BIZMATCH
POVEZUJEMO POSEL

DIREKTIVA NIS2

KREPITEV KIBERNETSKE ODPORNOSTI POSLOVANJA Z IMPLEMENTACIJO NIS2

Direktiva o varnosti omrežij in informacij (NIS) je ključna zakonodaja Evropske unije za izboljšanje kibernetske varnosti v EU. Z uvajanjem NIS2 pa direktiva prinaša številne spremembe, ki zahtevajo pozornost in prilagoditev s strani podjetij, vključenih v ključne sektorje.

KLJUČNE INFORMACIJE, KI BI MORALO POZNATI VSAKO PODJETJE

VEČ NA BLOGU

Direktiva NIS je zakonski okvir, ki ga je Evropska unija sprejela leta 2018 za izboljšanje varnosti kritične infrastrukture in IT storitev v EU. Njena nadgradnja, znana kot NIS2, ki je v veljavi od januarja 2023 in se pri nas prenese v nacionalno zakonodajo do 17. 10. 2024, prinaša številne spremembe. Razširja obseg zajetih sektorjev in organizacij, uvede dve kategoriji subjektov - bistvene in pomembne, ki morajo izpolnjevati enake zahteve, razlikuje pa se le v nadzornih ukrepih in višini kazni.

NIS2 opredeli 11 bistvenih in 7 pomembnih sektorjev. Uvaja strožja pravila za poročanje o varnostnih incidentih ter ukrepe za odpravljanje kibernetskih tveganj, hkrati pa vzpostavlja podroben nadzor in določa visoke finančne kazni za kršitve.

BISTVENA IN POMEMBNA INFRASTRUKTURA

VEČ NA BLOGU

Bistvena in pomembna infrastruktura po NIS2 zajema ključne sektorje, ki so nujni za delovanje družbe.

Med **bistvene storitve** po NIS2 spadajo energija, promet, bančništvo, infrastrukture finančnega trga, zdravstvo, pitna voda, odpadne vode, digitalna infrastruktura, podjetja za upravljanje medpodjetniških storitev, javna uprava in vesolje.

Poleg tega NIS2 zajema tudi **pomembne storitve**, kot so poštne in kurirske storitve, ravnanje z odpadki, izdelava in distribucija kemikalij, pridelava ter distribucija živil, proizvodnja medicinskih pripomočkov in računalnikov, ponudniki digitalnih storitev spletnih tržnic in platform za družabna omrežja ter raziskave.

KAKO SKLADNOST Z NIS2 KREPI ODPORNOST POSLOVANJA VAŠEGA PODJETJA?

VEČ NA BLOGU

S podrobno določenimi varnostnimi ukrepi, kot so ocene tveganj, uvedba kibernetskih varnostnih ukrepov, izobraževanje osebja in načrti za obvladovanje incidentov, krepi zaščito pred kibernetskimi napadi in zmanjšuje tveganja.

Pomembno je poudariti, da NIS 2 ne le zagotavlja varnost pred napadi, ampak tudi **spodbuja vzpostavitev odpornosti poslovanja**. To pomeni, da se organizacije osredotočajo na **zagotavljanje neprekinjenega obratovanja** in **vzpostavitev učinkovitih odzivov** v primeru izpadov, kar prispeva k trajnosti poslovanja.

Vabljeni na praktično delavnico:
KREPITEV KIBERNETSKE ODPORNOSTI POSLOVANJA Z IMPLEMENTACIJO DIREKTIVE NIS2

Delavnico vodi: Božo Berič, strokovnjak za kibernetsko varnost in operativno odpornost
Termini: 5. 6. 2024 (9.00 - 11.00) ali 14. 6. 2024 (9.00 - 11.00)
Cena: 99 EUR + DDV/oseba (30 % popust na 2. prijavljeno osebo iz istega podjetja)
Lokacija: Sinecon, d.o.o., Tacenska cesta 26, 1000 Ljubljana

VEČ INFORMACIJ IN PRIJAVA

Število mest je omejeno!

PRILAGODITEV POLITIKE INFORMACIJSKE VARNOSTI IN NEPREKINJENEGA POSLOVANJA

VEČ NA BLOGU

Veliko subjektov, zavezanih k izpolnjevanju NIS2, že ima vzpostavljeno strategijo informacijske varnosti in neprekinjenega poslovanja ter mehanizme za zagotavljanje odpornosti.

Prilagoditev na zahteve NIS2 vključuje:

1. Pregled ključnih področij
2. Posodobitev politik
3. Redno izobraževanje zaposlenih
4. Vzpostavitev komunikacijskih kanalov z organi
5. Izboljšanje odpornosti poslovanja

PRAKTIČNI NASVETI ZA IMPLEMENTACIJO NIS2 V VAŠE PODJETJE

VEČ NA BLOGU

Pri implementaciji NIS2 v vaše podjetje gre v večini primerov za prilagoditev politike informacijske varnosti in neprekinjenega poslovanja ter vzpostavitev sistema poročanja. Ključno pa je tudi vzpostaviti dejanske procese za izvedbo teh politik, ki zagotavljajo dejansko odpornost poslovanja.

To vključuje dosledno izvajanje varnostnih politik, prilagoditev infrastrukture ter življenjsko in uporabno izvajanje ukrepov za preprečevanje groženj, ki ne vplivajo na učinkovitost poslovanja.

Vabljeni na praktično delavnico:

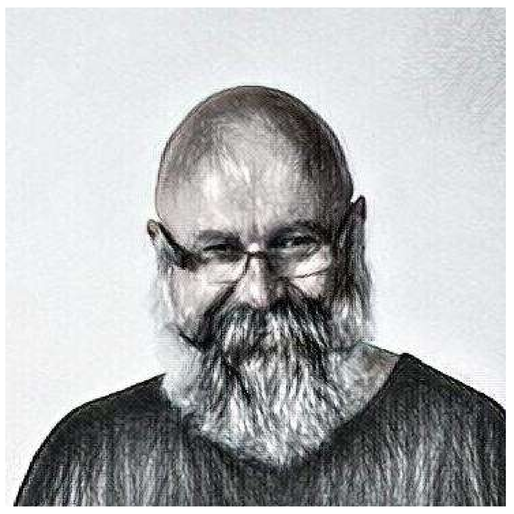
KREPITEV KIBERNETSKE ODPORNOSTI POSLOVANJA Z IMPLEMENTACIJO DIREKTIVE NIS2

Termini: 5. 6. 2024 (9.00 - 11.00) ali 14. 6. 2024 (9.00 - 11.00)
Cena: 99 EUR + DDV/oseba (30 % popust na 2. prijavljeno osebo iz istega podjetja)
Lokacija: Sinecon, d.o.o., Tacenska cesta 26, 1000 Ljubljana

Ključni poudarki:

- Zakaj je poznavanje direktive NIS2 nujno za odpornost poslovanja vašega podjetja
- Bistvene spremembe, ki jih prinaša NIS2, uvedba kategorij subjektov, poročanje, kazni za kršitve
- Praktični varnostni ukrepi in načrti za obvladovanje incidentov za zaščito pred kibernetskimi napadi
- Politika informacijske varnosti in praktični nasveti za vzpostavitev dejanskih procesov za izvajanje ukrepov

Delavnico vodi: Božo Berič



Božo je izkušen strokovnjak na področju kibernetske varnosti, operativne odpornosti in infrastrukture podatkovnih centrov. Njegova bogata kariera sega na področja podpore, upravljanja z incidenti, shranjevanja podatkov, sistemske administracije, svetovanja za vzpostavitev infrastrukture. Bil je eden od pionirjev pri uvedbi modela in koncepta zunanjega izvajanja storitev v Sloveniji ter razvil metodologijo ocene tveganj podporne infrastrukture informatike.

Skozi številna leta na področju, je Božo pridobil izjemno poznavanje infrastrukture podatkovnih centrov, optimizacije IT infrastrukture in procesov ter implementacije varnostnih rešitev. Njegova strokovnost je izkazana tudi s certifikati kot so vodilni presojevalec za standard ISO 27001, presojevalec za ISO 22301, ter certifikati kot DORATPro, NIS2DTP, IQ Net DPO ...

Zaradi dolge kariere v operativi, se Božo ne omejuje zgolj na teorijo, temveč tudi na praktično implementacijo rešitev. S pristopom, ki temelji na izkušnjah in prilagodljivosti, pomaga podjetjem razumeti in izboljšati odpornost poslovanja.

VEČ INFORMACIJ IN PRIJAVA

Število mest je omejeno!