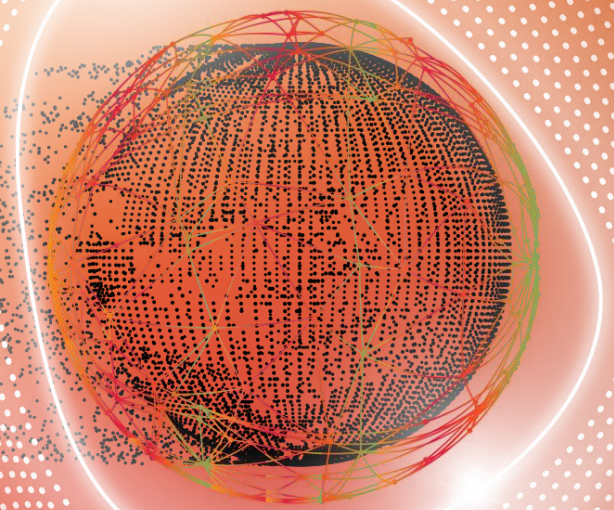


Roglit 25

NIS 2: Zakonska obveza ali zdrava kmečka pamet?

Katja Vrevc

Zavezništvo za močnejši IT ekosistem – Building a Stronger IT Ecosystem

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Agenda

- Splošne informacije o implementaciji NIS2
- Izzivi pri uvajanju zahtev iz prakse
- Ugotovitve povezane z implementacijo zahtev
- Priporočila ESCO pri implementaciji
- Dobre in slabe prakse
- Kako vam lahko ASTEC pomaga?

Od zakonske obveze do dolgoročne kibernetske odpornosti

Roglit 25

Ko pustite odklenjena vrata svojega doma, vas to skrbi. Kaj pa „odklenjena vrata“ vaše organizacije? NIS2 ni le še ena direktiva EU – je ključ do zaščite pred sodobnimi „vlomilci“ v digitalnem svetu. To ni birokratska obremenitev, ampak zdrava kmečka pamet za varno poslovanje.

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Splošne informacije o implementaciji NIS2

- Rok za prenos: **17.10.2024 –** v zakonodajo prenesle samo 4 članice

- Države, ki imajo trenutno objavljene samo osnutke (tudi Slovenija), predvidevajo da bo zakonodaja stopila v veljavo v Q1 2025

- **Pri ključni rok**: samo – registracija
- **Drugi ključni rok**: izvajanje varnostnih ukrepov

Izzivi organizacij

Različni pristopi k implementaciji zahtev:

- Klasifikacija subjektov
- Vključevanje sektorjev in raven mejnih vrednosti
- Razlike v časovnih okvirih poročanja o incidentih
- Različni roki za izpolnjevanje zahtev
- Različni okvirji (NIST, ENISA, ISO 27001/27002, GDPR, CIS Controls)

Ugotovitve povezane z implementacijo

1. Nesorazmeren vpliv na srednje velika podjetja
2. Nesorazmeren vpliv na večnacionalne družbe
3. Nesorazmeren vpliv na sektorje z nižjo stopnjo zrelosti kibernetske varnosti
4. Nesorazmeren vpliv na novo uvedene subjekte v področju uporabe
5. Neusklajenost področja uporabe in razvrščanja NIS2

Ugotovitve povezane z implementacijo

6. Raznolikost mednarodnega varnostnega okvira
7. Poročanje o incidentih po NIS2: Razlike v časovnih okvirjih in klasifikaciji
8. Pripravljenost proračuna: Investicijska vrzel v pripravljenosti organizacij
9. Vključenost vodstva: Kritična vrzel med regulativnimi predpisi in sedanjo prakso

Priporočila ECSO pri implementaciji

- Sodelovanje z deležniki
- Enotna točka za prijavo incidentov
- Standardizacija prijav incidentov
- Evropski okvir za upravljanje tveganj
- Harmonizacija varnosti dobavnih verig

Priporočila ECSO pri implementaciji

- Uporaba obstoječih standardov
- Interaktivna povezovalna tabela
- Ciljna podpora za prikrajšane subjekte
- Centraliziran informacijski center EU

Primeri dobrih praks

- PAM
- Izvajanje phishing kampanj
- Redna testiranja podpornih zmogljivosti
- Varnostna kopiranja z metodo 3 – 2 – 1
- CISO
- Stroge politike v AD
- Izvajanje notranjih presoj
- Implementacija „honey pot“ – omrežnih pasti
- Certifikacija

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Primeri dobrih praks

- ISO 27001 kot osnova za dober prehod na NIS2
- Upravljanje tveganj
- Izobraževanja in ozaveščanja
- Pridobitev certifikatov
- Odzivanje in upravljanje z incidenti
- Sodelovanje z organi in izmenjava informacij
- GAP analiza za prepoznavo področij za izboljšavo

Primeri slabih praks

- Popis sredstev: manjkajoč ali nepopoln
- Poslovni procesi: nepopoln popis
- Dostopne pravice: nedoslednosti pri dodeljevanju in odvzemanju
- Odgovorne osebe: nejasnosti pri odgovornostih za NNP v podpornih procesih
- Minimalna raven poslovanja: ni jasno določena
- Izobraževanje in usposabljanje: pomanjkanje za zaposlene v IT in vodilne
- Segmentacija omrežja: neustrezna ločitev omrežij

Primeri slabih praks

- Upravljanje ranljivosti: izhaja iz neizvedenega ali nepopolnega popisa sredstev
- Dobavna veriga: pomanjkljivo urejene varnostne zahteve
- Dokumentacija: neustrezno obvladovanje
- Usposobljen kader: Manjka kader za nadzor dobavne verige.
- Testiranje izrednih dogodkov: ni predpisanih postopkov ali izvedbe testov
- Varnostne kopije: ni izvedenih testiranj povrnitve
- Dnevniški zapisi: manjkajo

Kako vam lahko ASTEC pomaga?

Paket skladnosti: pregled stanja in priprava poročila + vzpostavitev skladnosti

Rezultat analize razkoraka:

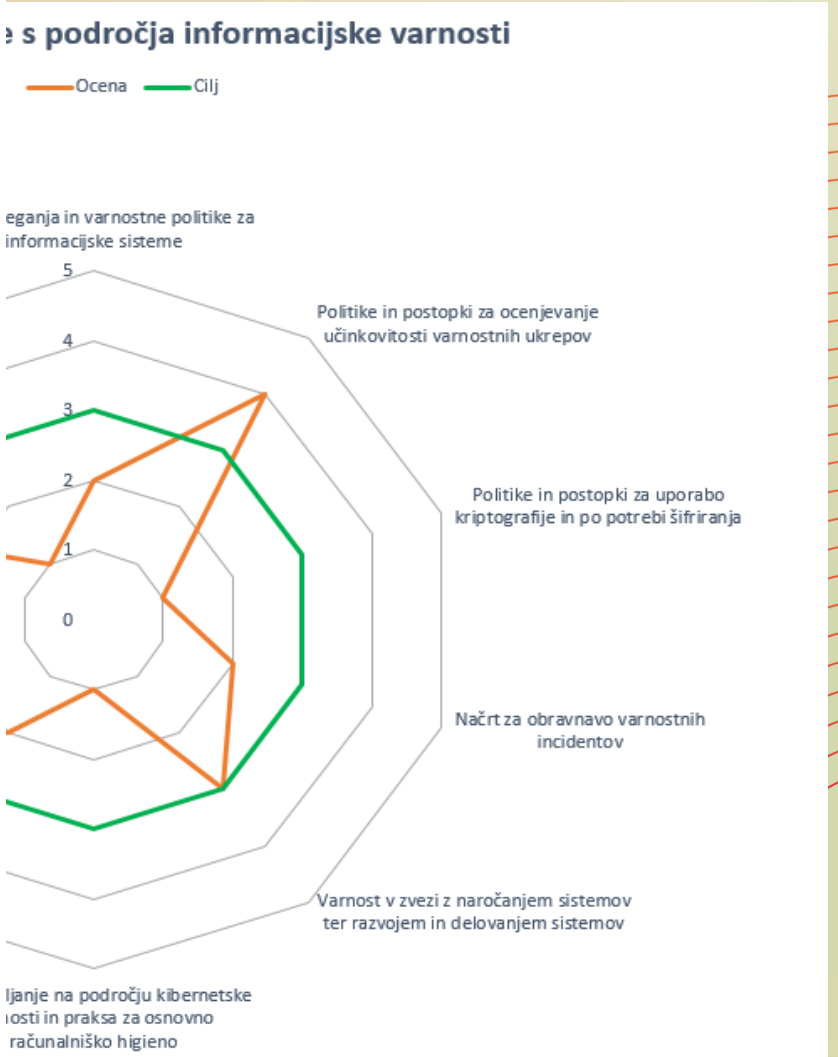
- Poročilo o izvedeni analizi
- Ocena stopnje zrelosti za posamezno domeno
- Predlog aktivnosti za zagotovitev skladnosti

Oceno zrelosti in skladnost z zahtevami lahko razširimo tudi za ISO/IEC 27001:2022 in ISO/IEC 22301:2019

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Ka ga?

Kazalo



Vprašanja?

Hvala za pozornost!

Za vsa vprašanja prosim kontaktirajte info@astec.si

Roglit 25

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Roglit 25

Zaključek

RoglIT is more than just another conference.

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company