KIBERNETSKA (NE)VARNOST

Matjaž Mravljak, Urad Vlade RS za informacijsko varnost


KOMUNALA – PERSPEKTIVE PRIHODNOSTI
13. konferenca komunalnega gospodarstva

FalconFeeds.io
@FalconFeedsio

🚨 MEDUSA Ransomware Alert 🚨

- Providence Public Schools 🇺🇸

Providence Public Schools, a major urban school district in the USA, has fallen victim to MEDUSA ransomware. The group claims to have obtained 201.40 GB of data and intends to publish it within 8-9 days.

- AmeriNat 🇺🇸

AmeriNat, a provider of customized financial solutions in the USA, has also been targeted by MEDUSA ransomware. The group claims to have accessed the organization's data and plans to publish it within 7-8 days.

#USA
#MEDUSA #Ransomware #DataBreach
#CyberAttack #Infosec #DarkWeb

@FalconFeedsio

🚨 RansomHub Ransomware Alert 🚨

Tape Ruvicha 🇵🇾

Tape Ruvicha, a leading provider of comprehensive products and services in Paraguay, has fallen victim to RansomHub ransomware. The group claims to have obtained 12 GB of the organization's data and plans to publish it within 13 – 14 days.

#Paraguay
#RansomHub #Ransomware #DataBreach
#CyberAttack #Infosec #DarkWeb

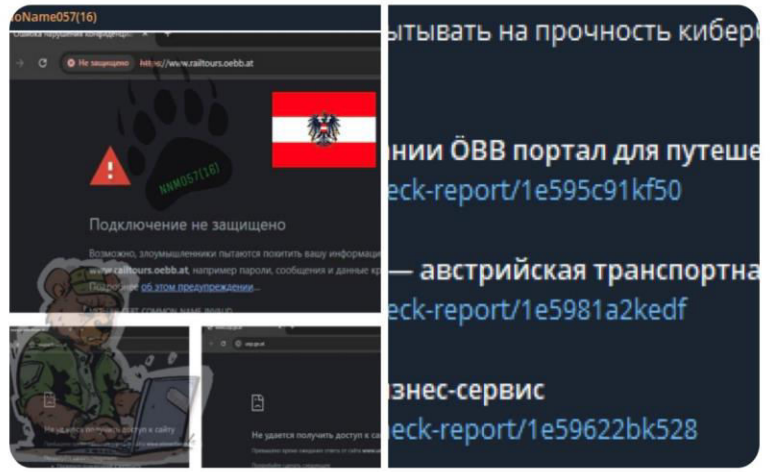
FalconFeeds.io
@FalconFeedsio

🚨 DDOS Alert 🚨

NoName claims to have targeted multiple websites in Austria.

- Wiener Linien
- Unternehmensserviceportal (USP)
- ÖBB

#Austria
#ddos #CyberAttack #threatintel #CTI



Hackread.com
@HackRead

#RansomHub ransomware group leaks alleged 487 GB of sensitive data stolen from Kawasaki Motors #Europe, following a cyberattack confirmed by the company earlier.

#CyberSecurity #CyberAttack #Kawasaki #Breach

Read:

From hackread.com

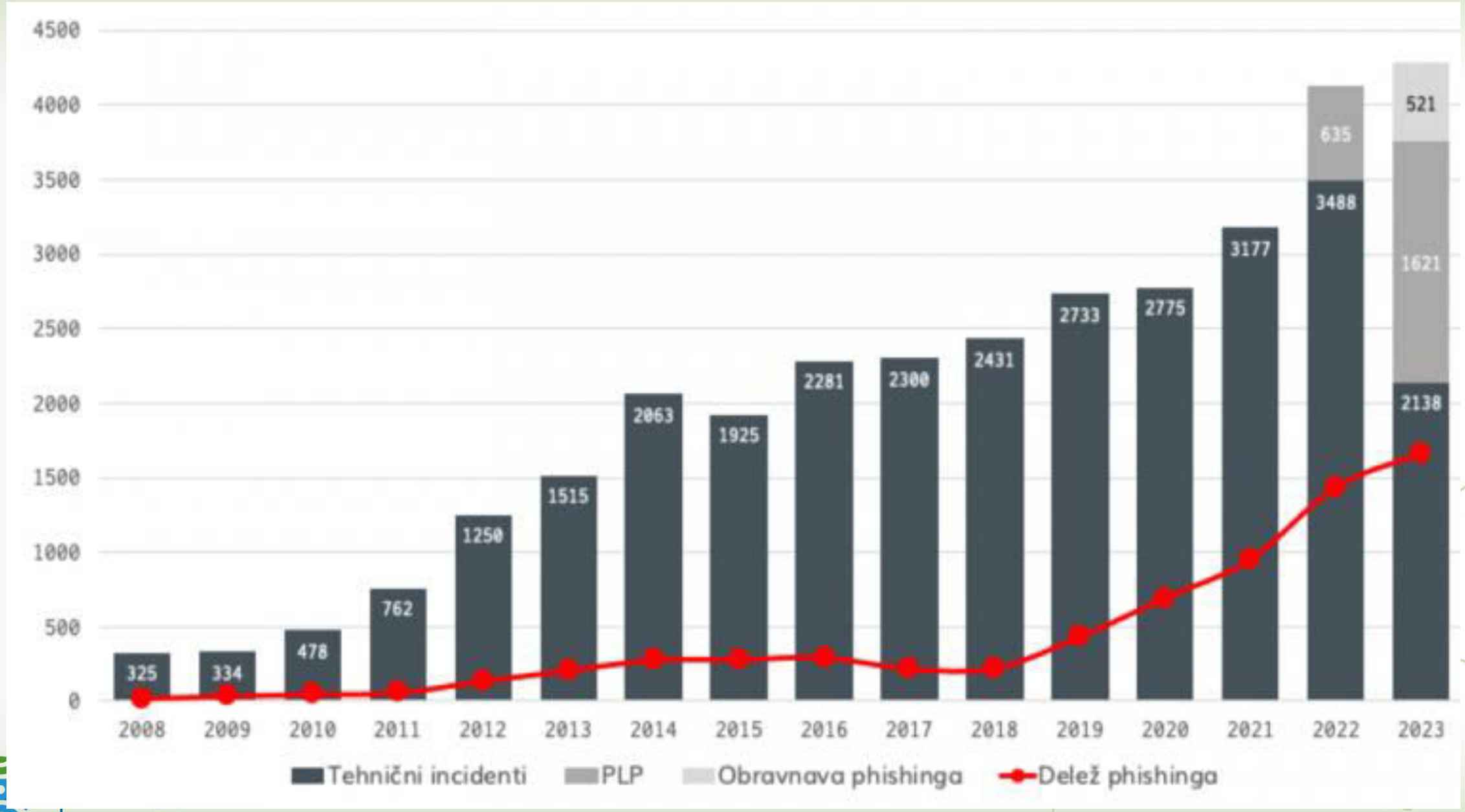
The Cyber Security Hub™
@TheCyberSecHub

Qilin ransomware attack on Synnovis impacted over 900,000 patients securityaffairs.com/168480/data-br... #BreakingNews #CyberCrime #DataBreach #Malware #Cybercrime

From securityaffairs.com

KIBERNETSKI INCIDENTI IN NAPADI V 2023 IN 2024:

- spletno ribarjenje (*Phishing*),
- izsiljevalska programska oprema (*Ransomware*),
- kraja osebnih in drugih občutljivih podatkov,
- finančne goljufije (*Man-in-the-Middle*),
- porazdeljena ohromitev storitve (*DDoS*),
- napredne vztrajne grožnje (*APT*).



https://www.cert.si/kibernetska-varnost-2023-v-stevilkah/

- V Evropski uniji je bilo v 2022 izvedenih **43 % kibernetskih napadov na mala in srednje velika podjetja**, ki niso imela vzpostavljenih ustreznih varnostnih mehanizmov.
- **83 %** napadenih malih in srednjih podjetij EU v 2022 **ni bilo pripravljenih na okrevanje po kibernetskem napadu**.
- Vsak dan je bilo v EU v 2022 poslanih **3,1 milijarde lažnih e-poštnih sporočil**, del teh lažnih sporočil je kljub varnostnim ukrepom pristal v e-poštnih predalih ljudi.
- Škoda zaradi kibernetskih napadov na svetu bo po ocenah revije Forbes do 2025 dosegla višino **10,5 trilijonov dolarjev škode** (več kot škoda zaradi vseh naravnih nesreč na svetu).

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 (EU) 2016/1148 EVROPSKEGA PARLAMENTA IN SVETA

z dne 6. julija 2016

o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji

- Je **vseevropska horizontalna zakonodaja** (nanaša se na različne sektorje gospodarstva, gospodarske družbe, javni sektor, operaterji, ipd.) **o kibernetski varnosti**.
- **Krepi varnostne ukrepe** in jih podrobneje določa ter sloni na **pristopu upoštevanja vseh nevarnosti** (fizična varnost, varnost dobavnih verig, politike kriptografije, večfaktorska avtentifikacija).
- Vzpostavlja osnovni okvir za **usklajeno razkrivanje ranljivosti**.
- Krepi **skupno situacijsko zavedanje in kolektivno sposobnost odzivanja na kibernetske napade** znotraj Evropske unije.
- Zagotavlja **povečanje splošne ravni kibernetske varnosti** v EU.

PRILOGA I: **VISOKO KRITIČNI SEKTORJI**:

1. **energija** (elektrika, daljinsko ogrevanje in hlajenje, nafta, vodik);
2. **promet** (zračni, železniški, vodni, cestni);
3. **bančništvo** (kreditne institucije);
4. **infrastruktura finančnega trga** (upravljalci mest trgovanja, centralne nasprotne stranke);
5. **zdravje** (izvajalci zdravstvenega varstva, referenčni laboratoriji, medicinski pripomočki);
6. **pitna voda** (dobavitelji in distributerji pitne vode – glavna dejavnost);
7. ***odpadna voda*** (zbiranje, odvajanje in čiščenje odpadne vode – glavna dejavnost);
8. ***digitalna infrastruktura*** (DNS, TLD, storitve zaupanja, operaterji javnih elektronski komunikacijskih omrežij ali storitev, podatkovni centri, storitve oblaka);
9. ***upravljanje storitev IKT*** (ponudniki upravljanih varnostnih storitev);
10. **javna uprava** (centralni nivo državna uprava, lokalni (regionalni) nivo);
11. ***vesolje*** (upravljalci talne infrastrukture, podpora opravljanja vesoljskih storitev).

PRILOGA II - **DRUGI KRITIČNI SEKTORJI**:

1. **Poštne in kurirske storitve** (izvajalci določenih poštnih in kurirskih storitev);
2. ***Ravnanje z odpadki*** (izvajalci – glavna dejavnost);
3. **Izdelava, proizvodnja in distribucija kemikalij** (proizvodnja in distribucija določenih snovi);
4. **Pridelava, predelava in distribucija živil** (prodaja na debelo, industrijska pri(e)delava);
5. **Proizvodnja določenih vrst izdelkov** (medicinski pripomočki; računalniki, elektronski in optični izdelki, proizvodnja električnih naprav, proizvodnja drugih strojev in naprav, proizvodnja motornih vozil, prikolic, polprikolic, proizvodnja drugih vozil in plovil);
6. ***Digitalni ponudniki*** (spletne tržnice, spletni iskalniki, platforme storitev družbenega mreženja);
7. **Raziskave** (raziskovalne organizacije).

BISTVENI SUBJEKTI:

- Vsi subjekti, iz **Priloge I** Direktive 2022/2555, ki imajo **vsaj 250 zaposlenih in letni promet vsaj 50 milijonov EUR** oziroma letno bilančno vsoto vsaj 42 milijonov EUR.
- Subjekti, ki so določeni kot kritični na podlagi zakona, ki ureja kritično infrastrukturo.
- Subjekti, ki so bili v skladu z Zakonom o informacijski varnosti določeni kot izvajalci bistvenih storitev pred 16. januarjem 2023.
- Vsi drugi subjekti vrste iz Prilog Direktive 2022/2555 I ali II, ki jih država članica identificira in jih na predlog pristojnega nacionalnega organa **določi vlada z odločbo**.

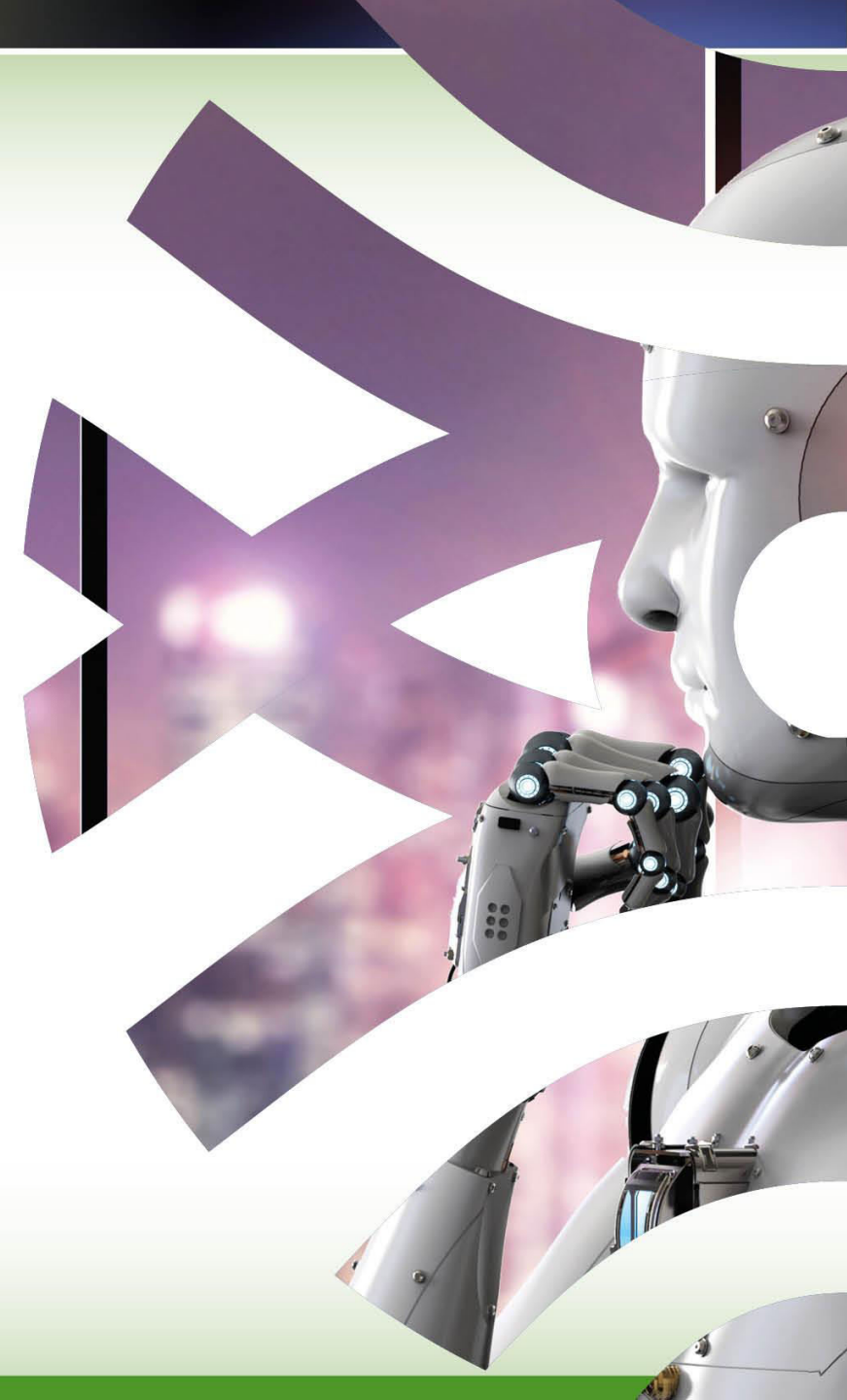
KRITERIJI ZA DOLOČITEV BISTVENEGA SUBJEKTA Z ODLOČBO:

Subjekt sodi v katero od kategorij iz Prilog Direktive 2022/2555 I ali II, ne glede na velikost **in**:

- je edini ponudnik storitve, ki je bistvena za ohranjanje kritičnih družbenih ali gospodarskih dejavnosti v Republiki Sloveniji,
- bi motnja pri opravljanju storitve subjekta lahko povzročila pomembno sistemsko tveganje, zlasti za sektorje, v katerih bi lahko taka motnja imela **čezmejni vpliv.**
- je subjekt kritičen zaradi njegovega posebnega pomena na državni, regionalni ali lokalni ravni za določen sektor ali vrsto storitve ali za druge medsebojno odvisne sektorje v Republiki Sloveniji,
- gre za subjekt javne uprave na državni ravni ali na regionalni oziroma lokalni ravni, če pri slednjem izhaja iz ocene tveganja, da opravljajo storitve, katerih motnje bi lahko pomembno negativno vplivale na ključne družbene ali gospodarske dejavnosti.

POMEMBNI SUBJEKTI:

Vsi subjekti, ki izvajajo vrste **dejavnosti iz Prilog I ali II** Direktive, in niso določeni kot bistveni subjekti, imajo pa **vsaj 50 zaposlenih** in letni promet oziroma letno **bilančno vsoto vsaj 10 milijonov EUR**.



NIS2 SCOPE – ESSENTIAL AND IMPORTANT ENTITIES

New sectors compared to NIS1

Essential entities

Important entities (unless designed as essential)

Designed or not as essential based on criticality criteria

Out of the scope, unless designed important or essential (criticality criteria)

* Defence, national security, public security, law enforcement (including the prevention, investigation, detection and prosecution of criminal offences)

Article 27.1 entities (covered by the Implementing Acts)

SECTORS & ENTITIES	MICRO (< 10)	SMALL (< 50)	MED. (< 250)	LARGE (> 250)
Annex I 1 Energy				
- ***Including electricity production (incl. nuclear), district heating and cooling, smart charging operators, and the hydrogen sector***				
Annex I 2 Transport (air, rail, road and water)				
Annex I 3 Banking sector (credit institutions)				
Annex I 4 Financial Market Infrastructures				
Annex I 5 Health				
- ***Including research and development activities of medicinal products, and manufacturing of basic pharmaceutical products and of medical devices considered as critical***				
Annex I 6 Drinking water *(excl. where the activity is only a non-essential part of the overall activity)*				
Annex I 7 Waster water *(excl. where the activity is only a non-essential part of the overall activity)*				
Annex I 8 Digital Infrastructure, including:				
- ***Cloud providers and data centres***				
- DNS providers (excl. root servers)				
- TLD name registries				
- ***Non-qualified trust service providers***				
- ***Qualified trust service providers***				
- ***Providers of electronic communications***				
Annex I 8a ICT-service management (B2B)				
Annex I 9 Public administration entities (excl. exclusion clause*, parliaments, judiciary and central banks)				
- ***Including regional entities*** (in accordance with national law)				
Annex I 10 Space				
Annex II (postal and courier services; waste management; chemicals; food; manufacturing; digital providers***; research)***				
Critical entities (Resilience of Critical Entities Directive)				
Operators of Essential Services (NIS1)				

OBVEZNOSTI BISTVENIH IN POMEMBNIH SUBJEKTOV:

- izvedba samo-registracije v aplikaciji pri PNO,
- usposabljanje članov poslovodnih organov na področju obvladovanja tveganj kibernetske varnosti,
- priprava predpisane varnostne dokumentacije,
- implementacija ukrepov za obvladovanje tveganj za kibernetsko varnost,
- priglašanje kibernetskih incidentov CSIRT in obveščanje,
- uporaba evropskih in mednarodnih standardov in tehničnih specifikacij (v čim večji meri).

RAZLIKE PRI BISTVENIH IN POMEMBNIH SUBJEKTIH:

- izvajanje periodične revizije skladnosti sprejetih ukrepov in izvajanje periodične samoocene skladnosti sprejetih ukrepov ter seznanitev pristojnega organa za nadzor (na dve leti),
- izvajanje nadzora nad zavezanci: *ex-ante* in *ex-post* nadzori (pogoji in ukrepi inšpektorja),
- višina predpisanih glob zaradi kršitve zakona.

PREDPISANA VARNOSTNA DOKUMENTACIJA ZAVEZANCEV:

1. natančen in posodobljen **popis informacijskih in drugih sredstev ter podatkov**, potrebnih za nemoteno delovanje omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev ter določitev njihovih upravljavcev;
2. **analiza obvladovanja tveganj**, vključno z določitvijo sprejemljive ravni tveganja in opisano uporabljeno metodologijo;
3. **politika in načrt neprekinjenega poslovanja**, vključno z **oceno vpliva na poslovanje**, navedbo postopkov zagotavljanja neprekinjenega poslovanja, določitvijo minimalne ravni poslovanja, upravljanjem varnostnih kopij in določitvijo vlog ter odgovornosti;

PREDPISANA VARNOSTNA DOKUMENTACIJA ZAVEZANCEV:

4. **načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov**, ki jih potrebujejo za svoje delovanje ali opravljanje storitev, vključno z opisom odgovornosti in postopkov za obnovitev delovanja teh sistemov po dogodku, ki povzroči prekinitev njihovega delovanja;

5. **načrt odzivanja na incidente** s protokolom obveščanja pristojnega CSIRT, vključno z opisom sistema za zaznavo in odziv na incidente informacijske varnosti ter opisom vlog in odgovornosti za odzivanje na incidente;

PREDPISANA VARNOSTNA DOKUMENTACIJA ZAVEZANCEV:

6. **politika s postopki za oceno učinkovitosti varnostnih ukrepov** za obvladovanje tveganj za informacijsko in kibernetsko varnost, vključno z določitvijo kazalnikov učinkovitosti in izvedeno analizo zbranih podatkov;

7. **načrt varnostnih ukrepov** za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za kibernetsko varnost, ki upošteva in področne posebnosti bistvenega ali pomembnega subjekta.

UKREPI ZA OBVLADOVANJE KIBERNETSKIH TVEGANJ:

- Zavezanci morajo pri izbiri varnostnih ukrepov **upoštevati najsodobnejše in ustrezne evropske ter mednarodne standarde**.
- Varnostni ukrepi morajo **zagotavljati raven varnosti** omrežnih in informacijskih sistemov, **ki ustreza obstoječim oziroma prepoznanim tveganjem**.
- Zavezanci morajo pri **ocenjevanju sorazmernosti varnostnih ukrepov** ustrezno upoštevati:

  - stopnjo izpostavljenosti tveganjem,
  - velikost subjekta,
  - verjetnost pojava incidentov in
  - resnost morebitnih incidentov, vključno z njihovim družbenim in gospodarskim vplivom.

UKREPI ZA OBVLADOVANJE KIBERNETSKIH TVEGANJ:

Varnostni ukrepi morajo temeljiti na pristopu **upoštevanja vseh nevarnosti**, in morajo obsegati **najmanj**:

1. **podporo vodstva subjekta** pri zagotavljanju informacijske in kibernetske varnosti in vključitvijo področja informacijske in kibernetske varnosti v letni načrt poslovanja oziroma letni program dela;
2. **zagotavljanje integritete kadrov** v povezavi z informacijsko varnostjo pred zaposlitvijo, med zaposlitvijo in ob prenehanju ali spremembi zaposlitve;
3. **osnovne prakse kibernetske higiene in usposabljanje** na področju informacijske in kibernetske varnosti;

<u>UKREPI ZA OBVLADOVANJE KIBERNETSKIH TVEGANJ</u>:

4. varnost človeških virov, preverjanje identitete uporabnikov, zagotavljanje ravni dostopnosti informacij in upravljanje pooblastil za dostop;
5. **izvajanje in upravljanje varnostnih kopij podatkov**;
6. **zagotavljanje in ohranjanje dnevniških zapisov** o delovanju omrežnih in informacijskih sistemov;
7. **upravljanje omrežnih in informacijskih sistemov**, ki jih uporabljajo za svoje delovanje ali opravljanje storitev z **določitvijo odgovornosti za njihovo zaščito**;
8. politike in postopke v zvezi z **uporabo kriptografije** in po potrebi s šifriranjem;

<u>UKREPI ZA OBVLADOVANJE KIBERNETSKIH TVEGANJ</u>:

9. **upravljanje prometa in komunikacij**;
10. **varnost dobavne verige** z določitvijo ustreznih minimalnih zahtev povezanih s kibernetsko varnostjo za ključne dobavitelje ali ponudnike storitev;
11. **fizično in tehnično varovanje** prostorov in dostopov do prostorov, kjer so ključni deli omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev;
12. **varnostne mehanizme v aplikativni programski opremi** za izvajanje dejavnosti, vključno z varnostjo pri pridobivanju, razvoju in vzdrževanju omrežnih in informacijskih sistemov ter **obravnavanjem in razkrivanjem ranljivosti**;

<u>UKREPI ZA OBVLADOVANJE KIBERNETSKIH TVEGANJ</u>:

13. **upravljanje in preprečevanje izrab tehničnih ranljivosti**;
14. **zaščita pred zlonamerno programsko kodo, zaznavanje poskusov vdorov in preprečevanje incidentov**;
15. **uporabo večfaktorske avtentikacije** ali rešitev neprekinjene avtentikacije, kadar je to potrebno zaradi obvladovanja tveganj za kibernetsko varnost in;
16. **uporabo varovanih glasovnih, video in besedilnih komunikacij in varnih sistemov za komunikacije v sili znotraj subjekta,** kadar je glede na dejavnost subjekta to primerno.

UKREPI ZA VARNOST DOBAVNE VERIGE:

- Zavezanci morajo pri oceni in izvedbi ustreznih varnostnih ukrepov za varnost dobavne verige **upoštevati ranljivosti, ki so specifične za posameznega neposrednega dobavitelja in ponudnika storitev ter splošno kakovost proizvodov ter praks svojih dobaviteljev** in ponudnikov storitev na področju kibernetske varnosti, vključno z njihovimi varnimi razvojnimi postopki.
- Zavezanci **morajo ugotavljati, kateri varnostni ukrepi so ustrezni in primerni za zagotovitev varnosti dobavne verige ter lahko preverjajo njihovo izvajanje pri dobaviteljih in ponudnikih storitev**. Pri tem upoštevajo rezultate morebitnih usklajenih ocen tveganja za kritične dobavne verige, ki jih pripravi Skupina za sodelovanje v sodelovanju z Evropsko komisijo in ENISA.

NEKATERE UGOTOVITVE IZ INŠPEKCIJSKIH NADZOROV ZAVEZANCEV IZ SEGMENTA KRITIČNE INFRASTRUKTURE:

- Zavezanci **nimajo izvedenega ustreznega popisa sredstev** (če pa že, pa je to samo parcialne rešitve, samo za ozke segmente poslovanja, za katere se izkazuje, da niso povezani z izvajanjem bistvenih storitev).
- Zavezanci **nimajo ali imajo samo delno izvedene popise poslovnih procesov**, posledično **ni izvedene BIA analize**. Izzivi nastajajo pri prepoznavi in popisu vseh procesov, s katerimi obvladujejo izvajanje bistvene storitve.
- Odgovorne osebe za neprekinjeno poslovanje so sicer prepoznane, **niso pa ti ključni kadri prepoznani v podpornih procesih** (ni zagotovljene dosegljivosti ključnega kadra izven delovnega časa).
- **Ni določene minimalne ravni poslovanja**.

NEKATERE UGOTOVITVE IZ INŠPEKCIJSKIH NADZOROV ZAVEZANCEV IZ SEGMENTA KRITIČNE INFRASTRUKTURE:

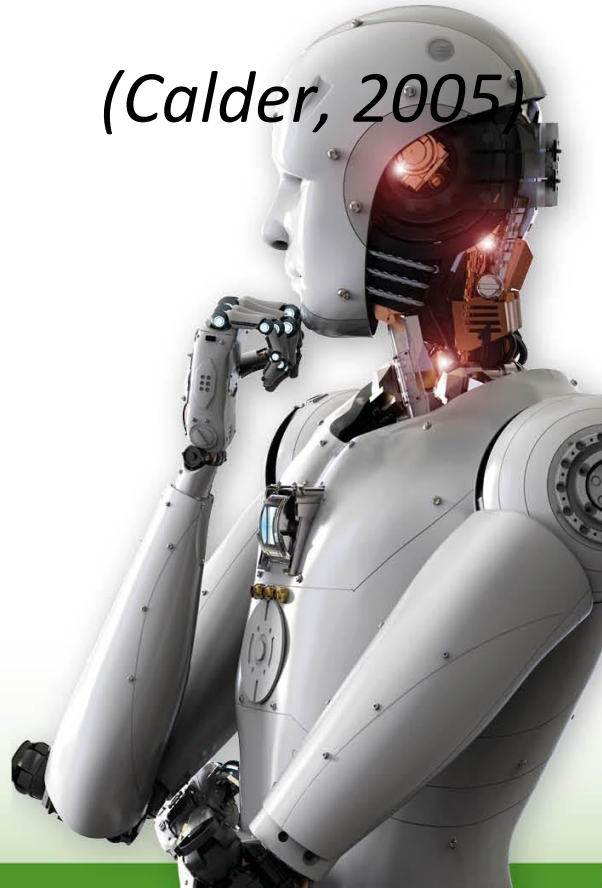
- Ker ni dobro izvedenega in redno ažuriranega popisa sredstev je **upravljanje in preprečevanje izrab tehničnih ranljivosti zelo oteženo** (odziv je šele na obvestila SI-CERT ali na obvestila zunanjih ponudnikov storitev, če ti sploh obveščajo).
- Velika večina zavezancev za IT področje najema zunanje ponudnike storitev, **varnostne zahteve za ključne dobavitelje pa niso opredeljene v internih aktih niti vključene v pogodbe**, zavezanci pa **nimajo potrebnega znanja za izvajanja dolžnega nadzorstva** nad izvajanjem storitev zunanjih ponudnikov.
- Zavezanci **ne izvajajo rednega izobraževanja zaposlenih** na področju informacijske varnosti in **ne zagotavljajo zadostnega usposabljanja in izpopolnjevanja za ključen IT kader**.

NAMESTO ZAKLJUČKA:

- Odgovorne osebe pravnih oseb oziroma **člani poslovodnih organov** bistvenih ali pomembnih subjektov **so odgovorni za izvajanje ukrepov** za obvladovanje tveganj za kibernetsko varnost.
- Bistveni in pomembni subjekti **so odgovorni za informacijsko varnost** in skladnost s predpisi tudi v primeru, ko **izvajanje informacijskih storitev najemajo pri zunanjem ponudniku storitev**.

Kibernetska varnost je potovanje, ne cilj!

(Calder, 2005)



Matjaž Mravljak, matjaz.mravljak@gov.si
direktor Inšpekcije za informacijsko varnost

URSIV

gp.uiv@gov.si
www.uiv.gov.si
Twitter: @URSIV_Slovenia