Kaj podjetjem prinaša NIS 2 direktiva in kako se na njo pripraviti?

10. oktober 2023, 10:00-11:30
Zoom platforma, GZS

Ključna sporočila NIS 2

Podjetja, ki spadajo v področje uporabe direktive NIS 2, morajo:

- Izvesti oceno tveganja kibernetske varnosti podjetij, s katerimi sodelujejo v EU oskrbovalnih verigah.
- Podjetja morajo vzpostaviti ustrezno + sorazmerne varnostne ukrepe.
- Vsaka država EU mora obravnavati poročanje o incidentih, razkritja ranljivosti in nadzor.
- Vsaka država EU mora izvajati nacionalno strategijo kibernetske varnosti.

IKT horizontalna mreža

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

URSIV

Namen in cilji

- Države članice vzpostavijo niz pravil po katerih podjetja izvajajo oceno tveganj dobaviteljev.
- Ključni cilj NIS 2 je izboljšanje usklajenost ukrepov po EU, kar se mora odraziti v nacionalni zakonodaji.
- Preprečevaje razdrobljenosti internih trgov.

IKT horizontalna mreža

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

URSIV

Harmonizacija varnostnih zahtev in poročanje o incidentih

- Vodilni so odgovorni za neskladnosti pri obvladovanju kibernetskih tveganj

- Pristop zasnovan na tveganjih: ustrezni in proporcionalni ukrepi kibernetske varnosti

- Minimalni nabor ukrepov (analiza tveganj, informacijska varnostna politika, obravnava incidentov, neprekinjenost poslovanja, varnost v dobavnih verigah)

IKT horizontalna mreža

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

URSIV

Agenda

URA	GOVORCI
10.00-10.10	**Uvodni pozdrav** Mihael Nagelj, predsednik Sekcije za kibernetsko varnost (SeKV), ZIT
10.10-10.40	**Glavno predavanje: Vloga URSIV pri implementaciji NIS 2 v Sloveniji** dr. Uroš Svete, direktor, Urad Vlade Republike Slovenije za informacijsko varnost (URSIV)
10.40-10.55	**Kateri so nujni in potrebni koraki za učinkovito naslavljanje NIS 2 direktive s fokusom na analizo tveganj** Uroš Majcen, direktor kibernetske odpornosti in Andrej Skamen, tehnični svetovalec za informacijsko varnost, Kontron d.o.o.
10.55-11.10	**Kako zagotoviti neprekinjeno poslovanje in krizno upravljanje skladno z NIS 2** Klaus Samadržič, vodilni inženir za kibernetsko varnost, Smart Com d.o.o.
11.10-11.25	**Obvladovanje tveganj zunanjih izvajalcev in ključnih dobaviteljev – primeri iz prakse** dr. Andrej Rakar, vodja informacijske varnosti, Petrol d.d.
11.25-11.40	**Vprašanja in odgovori**

IKT horizontalna mreža

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

URSIV

REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST

URSIV

Vloga URSIV pri implementaciji NIS 2 v Sloveniji

Dr. Uroš Svete, direktor, Urad Vlade Republike Slovenije za informacijsko varnost

GZS, ZIT, Kaj podjetjem prinaša NIS 2 in kako se nanjo pripraviti?

Ljubljana, oktober 2023

Pregled vsebine

- Sprejem NIS2
- Kibernetski incidenti na ravni EU
- Namen in obseg NIS2
- Vloga URSIV
- Bistveni subjekti (visoko kritični sektorji)
- Pomembni subjekti (drugi kritični sektorji)
- Zavezanci po NIS 2
- Zavezanci NIS 1 vs NIS 2
- Zavezanci po NIS 2 – pregled
- Nadzor nad zavezanci
- Obveznost poročanja o incidentih
- Drugi poudarki iz NIS 2

Sprejem NIS2

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:

- **vseevropska horizontalna zakonodaja** (sektorji gospodarstva, gospodarske družbe, javni sektor, operaterji elektronskih komunikacij, ipd.);
- **veljavnost od 16. 1. 2023;**
- **Rok za prenos** v nacionalno zakonodajo (z ZInfV-1): **17. 10. 2024**.

Kibernetski incidenti na ravni EU

- V EU v 2022 izvedenih **43 % kibernetskih napadov na mala in srednje velika podjetja** (niso imela vzpostavljenih 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 je kljub varnostnim ukrepom pristalo v e-pošti posameznikov);
- Povzročanje velike gospodarske škode.

Vloga URSIV

- URSIV kot pristojni nacionalni organ za informacijsko varnost (PNO) in organ za krizno odzivanje na področju informacijske varnosti;
- Mehanizem za določanje zavezancev – samo prepoznava;
- Kriteriji za samo prepoznavo (v nadaljevanju);
- Izvajanje direktive – priprava ZInfV-1

Namen in obseg NIS 2

- **Povečanje splošne ravni kibernetske varnosti** v EU;
- Države članice EU lahko sprejmejo ali ohranijo določbe, ki zagotavljajo **višjo raven kibernetske varnosti;**
- NIS 2 **se ne uporablja** za subjekte javne uprave, ki izvajajo dejavnosti na področju **nacionalne in javne varnosti, obrambe ali kazenskega pregona** (razen za ponudnika storitev zaupanja);

Namen in obseg NIS 2

- **Krepi varnostne ukrepe** - pristop upoštevanja vseh nevarnosti (fizična varnost, varnost dobavnih verig, politike kriptografije, večfaktorska avtentifikacija);
- Natančnejši **postopek poročanja o incidentih;**
- **Usklajeno razkrivanje ranljivosti;**
- Krepi **skupno situacijsko zavedanje in kolektivno sposobnost odzivanja** na kibernetske napade znotraj EU.

Bistveni subjekti (visoko kritični sektorji)

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).

Bistveni subjekti (visoko kritični sektorji)

NIS 1/ ZInfV

- Energija, promet, bančništvo, infrastruktura finančnega trga, zdravstvo, pitna voda, digitalna infrastruktura, varstvo okolja, preskrba s hrano (IBS);
- *Ponudniki digitalnih storitev (PDS)*
- *Javna uprava (ODU);*
- Subjekti, ki se povezujejo s centralnim državnim informacijsko-komunikacijskim sistemom (povezani subjekti).

NIS 2/ ZInfV-1

- Ravnanje z odpadno vodo;
- Upravljanje storitev IKT;
- Javna uprava;
- Vesolje.

Razširitev sektorja digitalna infrastruktura!

Pomembni subjekti (drugi kritični sektorji)

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).

Pomembni subjekti (drugi kritični sektorji)

NIS 1/ ZInfV

- Ponudniki digitalnih storitev (PDS)
- (*Ravnanje z odpadki!*)

NIS 2/ ZInfV-1

- Poštne in kurirske storitve;
- Ravnaje z odpadki;
- Izdelava, proizvodnja in distribucija kemikalij;
- Pridelava, predelava in distribucija živil;
- Proizvodnja določenih izdelkov;
- Ponudniki digitalnih storitev (razširitev);
- Raziskave.

Zavezanci po NIS 2

KRITERIJI ZA DOLOČITEV BISTVENIH SUBJEKTOV:

- Vsi subjekti, iz Priloge I Direktive 2022/2555, ki imajo vsaj 250 zaposlenih in letni promet vsaj 50 milijonov evrov oziroma letno bilančno vsoto vsaj 42 milijonov evrov;
- Ponudniki kvalificiranih storitev zaupanja in registri vrhnjih domenskih imen ter ponudniki storitev DNS, ne glede na njihovo velikost (člen 2);
- Ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev, ki imajo vsaj 50 zaposlenih in letni promet oziroma letno bilančno vsoto vsaj 10 milijonov evrov;

Zavezanci po NIS 2

KRITERIJI ZA DOLOČITEV BISTVENIH SUBJEKTOV:

- Subjekti javne uprave na državni ravni in določeni subjekti lokalne samouprave;
- Subjekti, ki so določeni kot kritični na podlagi zakona, ki ureja kritično infrastrukturo (člen 3);
- 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 I ali II Direktive 2022/2555, ki jih država članica identificira in jih na predlog pristojnega nacionalnega organa **določi vlada z odločbo**.

Zavezanci po NIS 2

KRITERIJI ZA DOLOČITEV BISTVENIH SUBJEKTOV Z ODLOČBO:

(kategorije iz Prilog I ali II Direktive 2022/2555, ne glede na velikost in (člen 2)):

- 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.

Zavezanci po NIS 2

POMEMBNI SUBJEKTI:

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

- POZOR – Izjema operaterji elektronskih komunikacij

Zavezanci NIS 1 vs NIS 2

NIS 1

- Izvajalci bistvenih storitev (49)
- Organi državne uprave (18)
- Ponudniki digitalnih storitev (1)
- Povezani subjekti

NIS 2

- **Bistveni subjekti** (visoko kritični sektorji)
- **Pomembni subjekti** (drugi kritični sektorji)

Srednja podjetja (704)
Velika podjetja (219)

Zavezanci po NIS 2 – pregled

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)				

Nadzor nad zavezanci

BISTVENI SUBJEKTI (člen 32):

- Inšpekcija za informacijsko varnost: Redni inšpekcijski nadzor (*ex-ante*), izredni inšpekcijski nadzor (*ex-post*) in odreditev ciljno usmerjene revizije informacijske varnosti.
- Zavezanci: Predpisano periodično izvajanje revizij varnosti informacijskih sistemov – PRIS.

Rezultati ciljno usmerjene revizije varnosti se dajo na vpogled pristojnemu organu. Stroške ciljno usmerjene revizije varnosti, ki jo opravi neodvisni organ, krije revidirani subjekt, razen v ustrezno utemeljenih primerih, ko pristojni organ odloči drugače.

Nadzor nad zavezanci

POMEMBNI SUBJEKTI (člen 33):

- Inšpekcija za informacijsko varnost: Izredni inšpekcijski nadzor (*ex-post*) in odreditev ciljno usmerjene revizije informacijske varnosti.
- Zavezanci: Predpisano periodično izvajanje revizij varnosti informacijskih sistemov – PRIS.

Inšpekcijski nadzor (*ex-post*) se uvede in naknadni nadzorni ukrepi odredijo v primeru, ko so organu predloženi dokazi, indici ali informacije, da pomembni subjekt **domnevno ni skladen** z direktivo oziroma zakonom.

Obveznost poročanja o incidentih

Bistveni in pomembni subjekti imajo dolžnost poročanja CSIRT/PNO, brez nepotrebnega odlašanja, o vseh incidentih, ki pomembno vplivajo na zagotavljanje njihovih storitev (člen 23)

Incident se šteje kot **pomemben**, če:

- je subjektu **povzročil ali bi mu lahko povzročil** znatne operativne motnje pri opravljanju storitev ali finančne izgube ali
- je **vplival ali bi lahko vplival** na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode.

Drugi poudarki iz NIS 2

- Obvezno usposabljanje članov **organov upravljanja** bistvenih in pomembnih subjektov, za prepoznavanje in ocenjevanje tveganj in za oceno praks obvladovanja tveganj za kibernetsko varnosti ter njihovega vpliva na storitve, ki jih opravlja subjekt (člen 20).
- Komisija do 17. oktobra 2024 **sprejme izvedbene akte**, ki določajo **tehnične in metodološke zahteve ukrepov** za obvladovanje kibernetski tveganj v zvezi s ponudniki storitev DNS, registri TLD imen, ponudniki storitev računalništva v oblaku, ponudniki storitev podatkovnih centrov, ponudniki omrežij za dostavo vsebine, ponudniki upravljanih storitev, ponudniki upravljanih varnostnih storitev, ponudniki spletnih tržnic, spletnih brskalnikov in platform za storitve družbenega mreženja in ponudnike storitev zaupanja.

Vprašanja?

REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST

URSIV

dr. Uroš Svete, direktor URSIV
uros.svete@gov.si

kontron

Kateri so nujni in potrebni koraki za učinkovito naslavljanje NIS 2 direktive s fokusom na analizo tveganj

Uroš Majcen, Direktor za kibernetsko odpornost
Andrej Skamen, tehnološki svetovalec

Kako mi vidimo NIS2 direktivo

kontron

Article 21.2.a

Risk Assessments & Security Policies

- Develop and implement a Cybersecurity policy framework.
- Define roles and responsibilities with regards to Cybersecurity
- Identify and assess the risks posed to the security of the organization's network and information systems
- Develop measures to manage those risks

Article 21.2.b

Incident Management

- Establish procedures for the detection, reporting, and response to incidents
- Develop incident response plans and procedures
- Conduct regular incident response training and testing
- Conduct post-incident analysis and improvement

Article 21.2.c

Business Continuity

- Develop and implement measures (such as a BC plan, Backup processes and Crisis Management) to ensure the continuity of services in the event of an incident
- Conduct regular business continuity testing and training

Article 21.2.d

Supply Chain Security

- Assess the cybersecurity risks to the organization's supply chain
- Implement measures to mitigate those risks
- Conduct regular supply chain risk assessments and testing

Article 21.3.e

System acquisition, development and maintenance

- Conduct regular vulnerability scanning and penetration testing
- Implement measures to mitigate vulnerabilities
- Conduct regular security testing training on cyber security and cyber hygiene

Article 21.2.f

Effectiveness of Security measures

- Have policies and procedures for evaluating the effectiveness of security measures.
- Conduct regular audits and testings

Article 21.2.g

Training & Awareness

- Conduct regular Cybersecurity training
- Follow up training with testing to reenforce learning and establish success and improvement of overall training & awareness program

Article 21.2.h

Encryption

- Use encryption to protect the confidentiality, integrity, and authenticity of data
- Implement secure key management practices
- Conduct regular encryption testing and training

Article 21.2.i

HR Security, Access Control & Asset Management

- Implement security procedures for employees with access to sensitive info
- Conduct regular access control testing and training
- Get an overview of all relevant assets and ensure they are properly utilized and handled

Article 21.2.j

Authentication solutions and Information transfer

- Implement MFA or continuous authentication solutions, voice, video, and text encryption, and encrypted internal emergency communication, when appropriate.

Kaj to pomeni?

Kako helikoptersko brati prejšni slide?

- V osnovi je to skupek dobrih praks in določenih “navodil” na področju informacijske in kibernetske varnosti
- Vsebuje tako organizacijske kot procesne ter tehnične ukrepe
- Skupek – celota naslavlja kibernetsko varnost celovito, pri tem pa daje še več poudarka na tehničnih ukrepih

Primerjava z ISO 27001:2022

NIS2 zahteve	ISO 27001:2022 kontrole
Risk Assessments & Security Policies (article 21.2.a)	• Clause 5.2
Effectiveness of Security measures (article 21.2.f)	• Clause 9.1, Clause 9.2, Clause 9.3, A.5.35
Incident Management (article 21.2.b)	• A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.6.28
Business Continuity (article 21.2.c)	• A.5.29, A.5.30, A.8.13, A.8.14
Encryption (article 21.2.h)	• A.8.24
HR Security, Access Control & Asset Management (article 21.2.i)	• A.5.9, A.5.10, A.5.15, A 5.16, A 5.17, A.5.18, A.6.1, A.6.2 A 6.4 A 6.5 A.6.6
Authentication solutions and Information transfer (article 21.2.j)	• A.5.14, A.5.16, A.5.17
System acquisition, development and maintenance (article 21.3)	• A.8.25 A.8.26.8.27 A.8.28 A.2.29 A.8.30, A.8.31, A.8.32, A.8.33
Supply chain security (article 21.2.d)	• A.5.19, A.5.20, A.5.21, A.5.22, A.5.23
Training & Awareness (article 21.2.g)	• Clause 7.3, Clause 7.4, A.6.3

Article 21.2.a - Risk Assessments & Security Policies

- Develop and implement a Cybersecurity policy framework
- Define roles and responsibilities with regards to Cybersecurity
- **Identify and assess the risks** posed to the security of the organization's network and information systems
- Develop measures to manage those risks

- Identify and asses the risks → Izvedba analize tveganj

Analiza tveganj

- S postopki za obvladovanje tveganj prepoznavamo in obravnavamo potencialne nevarnosti in dogodke, katerih uresničitev bi povzročila težave ali škodo pri poslovanju družbe.
- Namen analize tveganj je ugotavljanje verjetnosti, da se bodo omenjene nevarnosti ali dogodki uresničili, in njihovih posledic, ugotavljanje učinkovitosti protiukrepov ter ovrednotenje in primerjava posameznih tveganj.
- Namen obravnavanja tveganj je določiti odgovornosti in primerne ukrepe za obvladovanje prepoznanih tveganj ter vzpostavitev stalnega nadzora nad tveganji, ki spremljajo spremembe v okolju in poslovanju družbe, da bi se na ta način izognili neželenim dogodkom in potencialni poslovni škodi.
- Analiza tveganj informacijske varnosti predstavlja formalni pristop za ocenitev izpostavljenosti ključnih poslovnih funkcij specifičnim tveganjem, povezanim z informacijsko varnostjo.

Analiza tveganj

Predpogoj

› V posameznih poslovnih procesih oz. v različnih storitvah za različne stranke se uporabljajo različna informacijska sredstva oz. skupine sredstev. Za ocenjevanje tveganj informacijske varnosti se uporabi spisek informacijskih sredstev, ki zajema: infrastrukturo, strojno in programsko opremo, podatke in dokumente oziroma druge nosilce podatkov, ljudi ter elemente pomembne za razvoj družbe (ideje o novih proizvodih in rešitvah, izvorne kode). Ocenjevanje tveganj praviloma izvajamo po procesih / storitvah za informacijska sredstva, ki se v posameznem procesu uporabljajo.

Analiza tveganj

Kaj ocenjujemo - primer

34	Nepooblaščen (neavtoriziran) dostop do sistema/podatkov s strani zaposlenih ali zunanjih izvajalce	Tehnične grožnje		Z	C	R		SW					Organization	Ne centralizirano upravljanje sistemskih in uporabniških dostopov
34	Nepooblaščen (neavtoriziran) dostop do sistema/podatkov s strani zaposlenih ali zunanjih izvajalce	Tehnične grožnje		Z	C	R		SW					Organization	Uporaba nenamenskih privilegiranih uporabniških računov za izvajanje vsakdanjih administrativnih posegov
34	Nepooblaščen (neavtoriziran) dostop do sistema/podatkov s strani zaposlenih ali zunanjih izvajalce	Tehnične grožnje		Z	C	R		SW					Organization	Ločevanje opravil za sistemske administratorje ni vzpostavljeno na logičnem nivoju
34	Nepooblaščen (neavtoriziran) dostop do sistema/podatkov s strani zaposlenih ali zunanjih izvajalce	Tehnične grožnje		Z	C	R		SW					Organization	Neustrezno hranjenje in dostop do korenskih privilegiranih administrativnih računov
34	Nepooblaščen (neavtoriziran) dostop do sistema/podatkov s strani zaposlenih ali zunanjih izvajalce	Tehnične grožnje		Z	C	R		SW					Organization	Neustrezni postopki dodeljevanja in odvzemanja uporabniških ter privilegiranih računov
34	Nepooblaščen (neavtoriziran) dostop do sistema/podatkov s strani zaposlenih ali zunanjih izvajalce	Tehnične grožnje		Z	C	R		SW					Organization	Pomankljiva kontrola nad pravicami dostopov
34	Nepooblaščen (neavtoriziran) dostop do sistema/podatkov s strani zaposlenih ali zunanjih izvajalce	Tehnične grožnje		Z	C	R		SW					Organization	Pomanjkljiva kontrola uporabe servisnih računov
34	Nepooblaščen (neavtoriziran) dostop do sistema/podatkov s strani zaposlenih ali zunanjih izvajalce	Tehnične grožnje		Z	C	R		SW					Organization	Pomankljiva kontrola vključitve naprav v omrežje
34	Nepooblaščen (neavtoriziran) dostop do sistema/podatkov s strani zaposlenih ali zunanjih izvajalce	Tehnične grožnje		Z	C	R		SW					Organization	Omogočen stalni privilegirani oddaljeni dostop do IT sistemov za zunanje izvajalce?
34	Nepooblaščen (neavtoriziran) dostop do sistema/podatkov s strani zaposlenih ali zunanjih izvajalce	Tehnične grožnje		Z	C	R		SW					Organization	Ne segmentirano omrežje
34	Nepooblaščen (neavtoriziran) dostop do sistema/podatkov s strani zaposlenih ali zunanjih izvajalce	Tehnične grožnje		Z	C	R		SW					Organization	Pomanjkljive kontrole prehajanja med posameznimo segmenti v omrežju
34	Nepooblaščen (neavtoriziran) dostop do sistema/podatkov s strani zaposlenih ali zunanjih izvajalce	Tehnične grožnje		Z	C	R		SW					Organization	Uporaba direktnih dostopo do ciljnih sistemov za potrebe vzdrževanja za pogodbenike in zunanje sodelavce
34	Nepooblaščen (neavtoriziran) dostop do sistema/podatkov s strani zaposlenih ali zunanjih izvajalce	Tehnične grožnje		Z	C	R		SW					Organization	Pomankljivosti pri dodeljevanju pravic dostopa z apogodbenike in znanje izvajalce
34	Nepooblaščen (neavtoriziran) dostop do sistema/podatkov s strani zaposlenih ali zunanjih izvajalce	Tehnične grožnje		Z	C	R		SW					Organization	Neustrezno sledenje ob oddaljenih privilegiranih dostopov v IT sistem
34	Nepooblaščen (neavtoriziran) dostop do sistema/podatkov s strani zaposlenih ali zunanjih izvajalce	Tehnične grožnje		Z	C	R					Data		Organization	Uporaba produkcijskih podatkov za testiranje
35	Ponarejanje dostopnih pravic	Tehnične grožnje		Z	C	R		SW					Organization	Uporaba poverilnic za prijave privilegiranih uporabnikov na kritične sisteme
35	Ponarejanje dostopnih pravic	Tehnične grožnje		Z	C	R		SW					Organization	Ne dovolj varna politika gesel
35	Ponarejanje dostopnih pravic	Tehnične grožnje		Z	C	R		SW					Organization	Ne centralizirano upravljanje sistemskih in uporabniških dostopov
36	Nekontrolirana uporaba opreme (tiskalniki, skenerji in podobne naprave)	Tehnične grožnje		Z	C	R	HW						Organization	omrežni tiskalniki
36	Nekontrolirana uporaba opreme (tiskalniki, skenerji in podobne naprave)	Tehnične grožnje		Z	C	R	HW							Avtorizacija tiskanja ni vzpostavljena za omrežne tiskalnike
37	Zloraba varnostnih napak programske opreme (sistemska in aplikativna programska oprema)	Tehnične grožnje		Z	C	R		SW	NTW				Organization	Neustrezno upravljanje s popravki
37	Zloraba varnostnih napak programske opreme (sistemska in aplikativna programska oprema)	Tehnične grožnje		Z	C	R		SW	NTW					Neustrezno upravljanje z ranljivostmi
37	Zloraba varnostnih napak programske opreme (sistemska in aplikativna programska oprema)	Tehnične grožnje		Z	C	R		SW	NTW					Ne prisotnost testnih sistemov za testiranje popravkov
37	Zloraba varnostnih napak programske opreme (sistemska in aplikativna programska oprema)	Tehnične grožnje		Z	C	R		SW	NTW				Organization	Pomakljivi postopki odkrivanja varostnih pomanjkljivosti kupljenih sistemov
37	Zloraba varnostnih napak programske opreme (sistemska in aplikativna programska oprema)	Tehnične grožnje		Z	C	R		SW	NTW				Organization	Pomankljivi postopki odkrivanja varostnih pomanjkljivosti lastno razvitih sistemov
38	Sistemski kibernetski napad ((D)DOS, APT, zaznavanje)	Tehnične grožnje		Z	C	R		SW	NTW	Data				Neprisotnost zaščite pred D(D)OS napadi?
39	Sistemski kibernetski napad ((D)DOS, APT, zaznavanje)	Tehnične grožnje		Z	C	R		SW	NTW	Data			Organization	Neprisotnost izvajanja varnostnega prilagajanja IT sistemov pred vključitvijo v produkcijo

Zaključek

- To ni neznano področje, tako, da nas ni potrebno biti strah pred tem
- Je samo eden izmed elementov naslavljanja informacijske in kibernetske varnosti
- Potrebujemo pa izvesti tudi predpogoj: imeti spisek informacijskih sredstev

- In, DA, gre za potovanje. Na tem je potrebno ves čas delati

kontron

Hvala za pozornost

URSIV

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

Kaj podjetjem prinaša NIS 2 direktiva in kako se na njo pripraviti?

10. oktober 2023, 10:00-11:40
Zoom platforma, GZS

Obvladovanje tveganj zunanjih izvajalcev in ključnih dobaviteljev – primeri iz prakse

dr. Andrej Rakar, Vodja informacijske varnosti
Petrol d.d.

PETROL

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

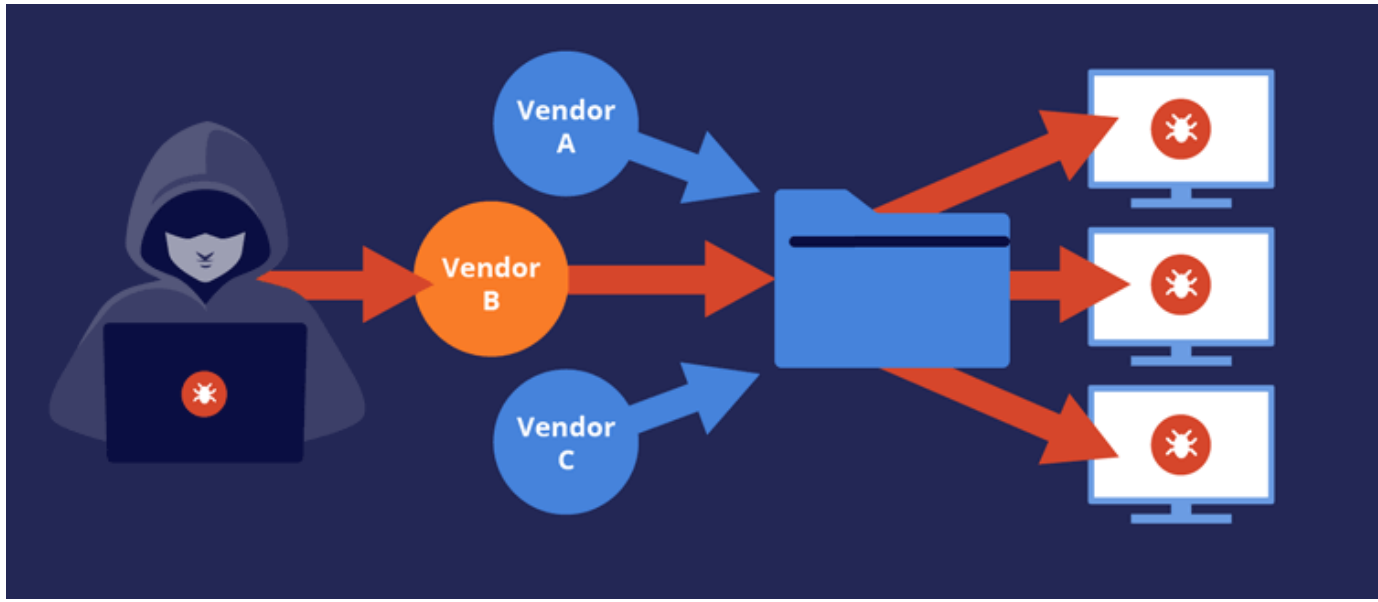
URSIV

Dobavna veriga

Znani napadi na dobavno verigo

PETROL

- SolarWinds
- Dragonfly
- MIMECAST
- ShadowHammer (ASUS)
- Kaseya
- Codecov
- Ua-parser-js, Log4j, OpenSSL 3.x
- BlueBleed (Microsoft)



zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

URSIV

Ranljivosti dobavne verige

SUPPLIER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack
Malware Infection	Pre-existing Software
Social Engineering	Software Libraries
Brute-Force Attack	Code
Exploiting Software Vulnerability	Configurations
Exploiting Configuration Vulnerability	Data
Open-Source Intelligence (OSINT)	Processes
	Hardware
	People
	Supplier

CUSTOMER	
Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Trusted Relationship [T1199]	Data
Drive-by Compromise [T1189]	Personal Data
Phishing [T1566]	Intellectual Property
Malware Infection	Software
Physical Attack or Modification	Processes
Counterfeiting	Bandwidth
	Financial
	People

PETROL

enisa

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

URSIV

Upravljanje tveganj

Zakonodaja

PETROL

GDPR

ZVOP-2

ZTP

NIS 2

ZinfV

ZVDAGA-A

ZEKOM-2

eIDAS

ENISA smernice

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

URSIV

ZinfV varnostni ukrepi (povzetek)

- Opredelitev varnostnih zahtev za ključne dobavitelje
- Izvajanje dolžnega nadzorstva nad ključnimi dobavitelji
- Upravljanje prometa in komunikacij
- Zagotavljanje ravni dostopnosti informacij in upravljanje pooblastil za dostop
- Evidentiranje dejavnosti ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, njihovih uporabnikov in administratorjev

NIS 2 direktiva (EU 2022/2555)

PETROL

Člen 21: Ukrepi za obvladovanje tveganj za kibernetsko varnost:

2.

(d) varnost dobavne verige, vključno z vidiki, povezanimi z varnostjo, ki se nanašajo na odnose med posameznim subjektom in njegovimi neposrednimi dobavitelji ali ponudniki storitev;

3. Države članice zagotovijo, da subjekti pri preučevanju ustreznih ukrepov iz odstavka 2, točka (d), tega člena, upoštevajo 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. Države članice zagotovijo tudi, da morajo subjekti pri ugotavljanju, kateri ukrepi iz navedene točke so ustrezni, upoštevati rezultate usklajenih ocen tveganja za kritične dobavne verige, izvedenih v skladu s členom 22(1).

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

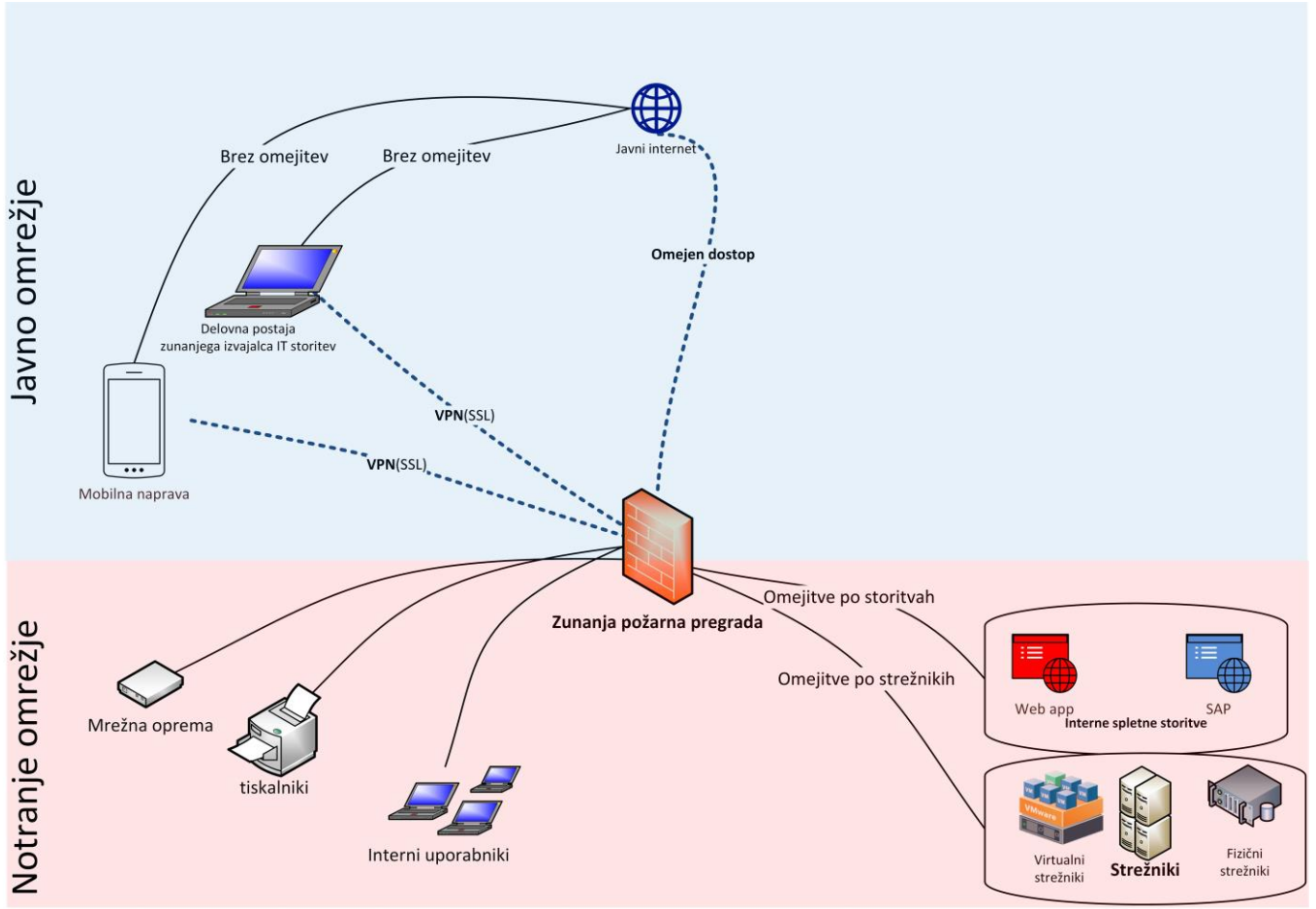
Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

URSIV

Ukrep: kontrola zunanjih dostopov

- Direkten dostop do omrežja
- Ni kontrole nad dostopi
- izmenjava poverilnic
- kompleksnost mrežne arhitekture in administracije



Ključni cilji, ki smo jih želeli doseči

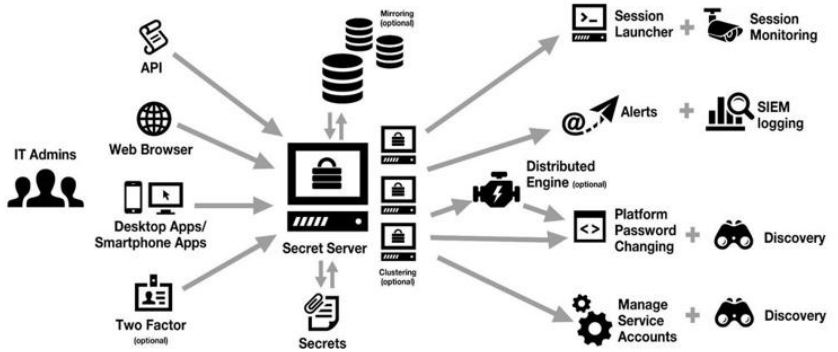
- Poenostavitev omrežja enotna varna točka dostopa brez direktnega do IS podjetja povezave (smart proxy)
- Varen dostop za notranje in zunanje administratorje (password-less)
- Shramba poverilnic Upravljanje sprememb (Sef)
- Natančno določena pravila za dostope (role, časovna omejitev)
- Avtomatizirana menjava poverilnic
- Enotno beleženje, alarmiranje in poročanje
- Snemanje sej za nedvoumne revizijske sledi

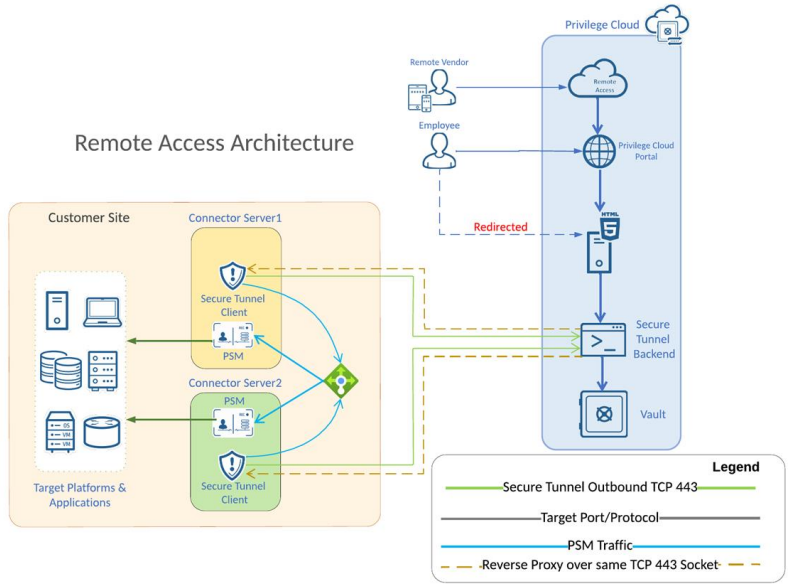
Ključ do uspeha: pravilni pristopi + PAM

PETROL

Pokrivanje ključnih ciljev:

- Poenostavitev omrežja enotna varna točka dostopa brez direktnega do IS podjetja povezave (smart proxy + cloudPC + PAM)
- Varen dostop za notranje in zunanje administratorje (password-less) - PAM
- Shramba poverilnic Upravljanje sprememb (Sef) - PAM
- Natančno določena pravila za dostope (role, časovna omejitev) - PAM
- Avtomatizirana menjava poverilnic - PAM
- Enotno beleženje, alarmiranje in poročanje -PAM
- Snemanje sej za nedvoumne revizijske sledi - PAM





zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

URSIV

Ukrep: varnostno ocenjevanje

PETROL

- Orodje za varnostno ocenjevanje ključnih dobaviteljev:
  - ✓avtomatizirano
  - ✓pravno ustrezno
  - ✓cenovno sprejemljivo
  - ✓ocena na osnovi javno dostopnih informacij
  - ✓ni obdelave osebnih podatkov tretjih strank

Faktorji ocenjevanja:

- Network Security
- DNS Health
- Patching Cadence
- Endpoint Security
- IP Reputation
- Application Security
- Cubit Score
- Hacker Chatter
- Information Leak
- Social Engineering

Security Scorecard

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

URSIV

SecurityScorecard v podjetju Petrol d.d.

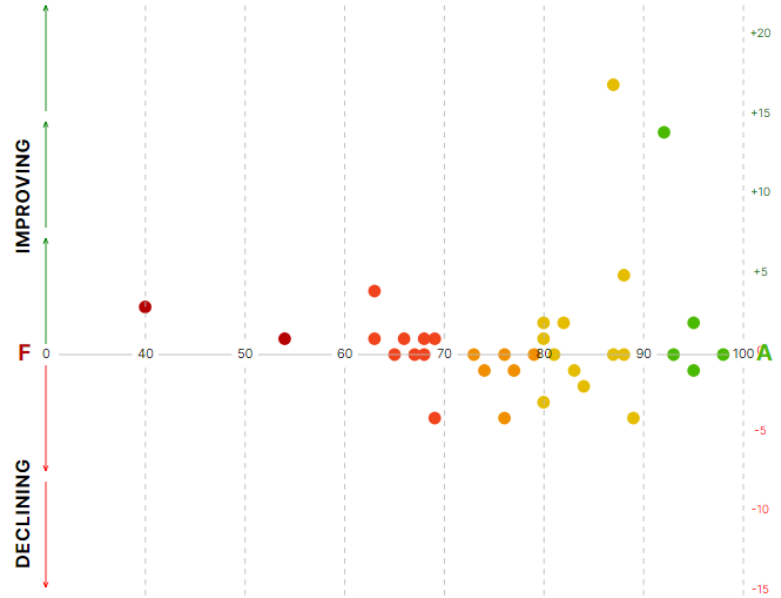
PETROL

Overall Vendor Risk Brief for petrol.si

Prepared on Aug 28, 2023

OUR OVERALL VENDOR RISK SCORE	OUR VENDOR BREACHES LTM	OPEN VENDOR CRITICAL ISSUES
C 78	1	1,360

PERFORMANCE TREND OVER 30 DAYS



Security Scorecard

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

URSIV

SecurityScorecard v podjetju Petrol d.d.

PETROL

- Ocena varnosti - ocenjuje javno varnostno držo organizacije
- Ocena tretjih strank - ocenjevanje varnosti dobaviteljev in partnerjev
- Spremljanje ranljivosti - pomoč pri nadzoru in upravljanju ranljivosti
- Primerjava znotraj panoge - primerjava z drugimi podjetji v panogi
- Zunanji viri podatkov - uporaba zunanjih virov za natančnejše ocene
- Poročila in analize - ustvarjanje podrobnih poročil

Security Scorecard

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

URSIV

Zaključek

- Prvi korak je prepoznati tveganje dobavnih verig
- Zahteva po večji transparentnosti dobaviteljev (66% neznani viri napadov)
- Vključitev varnostnih zahtev v nabavnem procesu
- Omajano zaupanje v ekosisteme programskih rešitev (problem že v razvojni fazi)
- Povečano tveganje ponudnikov oblačnih storitev
- Potreba po usklajenih aktivnostih na ravni EU (ENISA)

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

URSIV

Vprašanja

Kaj podjetjem prinaša NIS 2 direktiva in kako se na njo pripraviti?

10. oktober 2023, 10:00-11:40
Zoom platforma, GZS

Agenda

URA	GOVORCI
10.00-10.10	**Uvodni pozdrav** Mihael Nagelj, predsednik Sekcije za kibernetsko varnost (SeKV)
10.10-10.40	**Glavno predavanje: Vloga URSIV pri implementaciji NIS 2 v Sloveniji** dr. Uroš Svete, direktor, Urad Vlade RS za informacijsko varnost (URSIV)
10.40-10.55	**Kateri so nujni in potrebni koraki za učinkovito naslavljanje NIS 2 direktive s fokusom na analizo tveganj** Uroš Majcen, direktor kibernetske odpornosti in Andrej Skamen, tehnični svetovalec za informacijsko varnost, Kontron d.o.o.
10.55-11.10	**Kako zagotoviti neprekinjeno poslovanje in krizno upravljanje skladno z NIS 2** Klaus Samadržić, vodilni inženir za kibernetsko varnost, Smart Com d.o.o.
11.10-11.25	**Obvladovanje tveganj zunanjih izvajalcev in ključnih dobaviteljev – primeri iz prakse** dr. Andrej Rakar, vodja informacijske varnosti, Petrol d.d.
11.25-11.40	**Vprašanja in odgovori**

IKT horizontalna mreža

zit SeKV Združenje za informatiko in telekomunikacije Kibernetska varnost

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

URSIV

Organizatorji dogodka:

URSIV

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Gospodarska zbornica Slovenije

zit
Združenje za informatiko in telekomunikacije

IKT horizontalna mreža

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA GOSPODARSKI RAZVOJ IN TEHNOLOGIJO

EVROPSKA UNIJA
EVROPSKI SKLAD ZA REGIONALNI RAZVOJ
NALOŽBA V VAŠO PRIHODNOST

»Naložbo sofinancira Evropska unija iz Evropskega sklada za regionalni razvoj«