DATAINFO

Nova evropska zakonodaja o informacijski varnosti

Miroslav Ekart, Datainfo.si
16. Maj 2024
Dogodek A1 v BTC Ljubljana

EKIPA DATAINFO.SI

- ➔ Varstvo podatkov.
- ➔ Informacijska varnost.
- ➔ 400+ strank v Sloveniji in EU.
- ➔ Ekipa 15 strokovnjakov.
- ➔ 500+ izobraževanj letno.
- ➔ 25.000+ udeležencev letno.
- ➔ Izkušnje v več kot 125 inšpekcijskih postopkih.
- ➔ Delujemo po ISO 27001 standardih.

DATAINFO


Informacijski pooblaščenec
Republike Slovenije

izreka

priznanje

DATAINFO.SI d.o.o.

za pridobitev certifikata po
standardu za sistem vodenja varovanja informacij
ISO/IEC 27001:2013
in s tem povezanimi prizadevanji
za zavarovanje osebnih podatkov

V Ljubljani, 28. januarja 2022

Informacijska pooblaščenka
Mojca Prelesnik

info@datainfo.si 02 620 43 00

B. V.

4. maj 2024 ob 15.52
Zadnji poseg: 4. maj 2024 ob 19.09
Ljubljana - MMC RTV SLO, Radio Slovenija, Televizija Slovenija

Ruski hekerji objavili nov videoposnetek z grožnjo Sloveniji

Že pred časom so hekerji napadli več slovenskih spletnih strani

Ruski hekerji so objavili nov anonimni videoposnetek v angleškem jeziku, v katerem so napovedali napa Slovenijo. Zagrozili, da bo država ostala teden dni brez elektrike zaradi njene politike do Ukrajine.

DATAINFO

Neomejena sredstva napadalcev?

Nova zakonodaja o informacijski varnosti

- ➔ UREDBA EU DORA (finančni sektor, januar 2025)
- ➔ DIREKTIVA EU NIS 2 (oktober 2024 – potrebuje slovenski zakon ZINFV-1)
- ➔ Slovenski zakon ZVOP-2 23. člen (uporaba člena od 26.1. 2026)
- DIREKTIVA EU CER o odpornosti kritičnih subjektov

- ➔ Nemoteno delovanje države v vseh varnostnih razmerah...
- ➔ Krepitev odpornosti podjetij na kibernetske grožnje pri bistvenih dejavnostih za gospodarstvo in družbo.

DORA (Digital Operational Resiliance Act)

UREDBA (EU) 2022/2554 EVROPSKEGA PARLAMENTA IN SVETA z dne 14.12.22 o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011

- ➔ Uredba EU DORA velja neposredno brez slovenskega zakona
- ➔ Predvsem za finančni sektor (banke, zavarovalnice...)
- ➔ Začetek uporabe 25. januar 2025

- ➔ Banka Slovenije že preverja pripravljanje zavezancev
- ➔ Dobavitelji?

NIS 2 (Network Information Security)

DIREKTIVA (EU) 2022/2555 EVROPSKEGA PARLAMENTA IN SVETA z dne 14. 12. 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji - NIS 2

- ➔ Direktive EU potrebujejo zakon za prenos v slovensko zakonodajo
- ➔ 144 uvodnih določb, 46 členov, 3 priloge.
- ➔ Rok za prenos NIS 2 v slovensko zakonodajo je 17. 10. 2024.

- ➔ Nov Zakon o informacijski varnosti (ZInfV-1) - osnutek predloga

  objavljen ZInfV-1 je dne 16. 2. 2024

CER (Critical Entities Resilience)

DIREKTIVA (EU) 2022/2557 EVROPSKEGA PARLAMENTA IN SVETA z dne 14. decembra 2022 o odpornosti kritičnih subjektov in razveljavitvi Direktive Sveta 2008/114/ES

- ➔ Direktive EU potrebujejo zakon za prenos v slovensko zakonodajo
- ➔ Identifikacija zavezancev s strani Vlade do 17. julija 2026.

- ➔ Predlog Zakon o spremembah in dopolnitvah zakona o kritični infrastrukturi, javna razprava od 8.5.2024

23. člen Zakona o varstvu osebnih podatkov ZVOP-2

Informacijski sistemi, v katerih:

- obdelave osebnih podatkov določene z zakoni (obramba, SOVA, policija, obvezno zdravstveno zavarovanje, finančna uprava, zdravstveno varstvo...
- osebni podatki 100.000 + oseb na podlagi zakona
- vaša temeljna dejavnost je obsežna obdelava posebnih vrst osebnih podatkov (zdravstvo, biometrija, sindikat...)
- se obdeluje posebne vrste osebnih podatkov več kot 10.000 oseb

Smiselna uporaba zakona o informacijski varnosti o varnostnih zahtevah in priglasitvah incidentov

Cca. 1.000 novih zavezancev NIS 2 (ocene gredo do 2.000...)

- ➔ Javni ali zasebni subjekti.

- ➔ 50 + zaposlenih
- ➔ 10 mio EUR prihodkov
- ➔ 10 mio EUR bilančna vsota
- ➔ IN KRITERIJ DEJAVNOSTI

- ➔ Nekateri ne glede na dejavnost!

NIS 2 BISTVENI SUBJEKTI - Velikost in še: (visoko kritični sektorji)

DATAINFO

NIS 2 - PRILOGA I: VISOKO KRITIČNI SEKTORJI:

1. energija (elektrika, daljinsko ogrevanje in hlajenje, nafta, plin, 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, proizvajalci medicinskih pripomočkov);
6. pitna voda (dobavitelji in distributerji pitne vode kot glavne dejavnosti);
7. odpadna voda (podjetja, ki zbirajo, odvajajo ali čistijo komunalno odpadno vodo kot glavno dejavnost);
8. digitalna infrastruktura (DNS, TLD, oblačne storitve, podatkovni centri, ponudniki storitev zaupanja);
9. upravljanje storitev IKT (ponudniki upravljanih varnostnih storitev);
10. javna uprava (na centralni ravni države, na regionalni ravni);
11. vesolje (upravljalci talne infrastrukture, ki podpira opravljanja vesoljskih storitev).

NIS 2 POMEMBNI SUBJEKTI – Velikost in še: (drugi kritični sektorji)

DATAINFO

NIS2 - 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).

ZAVEZANCI NE GLEDE NA VELIKOST: ZInfV-1 (3. in 6. čl.) + NIS2

Javni in zasebni subjekti iz NIS 2 Priloge I in II ne glede na velikost:

- ponudniki javnih elektronskih komunikacijskih omrežij;
- ponudniki storitev zaupanja;
- registri vrhnjih domenskim imen in sistemskih domenskim imen;
- edini ponudnik storitev, ki je bistvena za ohranjanje kritičnih ali gospodarskih dejavnosti v RS;
- motnja pri opravljanju storitve lahko pomembno vplivala na javni red, javno varnost ali javno zdravje;
- motnja pri opravljanju storitve lahko povzročila pomembno sistemsko tveganje, zlasti ob čez mejnem vplivu;
- 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 RS;
- gre za subjekt javne uprave na državni ravni ali na regionalni ravni in
- gre za subjekt javne uprave na lokalni ravni, če pri slednjem izhaja iz njegove ocene tveganja, da opravlja storitve, katerih motnje bi lahko pomembno negativno vplivale na ključne družbene ali gospodarske dejavnosti.

ZAVEZANCI (dodatno)

- **Kritični subjekti, določeni na podlagi Zakona o kritični infrastrukturi** (Direktiva (EU) 2022/2557 (CER)), ne glede na njihovo velikost.
- Subjekti, ki opravljajo storitve registracije domenskih imen, ne glede na velikost.
- Subjekti lokalne samouprave, mestne občine in občine, ki imajo sedeže v krajih, kjer je sedež upravnih enot (teh je 58).
- Subjekti, ki jih **Vlada RS identificira kot pomembne, zaradi pomembnega negativnega vpliva na življenje, zdravje ali okolje v primeru incidenta.**
- **Subjekti, ki so bili določeni po (trenutnem) ZInfV pred 16.1.2023**
- NIS2 se **NE** uporablja za subjekte javne uprave iz področja nacionalne varnosti, javne varnosti, obrambe ali kazenskega pregona, vključno s preprečevanjem, preiskovanjem, odkrivanjem in pregonom kaznivih dejanj.

Samoregistracija zavezancev (po NIS 2)

- ➔ **Obvezna samoregistracija!**
- ➔ Določitev kontaktne osebe in namestnika
- ➔ Seznam držav članic, kjer opravljate storitve;
- ➔ Sprotno sporočanje sprememb (v 10 dneh).

VODSTVO JE ODGOVORNO ZA OBVLADOVANJE TVEGANJ (NIS 2)

- ➔ **odobrijo** ukrepe.
- ➔ **nadzirajo** izvajanje.
- ➔ **morajo usposabljati.**

- ➔ **Globe za odgovorne osebe, če tega ne izvajajo.**

IZOBRAŽEVANJE IN USPOSABLJANJE IZ KIBERNETSKE VARNOSTI (NIS 2)

- ➔ Odgovorne osebe se **morajo usposabljati iz obvladovanja tveganj kibernetske varnosti.**
- ➔ **Zaposleni** se **redno usposabljajo**, da pridobijo dovolj **znanj in spretnosti**, za prepoznavo in oceno tveganj ter oceno praks obvladovanja tveganj.
- ➔ Vsi **skrbniki IKT sistemov** obveznost rednega letnega usposabljanja.

Varnostna dokumentacija (20. čl ZInfV-1)

1. popis informacijskih in drugih sredstev ter podatkov
2. analizo obvladovanja tveganj,
3. politiko in načrt neprekinjenega poslovanja, upravljanjem varnostnih kopij;
4. načrt obnovitve in ponovne vzpostavitve delovanja
5. načrt odzivanja na incidente s protokolom obveščanja
6. načrt varnostnih ukrepov za zagotavljanje **celovitosti, avtentičnosti, zaupnosti in razpoložljivosti** omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za kibernetsko varnost,
7. politiko s postopki za oceno učinkovitosti varnostnih ukrepov za obvladovanje tveganj

UKREPI ZA OBVLADOVANJE TVEGANJ (21. čl. ZINFV-1)

1. podporo vodstva subjekta
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;
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 - 6 mesecev

UKREPI ZA OBVLADOVANJE TVEGANJ (21. čl. ZINFV-1)

7. upravljanje omrežnih in informacijskih sistemov
8. politike in postopke v zvezi z uporabo kriptografije in po potrebi šifriranjem;
9. upravljanje prometa in komunikacij;
10. varnost dobavne verige
11. fizično in tehnično varovanje prostorov in dostopov do prostorov

UKREPI ZA OBVLADOVANJE TVEGANJ (21. čl. ZINFV-1)

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,

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 OBVLADOVANJE TVEGANJ PO PREDLOGU ZInfV-1

- ➔ Preverjanje in dokumentiranje izpolnjevanja obvez v rednih časovnih obdobjih in ob zaznanih ranljivostih.
- ➔ Redno preverjanje izvajanja ukrepov.

POSTOPEK PRIGLASITVE INCIDENTOV

- ➔ Incident da/ne (hitra presoja - sami ali zunanja pomoč)
- ➔ Prijava SI-CERT(brez nepotrebnega odlašanja)
- ➔ V 24 urah po zaznavi – zgodnje opozorilo!
- ➔ V 72 urah po zaznavi – priglasitev incidenta
- ➔ Po enem mesecu končno poročilo (zelo podrobno)
- ➔ Če še po enem mesecu ni končano, se poda vmesno poročilo

VPRAŠANJA?

- Presoja vašega statusa kot možnega zavezanca po NIS 2
- Izvedbo analize vrzeli (GAP analiza)
- Izobraževanje za vodilnega presojevalca po ISO 27001?
- Izobraževanje za vodilnega implementatorja po ISO 27001?
- Dokumentacija (Pravilniki, politike, ocene tveganja, vzorci...)
- Svetovanje

info@datainfo.si 02 620 43 00