kibernetski cunami“ – GZS, 7.11.2025

Kaj je

(ne)varnost ?

Kaj je

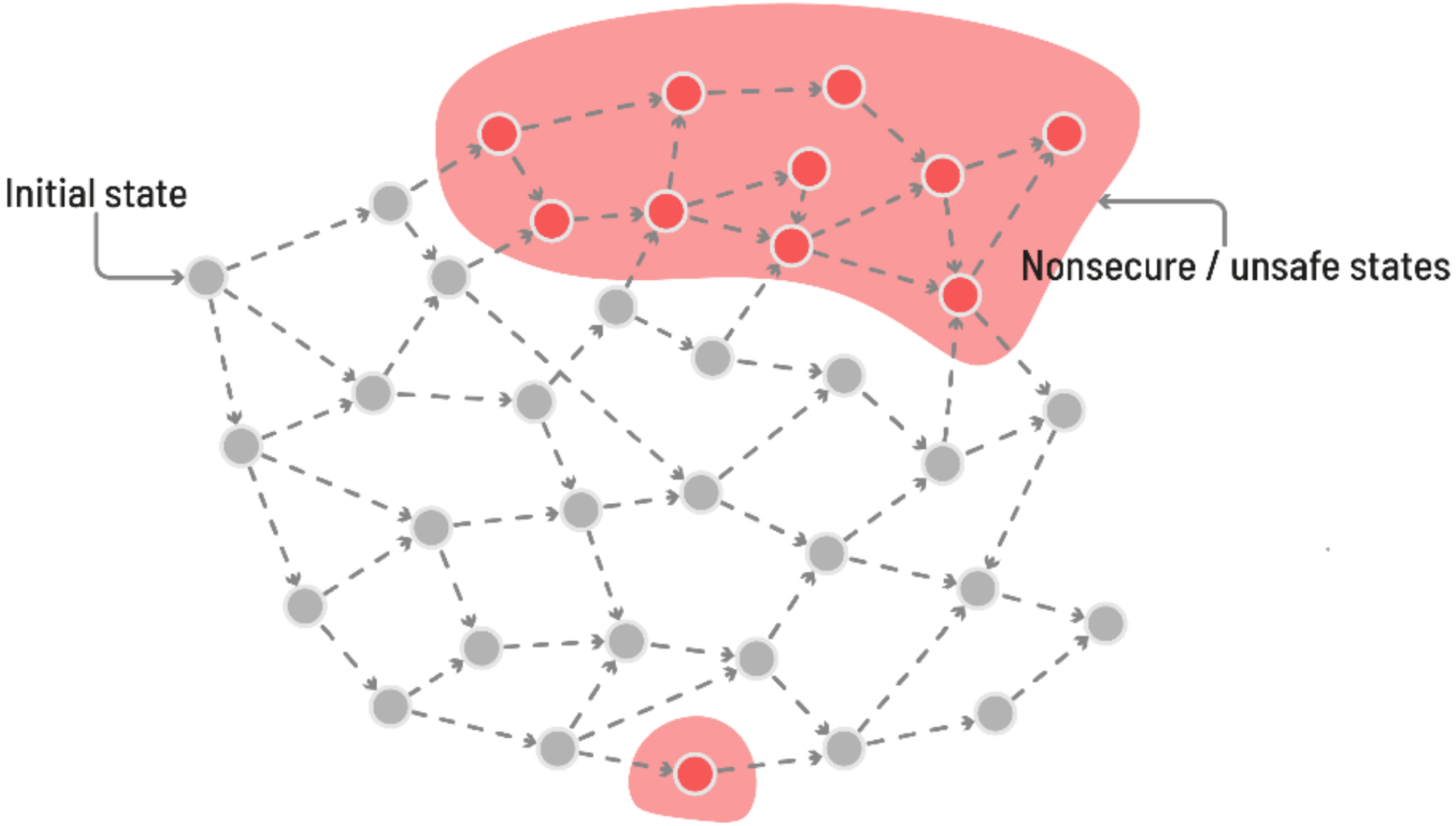
(ne)varnost ?

“nekaj kar me obvaruje”
“nekaj kar prepreči poškodovanje”

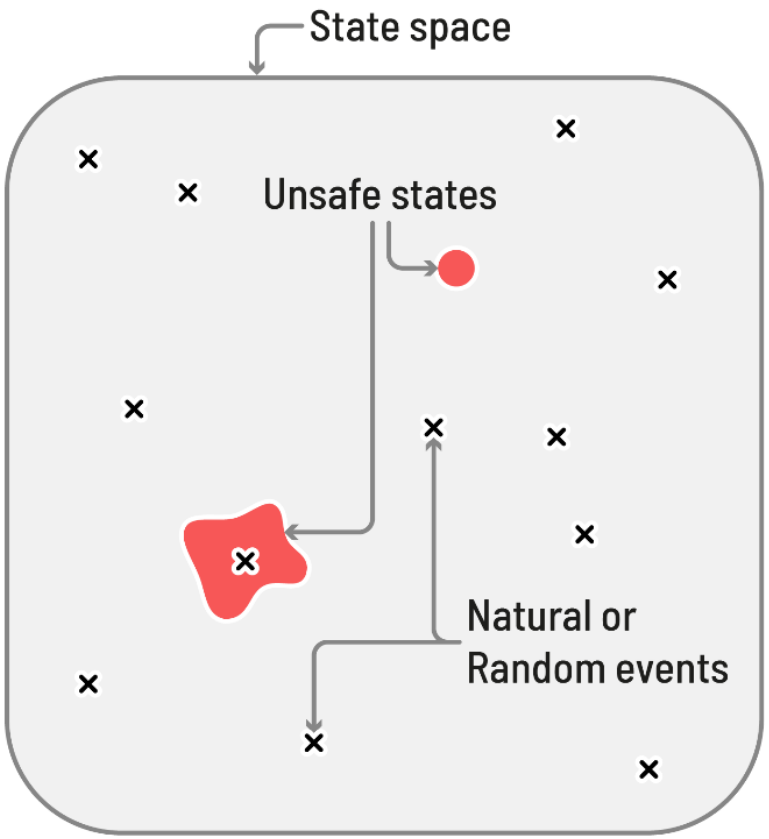
Varnost (safety)

Varnost (security)

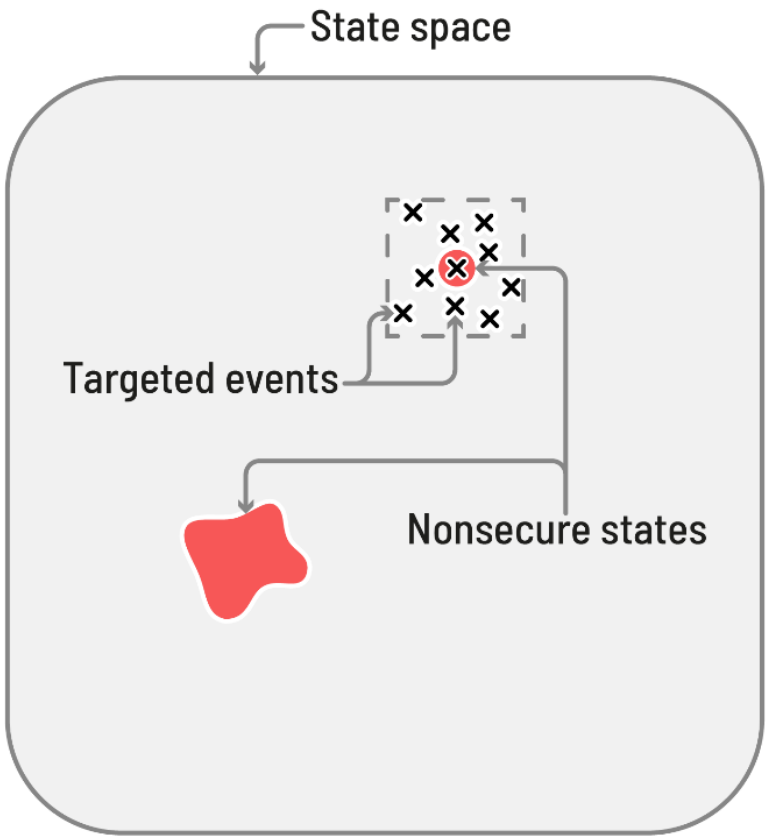
Shitterstock.com
https://www.google.com/imgres?q=unsafe%20knife%20position&imgurl=https%3A%2F%2Fwww.shutterstock.com



Safety versus Security



Numbers game



Targeting game

BEYOND SEMICONDUCTOR

Varnost (security)

Neformalni opis

- “nekaj kar me obvaruje”
- “nekaj kar prepreči poškodbe”
- Funkcionalne zahteve (vrata morajo zdržati pritisk s silo X N …)
- Seznam “kritičnih” lastnosti…

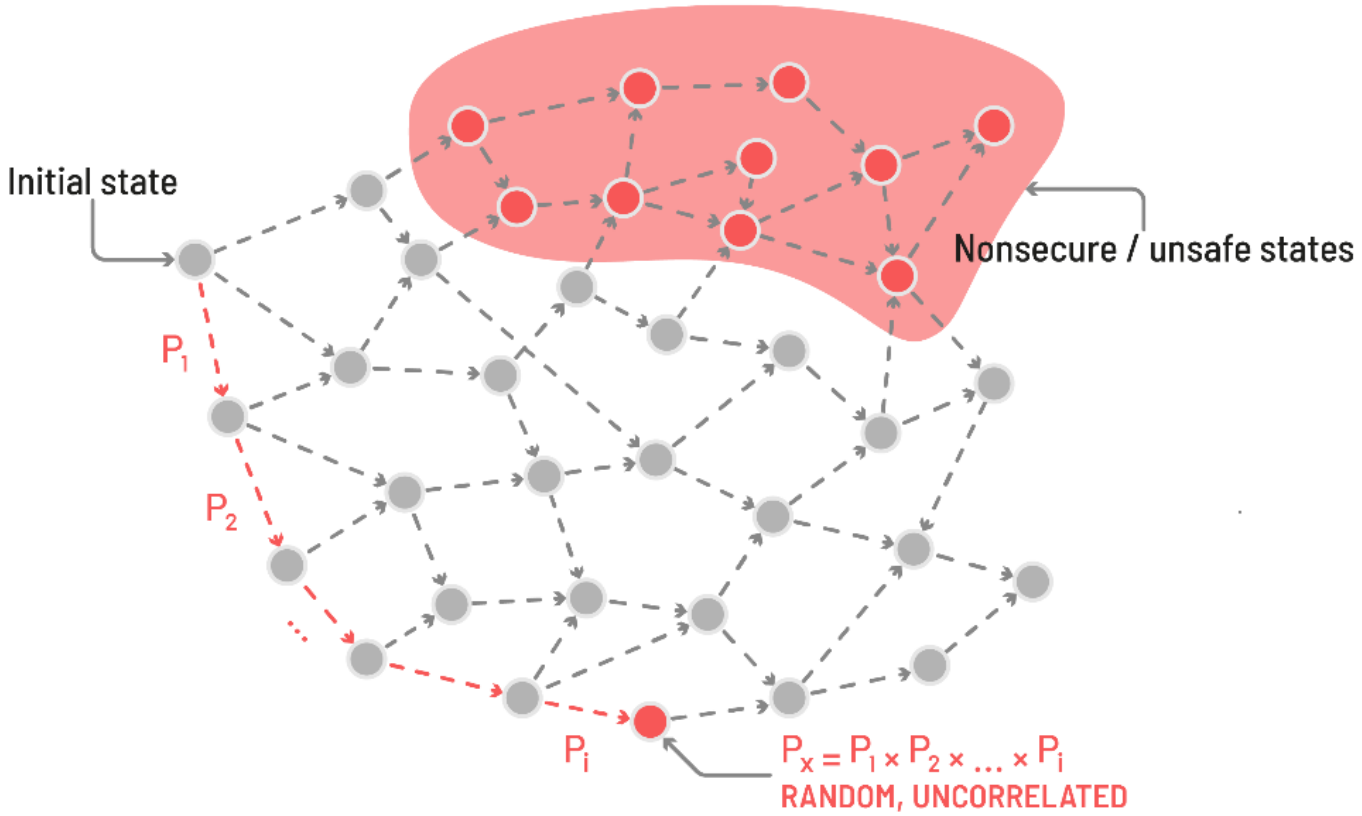
- Kaj je kontekst ?

Matematični opis

- Rushby: Non-interference
- seL4: information flow enforcement
- GWV / GWVr2: Non-exfiltration, non-infiltration, non-mediation

- Kaj je formalno (ne)varno ?

“Povečana” Varnost

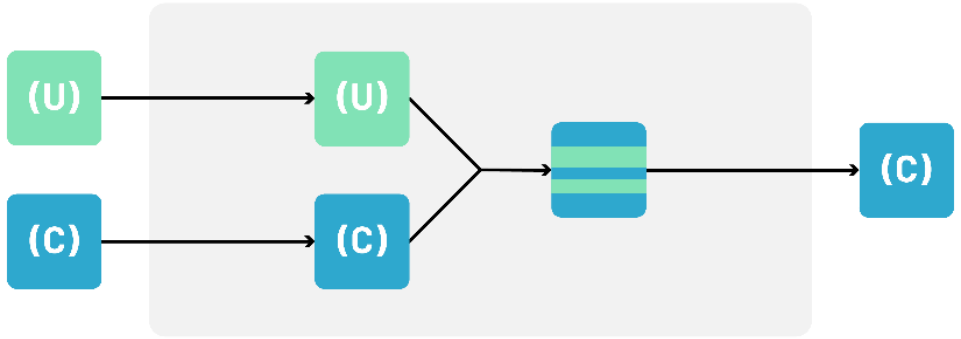


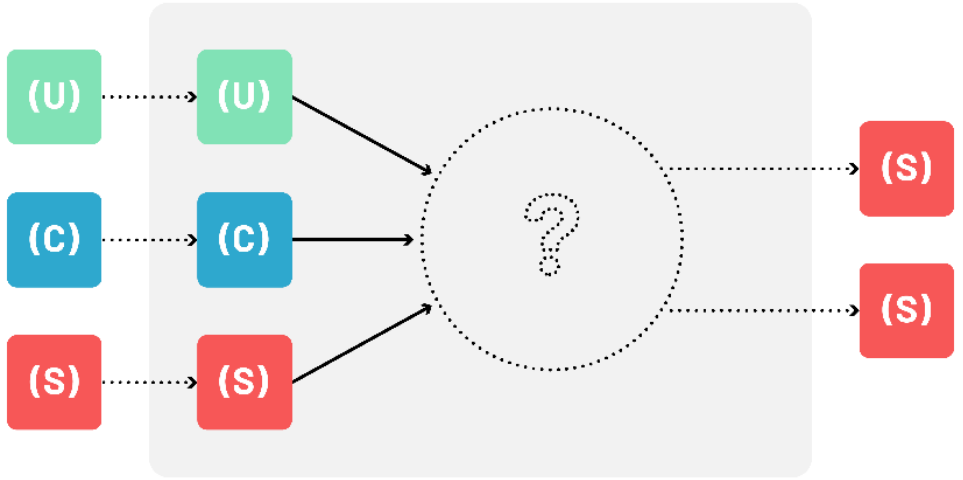
- AES-128 → AES-256
- Nestandardni ssh port
- Default password
- QR kriptografija
- Povečan prostor za gesla iz 10 na 1000 znakov (da preprečimo buffer overflow)
- Menjavanje gesel na 3 mesece

Varnostno pomembne lastnosti in modeli

- Bell–LaPadula model (confidentiality model)
- Biba Model (integrity model)
- Clark–Wilson model (integrity model)
- Graham–Denning model (protection rules)
- DAC (Discretionary access control)
- MAC (Mandatory access control)
- MLS (Multilevel security)
- MILS (Multiple Independent Levels of Security)
- …

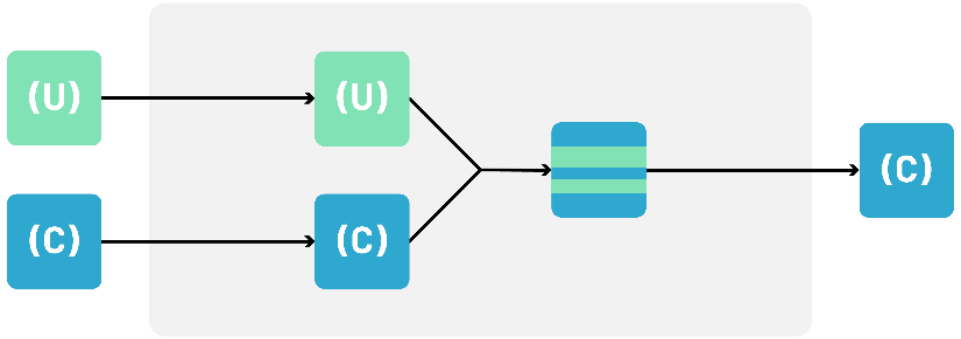
Confidentiality: composition rules

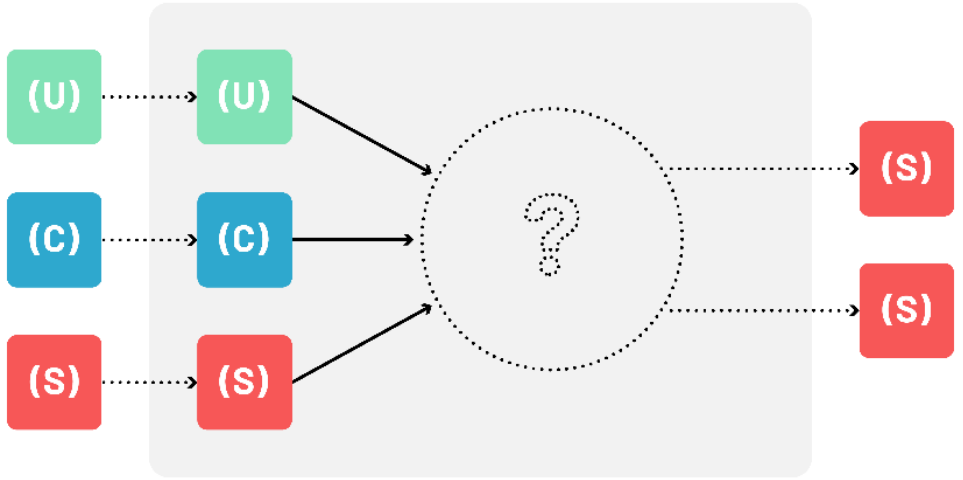




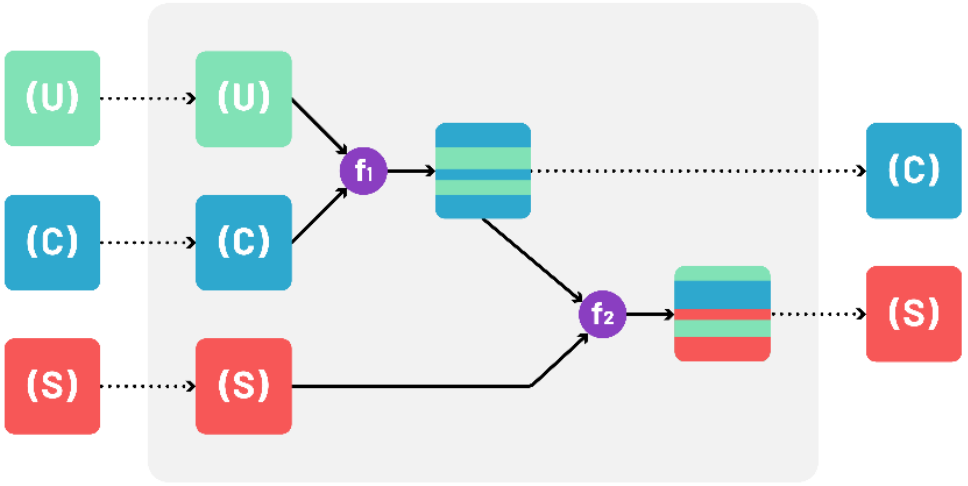
BEYOND SEMICONDUCTOR

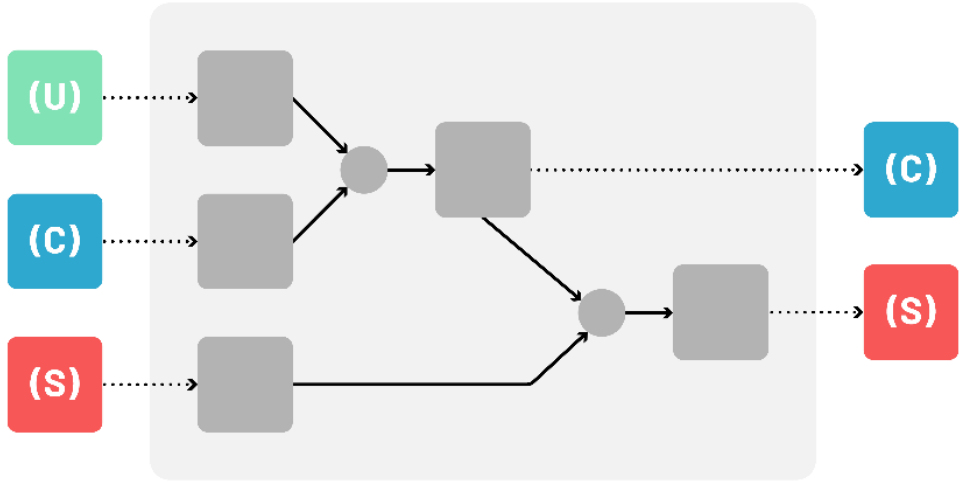
Confidentiality: composition rules



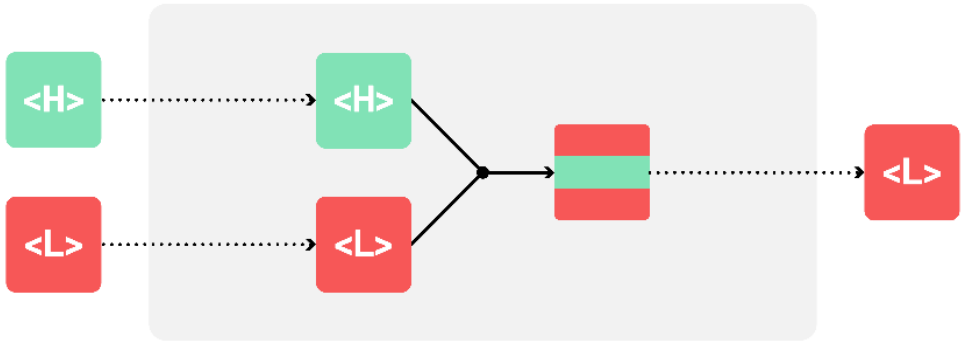


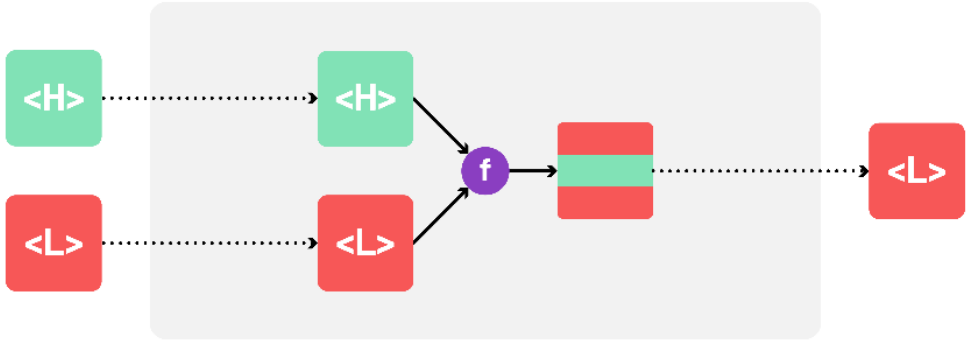
Can do better if “composition structure” is known





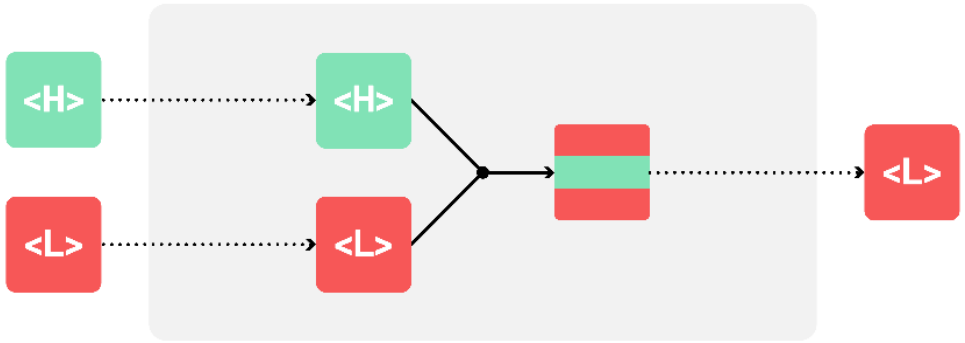
Integrity: composition rules – analogous?

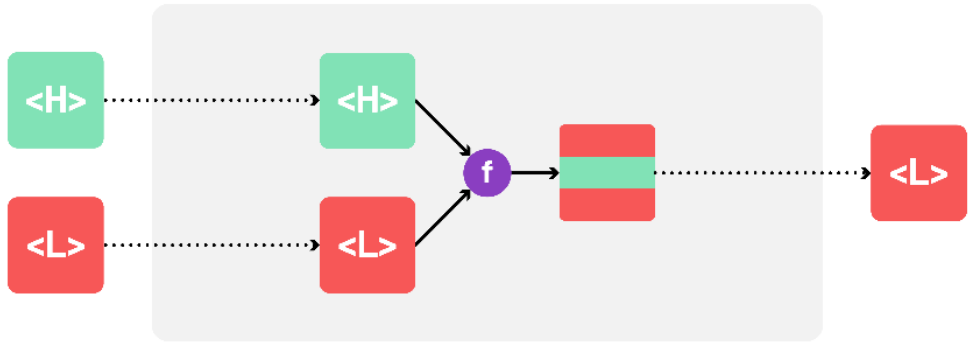




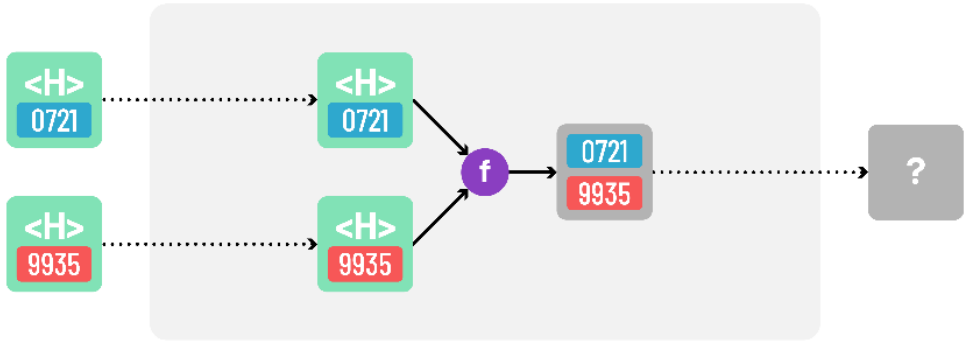
BEYOND SEMICONDUCTOR

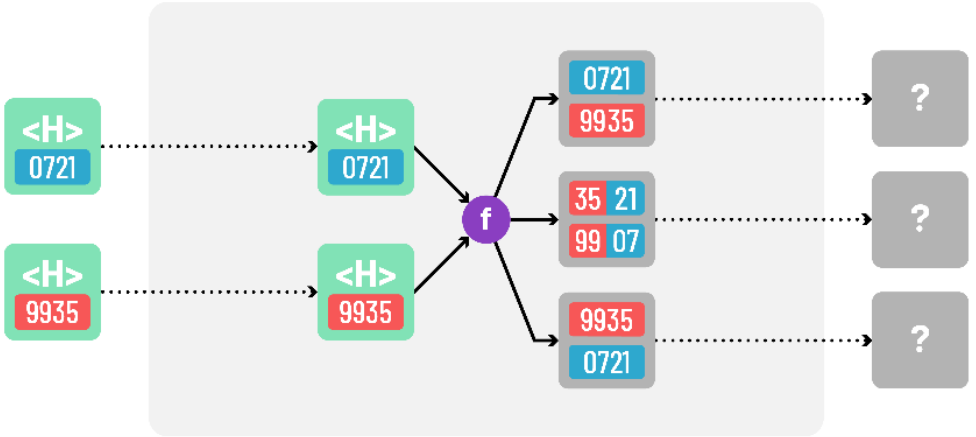
Integrity: composition rules – analogous?





Nice try, but the composition function is important!

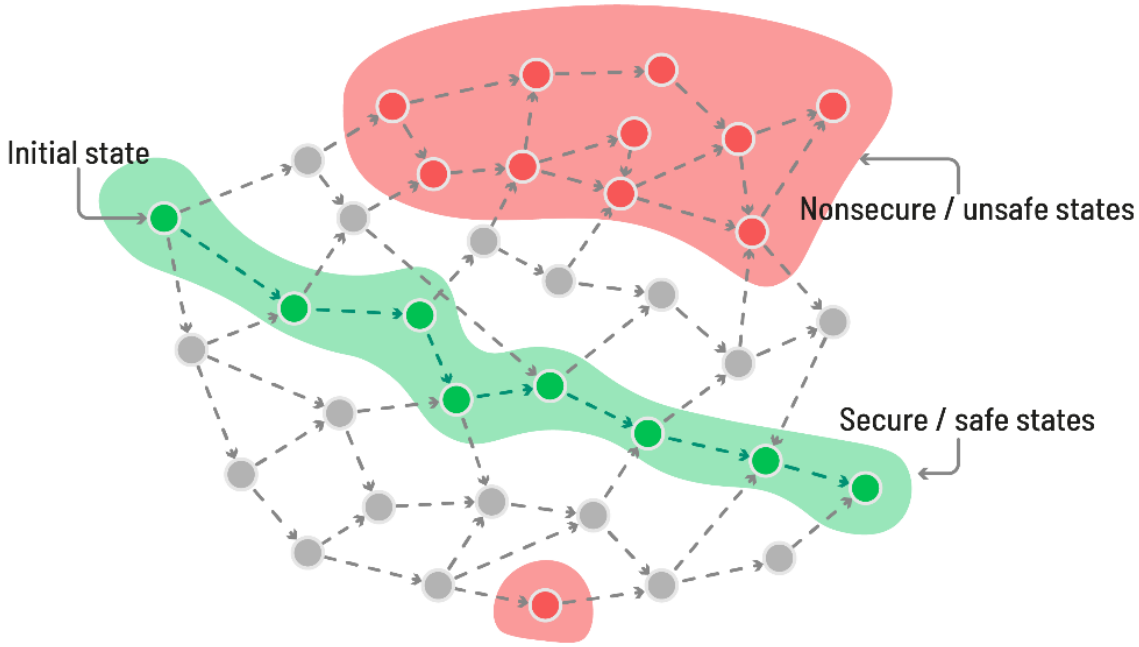




BEYOND SEMICONDUCTOR

Glavni poudarki

- Maksimalno omejiti prostor stanj in obržati le kar je absolutno nujno za dosego funkcionalnih ciljev
  - Deny all – allow nothing – add minimum needed (to achieve functionality)
- “Software” je običajno precej bolj riskanten kot “hardware”
  - Več kompleksnisti, večji proctor stanj, bolj programabilen
- Opomba: kaj pa military grade kriptografija ?



Kako preveriti celoten prostor stanj ?

So naši podatki bolj varni kot pred 10/20/30 leti ?

So naši podatki bolj varni kot pred 10/20/30 leti ?

- Veliko pozornosti, idej, raziskav, produktov, programov, “rešitev”,…
- Precej izgubljenega časa in truda, pogosto težko identificirati, kaj je vredno
- Večni napredek, polno izboljšav a brez bistvenih izboljšan in prebojev

$$Damage \propto N_{attacks} * P_{breach} * N_{assets} * V_{per\_asset}$$

Number of attacks

Value per asset

Number of Digitalized assets

Probability of breach is constant if attack and defense progress similarly

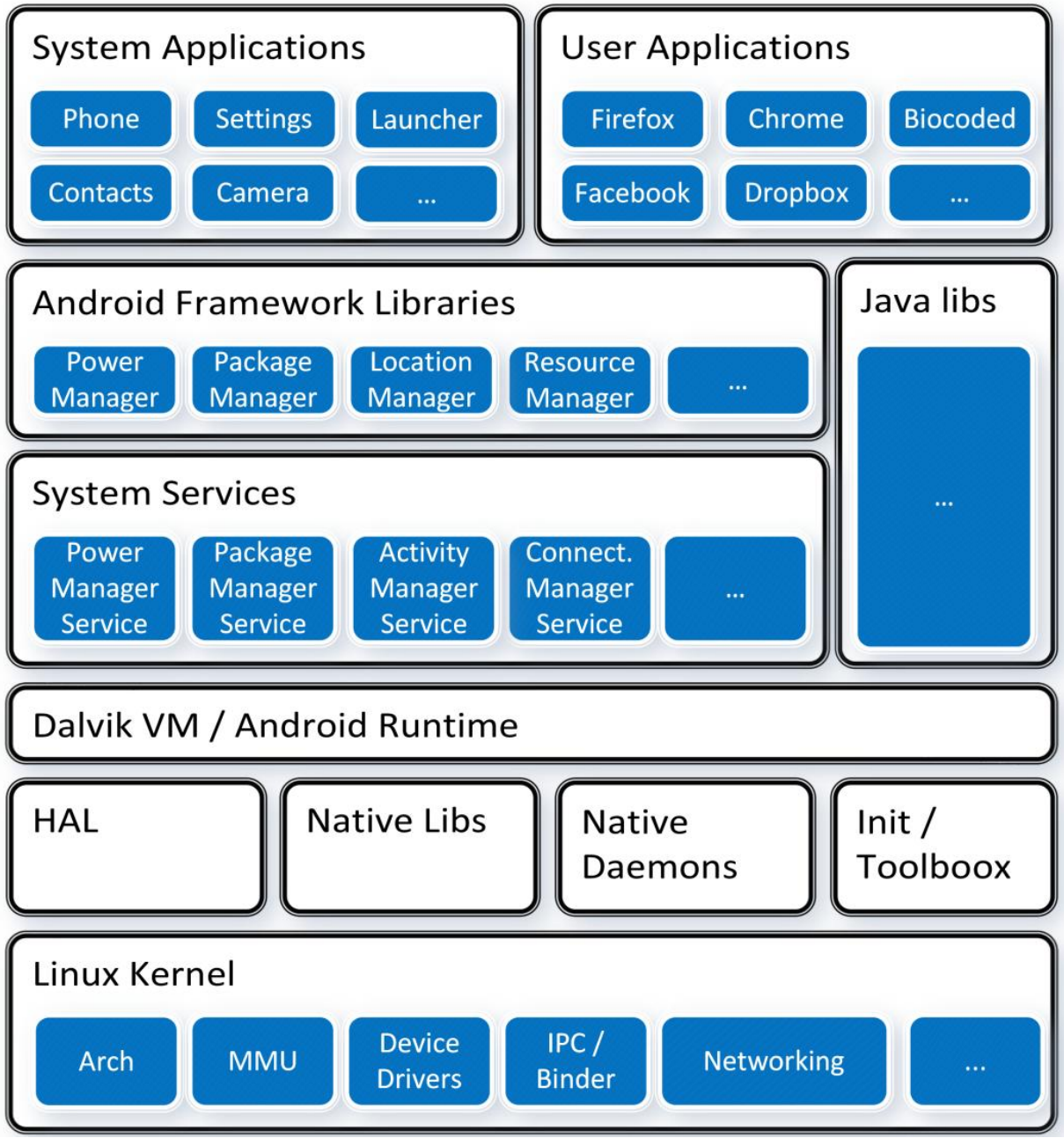
P_{breach} must go down to offset digitalization and increase of attacks

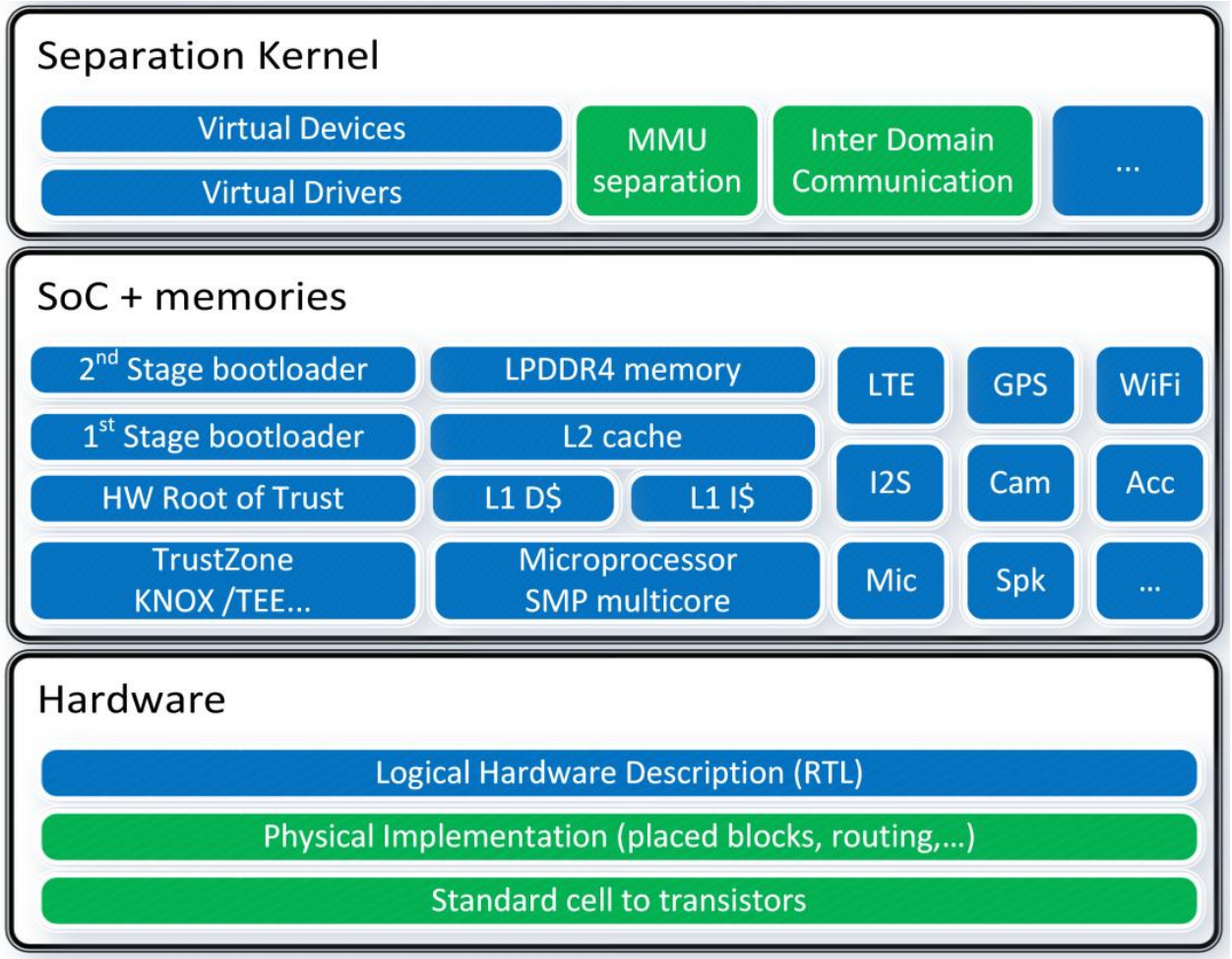
Zakaj je težko zaščiti sisteme ?

- Varnostne zahteve so zgolj nabor ***kompleksnih funkcionalnih zahtev***
  - Na prvi pogled majhne napake lahko povsem izničijo varnost sistema
- Ni načina za ***merjenje*** “nivoja zaščite”, ki je dejansko dosežen
  - Za razliko od porabe energije, performans, …
- Če razvijalcu ne uspe predreti varnost sistema to še ne pomeni, da komu drugemu ne bo uspelo.

- Zaščita sistemov mora zdržati trenutne napade in še vse ***prihodnje napade in grožnje***
  - Grožnje čez 3, 5, 10, 15… bodo morda precej drugačne
- Napadalci so pogosto ***”nation state sponsored attackers”*** razpolagajo z viri, so dobro financirani in zelo sposobni
  - Napadi so lahko targetirani – lažje je najti eno ranljivost kot odpraviti vse
- Čas je na strani napadalcev

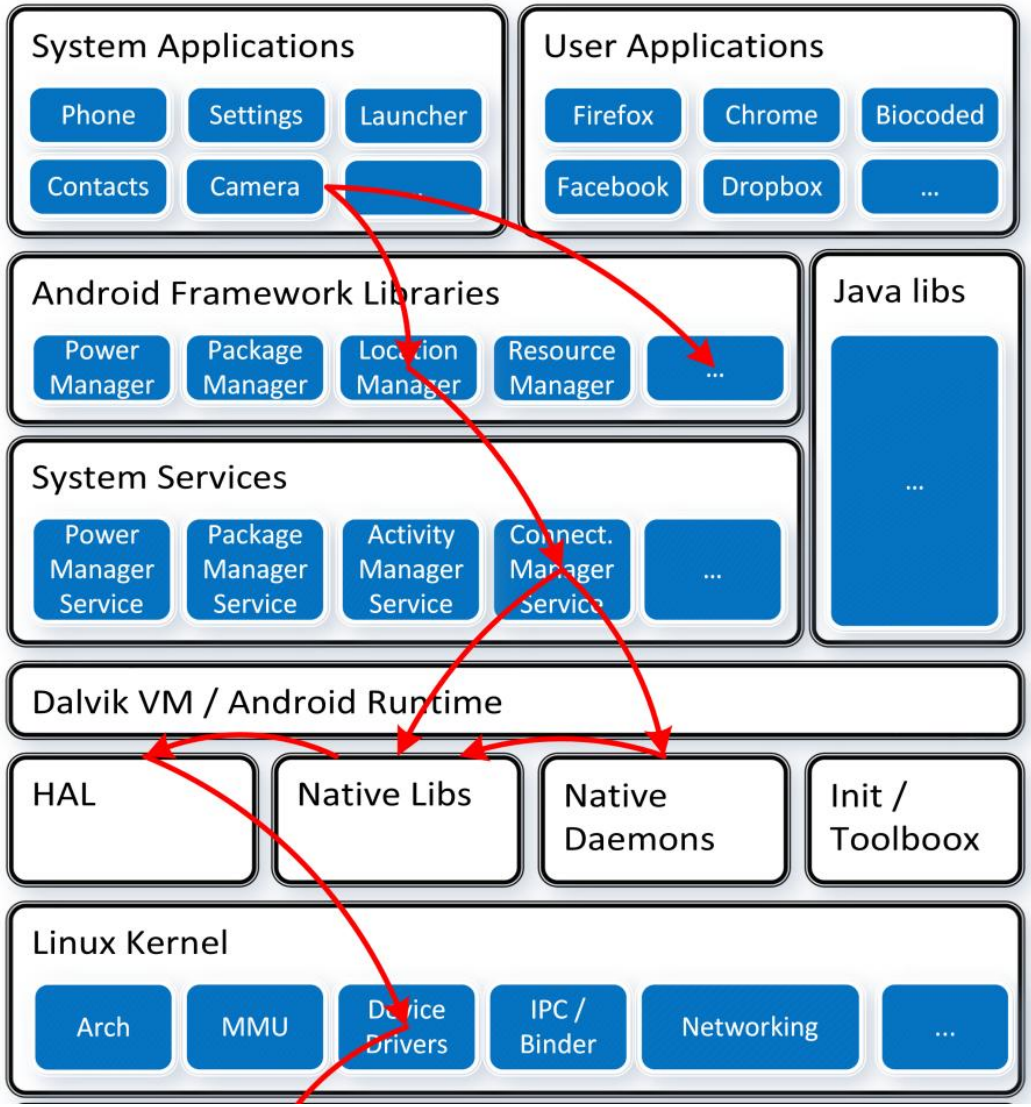
Above average phone stack

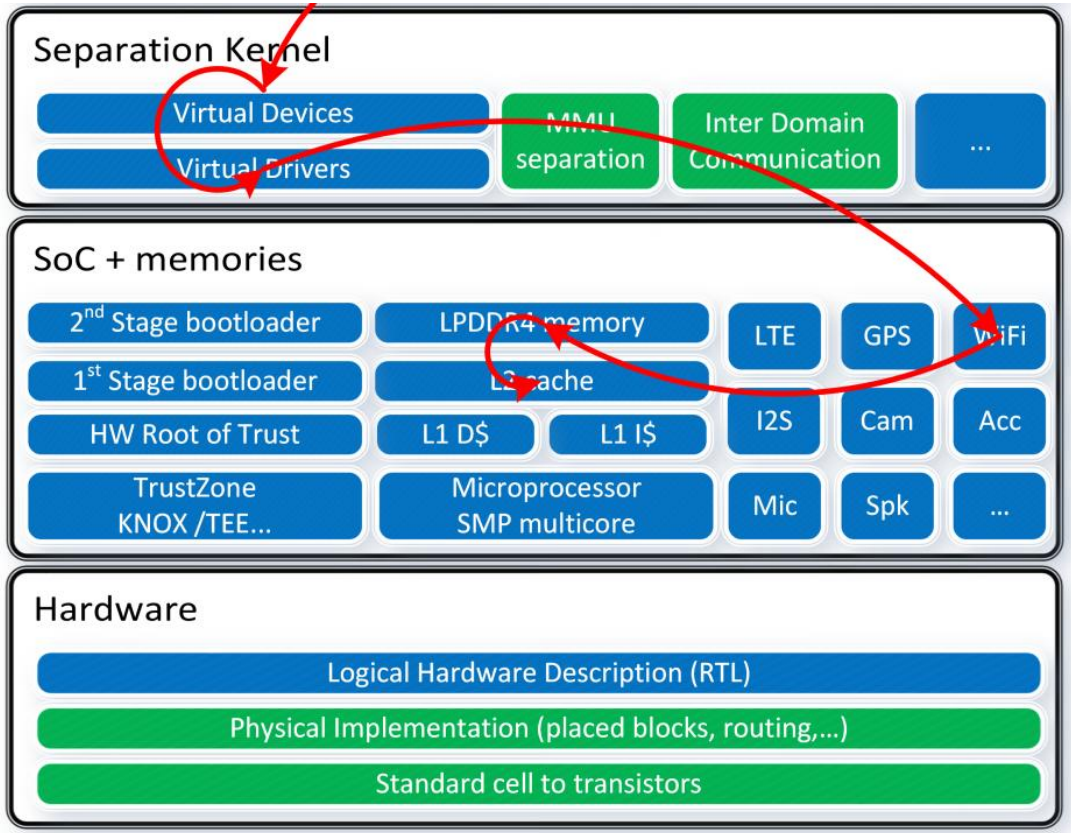




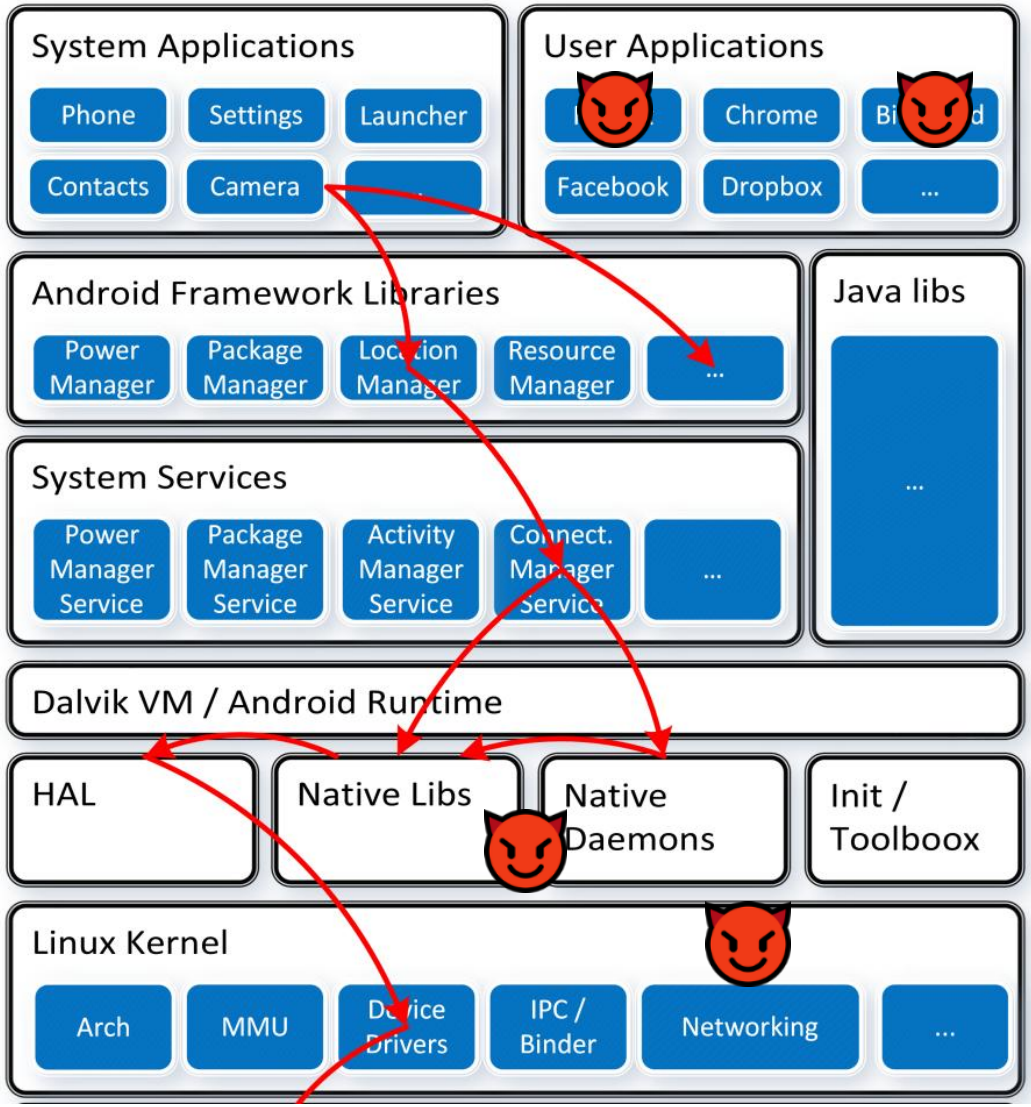
BEYOND SEMICONDUCTOR

Above average phone: Let's take a picture…





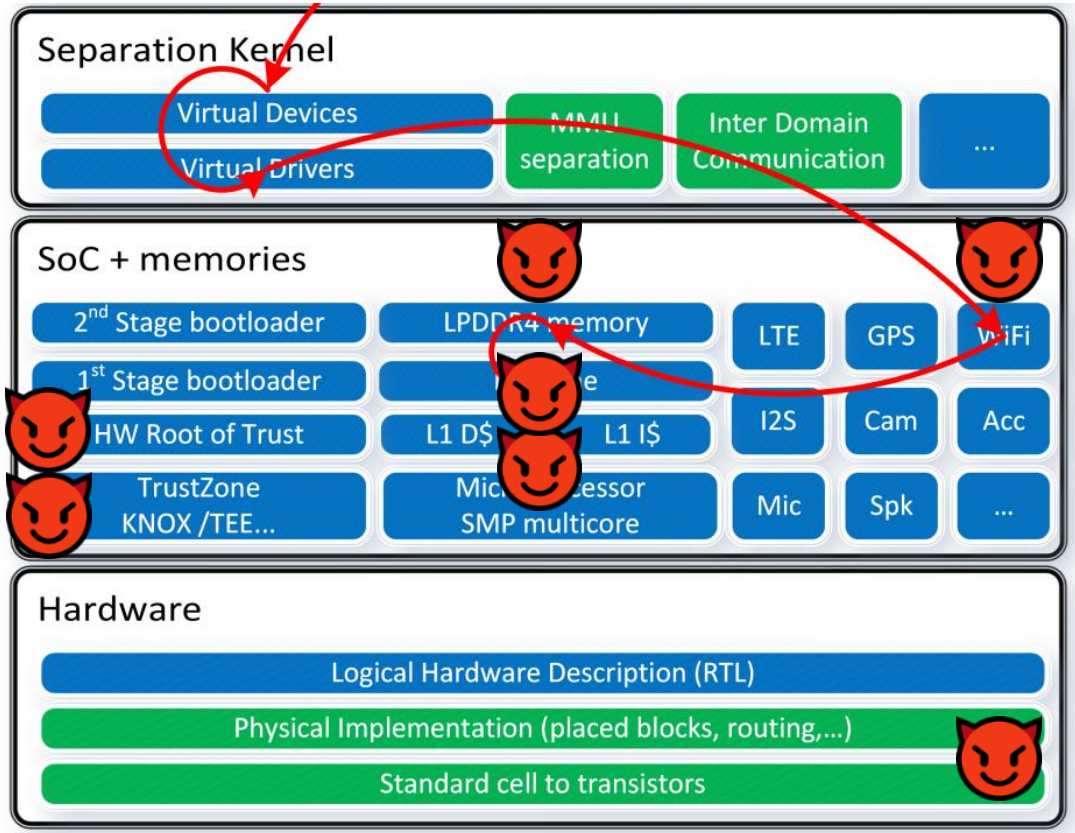
Above average phone: Let's take a picture…



What could ever go wrong ?

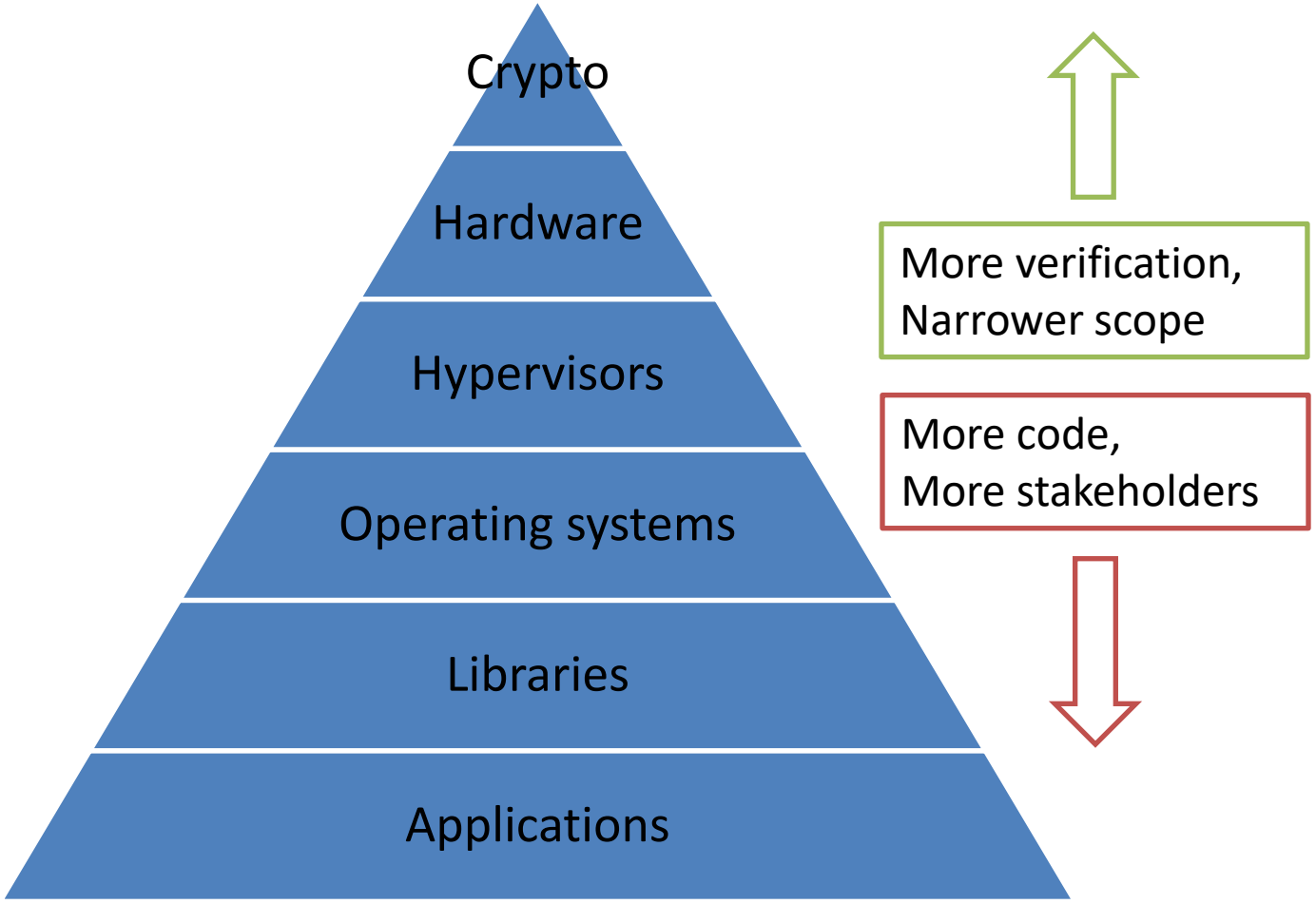
9 CVE's in April – June 2019

Based on presentation prepared by Beyond in June 2019, selection of issues.

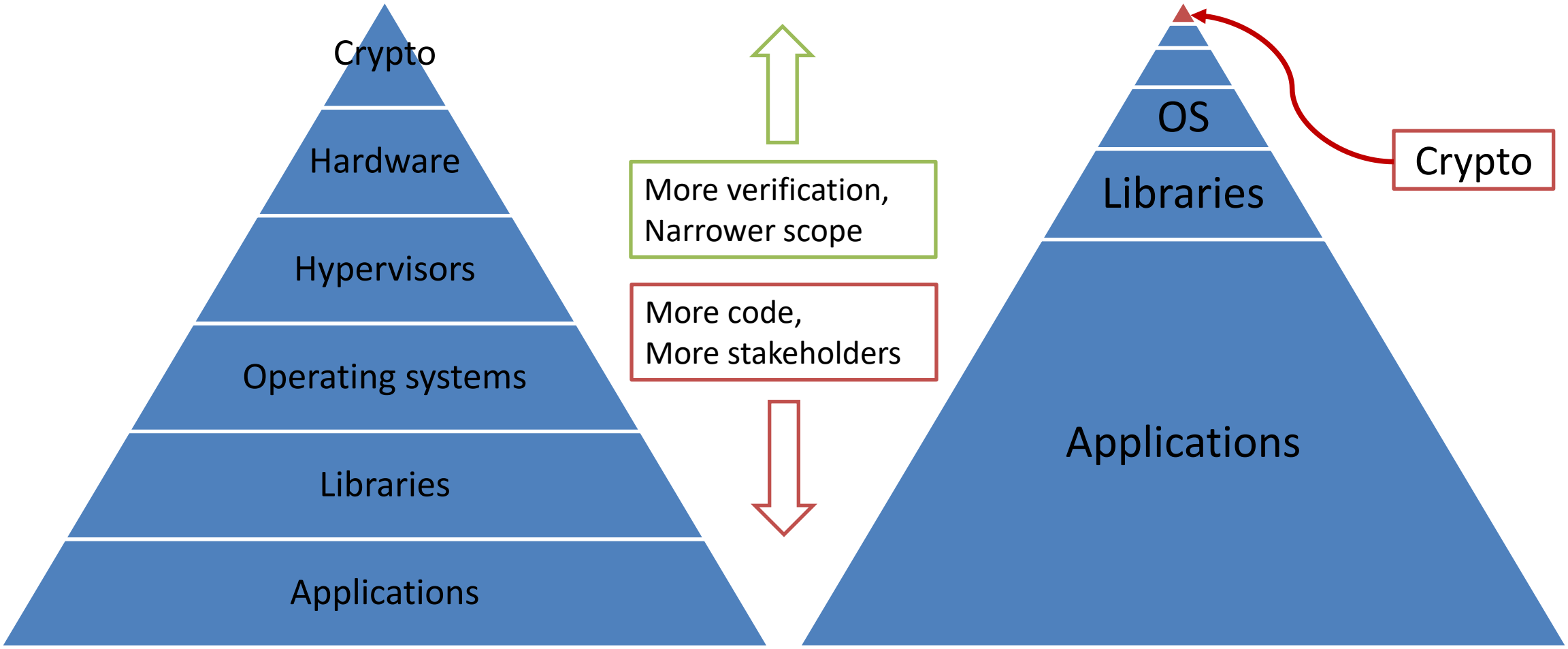


BEYOND SEMICONDUCTOR

Attack Surface / Risk

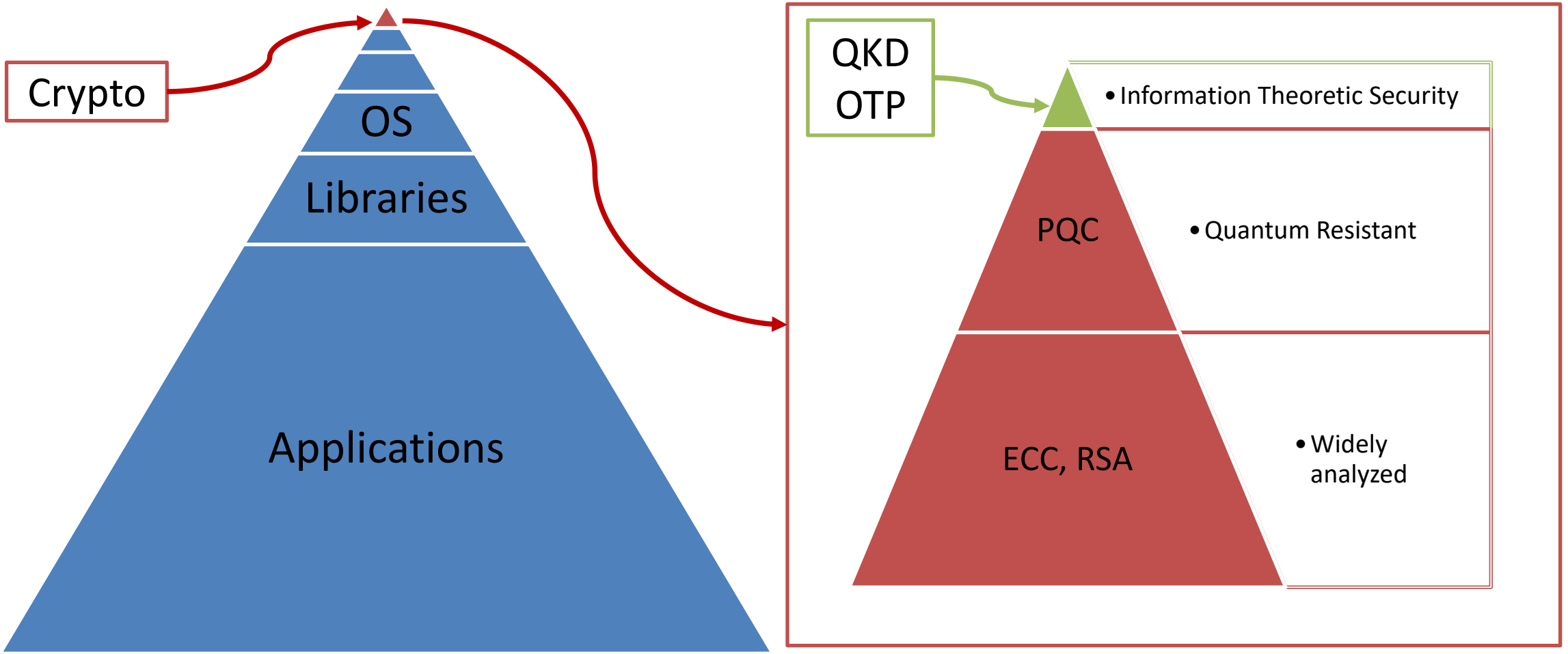


Attack Surface / Risk



BEYOND SEMICONDUCTOR

Attack Surface / Risk

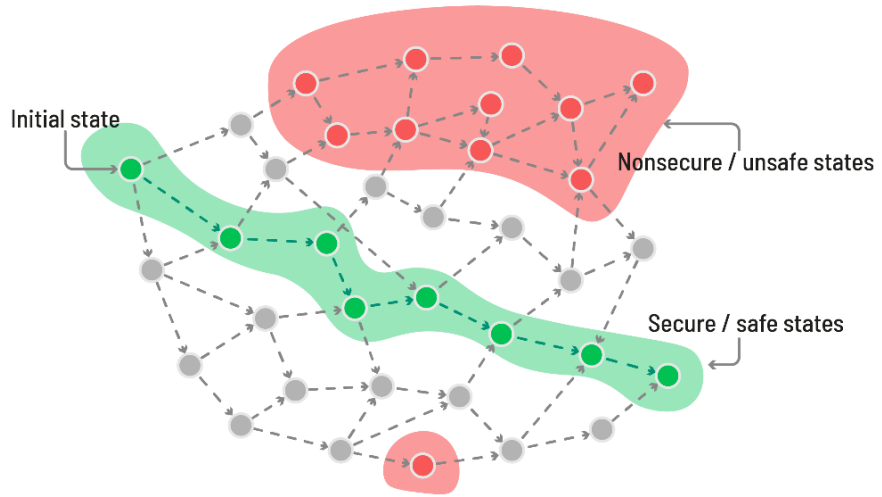


Orodja

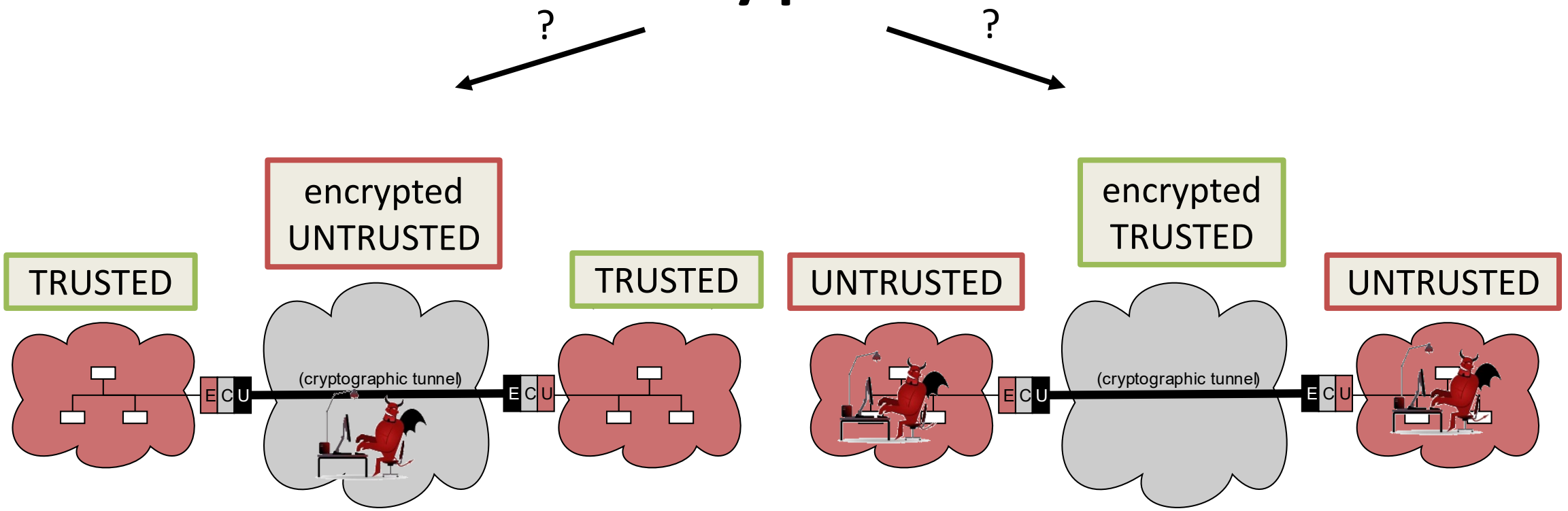
Formalne metode

- Formalna specifikacija
  - Matematično formulirane izjave
- Formalna verifikacija
  - Matematičen dokaz (npr. z dedukcijo)
- Običajno strojno preverjeni

- Da bi bili “prepričani” je potrebno preveriti vsa možna stanja
- Symbolično proti izčrpnemu (brute force)



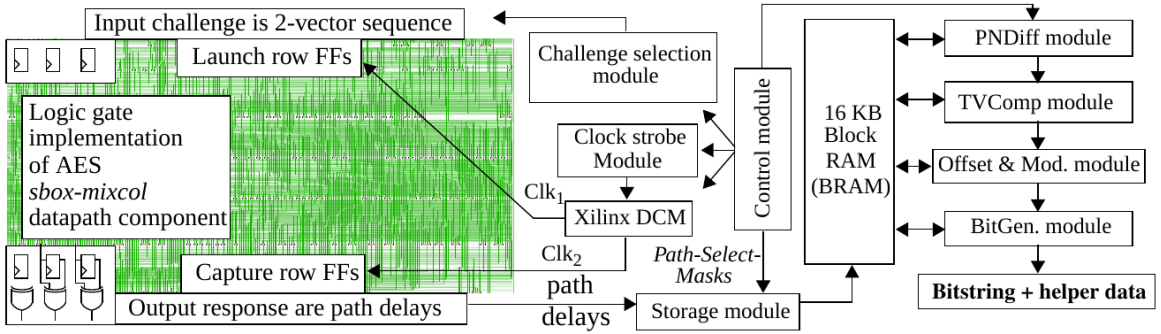
Crypto

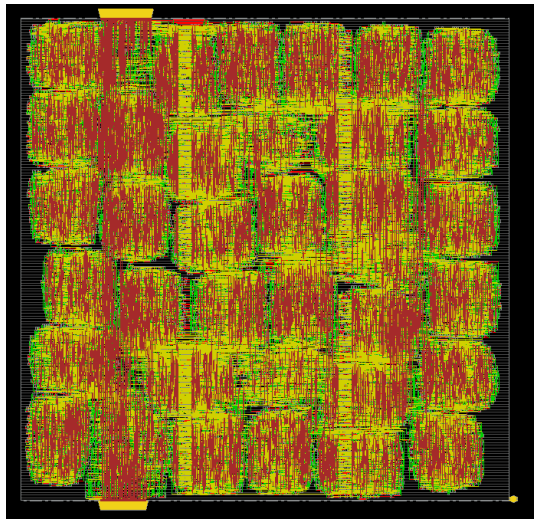


BEYOND SEMICONDUCTOR

PUF

PUF - Physically Uncloneable Function





CONPARF
22nm FD SOI
implementacija
PUF

- Fizična zaščita vrednosti
- Ob poskusu meritve se vrednost spremeni
- Močen vs. šibek PUF
- Uporaba za zaščiteno shranjevanje KEK-ov (običajno majhnega števila kriptografskih ključev)
- CONPARF implementacija Physically Uncloneable Function

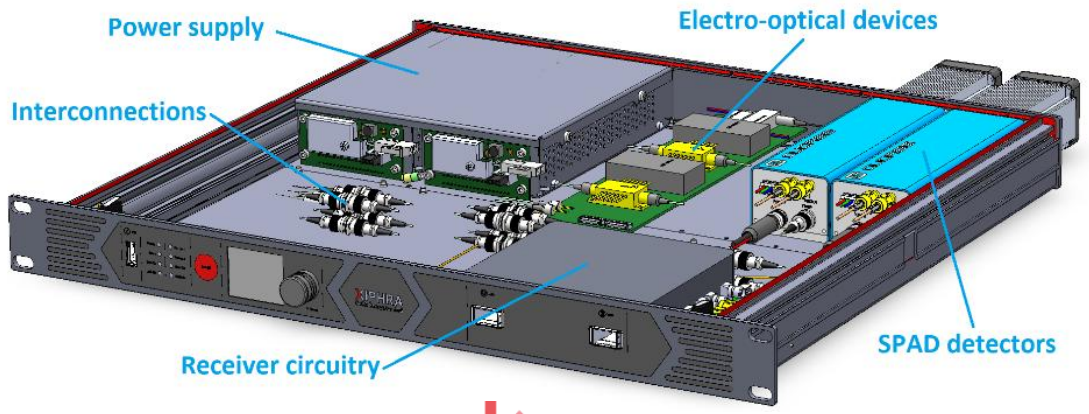
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA GOSPODARSTVO, TURIZEM IN ŠPORT
NAČRT ZA OKREVANJE IN ODPORNOST
Financira Evropska unija
NextGenerationEU

BEYOND SEMICONDUCTOR

Quantum “Magic” Powers

QKD: IT secure communication

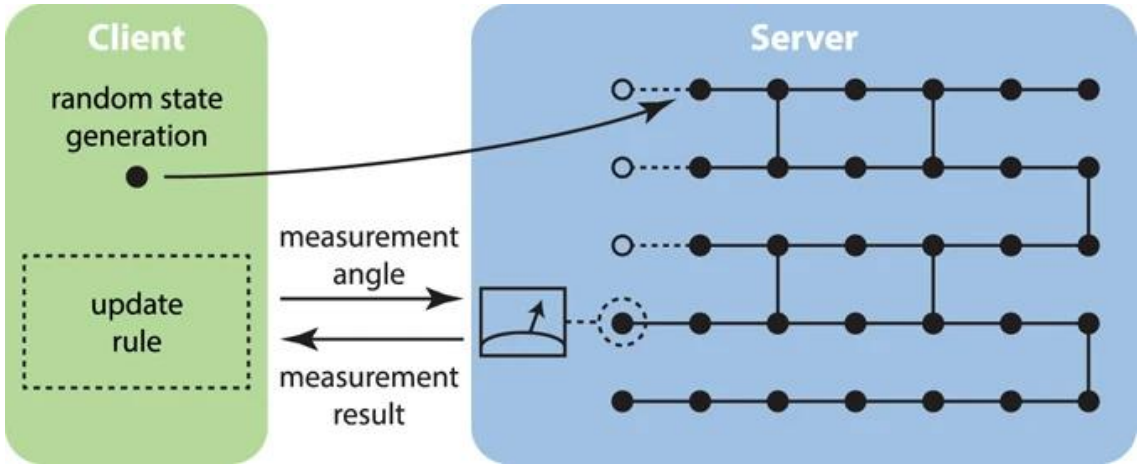
- Assumes only Quantum Mechanics and Information Theory
- Compromises **availability**, improves most trusted part of cybersecurity (crypto)
- Narrow use cases around long term sensitive secrets. **Step towards Quantum Internet**



SiQUID

UBQC: IT secure computation

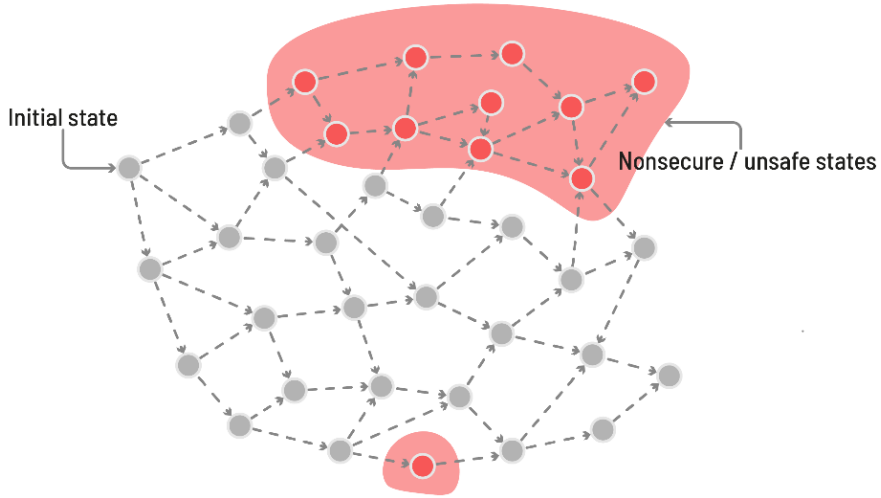
- Untrusted (quantum) server
- Confidentiality and integrity of clients computation
- No quantum memory, quantum computation required on client



REFERENCE: https://doi.org/10.1038/s41534-017-0025-3

BEYOND SEMICONDUCTOR

Varnost (safety)



Vprašanja?

Varnost (security)

Shitterstock.com
https://www.google.com/imgres?q=unsafe%20knife%20position&imgurl=https%3A%2F%2Fwww.shutterstock.com

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

Nove obvezne zahteve kibernetske varnosti za povezljive proizvode

Davorin Kacian, predavatelj, Slovenski institut za kakovost in meroslovje, Ljubljana

Davorin Kacian

Nove obvezne zahteve kibernetske varnosti za povezljive proizvode (EN 18031)

EN 18031 – uvod v nove obveznosti

Ko val napadov postane resničnost, postane ključno zaščititi povezljive izdelke digitalnega sveta, saj:

- EN 18031 uvaja enotne varnostne zahteve za povezljive izdelke v EU
- standard odgovarja na naraščajoče grožnje kibernetskih napadov,
- spodbuja varnost po zasnovi in odgovorno upravljanje tveganj,
- krepi zaupanje uporabnikov v varne digitalne tehnologije.

Namen in področje uporabe EN 18031

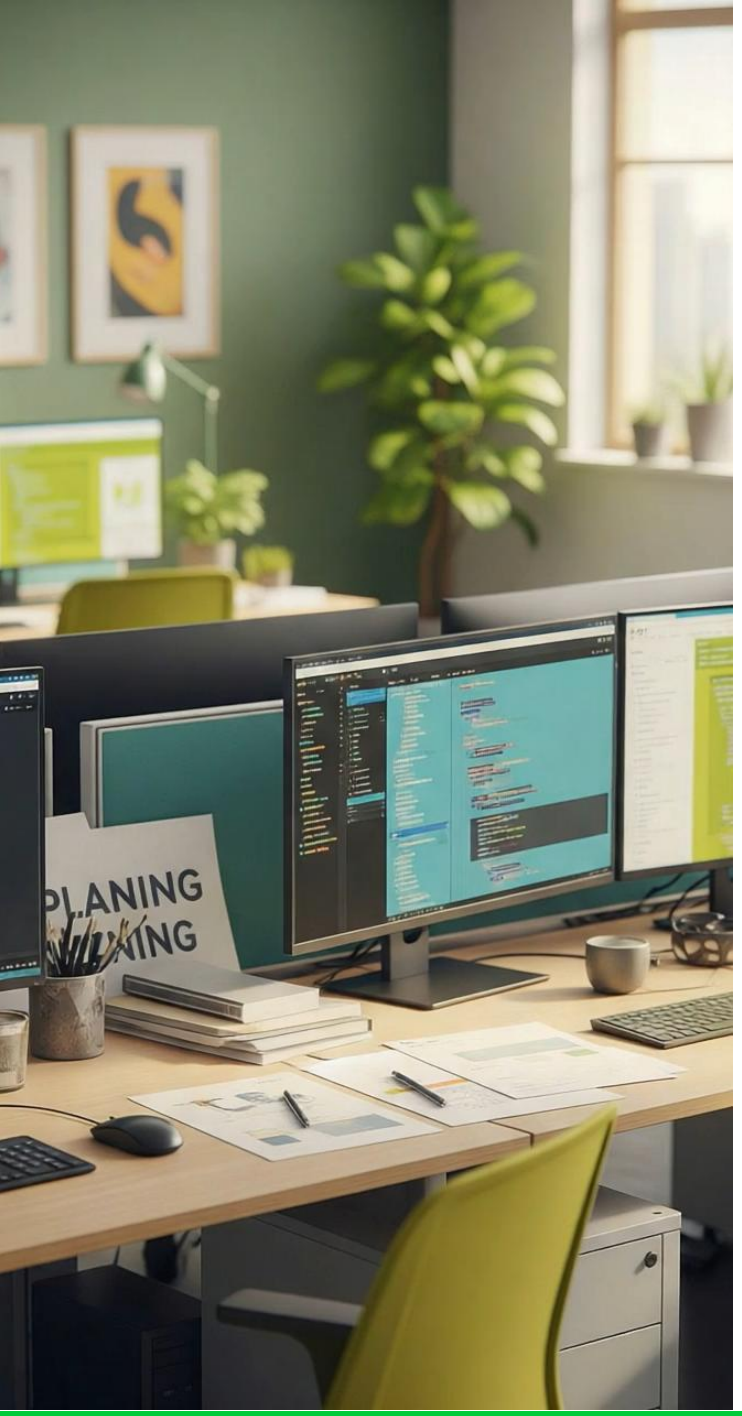
Standard določa varnostne zahteve in področje uporabe za povezljive izdelke, ker:

- zajema strojne, programske in hibridne naprave,
- nanaša se na potrošniške in industrijske IoT sisteme,
- uporablja se v fazi zasnove, razvoja in vzdrževanja,
- zagotavlja odpornost izdelkov na kibernetske grožnje.

Temeljna načela kibernetske varnosti

Standard temelji na načelih, ki zagotavljajo zaupanje in varnost, saj:

- spodbuja varnost po zasnovi (security by design),
- vključuje zaščito zasebnosti in integritete podatkov,
- določa zahteve za overjanje, avtorizacijo in šifriranje,
- zahteva pregledno upravljanje tveganj.



Varnost v fazi zasnove, razvoja in proizvodnje

Celoten življenjski cikel izdelka mora biti pod nadzorom varnosti, zato:

- varnostne funkcije morajo biti načrtovane že od začetka,
- razvoj zahteva nadzor dostopa in preverjanje pristnosti,
- preprečiti je treba vstavljanje zlonamerne kode,
- vse spremembe morajo biti dokumentirane in potrjene.

Upravljanje ranljivosti in varnostnih posodobitev

Nenehno obvladovanje ranljivosti je ključno za ohranjanje varnosti izdelkov, ker:

- proizvajalec mora imeti načrt za prepoznavanje in odpravo ranljivosti,
- posodobitve morajo biti kriptografsko zaščitene in preverljive,
- uporabnikom je treba omogočiti varno nameščanje nadgradenj,
- potrebno je vzpostaviti sistem za prijavo varnostnih težav.

Dokumentacija in presoja skladnosti

Dokumentacija in presoja skladnosti dokazujeta izpolnjevanje varnostnih zahtev, saj:

- vključujeta opis arhitekture in varnostnih funkcij,
- presoja zajema testiranje odpornosti na grožnje,
- rezultati se evidentirajo v tehničnem dosjeju,
- dokumentacija predstavlja osnovo za oznako CE.

Povezava z drugimi standardi kibernetske varnosti

EN 18031 dopolnjuje mednarodne standarde in povezuje tehnične zahteve, saj:

- uporablja smernice iz ISO/IEC 27400 o odpornosti IoT sistemov,
- opira se na ETSI EN 303 645 za potrošniške IoT naprave,
- razširja tehnične zahteve in zagotavlja njihovo uporabo v EU,
- povezuje tehnične in regulativne okvire v enotno strukturo.

Uporaba v praksi in priložnosti za industrijo

Usklajenost z EN 18031 prinaša obveznosti, hkrati pa tudi priložnosti za rast, saj:

- podjetja, ki zgodaj uvedejo skladnost, pridobijo zaupanje uporabnikov,
- varni izdelki postajajo konkurenčna prednost na trgu,
- standarda EN 18031 in ETSI EN 303 645 spodbujata trajnostni razvoj,
- skladnost postaja temelj inovativnih in varnih tehnologij.

Zaključek

EN 18031 predstavlja ključen korak k večji kibernetski varnosti, ker:

- združuje tehnične, organizacijske in regulativne zahteve,
- krepi zaupanje uporabnikov v varnost povezanih naprav,
- proizvajalcem omogoča dokazovanje skladnosti na enoten način,
- postavlja temelje za trajnostno in varno digitalno okolje.

Vprašanja?

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

Raziskovanje kibernetskih groženj in deljenje informacij

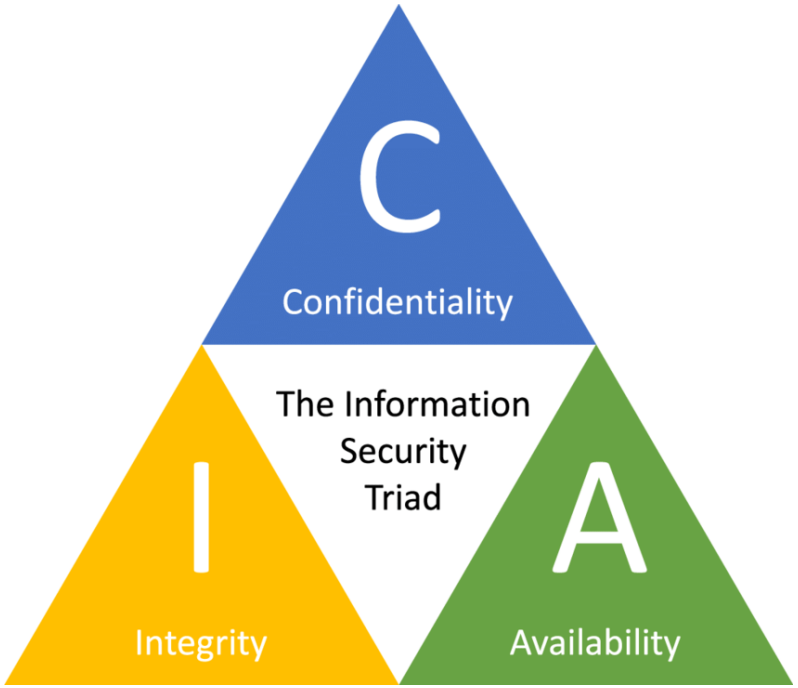
Metod Platiše,
Telekom Slovenije d.d.

Kaj so kibernetske grožnje?

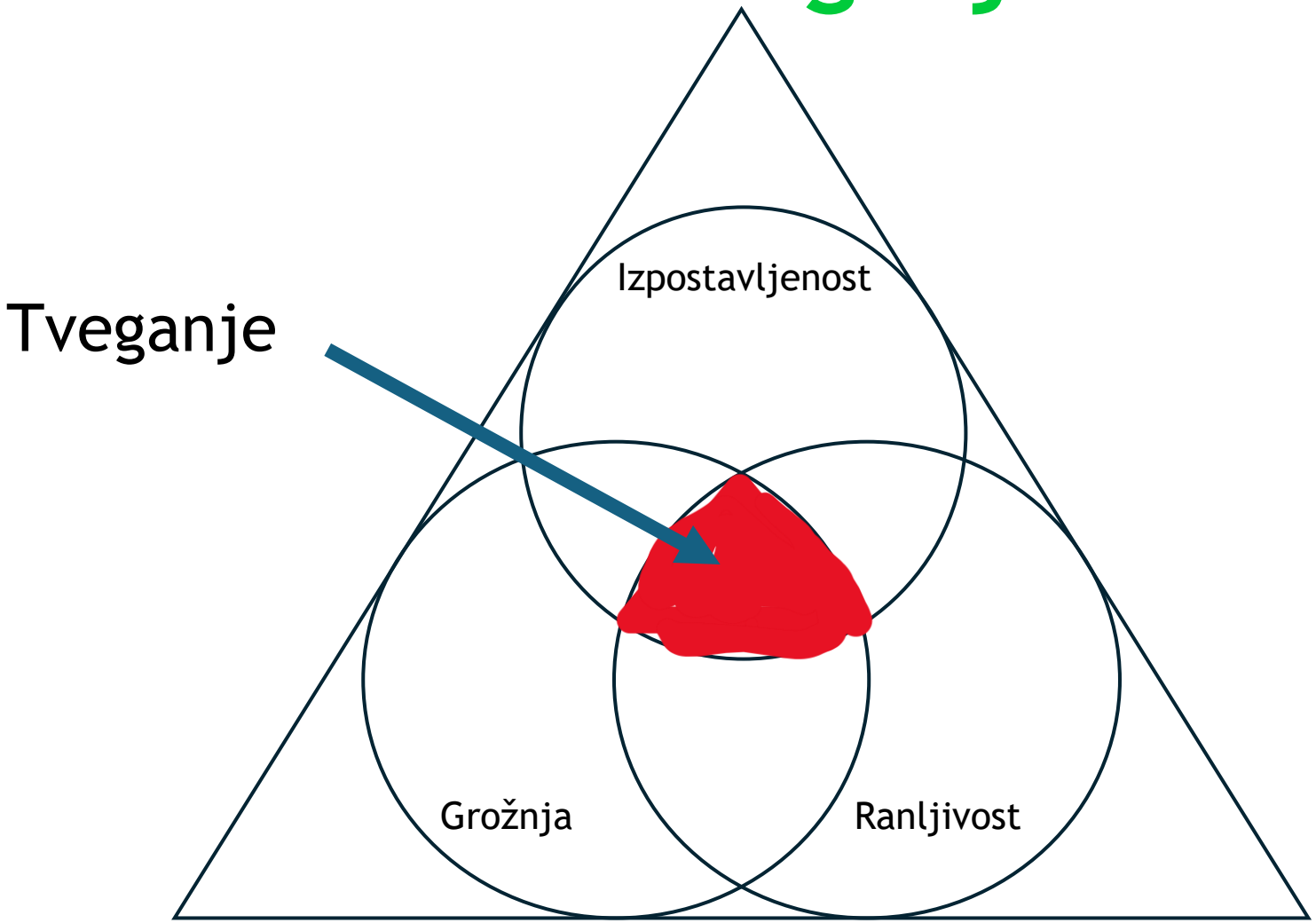
Vse kar ogroža katerikoli atribut informacijske varnosti.

Elementi grožnje:

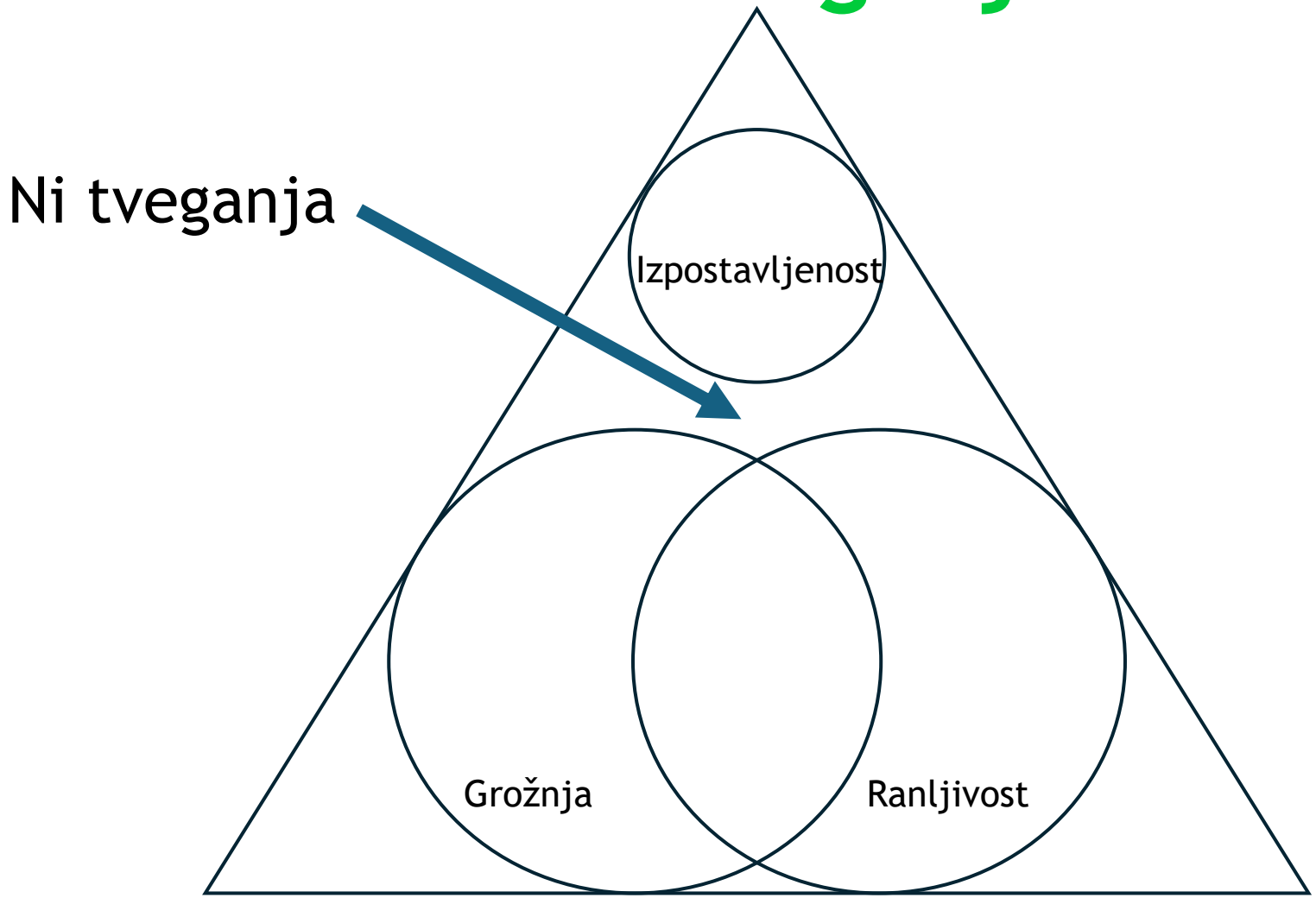
- Napadalec (kdo)
- Cilj in učinek (kaj, koliko)
- Motivacija (zakaj)
- Sredstva, načini, sposobnosti (kako, s čim)



Kaj pa kibernetska tveganja?



Kaj pa kibernetska tveganja?



Uporabniki kot tveganje

Na uporabnike preži:

- Phishing
- CEO prevara
- Ukraden račun

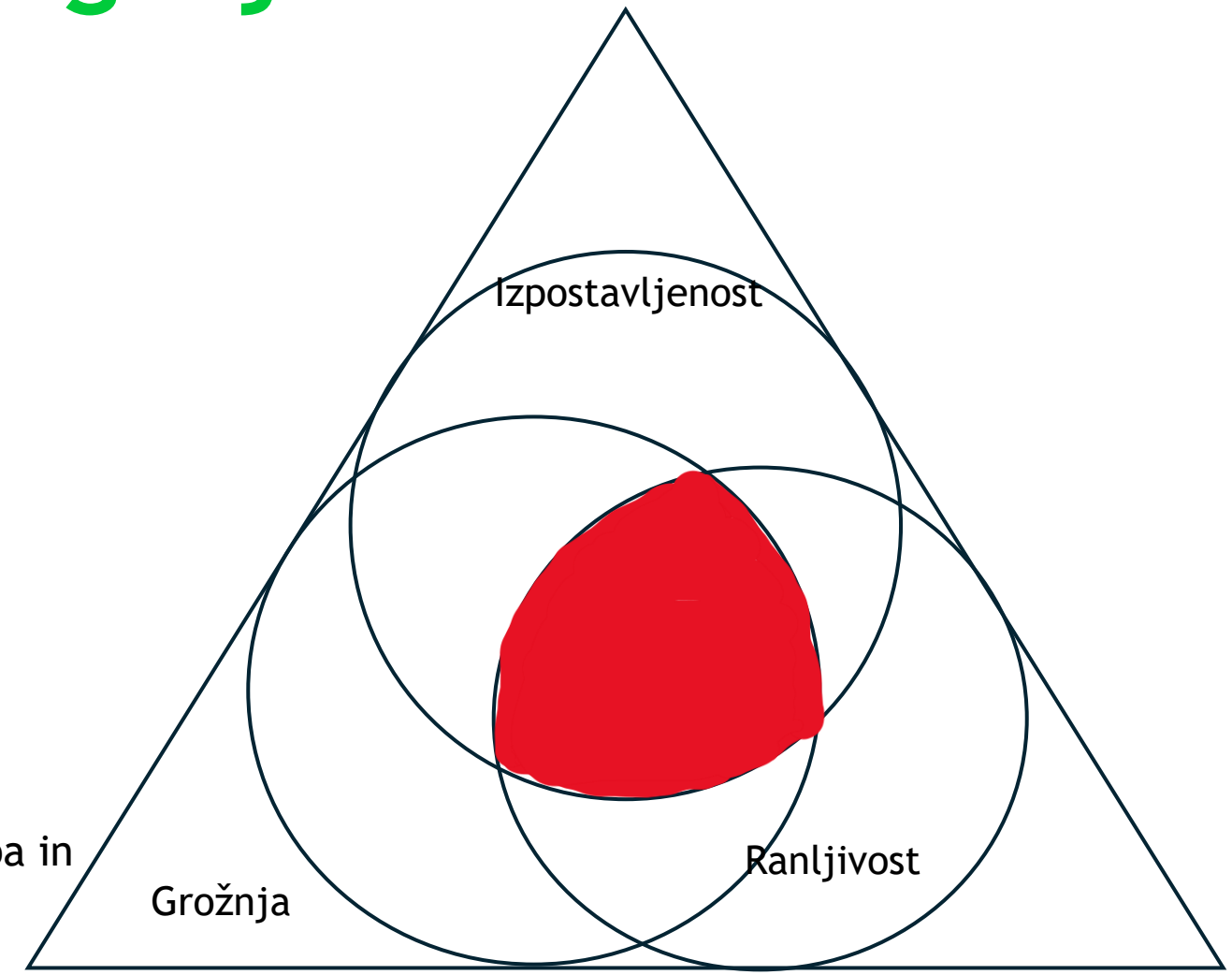
Na grožnjo ne moremo vplivati, lahko jo zaznamo in vplivamo na izpostavljenost in ranljivost

Primer velikega tveganja:

- Neozaveščen uporabnik, nobenih omejitev pri dostopu do interneta.
- Neozaveščen uporabnik, ni antispam filtra.

Primer majhnega tveganja:

- Neozaveščen uporabnik, nima internet dostopa in maila.



Zmanjšanje kibernetskih tveganj

Prepoznajte in zmanjšajte ranljivosti:

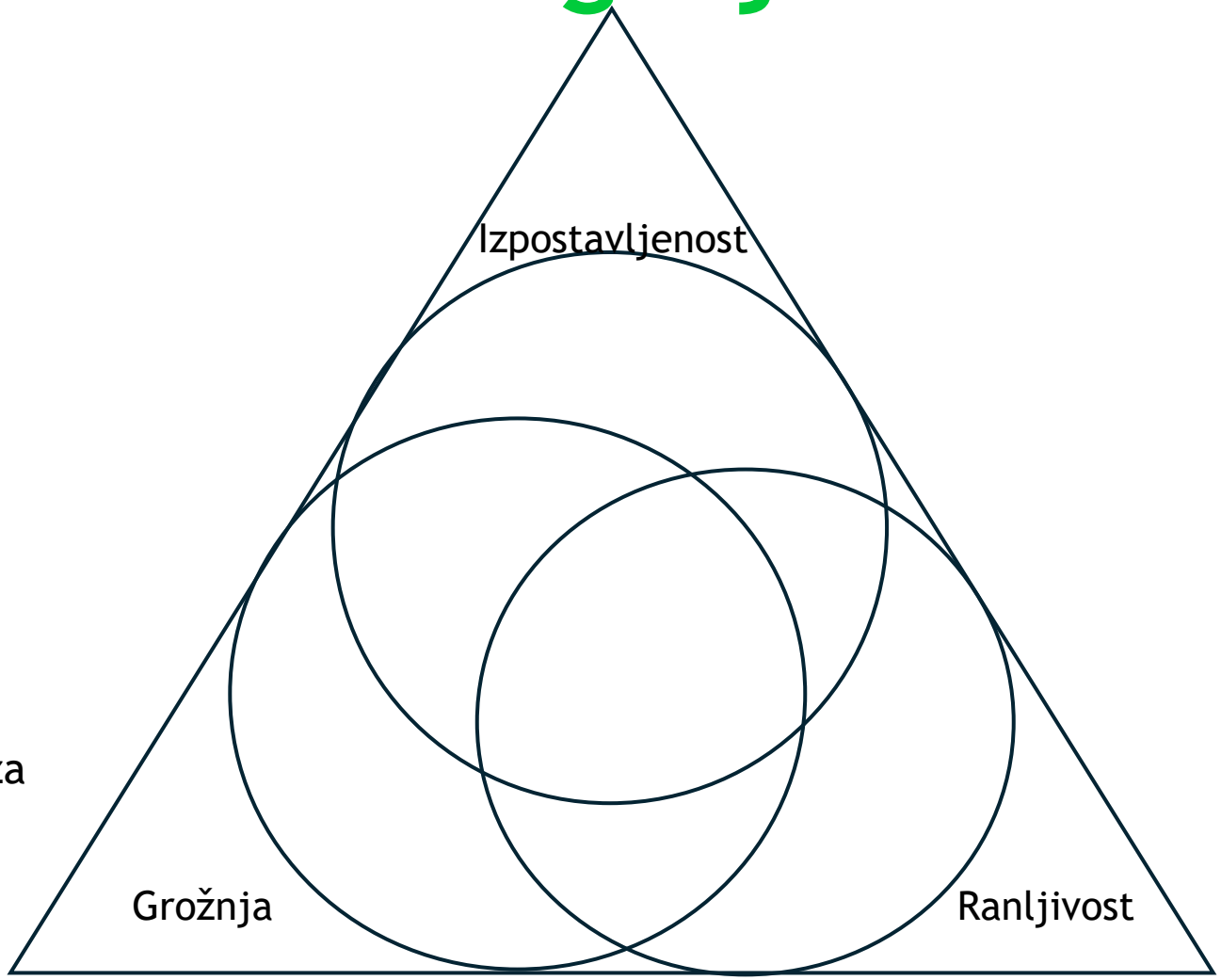
Redno izvajajte preglede ranljivosti, nameščajte popravke, utrjujte konfiguracije, da zmanjšate šibkosti v vaših sistemih.

Omejite izpostavljenost:

Uvedite segmentacijo omrežja, ustrezne varnostne kontrole, ukrepe za zmanjšanje tveganj, nadzor dostopa ter omejite nepotrebne storitve in promet.

Pripravite se na grožnje:

Bodite obveščeni o novih grožnjah prek storitev za obveščanje o grožnjah, izobražujte zaposlene o varnostni ozaveščenosti in vzpostavite učinkovit načrt odziva na incidente.



Ranljivosti

Bistvo razumevanja kibernetskih ranljivosti je v tem, da jih ne smemo gledati samo kot tehnične napake v sistemu, ampak kot posledico širših dejavnikov: sistemskih, tehničnih, procesnih in človeških:

- Sistemske: kompleksnost IKT arhitektur, medsistemske povezave, hibridna in večoblačna okolja, IT-OT povezanost, slaba politika varnosti.
- Tehnične: napake v programski kodi, nepravilne konfiguracije, zastarela programska oprema brez popravkov, odvisnosti in komponente tretjih, slabo upravljanje oblačnih in hibridnih sistemov, APIjev.
- Procesne: neposodabljanje, neustrezno upravljanje sprememb, neustrezno načrtovanje in uvajanje, neizvajanje varnostnih politik, pomanjkanje nadzora, počasno in neustrezno odzivanje.
- Človeške: napake uporabnikov in skrbnikov, zlonamerne aktivnosti, neozaveščenost.

Znane ranljivosti

Organizacija MITRE upravlja sistem registracije ranljivosti

CVE: Common Vulnerabilities and Exposures

Ranljivosti prijavljajo organizacije, poblaščene s strani MITRE, t.i. CNA (CVE Numbering Authority), ki dodeljujejo CVE ID-je, preverjajo in potrjujejo verodostojnost ranljivosti, objavljajo informacije v javni CVE bazi. CNA so proizvajalci SW in HW opreme, vladne organizacije, raziskovalne organizacije, trenutno jih je 450

Organizacija FIRST upravlja sistem ocenjevanja ranljivosti CVSS

Common Vulnerability Scoring System SIG

CVSS običajno dodajajo CNAji ali pa NIST/NVD

MITRE prav tako upravlja sistem registracije napak CWE, ki povzročajo ranljivosti CWE - Common Weakness Enumeration

CWE (vzrok) → CVE (posledica) → CVSS (ocena tveganja) → NVD (objava).

Znane ranljivosti v EU

Vzpostavljen je tudi evropski sistem registracije ranljivosti European Union vulnerability database Home | EUVD, ki povzema CVE in dodaja evropski kontekst.

Lastnost	MITRE/CVE	ENISA/EUVD
Namen	Globalni standard za identifikacijo ranljivosti	Evropski register s poudarkom na skladnosti in koordinaciji
Upravljavec	MITRE Corporation (ZDA)	ENISA (EU agencija)
Povezava	Root CNA in globalni register	Regionalni CNA in dopolnilna baza
Identifikator	CVE-ID (npr. CVE-2025-12345)	Drugačen CVE-ID, vezan na MITRE CVE, z dodatnimi EU metapodatki
Poudarek	Tehnični opis in resnost (CVSS)	Vpliv na evropske sektorje, CRA, NIS2

0-day ranljivosti

Bug Bounty

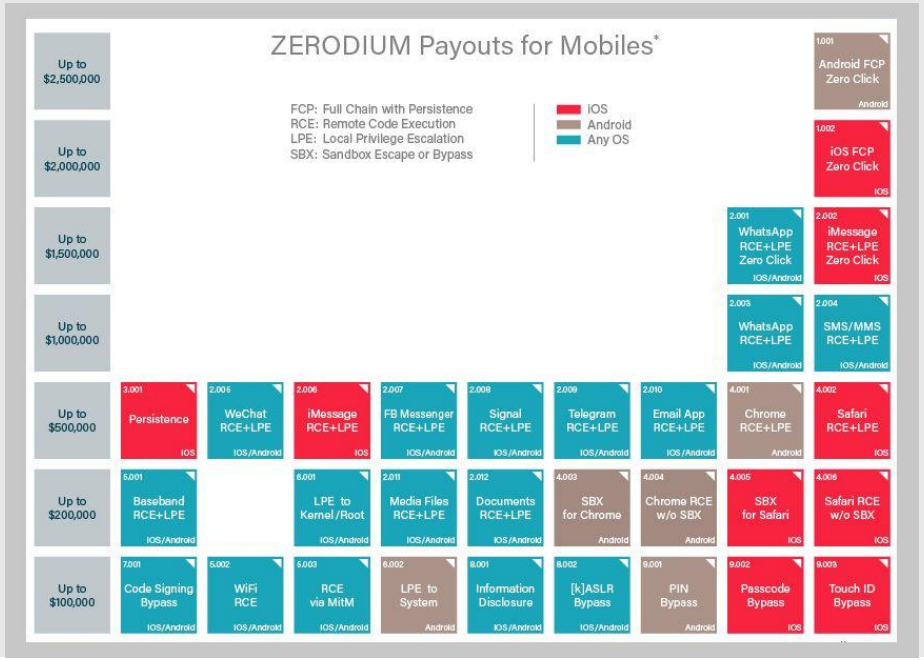
[Bug Bounty Platform | HackerOne]
[Managed Bug Bounty | Bugcrowd]
[Bug Bounty Services | Find & Fix Vulnerabilities | Intigriti]
[Google Bug Hunters - Google Bug Hunters]
[Microsoft Bounty Programs | MSRC]

Dark web

Abacus Market ,Russian Market
BriansClub, STYX / Styx Market,
TorZon, BidenCash,
WeTheNorth, Exodus, Awazon Market

Gray players

Spletna stran 2019



Spletna stran 2025

Digitalna identiteta in lastnina organizacije

TelekomSlovenije

Zaščita digitalne identitete in lastnine organizacije (Brand intelligence) pomeni zbiranje, analiziranje in preprečevanje zlorab identitete organizacije na digitalnih platformah, ki vključuje:

- Naziv in opis organizacije, logotipi, vizualije.
- Spletne strani, socialna omrežja.
- Spletne domene, mail domene, certifikati.
- Repositoriji kode.
- Mobilne aplikacije.
- VIP osebe, CxO.
- Omembe na dark web forumih.

Identitete in poverilnice oseb

Zaščita identitet in poverilnic (Identity Intelligence) je naslednji logični sklop CTI mozaika, usmerjen v uporabniške identitete, poverilnice in dostopne pravice, ki vključuje:

- Spremljanje digitalnih identitet, zaznavanje ukradenih poverilnic.
- Zaznavanje zlorabljenih dostopnih žetonov in API ključev.
- Spremljanje virov na temnem spletu, tržnicah in forumih.
- Zaznavanje nelegitimne uporabe prijavnih računov, ugotavljanje akterjev in namenov.
- Ugotavljanje načina kompromitacije poverilnic.
- Ocenjevanje kritičnosti kompromitiranih računov in prioritizacija ukrepov.

Podatki o ukradenih poverilnicah se pogosto reciklirajo, kar pomeni da se isti podatki pojavljajo v vedno novih zbirkah in to povzroča lažno pozitivne zaznave

Akterji

Akterji so posamezniki, skupine ali organizacije, ki izvajajo kibernetske napade. Groups | MITRE ATT&CK®

Atributi s katerimi jih opišemo

- Kategorija; kibernetski kriminalci, APT/državni, notranji, haktivisti, industrijski vohuni…
- Motivacija; denar, onesposobitev, poslovne informacije.
- Sposobnosti; začetniki, profesionalci, APT.
- TTP (taktike/tehnike/postopki), Matrix - Enterprise | MITRE ATT&CK®
- Geografski obseg, industrijski fokus (operativne lastnosti).

Določanje akterjev (atribucija)

- Uporabljeni TTPjev
- Infrastruktura in IOCji; domene, IP naslovi, hashi, lastnosti zlonamerne kode
- Operativne značilnosti, časovne povezave

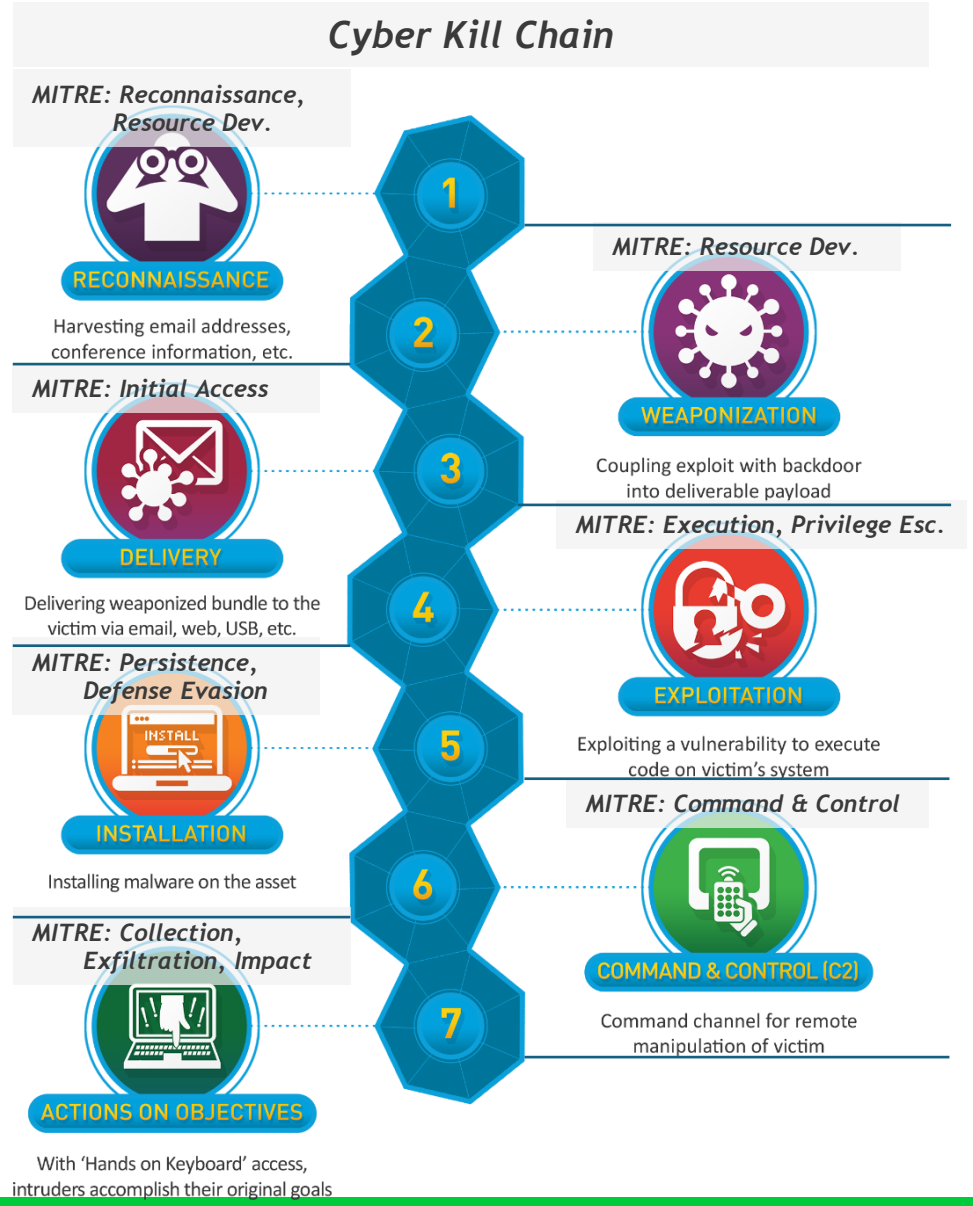
Določitev akterjev in ozadja je zahtevna naloga.

Dogodke zaznavamo tudi v svojem okolju

TelekomSlovenije

Faze zaznavanja

- Zaznava dogodkov se izvaja avtomatsko (SIEM, EDR, NDR, CTI) ali ročno (administrator, uporabnik), sproži se alarm.
- Triaža; preverjanje relevantnosti (false, true positive), določanje kritičnosti.
- Klasifikacija; razvrstitev dogodka glede na tip, vektor, učinek, resnost.
- Analiza in obogatitev; povezava z znanimi IOC, TTP (MITRE ATT&CK),preverjanje, določanje kampanje in akterja.
- Deljenje; priprava strukturiranega poročila ali STIX/MISP zapisa, označevanje z TLP, stopnja zanesljivosti in zaupanje.



Zakaj deliti informacije ?

Koristi deljenja lastnih zaznav:

- Preprečevanje širjenja napadov s tem, ko druge organizacije obvestimo o dogodku in se te lahko pravočasno pripravijo, s čimer zmanjšajo verjetnost, da bodo same postale tarča ali ublažitev učinka, če so že napadene.
- Skladno z regulativo morajo zavezanci poročati o incidentih pristojnim organom, ni pa nujno deljenje skupnosti, vendar deljenje omogoča tudi ostalim organizacijam, da pravočasno identificirajo incident in ustrezneje poročajo.
- Skupno znanje in razumevanje groženj, prepoznavanje trendov, situacijsko zavedanje ki se gradi s povezovanjem, analiziranjem in dopolnjevanjem informacij iz več virov.
- Krepitev zaupanja med organizacijami, kar spodbuja sodelovanje in omogoča skupne obrambne strategije, ki so bolj učinkovite kot posamični izolirani pristopi.
- Krepitev zaupanja partnerjev, naročnikov in javnosti s pravočasnim in celovitim obveščanjem.

Zakaj jih ne delimo ?

Ovire (ne moremo), zadržki (ne vemo ali bi) in izzivi (ne vemo kako bi) :

- Pravne in regulatorne omejitve
  - Varovanje poslovnih skrivnosti
  - Pogodbene omejitve dobaviteljev, partnerjev
  - GDPR/ZVOP-2 omejuje uporabo osebnih podatkov
- Organizacijske in poslovno-kulturne ovire
  - Nezaupanje, konkurenčnost
  - Strah pred izgubo ugleda, slabe stvari držimo zase
  - Pomanjkljive notranje politike
- Procesni izzivi
  - Nedefinirani in nejasni postopki
  - Pomanjkanje ljudi in časa, preplavljenost z dogodki
  - Ni povratne informacije o koristi delitve
- Psihološki in osebni zadržki
  - Strah pred krivdo, nezaupanje v delovanje skupnosti in zaščito podatkov
- Mednarodni in čezsektorski izzivi
  - Različni pravno-regulatorni okvirji, interoperabilnost taksonomij, jezikovne in terminološke razlikec

Uspešno in učinkovito deljenje

Za uspešno in učinkovito deljenje upoštevajmo:

- Pravna in regulatorna skladnost, kaj moramo, kaj lahko in pod kakšnimi pogoji in kaj ne smemo.
- Opredelitev namena, obsega deljenja, ureditev notra
- Anonimizacija ali pseudonimizacija osebnih podatko
- Vzpostavitev in vključitev v skupnosti, opredelitev n
- Varnost prenosa, dostopa in hrambe informacij (TLP
- Kakovost, točnost, (domneva, sum, potrjeno), razši
- Standardna struktura informacij (TAXII).
- Uporaba uveljavljenih tehnoloških platform (STIX, M


```
"type": "observed-data",
"id": "observed-data--a1b2c3d4-5678-90ef-ghij-1234567890ab",
"created": "2025-10-26T10:30:00Z",
"modified": "2025-10-26T11:00:00Z",
"first_observed": "2025-10-26T08:43:00Z",
"last_observed": "2025-10-26T09:00:00Z",
"number_observed": 1,
"objects": {
    "0": {
        "type": "ipv4-addr",
        "value": "45.83.22.104"
    },
    "1": {
        "type": "url",
        "value": "hxxp://login-portal-auth[.]net/update"
    }
},
"labels": [
    "phishing",
    "initial-access"
],
"confidence": 70,
"extensions": {
    "tlp": "TLP:AMBER"
```


STIX opis grožnje

ALiEnS-SOC

Artificial Intelligence for Slovenian Electro-Energy Sector Security Operation Centre

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

The project funded under Grant Agreement No. 101190349 is supported by the European Cybersecurity Competence Centre.

Why Cybersecurity Matters in the Electro-Energy Sector

THE ENERGY BACKBONE OF THE DIGITAL WORLD

Electricity powers every part of modern life - from hospitals to finance and transport.

The grid has become a digital ecosystem, merging IT and OT systems that must stay secure.

GROWING EXPOSURE TO CYBER THREATS

Rapid digitalization expands exposure to cyberattacks.

Legacy systems and complex networks make energy infrastructures vulnerable.

WHY ACTION IS URGENT

Cyber incidents can disrupt nations and critical services.

Strengthening cybersecurity in the energy sector is vital for stability, safety, and resilience.

Current Cybersecurity Landscape in the Electro-Energy Sector

WHERE WE ARE

- Slovenia's electricity system combines one national transmission operator (ELES) and several regional distribution companies supplying homes and industries.
- Together they form critical national infrastructure, essential for everyday life.
- Most already comply with basic cybersecurity standards (ISO 27001, GDPR, national legislation).

WHAT WORKS WELL

- Two Security Operations Centres (SOCs) are already active – continuously monitoring threats and incidents.
- Solid foundations for governance, compliance, and awareness are in place.
- Existing collaboration between operators and national authorities (SI-CERT, URSIV) provides a starting point for improvement.

KEY GAPS AND CHALLENGES

- Limited visibility between IT and industrial (OT) systems.
- Manual and fragmented incident response processes.
- Inconsistent maturity levels across operators.
- Insufficient sharing of threat intelligence and best practices

The **ALiEnS-SOC** project is focused on strengthening cybersecurity in Slovenia’s electro-energy Security Operations Center (SOC) - ensuring faster detection, smarter defense, and stronger resilience.

Six Work Packages Driving One Vision

WP1 - PROJECT MANAGEMENT AND COORDINATION

WP2 - ECOSYSTEM AND GAP ANALYSIS

WP3 - AI AND CTI PLATFORM DEVELOPMENT

WP4 - PILOTS AND VALIDATION

WP5 - CROSS-BORDER SOC FRAMEWORK AND BUSINESS MODEL

WP6 – COMM & DISS, AND STAKEHOLDER ENGAGEMENT

Konzorcijski partnerji

ELES

INFORMACIJSKE STORITVE IN INŽENIRING, D.O.O.
INFORMATIKA

smartis
SMART INFORMATION SYSTEMS

TIKOPRO

si·cert
National Computer Emergency Response Team

KONČAR
DIGITAL

TelekomSlovenije

elektro gorenjska

Elektro Celje

URSIV

Elektro Primorska

ELEKTRO MARIBOR

Elektro Ljubljana

ALiEnS-SOC

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Povežite se z ALiEnS-SOC !

Povežite se in bodite obveščeni na digitalnih kanalih projekta.

LinkedIn:www.linkedin.com/company/aliens-soc
X platform: www.x.com/alienssoc
YouTube: www.youtube.com/@Aliens-Soc
Webpage: www.aliens-soc.eu

Vprašanja

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

KIBERNETSKI CUNAMI

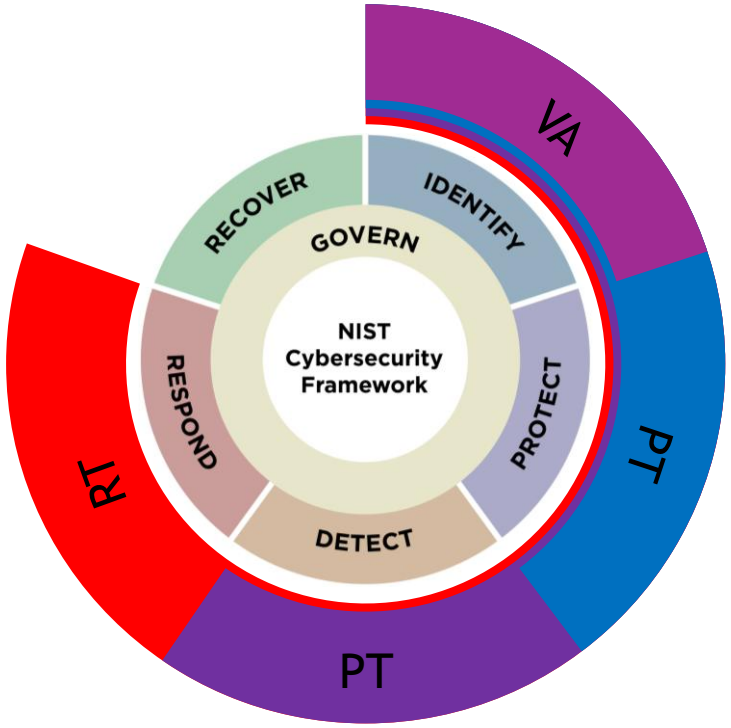
Ko val napadov postane realnost

»Higienski minimum« kibernetske varnosti v notranjem omrežju

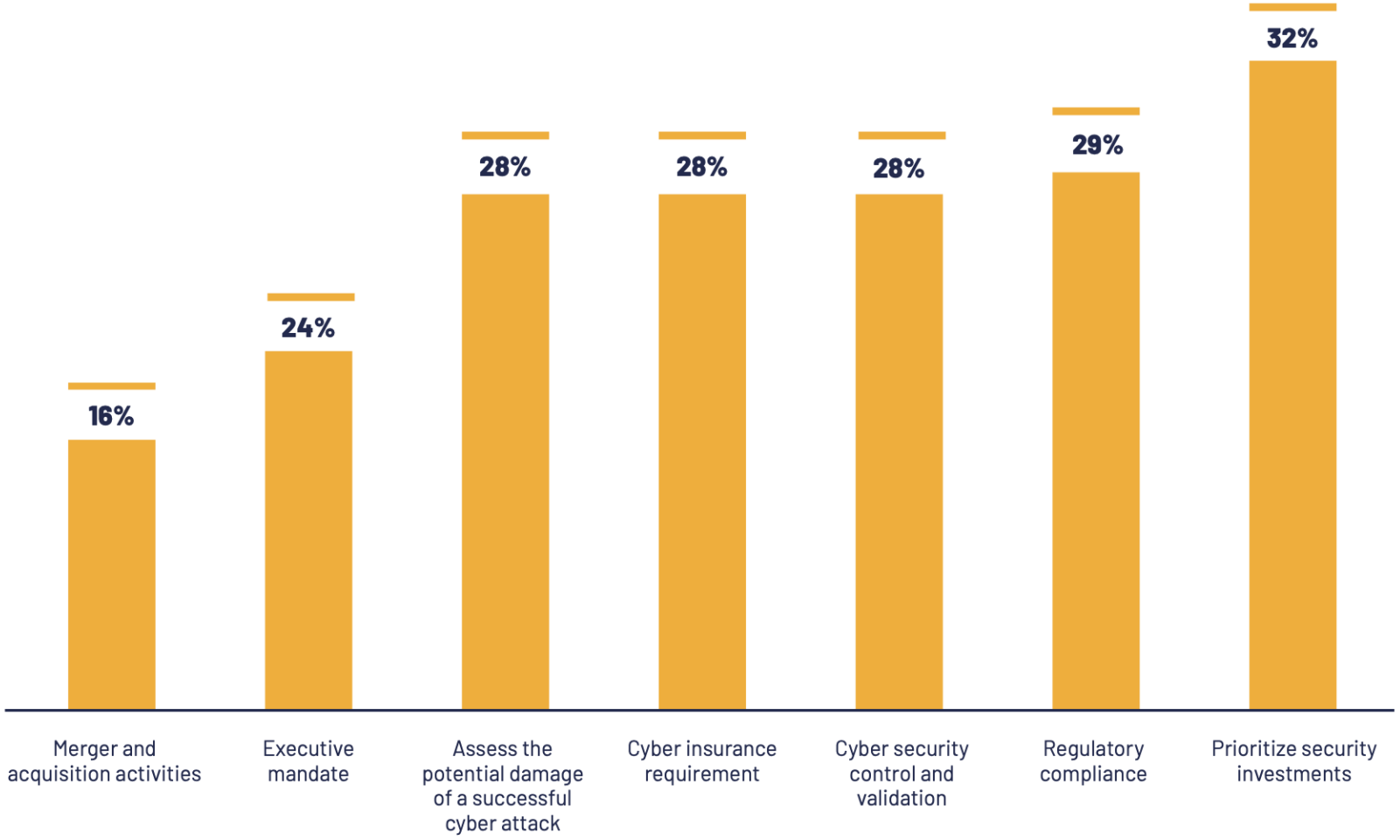
Grega Prešeren, tehnični direktor, Carbonsec d.o.o.

CARBONSEC
CYBERSECURE YOUR BUSINESS

“Kdo je kdo?”v svetu varnostnih testov



Glavni razlogi za izvajanje pentestov



Vir: https://pentera.io/resources/reports/global-state-of-pentesting-2025-survey-report/

O zrelosti ...


CONTROL 01 Inventory and Control of Enterprise Assets
5 Safeguards IG1 2/5 IG2 4/5 IG3 5/5
CONTROL 02 Inventory and Control of Software Assets
7 Safeguards IG1 3/7 IG2 6/7 IG3 7/7
CONTROL 03 Data Protection
14 Safeguards IG1 6/14 IG2 12/14 IG3 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software
12 Safeguards IG1 7/12 IG2 11/12 IG3 12/12
CONTROL 05 Account Management
6 Safeguards IG1 4/6 IG2 6/6 IG3 6/6
CONTROL 06 Access Control Management
8 Safeguards IG1 5/8 IG2 7/8 IG3 8/8
CONTROL 07 Continuous Vulnerability Management
7 Safeguards IG1 4/7 IG2 7/7 IG3 7/7
CONTROL 08 Audit Log Management
12 Safeguards IG1 3/12 IG2 11/12 IG3 12/12
CONTROL 09 Email and Web Browser Protections
7 Safeguards IG1 2/7 IG2 6/7 IG3 7/7
CONTROL 10 Malware Defenses
7 Safeguards IG1 3/7 IG2 7/7 IG3 7/7
CONTROL 11 Data Recovery
5 Safeguards IG1 4/5 IG2 5/5 IG3 5/5
CONTROL 12 Network Infrastructure Management
8 Safeguards IG1 1/8 IG2 7/8 IG3 8/8
CONTROL 13 Network Monitoring and Defense
11 Safeguards IG1 0/11 IG2 6/11 IG3 11/11
CONTROL 14 Security Awareness and Skills Training
9 Safeguards IG1 8/9 IG2 9/9 IG3 9/9
CONTROL 15 Service Provider Management
7 Safeguards IG1 1/7 IG2 4/7 IG3 7/7
CONTROL 16 Applications Software Security
14 Safeguards IG1 0/14 IG2 11/14 IG3 14/14
CONTROL 17 Incident Response Management
9 Safeguards IG1 3/9 IG2 8/9 IG3 9/9
CONTROL 18 Penetration Testing
5 Safeguards IG1 0/5 IG2 3/5 IG3 5/5

CARBONSEC
CYBERSECURE YOUR BUSINESS

Pridobitev visokih privilegijev

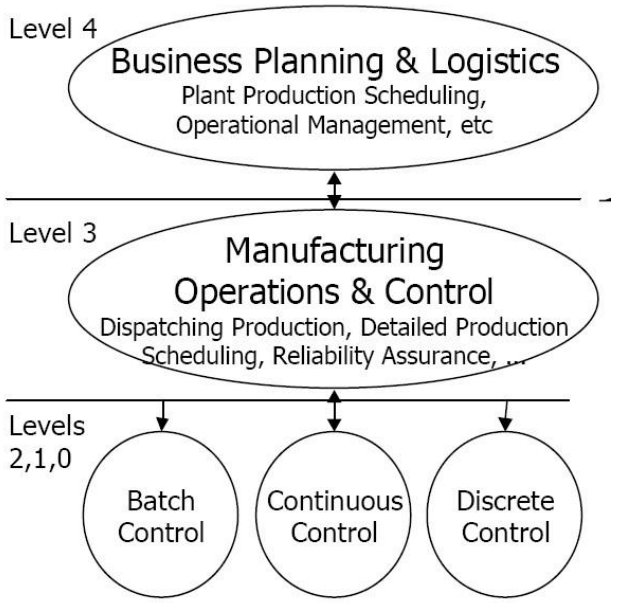
>95%

Ključne notranje tehnologije

- Aktivni imenik v 99%

Active Directory

- Arhitektura omrežja



Najpomembnejše ranljivosti

1) Uporaba nepodprtih operacijskih sistemov
2) Nenameščeni varnostni popravki
3) Ranljivi imenski protokoli
4) Šibka gesla
5) Možnost posredovanja poverilnic
6) Uporaba enakih gesel
7) Gesla v skupnih mapah
8) Predloge certifikatov
9) Arhitektura uporabniških računov
10) Kerberoasting
11) Nenameščena varnostna zaščita na strežnikih
12) Omogočen PowerShell

Kerberoasting

CARBONSEC
CYBERSECURE YOUR BUSINESS

Kako odpraviti Kerberoasting?

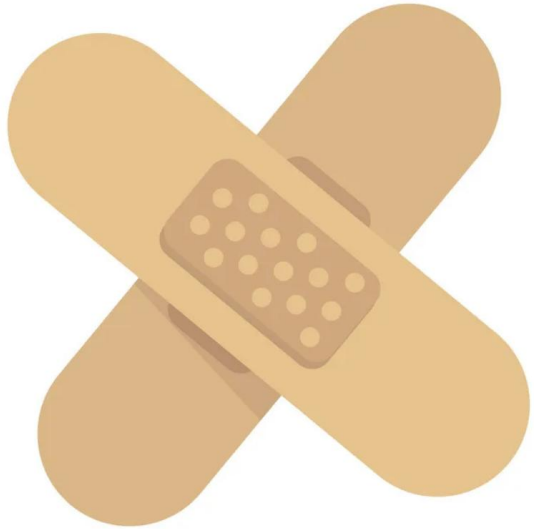
1. Uporaba gMSA ali dMSA
2. Ročna nastavitev naključnih dolgih gesel za servisne račune
    1. Prepoved razkritih in šibkih gesel
    2. Revizija gesel servisnih računov, da obstaja inventar servisnih računov s šibkimi gesli, ki jih je potrebno izboljšati
3. Servisni računi naj uporabljajo AES (128 and 256 bit) za šifriranje Kerberos ticket-ov
4. Odstranitev SPN z uporabniških računov, ki tega ne potrebujejo, za zmanjšanje površja napada

Nepopolne rešitve iz prakse

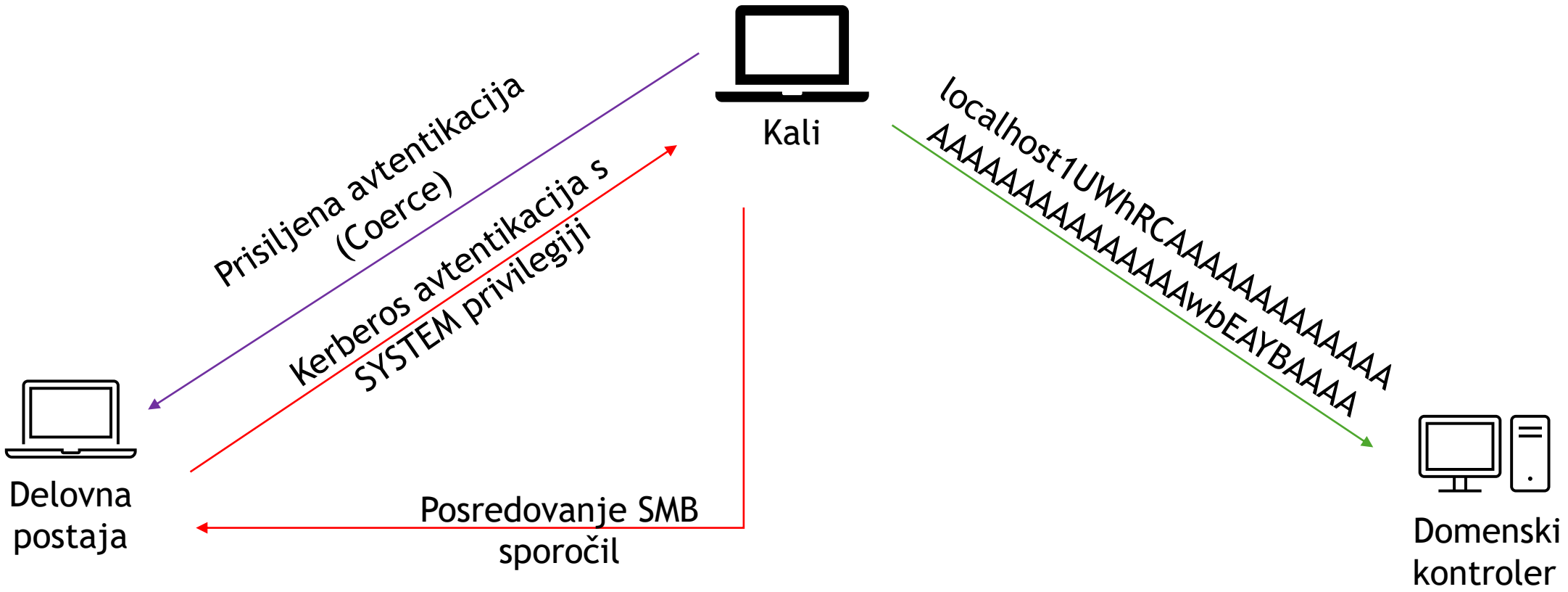
- Vključena uporaba AES (128 and 256 bit) za šifriranje Kerberos ticket-ov
  - Če uporabniški račun podpira uporabo AES, a geslo ni bilo na novo nastavljeno, se bo še naprej uporabljalo **šifriranje z RC4**
  - **Zamenjava uporabniškega gesla** sproži kreiranje novega povzetka gesla za AED šifriranje
- Brez implementacije dodatnih ukrepov
  - Uporaba računov končnih uporabnikov s SPN
  - Uporaba privilegiranih uporabniških računov s SPN
  - Ni nadzora nad šibkimi gesli (razbijanje gesel)

Nenameščeni varnostni popravki

- CVE-2025-33073
  - Objavljen: Jun 10, 2025
  - Vpliv: povišanje privilegijev
  - CVSS 3.1 ocena (Base Score): 8.8



Tako gre v praksi ...



Uporabljeni protokoli: LDAP MS RPC SMB

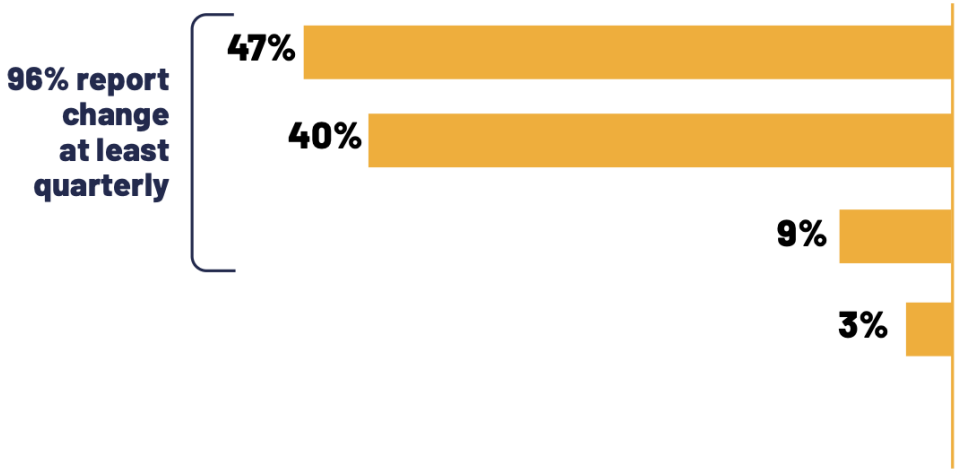
CARBONSEC
CYBERSECURE YOUR BUSINESS

Kako pogosto nameščati varnostne popravke?

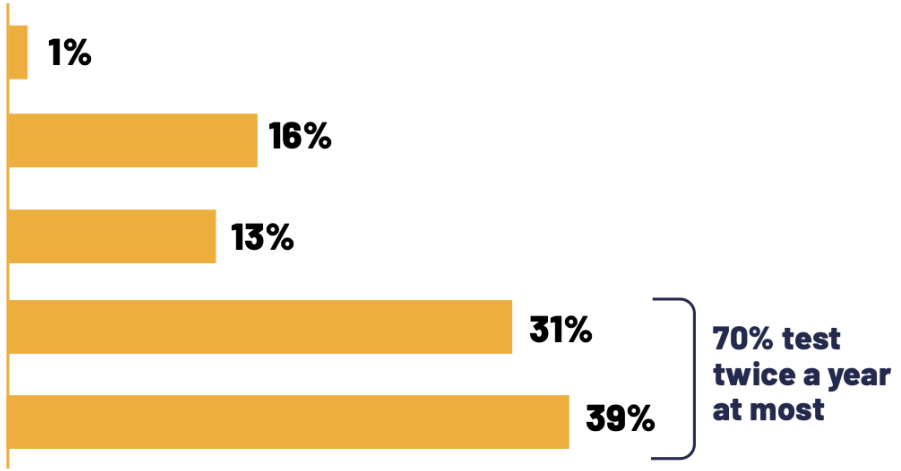
- Standardi večinoma ne določajo eksaktnih zahtev
- PCI DSS
  - Zahteva 6.2
    - Protect all system components and software from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

Rok trajanja vdornega testa?

How often are you adding and/or changing infrastructure



How often does your organization conduct pentest assessments?



Vir: https://pentera.io/resources/reports/global-state-of-pentesting-2025-survey-report/

Vprašanja

info@carbonsec.com

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

ODMOR

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

V živo – ali smo varni

Milan Gabor,
direktor, Viris d.o.o.

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

KIBERNETSKI CUNAMI

Okrogla miza: Ko se prah poleže – kako naprej po kibernetskem napadu?

moderator Renato Burazer, direktor, AREM d.o.o.,
s sogovorniki
dr. Izidorjem Golobom, Računalniški center Univerze v Mariboru
Pavlom Škerljem, Holding Slovenske elektrarne
Ksenijo Montani, Lekarna Ljubljana

HSE

Pavel Škerlj, izvršni direktor IT

Kaj

- NIČ
- Anomalije zaznane → napadalec ujet sredi dela

Vektor napada

- Račun zunanjega izvajalca

Število oseb pri reševanju

- Večji del interne ekipe
- Nekaj zunanjih partnerjev

Ponovna vzpostavitev

- Proizvodnja elektrarn je vseskozi tekla nemoteno
- Ročno vodenje za 4h, dokler se je preverjala integriteta tega okolja
- 5 dni za postavitev očiščenega okolja

Lekarna Ljubljana

Ksenija Montani, Pomočnica direktorja

Kaj

- Predvidoma vsi računalniki in strežniki, ki so bili prižgani v času napada, razen IS na tako imenovani cold backup lokaciji.
- Podatki niso bili odtujeni

Vektor napada

- Pod-virus RYUK preko elektronske pošte
- Kriptirani podatki na diskih

Število oseb pri reševanju

- Večji del interne ekipe
- Nekaj zunanjih partnerjev

Ponovna vzpostavitev

- 2 dni za prvo lokacijo (prioriteta: izdaja zdravil)
- 1 teden za celoten sistem, vse lokacije

Univerza v Mariboru

Dr. Izidor Golob, pomočnik glavnega tajnika, vodja Računalniškega centra

Univerza v Mariboru

Kaj

- Zelo ohromljen centralni računalniški sistem → visoka digitalizacija →vpliv na praktično vse procese
- Manj prizadeto: pedagoški proces, raziskovalno delo

Vektor napada

- Strežnik, ni možno določiti vektor napada (phishing in okužena datoteka z veliko verjetnostjo izključeni)

Število oseb pri reševanju

- 5 interno
- 15 zunanjih

Ponovna vzpostavitev

- Zaradi projektov v teku (večje spremembe strojne konfiguracije, migracije), potreb forenzike, prioritet, izkoristek trenutne situacije po spremembah → po 10 dneh vklapljanje prvih sistemov in storitev

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

Od pregleda do skladnosti: praktične izkušnje z ZInfV-1

Suzana Kužnik in Tevž Delak,
Forvis Mazars IT d.o.o.

Vsebina

- Izhodišča
- Pot od pregleda do skladnosti
- Analiza razkoraka
- Akcijski načrt
- Tipični rezultati iz prakse
- Stalno izboljševanje

Izhodišča - Zakonodaja

- Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 - direktiva **NIS 2**
- Zakon o informacijski varnosti (Uradni list RS, št. 40/25) - **ZInfV-1**
  - 62. člen (sprejetje ukrepov za obvladovanje tveganj): Bistveni in pomembni subjekti sprejmejo ukrepe za obvladovanje tveganj za informacijsko in kibernetsko varnost iz 21. in 22. člena tega zakona v osemnajstih mesecih od uveljavitve tega zakona **(do 19. 6. 2026)**.
  - e glede na prejšnji odstavek bistveni subjekti, ki so bili določeni kot izvajalci bistvenih storitev na podlagi 6. člena ZInfV in organi državne uprave, ki so bili določeni na podlagi 9. člena ZInfV, sprejmejo ukrepe za obvladovanje tveganj za informacijsko in kibernetsko varnost iz 21. in 22. člena tega zakona v enem letu od uveljavitve tega zakona (**do 19. 12. 2026**).

Zakaj “od pregleda do skladnosti” ni samoumevna pot

Kje trenutno smo?

Analiza vrzeli in pregled začetnega stanja

Priprava akcijskega načrta

Izzivi in pot do cilja…

Implementacija akcijskega načrta

Vzpostavitev sistemskega pristopa

Stalno izboljševanje in preverjanje

Notranje presoje

Revizijski pregledi

Skladnost ni le “popraviti, kar manjka”, ampak **vzpostaviti sistemski pristop**.

Analiza razkoraka

Ključna področja analize:

- Organizacijska struktura
- Upravljanje, vloge in odgovornosti
- Politike, postopki, procesi (praksa)
- Upravljanje tveganj
- Pogodbeni odnosi z zunanjimi izvajalci
- Tehnični in organizacijski ukrepi

Izvede se celovit, ne le tehničen pogled IT okolja.

Cilj in rezultati

- Organizacija (vodstvo) pridobi jasen vpogled v trenutno stanje z realno sliko zrelosti
- Seznam identificiranih vrzeli z oceno tveganja
- Izhodišča za pripravo akcijskega načrta.

Kako se lotiti analize razkoraka v praksi

Največja vrednost GAP analize je **preglednost**.

Tipični rezultati iz prakse

- Neobstoj politik oz. pomanjkljiva vsebina
- Nedefinirane odgovornosti oz. je za večino področij odgovoren „IT“
- Pogodbe ne vključujejo zahtev z vidika informacijske varnostnih in neprekinjenosti delovanja
- Odsotnost ocene tveganj oz. v kolikor je, ni povezana z odločitvami in konkretnimi ukrepi
- Postopki odziva na incidente in motnje delovanja niso dokumentirani in testirani

Največja nevarnost ni v pomanjkanju dokumentov, ampak v tem, da **organizacija nima jasno opredeljenih in dogovorjenih odgovornosti.**

Kako rezultate analize uporabiti – Akcijski načrt

Od analize do akcije

- Pretvori ugotovitve in tveganja v ukrepe, naloge in aktivnosti
- Določi prioritete glede na pomembnost, zahtevnost in trajanje nalog
- Določi odgovorne osebe
- Postavi realne roke
- Spremljaj napredek in rezultate

GAP analiza ni poročilo, ampak **začetek procesa**.
Ko jo prevedemo v konkretne ukrepe z odgovornimi osebami, se zgodi sprememba. To je trenutek, ko skladnost postane del kulture, ne projekt s končnim datumom.

Vloga vodstva

Vodstvo mora:

- Razumeti cilje in rezultate analize razkoraka
- Podpreti sodelovanje celotne organizacije (vodstvo, poslovni del, IT, OT idr.)
- Uporabiti rezultate pri odločanju in določanju ukrepov

Ključno vprašanje:

“Ali razumemo, katera tveganja so zares pomembna za naše poslovanje?”

GAP analiza je uspešna le, če jo vodstvo razume kot **strateško orodje**, ne tehnični pregled.

Stalno izboljševanje

- Analiza razkoraka pokaže trenutno stanje in razkrije vrzeli
- Revizija sledi po uvedbi ukrepov, preveri se ali so izboljšave učinkovite in potrdi napredek

Skupaj tvorita stalno izboljševanje.

Ko je GAP analiza narejena in ukrepi uvedeni, ima revizija smisel. GAP torej pripravi teren, revizija pa potrdi napredek.

Izvajanje revizij je še posebej pomembno za **zavezance po zakonodaji**, saj z njimi dokazujejo, da skladnost ni le formalna, temveč tudi dejanska.

Vprašanja?

Suzana Kužnik
suzana.kuznik@forvismazars.com
030 270 179

Tevž Delak
tevz.delak@forvismazars.com
040 454 616

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

Umetna inteligenca: priložnost za podjetja, ne grožnja

Marko Zavadlav,
senior svetovalec, Actual IT d.d.

Umetna inteligenca: priložnost za podjetja, ne grožnja

SISTEM UPRAVLJANJA UMETNE INTELIGENCE PO AKTU IN ISO 42001

Marko Zavadlav

astec
Član skupine Actual I.T.

UPORABA SISTEMOV UI:

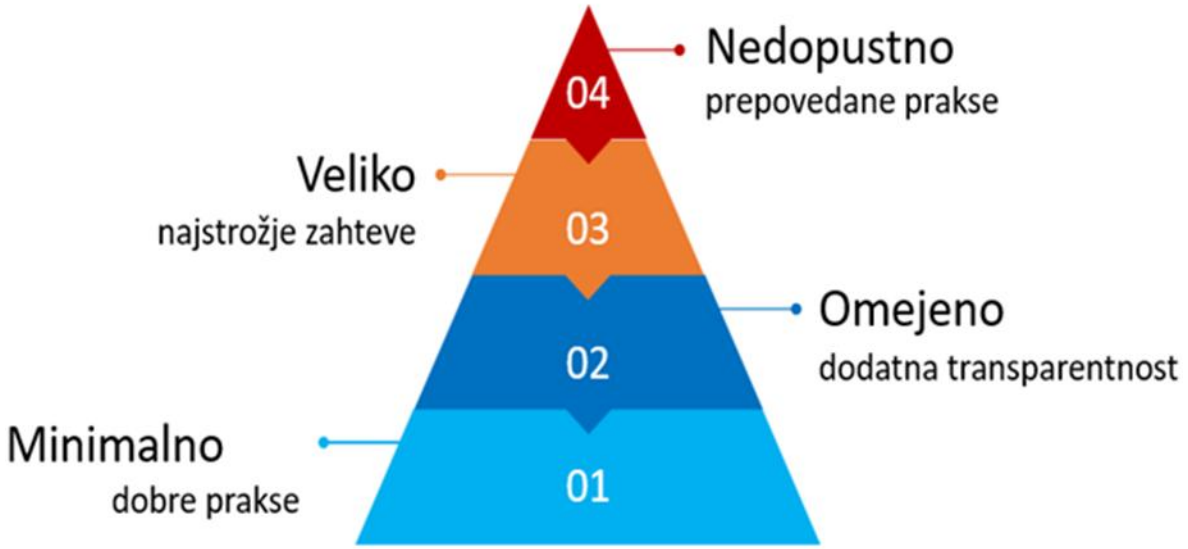
- Avtomatizacija odločanja.
- Optimizacija procesov.
- Interakcija z uporabniki.

AKT O UI

- Regulativa EU
- Zakonodajni okvir EU, ki ureja razvoj in uporabo UI
- Temelj: pristop na podlagi tveganj (»risk-based approach«)
- Cilj: varnost, zanesljivost in spoštovanje človekovih pravic

astec
Član skupine Actual I.T.

DELITEV AKTA



astec
Član skupine Actual I.T.

ZAVEZANCI

- Ponudniki, ki razvijajo ali dajejo na trg sisteme UI
- Uporabniki sistemov UI, ko delujejo na območju EU
- Uvozniki in distributerji, ki sisteme UI uvažajo ali distribuirajo v EU
- Proizvajalci zunaj EU, če se sistemi UI uporabljajo v EU ali vplivajo na njene uporabnike
- Pooblaščeni zastopniki za sisteme UI v EU

AKT O UI

- Sistem upravljanja tveganj (člen 9),
- Kakovost in ustreznost podatkov (člen 10),
- Tehnična dokumentacija (člen 11),
- Preglednost in informacije (člen 13),
- Človeški nadzor (člen 14),
- Robustnost, natančnost in kibernetsko varnost (člen 15).

- Temelji.

astec
Član skupine Actual I.T.

UPRAVLJANJE

- **UI JE POTREBNO UPRAVLJATI KOT SISTEM TVEGANJ IN ODGOVORNOSTI, NE LE KOT TEHNIČNO REŠITEV.**

astec
Član skupine Actual I.T.

SKLADNOST Z ISO 42001

- Ni dodatna birokracija, ampak zemljevid in varovalna mreža. Omogoča lažje dokazovanje skladnosti in krepi zaupanje partnerjev in strank.

- Etična, varna in tehnična uporaba.

- Odgovorna in varna raba.

astec
Član skupine Actual I.T.

ZAHTEVE ISO 42001

- Kontekst organizacije (kje, zakaj in kako),
- zavezanost vodstva,
- Načrtovanje, upravljanje tveganj in vplivov
- kompetence in ozaveščenost posameznikov,
- **delovanje in nadzor,**
- merjenje učinkovitosti, notranje presoje.

astec
Član skupine Actual I.T.

DELOVANJE IN NADZOR

- Upravljanje virov UI
- Ocenjevanje vplivov
- Življenjski cikel sistema UI (načrtovanja - ukinitve)
- Upravljanje podatkov in kakovost
- Informacije za zainteresirane strani
- Uporaba sistemov UI
- Odnosi s tretjimi stranmi in strankami

KAKO VAM LAHKO ASTEC POMAGA?

- **Paket skladnosti**: pregled stanja in priprava poročila + vzpostavitev skladnosti

- Rezultat analize razkoraka:
- Poročilo o izvedeni analizi
- Ocena stopnje zrelosti za posamezno domeno
- Predlog aktivnosti za zagotovitev skladnosti

- Oceno zrelosti in skladnost z zahtevami lahko razširimo tudi za ISO/IEC 42001

astec
Član skupine Actual I.T.

PRIMERI IZ PRAKSE

- GAP analiza
- Evidenca UI virov
- Ocena tveganj UI
- Krovna politika UI
- Področna politika UI

astec
Član skupine Actual I.T.

Vprašanja

astec
Član skupine Actual I.T.

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

Izzivi zagotavljanja skladnosti z ZinfV-1 v praksi

Dr. Andrej Rakar,
vodja informacijske varnosti,
Petrol d.d.

Izzivi zagotavljanja skladnosti z ZInfV-1 v praksi

Dr. Andrej Rakar, Petrol d.d., Ljubljana

PETROL

Uvod – pomen skladnosti z ZInfV-1

ZinfV-1

Določa okvir kibernetske varnosti v Sloveniji

Kdo je zavezanec?

Ne le kritična infrastruktura, vključena so tudi mala in srednja podjetja. To pomeni, da mnoga podjetja prvič postajajo zavezanci in morajo hitro ukrepati.

Visoke posledice neskladnosti!

globe lahko dosežejo do 10 milijonov € ali 2 % letnega prometa. Poleg tega je poslovodstvo osebno odgovorno za zagotavljanje varnosti.

Kibernetska varnost kot prioriteta!

Skladnost ni le pravna obveznost, ampak priložnost za **dvig kibernetske odpornosti** organizacije. Spodbuja strateški pristop k varnosti, kar dolgoročno zmanjšuje tveganja in potencialne škode ob incidentih.

ZInfV-1 – koga in kaj zadeva

- **Bistveni in pomembni subjekti: Bistveni subjekti** vključujejo organizacije v kritičnih sektorjih (npr. energetika, zdravstvo, finance itd.), običajno večje velikosti. **Pomembni subjekti** so srednje velika podjetja v navedenih.
- **Ugotavljanje statusa zavezanca:** Prvi izziv za organizacije je **razumevanje, ali jih zakon zavezuje**. Če organizacija spada med zavezance (glede na panogo in velikost), se mora **samoregistrirati** pri pristojnem organu (URSIV) v zakonskem roku. Na voljo so smernice in orodja (npr. spletni obrazec “Ali ste zavezanec?”) za pomoč pri tej presoji.
- **Obseg zakonskih obveznosti:** Zavezanci morajo izvesti **vrsto varnostnih ukrepov** na področju upravljanja tveganj, zagotavljati poročanje o incidentih ter sodelovati z državnimi organi. Za mnoge organizacije je zahtevnost v razumevanju *kaj vse obsega skladnost*.

Ključne zahteve zakona

- **Celovit sistem varnosti:** Vzpostavitev upravljanja informacijske varnosti z tehničnimi, organizacijskimi in kadrovskimi ukrepi, sorazmernimi tveganjem.
- **Področja ukrepov:** Pokritost vseh ključnih vidikov – infrastruktura, fizična varnost, dostopi, kadri, varnostne kopije, kriptografija, dobavna veriga.
- **Dokumentacija in nadzor:** Politike, postopki, imenovanje odgovornih oseb ter redno spremljanje učinkovitosti ukrepov.

Izziv 1 - razumevanje zakonskih obveznosti v praksi

Izziv 2 – usklajevanje z obstoječimi standardi in praksami

- **Integracija z ISO/IEC 27001**:

Veliko organizacij že izvaja **standarde informacijske varnosti** (ISO/IEC 27001, CIS Controls, NIST…). Izziv je **preslikati zahteve ZInfV-1** v obstoječe kontrole.

- **Ohranjanje obstoječih dobrih praks:**

Zakon **spodbuja** nadgradijo **obstoječega sistema upravljanja varovanja informacij (SUVI)** z dodatnimi elementi, ki jih prinaša zakon.

- **Standardizirane smernice:**

URSIV in strokovna združenja pripravljajo **smernice, ki povezujejo zahteve ZInfV-1** z znanimi okvirji (npr. ISO 27001, ISO 22301) ter s tem olajšajo razumevanje.

- **Izogibanje "checkbox" mentaliteti:**

Ne gre za birokratsko kljukanje zahtev. Pomembno je **zagotoviti učinkovitost ukrepov** – vsak kontrolni mehanizem naj ima jasno varnostno funkcijo.

Izziv 3 – zagotavljanje dokazljivosti izvajanja ukrepov

- **“Če ni zapisano, ne obstaja”:** Za vsak ukrep je treba **dokazati njegovo izvajanje**. To vključuje hranjenje **politik, načrtov, poročil o izvedenih aktivnostih, log datotek** in drugih dokazil.
- **Dokazljiva skladnost vodstva:** V praksi to pomeni redne sestanke odbora za varnost, potrjevanje poročil o stanju varnosti, odobravanje virov za varnostne projekte, ipd. Vsaka aktivnost mora biti **zapisana.**
- **Skladnost skozi evidence:** Za **vsak ukrep** določite **evidence,** npr. **seznami udeležencev in vsebine usposabljanj, evidenca dodeljenih pravic** in rednih revizij dostopov, za varnostne kopije **poročila o testnih obnovitvah,** itd.
- **Notranje presojanje in revizije:** Neodvisna notranja presoja ali zunanji pregled preveri, ali so vsi zahtevani ukrepi implementirani in **podkrepljeni z dokazi**.

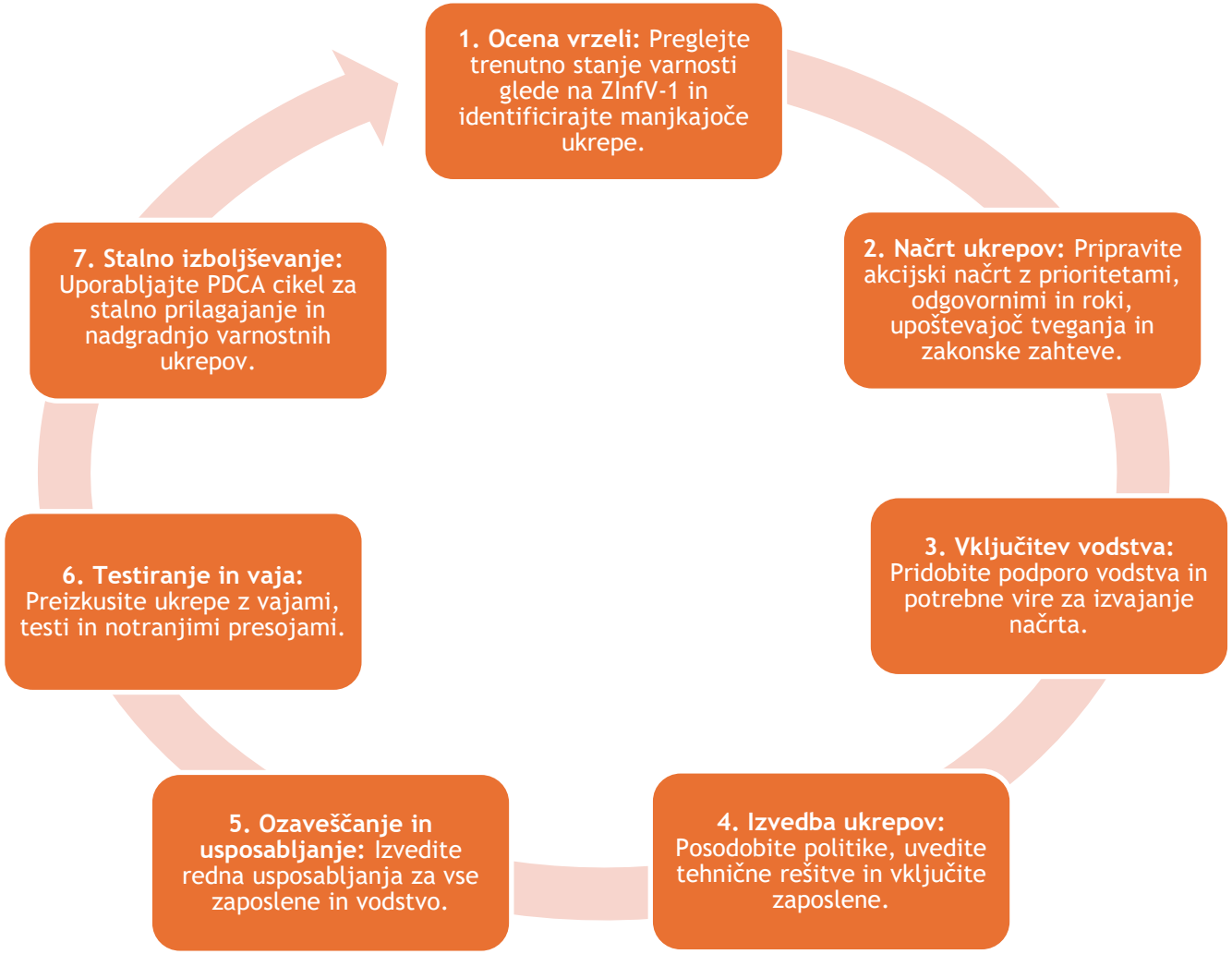
Izziv 4 – sodelovanje z zunanjimi ponudniki in dobavitelji

- **Varnost dobavne verige** – zavezanci so dolžni poskrbeti, da **ključni zunanji ponudniki** storitev in dobavitelji ne predstavljajo šibkega člena.
- **Varnostne zahteve v pogodbah:** P**ogodbe z dobavitelji** morajo vključevati **varnostne določbe**. To lahko zajema zahtevo po določenih certifikatih (npr. ISO 27001), **pravico do varnostnega pregleda,** poročanje incidentov **ali audita** pri ponudniku.
- **Skupno upravljanje tveganj:** Organizacija naj vključi dobavitelje v svoj sistem upravljanja varnostnih tveganj
- **Zunanje storitve:** Mnoga podjetja zaupajo izvajanje IT varnosti zunanjim podjetjem (npr. **varnostno operativni centri SOC**). Potrebno je definirati **SLA z varnostnimi kazalniki.**

Izziv 5 – učinkovito odzivanje na kibernetske incidente

- **Obvezen načrt odzivanja:** Potrebno je razviti načrt, ki vključuje **postopke od zaznave do sanacije**, opredeljene vloge (npr. kdo obvešča vodstvo, medije) in **stik z nacionalnim CSIRT**.
- **Poročanje incidentov:** Zahteva po **pravočasnem poročanju** večjih incidentov. **Kritične incidente** mora zavezanec prijaviti **v 24 urah** od zaznave (zgodnje sporočilo), nato pa priglasiti incident **v 72 urah**. Izziv je opredeliti, kateri incidenti so “pomembni” za prijavo.
- **Testiranje odzivnih postopkov:** Dobre prakse vključujejo **simulacije incidentov** in **namizne vaje** za tehnične ekipe in vodstvo.
- **Sodelovanje z organi in forenzika:** Ob resnem incidentu bo pogosto vključen tudi **URSIV/SI-CERT** ter lahko organi pregona.

PETROL - koraki za doseganje skladnosti z ZInfV-1



Pogoste napake in pasti pri izpolnjevanju zahtev

- Čakanje “da bo več jasno” ali do prvega incidenta, lahko privede do **hitenja v zadnjem trenutku**, napak ali sankcij.
- Pogosti izzivi so **pomanjkanje strokovnega kadra**, **sredstva** in **čas**. Realno načrtujte potrebe, pridobite podporo vodstva za dodatne vire ali zunanje izvajalce.
- To ni **IT-projekt**. Zahteve pokrivajo tudi **organizacijske** in **kadrovske** vidike.
- Brez dokazil ukrepi **ne štejejo**. Dokumentacija mora biti **ažurna in odražati dejansko stanje**.
- Poskusi skrivanja incidenta in pozno poročanje poročanje. **Neučinkovit odziv** lahko incident dramatično podaljša.
- Če zunanjega partnerja ne preverite, lahko ravno preko njega pride do incidenta. Zato vedno opravite **due diligence** pri izbiri partnerjev in redno **preverjajte njihovo varnost**.

Zaključek

- ZInfV-1 = priložnost za izboljšanje
- Varnost kot stalna aktivnost
- Pomen sodelovanja znotraj in navzven
- Podpora in viri za večjo odpornost

Izpolnjevanje zahtev je konkurenčna prednost in prispevek k varnejši družbi. Izzivi skladnosti so hkrati priložnosti za rast in izboljšave na področju informacijske varnosti.

Vprašanja

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

Phishing 2.0: Stara grožnja, nove metode – kako se branimo danes?

Lucija Starc,
SOC analitičarka, W4C, T – 2 d.o.o.

Phishing 2.0: Stara grožnja, nove metode - kako se branimo danes?

Lucija Starc, SOC analitik, T-2

Uvod

- SOC analitik – sedež v prvi vrsti
- E-pošta je najuspešnejši način za vdor
- Statistika in trendi phishing napadov

SLOVENIJA

Nova prevara: napadi na uporabnike e-bančnih storitev, škoda že več kot milijon

Ljubljana , 24. 10. 2025 18.37 | Posodobljeno pred 9 dnevi

PREDVIDEN ČAS BRANJA: **3 min**

AVTOR **A.K.** | KOMENTARJI **60**

Policija je v zadnjih dneh prejela okrog 10 prijav oškodovanja pravnih oseb v vrednosti več kot milijon evrov. Spletni goljufi izkoriščajo novo SEPA zakonodajo in pošiljajo lažna sporočila o posodobitvi aplikacij, pri čemer se izdajajo tudi za podjetje Halcom. Družba Halcom je že opozorila, da s temi napadi ni povezana.

ČRNA KRONIKA

Podjetju s spletno goljufijo ukradli več kot 2000 evrov

Ajdovščina, 20. 03. 2025 14.57 |

PREDVIDEN ČAS BRANJA: **2 min**

AVTOR **K.K.** | KOMENTARJI **5**

V sredo so bili policisti obveščeni o spletni goljufiji na škodo ene od gospodarskih družb v občini Ajdovščina. Neznani storilec je prek lažne e-pošte pridobil oškodovančeve podatke in ga kontaktiral celo prek telefonskega klica, nato pa pridobil nepooblaščen vstop v spletno banko podjetja in jih oškodoval za 2222 evrov. Preiskava je še v teku.

ČRNA KRONIKA

Zavedli osebje dveh podjetij, z računov ukradli več deset tisoč evrov

Kranj, 26. 02. 2025 11.20 |

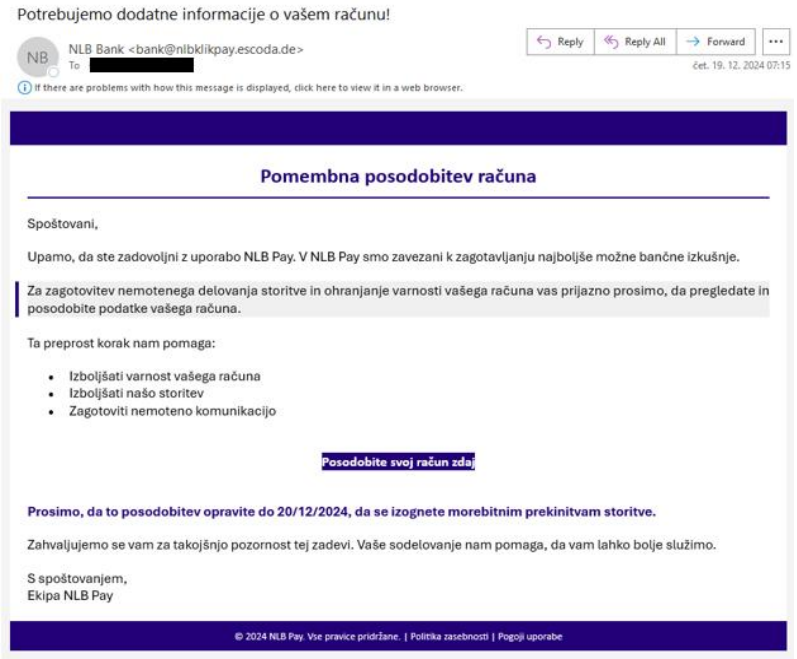
PREDVIDEN ČAS BRANJA: **3 min**

AVTOR **M.P.** | KOMENTARJI **39**

Policija poroča o več primerih spletnih prevar. Goljufi so v dveh primerih oškodovali podjetji na območju Gorenjske in Severne Primorske. Osebju družb so se neznanci predstavili kot predstavniki banke, na ta način zavedli osebje ter z bančnih računov ukradli večjo količino denarja. V še enem primeru pa so spletni goljufi za več deset tisoč evrov oškodovali občana. Na Policijski upravi Kranj ob tem opozarjajo, da so v zadnjem obdobju obravnavali večje število spletnih goljufij, ki se začnejo s klici lažnih bankirjev, trgovcev s kriptovalutami oz. z lažno e-pošto v imenu bančnih ustanov.

Tipične oblike napadov prek e-pošte

- **Klasični phishing** – ponarejene vpisne strani, mobilne banke…
- **Spear phishing** – targetirane osebe na vplivnih položajih
- **Socialni inženiring** - manipulacija ljudi za razkritje informacij



Potrebujemo dodatne informacije o vašem računu!

Reply | Reply All | Forward | ...

NB NLB Bank <bank@nlbklikpay.escoda.de>
To [redacted]
čet. 19. 12. 2024 07:15

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

Pomembna posodobitev računa

Spoštovani,

Upamo, da ste zadovoljni z uporabo NLB Pay. V NLB Pay smo zavezani k zagotavljanju najboljše možne bančne izkušnje.

Za zagotovitev nemotenega delovanja storitve in ohranjanje varnosti vašega računa vas prijazno prosimo, da pregledate in posodobite podatke vašega računa.

Ta preprost korak nam pomaga:

- Izboljšati varnost vašega računa
- Izboljšati našo storitev
- Zagotoviti nemoteno komunikacijo

Posodobite svoj račun zdaj

Prosimo, da to posodobitev opravite do 20/12/2024, da se izognete morebitnim prekinitvam storitve.

Zahvaljujemo se vam za takojšnjo pozornost tej zadevi. Vaše sodelovanje nam pomaga, da vam lahko bolje služimo.

S spoštovanjem,
Ekipa NLB Pay

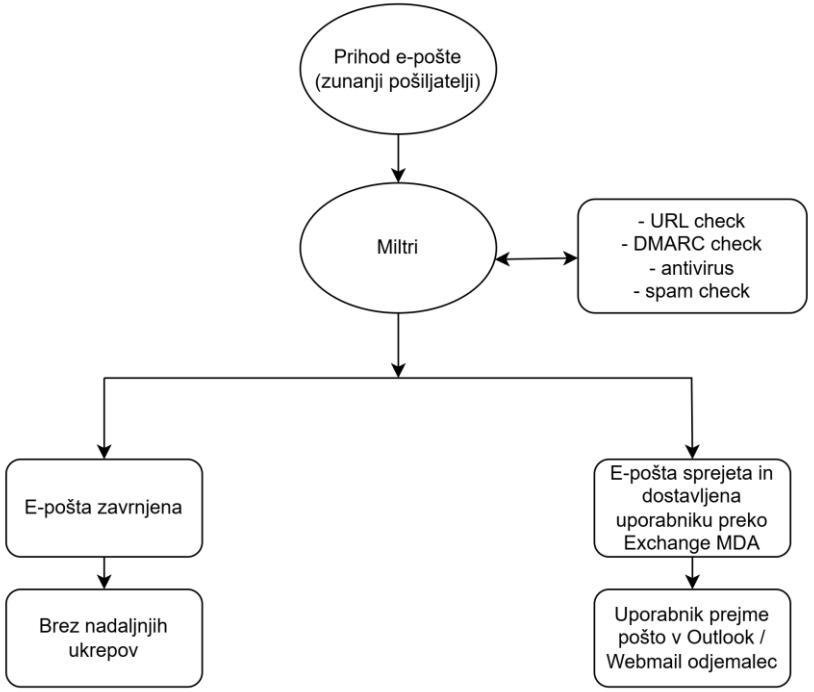
© 2024 NLB Pay. Vse pravice pridržane. | Politika zasebnosti | Pogoji uporabe

- Vtis nujnosti
- Domena, ki posnema znano podjetje
- Klik na povezavo
- Slovnično in slogovno izpopolnjeno besedilo

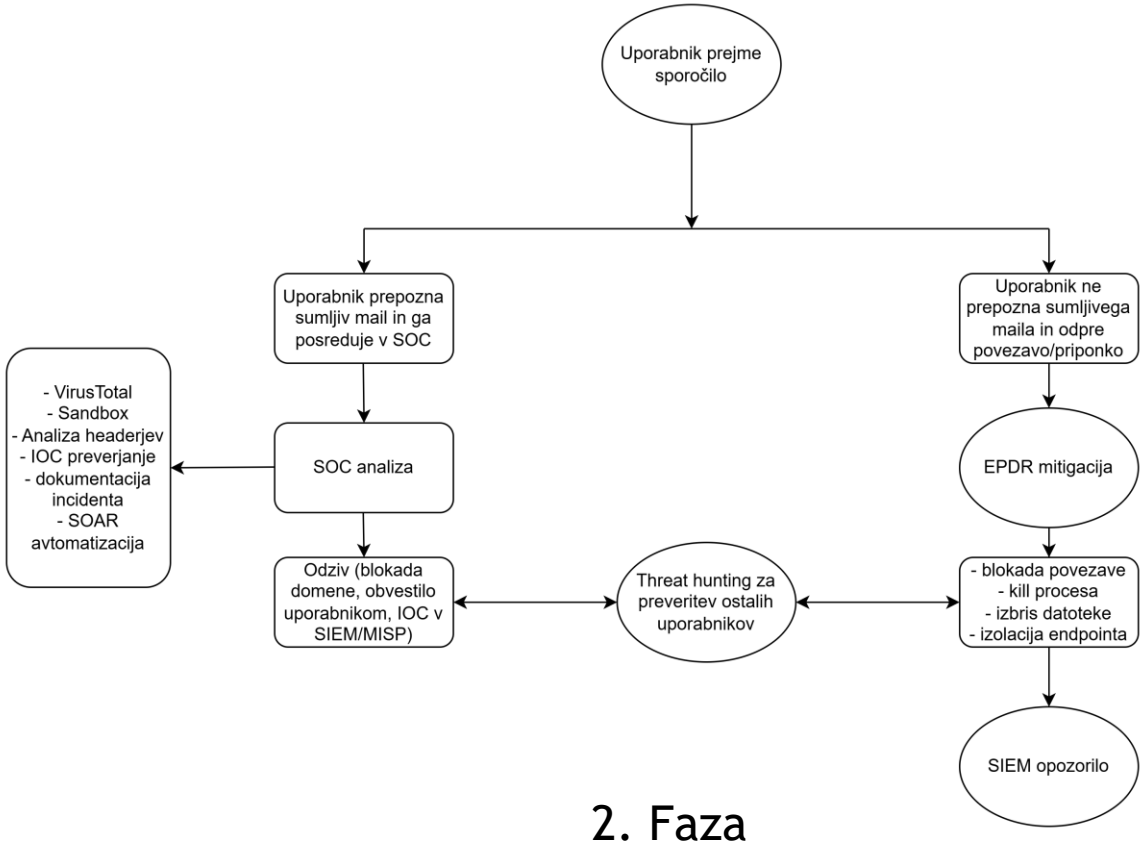
Zakaj so ti napadi še vedno uspešni?

- Tehnični izzivi: SPF/DKIM/DMARC ne preprečujejo vsega
- Napadalci se prilagajajo: uporaba legitimnih domen, generativni AI
- Človeški faktor: zaupanje, hitrost dela, rutina, slaba ozaveščenost

Kako se z napadi soočamo v praksi?



1. Faza



2. Faza

Vloga orodij: SOAR in EPDR

- **EPDR (Endpoint Protection, Detection & Response) -** zazna in prepreči posledice klikov
- **SOAR (Security Orchestration, Automation and Response)** - avtomatizacija odziva in pomen playbookov:
  - samodejno zbiranje IOC-jev,
  - preverjanje URL-jev,
  - blokiranje pošiljateljev ali domen,
  - povezava s ticketing sistemom

Učinkovite rešitve in dobre prakse

- Tehnične: večnivojska zaščita (gateway filtering, sandbox, EPDR).
- Organizacijske: izobraževanje zaposlenih, simulacije phishinga, politika poročanja o incidentih.
- SOC perspektiva: korelacija z drugimi vektorji, Threat Intelligence integracije (npr. MISP)

INTERCEPT

CYBERSECURITY

Co-funded by
the European Union

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

The project funded under Grant Agreement No. 101190460 is supported by the European Cybersecurity Competence Centre.

Vprašanja?

Lucija Starc

lucija.starc@t-2.com

064 29 29 00

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

Kaj storiti v primeru kibernetskega napada

Uroš Lesjak,
MBA, direktor, Inovis IT d.o.o.

KAJ STORITI V PRIMERU KIBERNETSKEGA NAPADA

[odzivi-postopki-ukrepi]

Uroš Lesjak, MBA

INOVIS IT | 07.11.2025

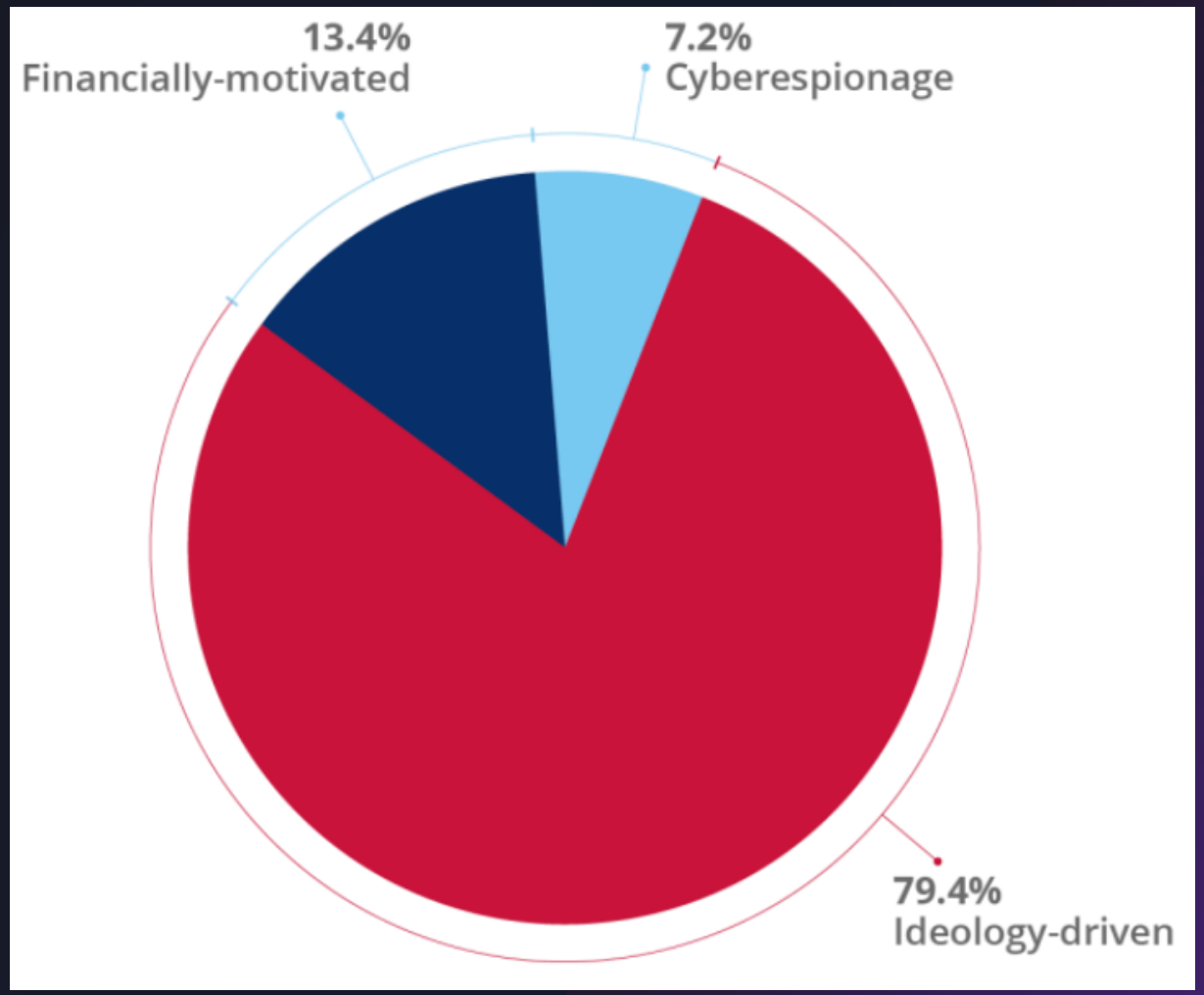
Kibernetski napadi in posledice – Europa (2024-25)

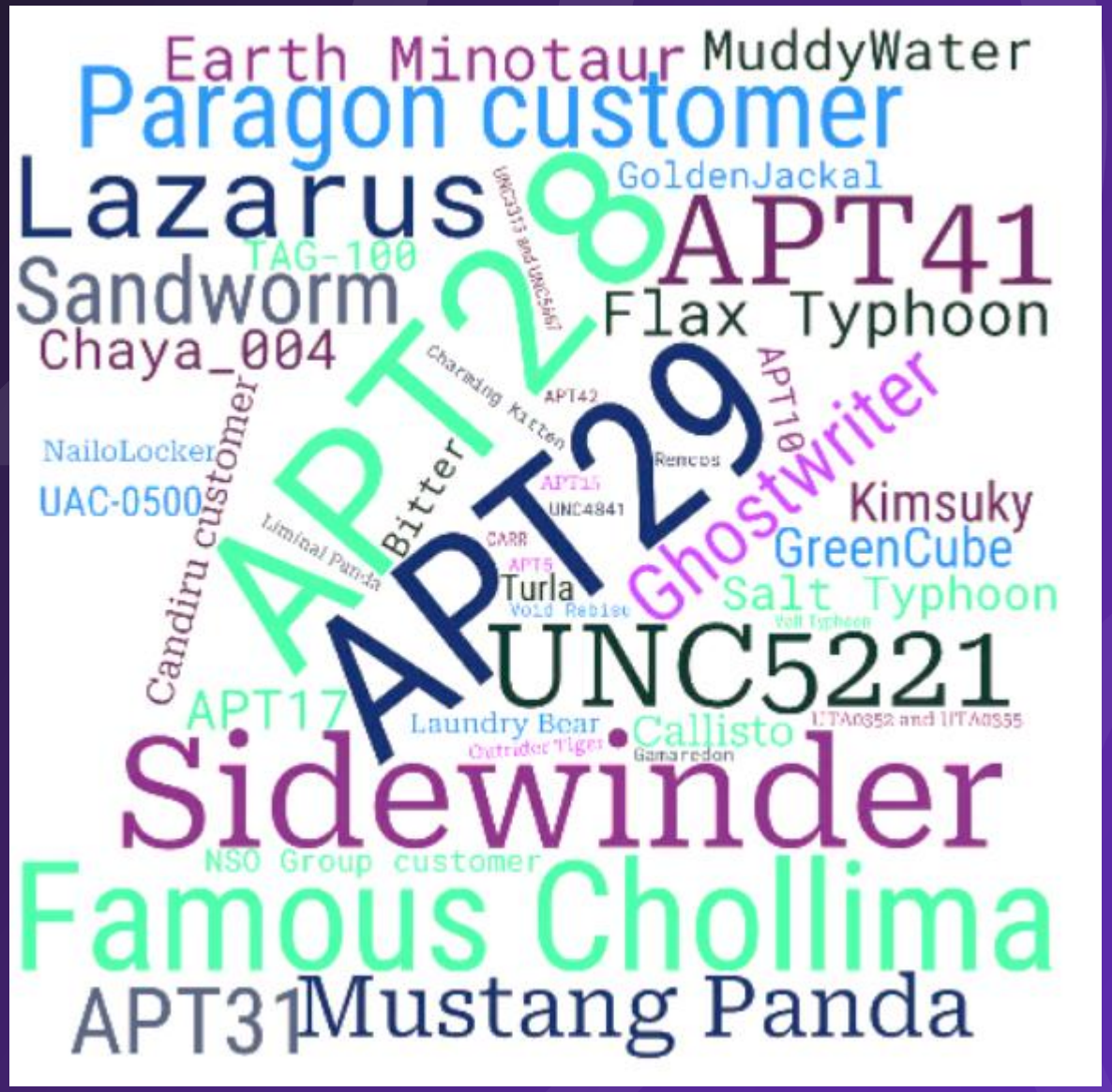
Sector	Date	Organisation	Impacted EU MS	Reported impact
Transport	07-2024	Split St. Jerome Airport	HR	Flights cancelled/ delayed; manual check-in implemented
Public administration	07-2024	Comune di Fabriano	IT	Digital municipal services disrupted
Media & Entertainment	08-2024	RMN-Grand Palais	FR	Boutiques & webshop disrupted; venues OK
Education	08-2024	Université Paris-Saclay	FR	All internal servers down; weeks in degraded mode
Health	09-2024	Weitzckliniken (Bavaria)	DE	IT outage; operations cancelled; analog fallback
Manufacturing	09-2024	Kawasaki Motors Europe (KME)	NL	Servers isolated after ransomware;EU dealer/supplier ops disrupted
Media & Entertainment	09-2024	Bayard / La Croix	FR	No print edition; tools & e-commerce degraded
Media & Entertainment	09-2024	Agence France-Presse (AFP)	FR	News delivery to clients disrupted
Health	10-2024	Johannestift Diakonie	DE	Central servers encrypted; planned procedures postponed
Media & Entertainment	10-2024	Libération	FR	Print layout blocked; degraded weekend print
Ratail & Commerce	11-2024	Inforsista	ES	Operations paralysed during Black Friday; gradual recovery
Manufacturing	11-2024	U.S. Blue Yonder - > BIC	FR	EU shipping delays at BIC from upstream outage
Energy	12-2024	Electrica Group	RO	Customer-facing IT affected; critical systems isolated
Transport	04-2025	Plus Service / Telemaco	IT	Public transport ticketing systems down for two days; disruption for userd

Povprečni čas, preden se v sistemu zazna škodljivo dogajanje: **248 dni**

Vir: ENISA 2025 Cost of a Data Breach Report

Demografija groženj





Vir: ENISA 2025

EU Vulnerability Database (EUVD)

Critical vulnerabilities

ID	Alternative ID	Exploitation	CVSS	Vendor	Changed
EUVD-2024-37356	CVE-2024-38475	⚠	v3.1: **9.1**	Apache Software Foundation	3 hours ago
Improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to map URLs to…					
EUVD-2024-47042	CVE-2024-5910	⚠	v4.0: **9.3**	Palo Alto Networks	3 hours ago
Missing authentication for a critical function in Palo Alto Networks Expedition can lead to an Expedition admin account takeov…					
EUVD-2024-46457	CVE-2024-5217	⚠	v4.0: **9.2**	Servicenow	3 hours ago
ServiceNow has addressed an input validation vulnerability that was identified in the Washington DC, Vancouver, and earlier…					
EUVD-2024-44451	CVE-2024-4879	⚠	v4.0: **9.3**	Servicenow	3 hours ago
ServiceNow has addressed an input validation vulnerability that was identified in Vancouver and Washington DC Now Platfor…					

More critical vulnerabilities →

Exploited vulnerabilities

ID	Alternative ID	Exploitation	CVSS	Vendor	Changed
EUVD-2025-8008	CVE-2025-2746	⚠	v3.1: **9.8**	Kentico	3 hours ago
An authentication bypass vulnerability in Kentico Xperience allows authentication bypass via the Staging Sync Server passw…					
EUVD-2025-17737	CVE-2025-33073	⚠	v3.1: **8.8**	Microsoft	3 hours ago
Improper access control in Windows SMB allows an authorized attacker to elevate privileges over a network.					
EUVD-2025-33878	CVE-2025-61884 GHSA-rcj9-qvh8-q3c8	⚠	v3.1: **7.5**	Oracle Corporation	18 hours ago
Vulnerability in the Oracle Configurator product of Oracle E-Business Suite (component: Runtime UI). Supported versions tha…					
EUVD-2022-51199	CVE-2022-48503 GSD-2022-48503	⚠	v3.1: **8.8**	Apple	1 day ago
The issue was addressed with improved bounds checks. This issue is fixed in tvOS 15.6, watchOS 8.7, iOS 15.6 and iPadOS…					

More exploited vulnerabilities →

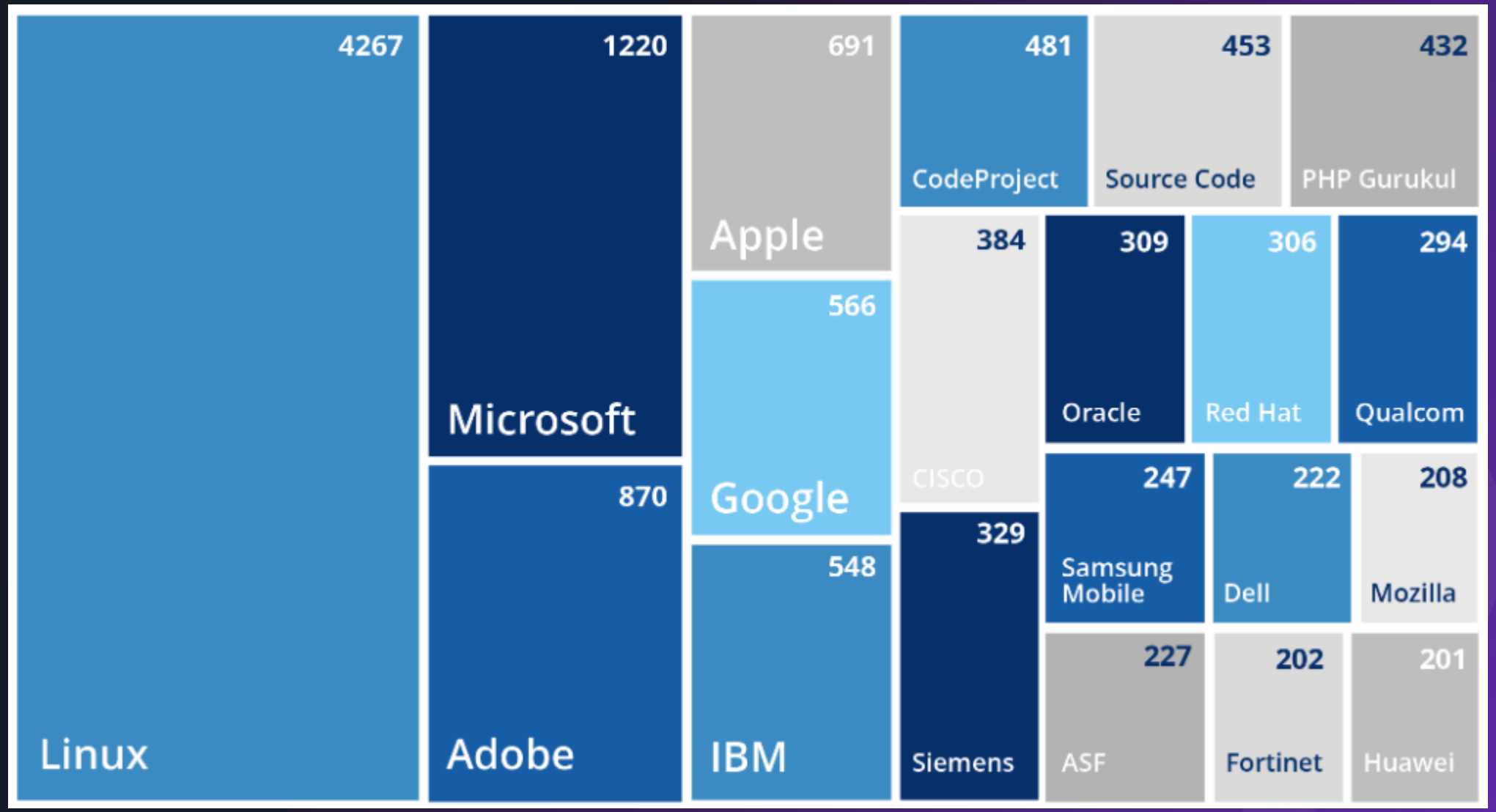
EU CSIRT coordinated vulnerabilities

ID	Alternative ID	Exploitation	CVSS	Description	Vendor	Changed
EUVD-2025-35175	CVE-2025-9339	Not available	v4.0: **7.1**	SQL injection vulnerability in the fields of warehouse document filtering form in SIMPLE.ERP software allows logged-in user to send a payload of up to 20…	Simple SA	7 hours ago
EUVD-2025-34736	CVE-2025-41018	**0.03%**	v4.0: **9.3**	SQL injection in Sergestec's Exito v8.0. This vulnerability allows an attacker to retrieve, create, update, and delete databases through the 'cat' parameter in '/…	Sergestec	7 hours ago
EUVD-2025-34733	CVE-2025-41020	**0.04%**	v4.0: **7.1**	Insecure direct object reference (IDOR) vulnerability in Sergestec's Exito v8.0. This vulnerability allows an attacker to access data belonging to other customer…	Sergestec	7 hours ago
EUVD-2025-34732	CVE-2025-41021	**0.16%**	v4.0: **5.1**	Stored Cross-Site Scripting (XSS) in Sergestec's Exito v8.0, consisting of a stored XSS due to a lack of proper validation of user input by sending a POST…	Sergestec	7 hours ago

More EU CSIRT coordinated vulnerabilities →

Vir: https://euvd.enisa.europa.eu/

Izpostavljeni sistemi IT okolja



Vir: EUVD 2025

ODZIV NA KIBERNETSKI NAPAD

IDENTIFIKACIJA NAPADA

29%

Zaznava napada

Obseg in način napada

Prizadeti servisi in storitve

Odtujeni podatki

OMEJITEV OGROŽENOSTI

31%

Onemogočanje dostopov uporabnikov

Izklop/Omejitev omrežnih povezav

Izolacija napadenih storitev

KOMUNIKACIJA

17%

Sprotno obveščanje odgovornih

Dobro sodelovanje z odzivnim centrom

Odkrita komunikacija s poslovnimi partnerji

DOKUMENTIRANJE

15%

Ključni so podatki s časovnim žigom

Skrbno beleženje vseh izvedenih sprememb

(Za)Varovanje vseh dnevniških zapisov

PRIPRAVA NA OKREVANJE

8%

Odstranjevanje zlonamerne kode in okuženih sistemov

Posodabljanje vseh ogroženih sistemov (patch)

ODZIV NA KIBERNETSKI NAPAD TER OKREVANJE

OBNOVITEV SISTEMA/STORITEV

37%

Preverjanje stanja varnostnih kopij

Varnostne kopije BREZ zlonamerne kode

Testiranje v izoliranem okolju

Intervjuji z uporabniki

Preverjanje vseh zaznanih ranljivosti

Analiza pridobljenih podatkov

21%

RAZISKOVANJE VZROKA

PREGLED UČNE LEKCIJE

22%

Analiza KAJ in ZAKAJ se je zgodilo

Uporaba izsledkov za spremembe

Evaluacija procesov odzivne ekipe

Ovrednotiti čas za okrevanje in ga optimirati

Uvedba programa za okrevanje ob izpadih

Revizija nastavitev in uvedba sprememb

9%

POSODOBITEV KONFIGURACIJE

VAJE IN IZOBRAŽEVANJE

11%

Izvedba „požarnih vaj“ – PenTest, Table-top

Sprotno izobraževanje uporabnikov in skrbnikov IT okolja

UKREPI ZA OMEJITEV IN HITREJŠE OKREVANJE

#1 **Posodobljeni sistemi in infrastruktura**

Tako OS, gonilniki, Firmware, SCADA, Android IoT
Security Hardening – AD, DNS, Firewall, ACLs. WiFi

#2 **Nadzor in vzpostavljeni procesi odziva**

24/7 Nadzor nad dogodki, storitvami in uprabniki
Uvedba SOC (In-House, Co-Managed, SOCaaS)
Table-top-exercise za preverjanje usklajenosti ekipe in dokumentiranih procesov

#3 **Varnostno kopiranje in kontinuirano poslovanje**

3-2-1 → 3-2-1-1-0
Rezervna lokacija in primerni scenariji uporabe/zagona

#4 **Dnevniški zapisi**

Sprotno beleženje, dislocirana lokacija, nespremenljivost

#5 **Izobraževanje in preverjanje procesov**

Redno izobraževanje uporabnikov in celotne odgovorne ekipe
Redno preverjanje vzpostavljenih procesov zaznavanja in okrevanja

NIS 2/ZInfV-1 namen in koristi

#1

Napotki za skladnost

Pripravljena navodila in priporočila

#2

Standardizacija vzpostavljenega IT okolja

ISO27001, NIST, TISAX, SOC 2 – ista osnova za vse sektorje

#3

Zahtevana skladnost in sankcioniranje

Odgovornost tudi uprave podjetij in finančna odgovornost

#4

Dobavna veriga

Širitev odgovornosti in skladnost tudi na poslovne partnerje

inovis

Vprašanja

KIBERNETSKI CUNAMI

Ko val napadov postane realnost

ZLATA PARTNERJA

SIQ
www.siq.si

TelekomSlovenije

ORGANIZATORJI

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

CyberHubs Slovenia

I FEEL SLOVENIA

SRIP GoDigital

Sofinancira Evropska unija

KIBERNETSKI CUNAMI

Ko val napadov postane realnost