BIZMATCH
POVEZUJEMO POSEL

VARNO V FINANCAH

GRADNJA ODPORNOSTI POSLOVANJA V DIGITALNI DOBI Z UREDBO DORA

DORA predstavlja pomemben korak v smeri zagotavljanja visoke ravni kibernetske varnosti in operativne odpornosti v finančnem sektorju. Z uvajanjem standardiziranih smernic in zahtev za varovanje podatkov ter odzivanje na kibernetske grožnje, DORA postavlja temelje za trajno zaščito finančnih institucij pred vedno bolj kompleksnimi kibernetskimi napadi.

KAKO DORA VPLIVA NA ODPORNOST POSLOVANJA?

VEČ NA BLOGU

DORA predpisuje osnovno kibernetsko higieno za vse udeležence na finančnem trgu kot so banke, investicijska podjetja, zavarovalnice in posredniki, ponudniki kripto sredstev ... vključno z zunanjimi ali tretjimi ponudniki storitev IKT.

Pomemben vidik, ki ga uvaja DORA, in ima velik vpliv na zagotavljanje odpornosti poslovanja, pa je tudi poročanje o incidentih ter deljenje informacij o kibernetskih grožnjah, kar omogoča lažji in boljši ter usklajen odziv na kibernetske grožnje.

Glavni cilji uredbe DORA:

- **Okrepiti odpornost poslovanja v finančnem sektorju.**
- **Zmanjšati verjetnost in resnost kibernetskih incidentov.**
- **Omogočiti učinkovit odziv v primeru njihovega nastanka.**

PRAKTIČNI NASVETI ZA USPEŠNO IMPLEMENTACIJO

VEČ NA BLOGU

DORA vzpostavlja regulativni okvir za digitalno operativno odpornost, pri čemer morajo vsa podjetja zagotoviti, da lahko vzdržijo različne vrste motenj in groženj, povezane z IKT, ter se nanje odzovejo in si opomorejo. Večina podjetij v finančnem sektorju ima že sedaj vzpostavljeno strategijo informacijske varnosti in neprekinjenega poslovanja ter določene mehanizme za zagotavljanje odpornosti poslovanja. Tako se obstoječe stanje prilagodi in po potrebi nadgradi za skladnost z uredbo DORA.

DORA uvaja politike za:

- **obvladovanje tveganj,**
- **testiranje digitalne operativne odpornosti,**
- **izmenjavo informacij in obveščevalnih podatkov v zvezi s kibernetskimi grožnjami.**

Implementacija teh smernic zahteva usklajeno delo med različnimi oddelki v podjetju ter pogosto sodelovanje s tretjimi ponudniki storitev IKT.

ZAKAJ JE SKLADNOST NUJNA ZA ZAŠČITO PODATKOV VAŠIH STRANK?

VEČ NA BLOGU

Zahteve uredbe DORA so namenjene zagotavljanju odpornosti poslovanja, kar pomeni tudi razpoložljivost, avtentičnost, celovitost in zaupnost podatkov. Tako je skladnost z uredbo DORA med drugim pomembna tudi za zaščito podatkov vaših strank.

Vabljeni na praktično delavnico:

GRADNJA ODPORNOSTI POSLOVANJA IN KONTINUIRANEGA DELOVANJA ZA PODJETJA V FINANČNEM SEKTORJU

Delavnico vodi: Božo Berič, strokovnjak za kibernetsko varnost in operativno odpornost
Termini: 10. 6. 2024 (9.00 - 11.00) ali 17. 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:

- Pomen odpornosti poslovanja v finančnem sektorju in pregled ključnih standardov in regulativ
- Praktični nasveti za uspešno implementacijo uredbe DORA v podjetjih in za izboljšanje odpornosti poslovanja

VEČ INFORMACIJ IN PRIJAVA

Število mest je omejeno!

KAKO IZGRADITI ROBUSTNO OKOLJE, SKLADNO Z ZAHTEVAMI UREDBE DORA?

VEČ NA BLOGU

Izgradnja robustnega okolja, ki je skladno z zahtevami uredbe DORA, zahteva celovit pristop in integracijo različnih vidikov kibernetske varnosti ter operativne odpornosti.

Koraki, ki lahko pomagajo pri tem, so:

1. Izdelava analize vplivov na poslovanje.
2. Ocena tveganj (vključno z zunanjimi in 3. ponudniki storitev IKT).
3. Vzpostavitev politik in postopkov.
4. Vzpostavitev mehanizmov za odkrivanje in odzivanje.
5. Vzpostavitev sistema poročanja pristojnim organom.

Po potrebi sodelujte z zunanjimi strokovnjaki, kot so svetovalci za kibernetsko varnost, ki vam lahko pomagajo pri izgradnji robustnega okolja skladno z zahtevami DORA. Ti strokovnjaki lahko zagotovijo dragocene nasvete in podporo pri izvajanju najboljših praks ter pomagajo pri identifikaciji ranljivosti in izboljšanju celotne kibernetske varnosti v vašem podjetju.

POMEN PODPORNE INFRASTRUKTURE ZA ODPORNOST POSLOVANJA IN ANALIZA TVEGANJ PODPORNE INFRASTRUKTURE

VEČ NA BLOGU

DORA ne pomeni zgolj stroge osredotočenosti na kibernetsko varnost, ampak tudi na kibernetsko odpornost. V praksi to pomeni, da se organizacije ne borijo le proti grožnjam, ki jih lahko predstavljajo kibernetski napadi, ampak da storijo vse za ohranitev poslovanja, tudi z vzpostavitvijo primerne podporne infrastrukture, ki bo zagotavljala neprekinjeno obratovanje in vzpostavitev odzivov v primeru izpadov.

Podporna infrastruktura je tisti prepogosto zanemarjen in podcenjen, najnižji nivo informatike. A v resnici gre za tako osnovne zadeve, kot so fizična varnost, prostor, napajanje, hlajenje ... V kolikor bi IKT sistem primerjali s hišo, bi podporna infrastruktura predstavljala temelje, na katerih stoji vsa nadaljnja struktura.

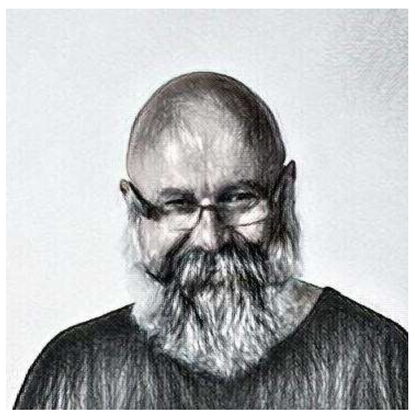
Vabljeni na praktično delavnico:

GRADNJA ODPORNOSTI POSLOVANJA IN KONTINUIRANEGA DELOVANJA ZA PODJETJA V FINANČNEM SEKTORJU

Termini: 10. 6. 2024 (9.00 - 11.00) ali 17. 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:

- Pomen odpornosti poslovanja v finančnem sektorju in pregled ključnih standardov in regulativ
- Praktični nasveti za uspešno implementacijo uredbe DORA v podjetjih in za izboljšanje odpornosti poslovanja

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!