Varuhi kibernetske varnosti

Mesec kibernetske varnosti

Vse večji razkorak med organizacijami, ki primerno obvladujejo kibernetska tveganja in tistimi, ki jih ne

Kako premostiti vrzel?

Vse večji razkorak med organizacijami, ki primerno obvladujejo kibernetska tveganja in med tistimi, ki jih ne

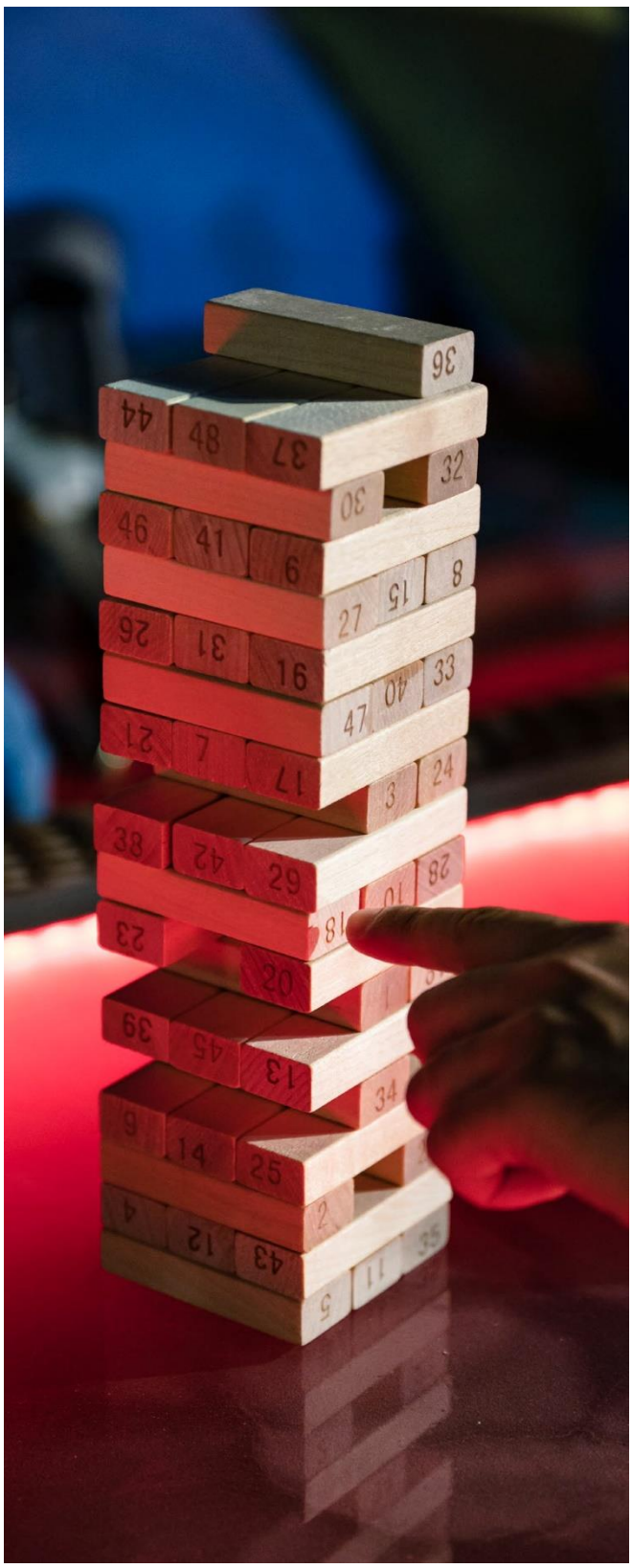
Naš nasvet

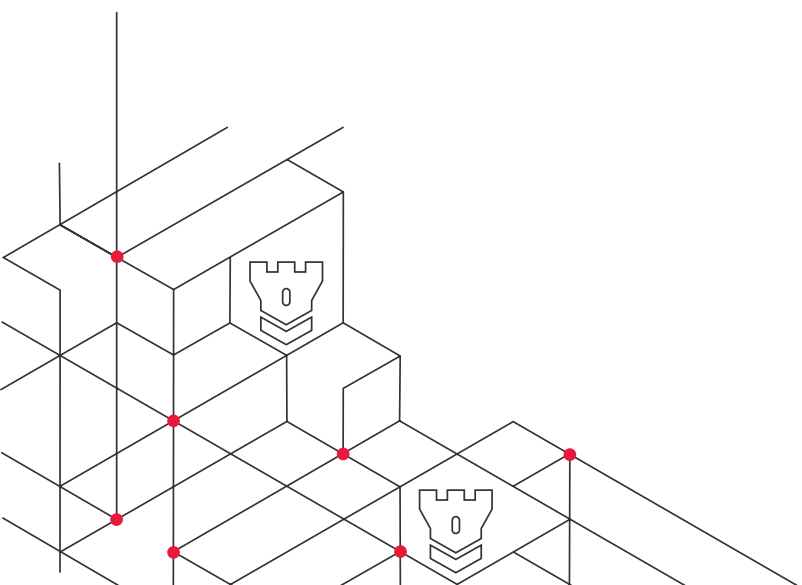
V letu 2024 so kibernetski napadi, ki so povzročali motnje v poslovanju, kot je npr. "ransomware", prizadeli organizacije v različnih panogah. Naštejmo le nekaj primerov: danski WS Audiology, Transport for London, igralnice MGM in Ceasar's Casino v ZDA, letališče SeaTac v Seattlu ter številne druge.

Zaradi vse večjih nevarnosti na tem področju je postalo obvladovanje tveganj v zvezi s tem ključnega pomena.

Ker so kibernetske grožnje vse pogostejše in bolj zapletene, se vrzel med organizacijami, ki tveganja na tem področju obvladujejo in tistimi, ki jih ne, povečuje. Nedavni incidenti opozarjajo na pomembne učinke kibernetskih napadov na ugled, finančni položaj in poslovanje organizacij.

Svetovni gospodarski forum navaja kibernetske napade kot eno največjih globalnih tveganj, pandemija COVID-19 pa je še povečala izpostavljenost organizacij tem tveganjem.





Razumevanje kibernetske varnosti

Obvladovanje kibernetskih tveganj je širši pojem kot tradicionalno zagotavljanje kibernetske varnosti, ki se osredotoča predvsem na preprečevanje napadov. Namesto tega zajema celovit pristop, ki vključuje sposobnost priprave na kibernetske incidente, odziva nanje in okrevanja po njih. Kibernetsko odporna organizacija ni sposobna le obrambe pred napadi, temveč tudi zagotavljanja kontinuitete in hitrega okrevanja, ko do incidenta pride.

Obvladovanje kibernetskih tveganj zahteva razumevanje teh tveganj ter premišljeno upravljanje z njimi. Primeren pristop upravljanja tveganj na tem področju vključuje zbiranje in analizo vseh ustreznih informacij, učenje iz incidentov in sprejemanje primernih odločitev, ki zmanjšujejo morebitne negativne vplive na organizacijo.

Bistveni elementi premišljenega obvladovanja tveganj so:

01

Prepoznavanje tveganj - Prepoznavanje morebitnih tveganj, ki bi lahko vplivala na organizacijo.

02

Ocena tveganja - Ocenjevanje verjetnosti nastanka in vpliva škodnega dogodka.

03

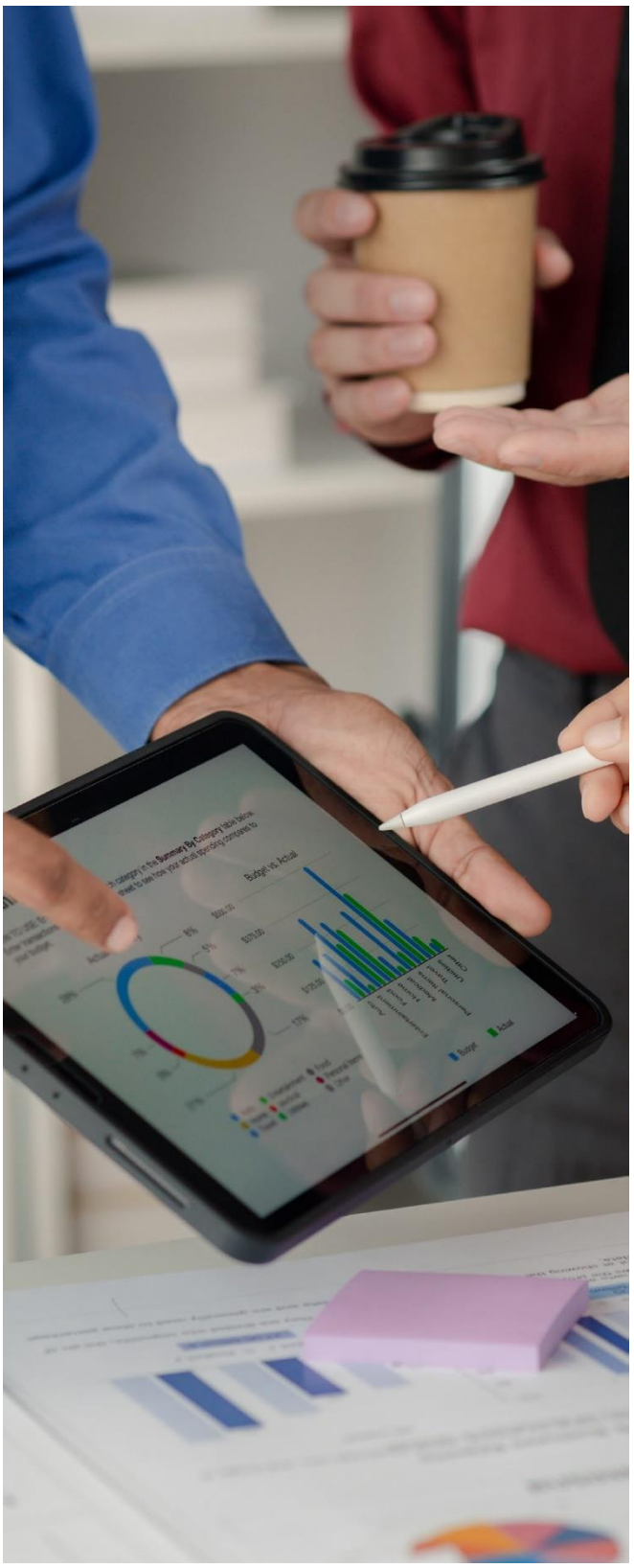
Določitev prioritetne liste tveganj - Identifikacija tveganj, ki jim je treba posvetiti takojšnjo pozornost glede na njihov potencialni vpliv.

04

Zmanjšanje tveganj - Izvajanje strategije za zmanjšanje ali obvladovanje ugotovljenih tveganj.

05

Stalno spremljanje, redno pregledovanje in posodabljanje izbrane strategije obvladovanja tveganj zaradi prilagajanja novim informacijam in spreminjajočim se okoliščinam.



Z uporabo takšnega pristopa k obvladovanju tveganj je zagotovljeno:

01

Preprečevanje:
Izvajanje zanesljivih ukrepov kibernetske varnosti za preprečevanje napadov.

02

Odkrivanje:
Hitro prepoznavanje in ocenjevanje kibernetskih groženj.

03

Odziv:
Učinkovito upravljanje in zmanjševanje vpliva kibernetskih incidentov.

04

Okrevanje:
Čim prejšnja/takojšnja ponovna vzpostavitev normalnega delovanja in učenje iz incidentov za izboljšanje odpornosti v prihodnosti.

V čem je ta vse večji razkorak med organizacijami, ki obvladujejo kibernetska tveganja in tistimi, ki ne obvladujejo kibernetskih tveganj?

Poročilo Svetovnega gospodarskega foruma Globalno poročilo o kibernetski varnosti, navaja, da se neenakost iz leta v leto povečuje. 90 % vodstvenih delavcev, anketiranih na letnem srečanju Svetovnega gospodarskega foruma o kibernetski varnosti v letu 2023, je izjavilo, da so za odpravo razlik potrebni nujni ukrepi.

Nekatere organizacije so pri obravnavanju kibernetskih tveganj in vzpostavljanju kibernetske odpornosti bolj pripravljene in proaktivne kot druge. Po podatkih poročila je 74 % organizacij še vedno novink na tem področju.

Organizacije, ki obvladujejo kibernetska tveganja, imajo jasno in celovito kibernetsko strategijo, močno in podporno kibernetsko kulturo, sposobnost privabljanja talentov, trdno in prožno kibernetsko tehnološko zmogljivost ter učinkovit in odgovoren program upravljanja kibernetskih tveganj.

Razvoj in uvajanje novih tehnologij bosta zagotovo povečala že obstoječe izzive, prav tako pa se bodo povečale vrzeli na področju kibernetskega znanja in spretnosti ter pomanjkanje nadarjenih kadrov. Poleg tega bo pojav umetne inteligence naslednjih letih nedvomno pospešil kibernetske napade.

Pomen obvladovanja kibernetskih tveganj

Primerno upravljanje kibernetskih tveganj je zaradi stalno naraščajočega tehnološkega napredka ob stalno naraščajoči prisotnosti kibernetskih groženj, neprecenljivo. Posledice kibernetskih incidentov so lahko hude - od finančnih izgub in motenj v delovanju do škode ugleda in finančnih posledic (kazni).

01

Finančna zaščita

Kibernetski napadi lahko povzročijo velike finančne izgube. Za organizacije, ki primerno obvladujejo kibernetska tveganja, bodo te izgube verjetno manjše, saj bodo okrevalni časi in povratek v normalno delovanje verjetno krajši kot pri ostalih.

02

Neprekinjeno delovanje

Ohranjanje poslovanja med kibernetskim napadom in po njem je ključnega pomena. Primerno obvladovanje tveganj na tem področju zagotavlja, da lahko organizacija zagotavlja izvajanje vsaj ključnih aktivnosti, kar zmanjšuje čas izpada in motenj.

03

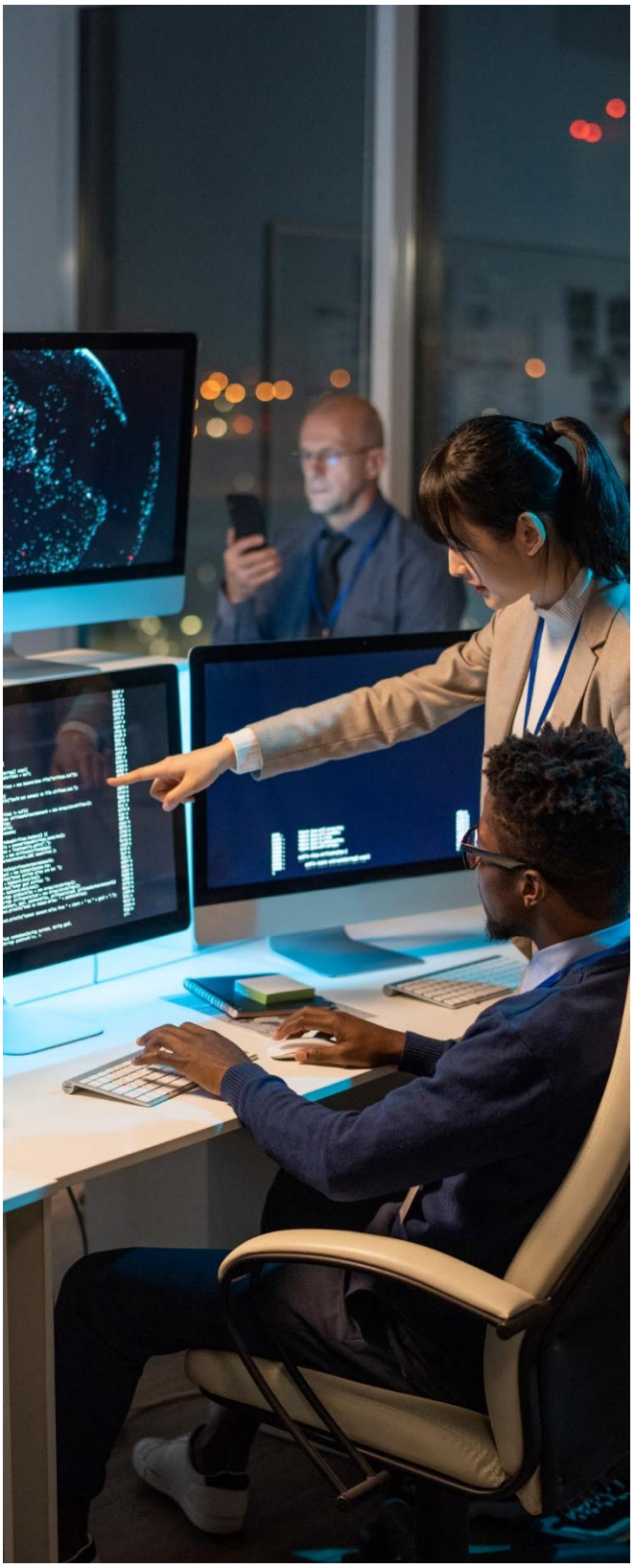
Integriteta ugleda

Zaupanje je dragoceno sredstvo. Organizacije, ki primerno obvladujejo kibernetska tveganja, bodo verjetno lažje ohranjala zaupanje svojih poslovnih partnerjev.

04

Skladnost s predpisi:

GDPR, DORA, NIS 2 so le nekateri od predpisov, ki zahtevajo primerno obvladovanje kibernetskih tveganj in v nasprotnem primeru predvidevajo visoke kazni.



Globalni pogledi na zagotavljanje kibernetske varnosti

Svetovne institucije, kot so vlade in Svetovni gospodarski forum (WEF), priznavajo ključno potrebo po ustreznem obvladovanju kibernetskih tveganj in zagotavljajo smernice za pomoč organizacijam pri krepitvi njihove obrambe.

01

Vladne pobude:

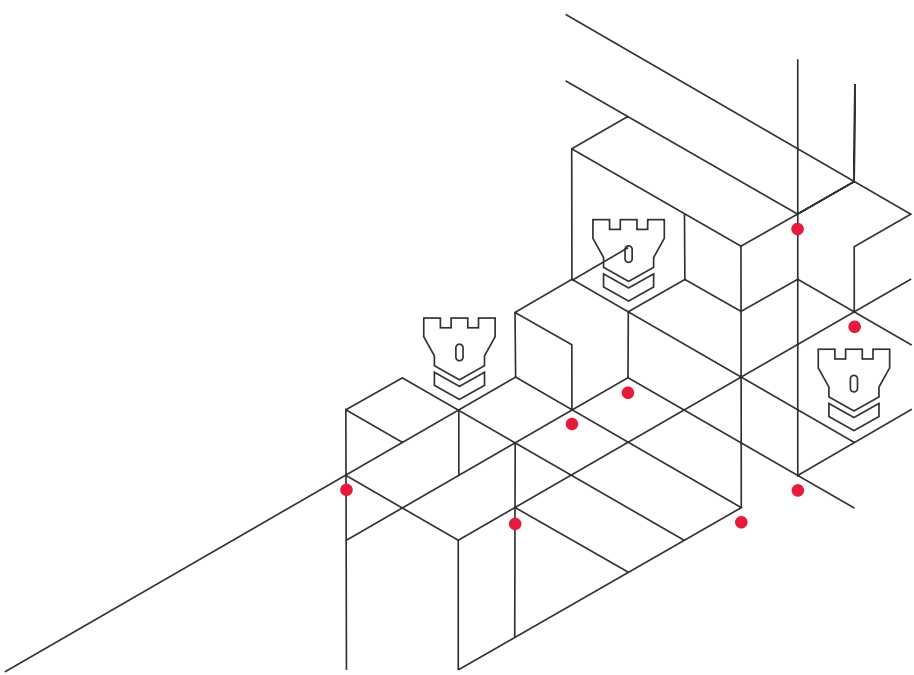
- **Okvir kibernetske varnosti NIST**: Nacionalni inštitut za standarde in tehnologijo ZDA (NIST) zagotavlja dobre prakse na področju zagotavljanja kibernetske varnosti, ki je splošno sprejet v različnih panogah.
- **Direktiva o ukrepih za visoko skupno raven kibernetske varnosti v EU (NIS 2)**: Organizacije v kritičnih sektorjih, kot so energetika, promet, bančništvo in zdravstvo, bodo morale izvajati ustrezne ukrepe za obvladovanje kibernetskih tveganj.
- **Akt EU o kibernetski varnosti**: Cilj Akta EU o kibernetski varnosti je okrepiti varnost digitalnih produktov in storitev ter spodbujati visoko raven kibernetske odpornosti v državah članicah.
- **ASEAN** še nima enotnega zakona ali direktive o kibernetski varnosti. Je pa pripravil celovito strategijo sodelovanja na področju kibernetske varnosti za obdobje 2021-2025, ki se osredotoča na pospeševanje kibernetske pripravljenosti, usklajevanje regionalnih kibernetskih politik, krepitev zaupanja v kibernetski prostor in krepitev regionalnih zmogljivosti.
- Gospodarska komisija Združenih narodov za Latinsko Ameriko in Karibe (ECLAC) je vključila kibernetsko varnost v svojo digitalno agendo.

02

Svetovni gospodarski forum (WEF):

- WEF poudarja pomen javno-zasebnih partnerstev pri krepitvi kibernetske varnosti. V svojih poročilih poudarjajo potrebo po skupnem pristopu k reševanju kibernetskih groženj in priporočajo dobre prakse za obvladovanje tveganj na tem področju.
- Center WEF za kibernetsko varnost se zavzema za globalno sodelovanje ter ponuja vire in forume, na katerih lahko organizacije izmenjujejo znanje in strategije na področju kibernetske zagotavljanja kibernetske varnosti.

Nova evropska direktiva Network and Information Security Directive 2 (NIS2) naj bi začela veljati že oktobra 2024. Tudi BDO je razvil zelo uporabno orodje za ocenjevanje NIS 2, ki vam lahko zagotovi takojšen vpogled v vašo trenutno situacijo.



Strategije za povečanje kibernetske varnosti

Za zagotavljanje čim boljše kibernetske varnosti za vašo organizacijo lahko sprejmete več proaktivnih ukrepov, kot so:

01

Pripravite načrt

Pripravite celovit načrt, ki zajema preventivne ukrepe, protokole za odzivanje na incidente in strategije obnovitve. Poskrbite, da bo načrt usklajen s poslovno strategijo in cilji; redno ga pregledujte in posodabljajte, da bo odražal spreminjajoče se kibernetsko okolje in poslovne potrebe.

02

Vlagajte v kibernetsko tehnologijo

Vlagajte v kibernetsko tehnologijo za upravljanje napadov, nadzor nad varovanjem podatkov, umetno inteligenco in strojno učenje. Ustvarite okolje, ki organizaciji omogoča odkrivanje kibernetskih groženj in incidentov, odzivanje nanje in okrevanje po njih, hkrati pa dragocenim virom zagotavlja možnost razbremenitve zaradi avtomatizacije nalog.

03

Spodbujajte kulturo kibernetske ozaveščenosti:

Spodbujajte kulturo, v kateri je kibernetska varnost skupna odgovornost in ki daje pooblastila vsem ravnem organizacije.

04

Izvajajte redna usposabljanja

95 % kibernetskih napadov je posledica človeških napak, kar daje izjemen pomen izobraževanju in ozaveščanju zaposlenih.

05

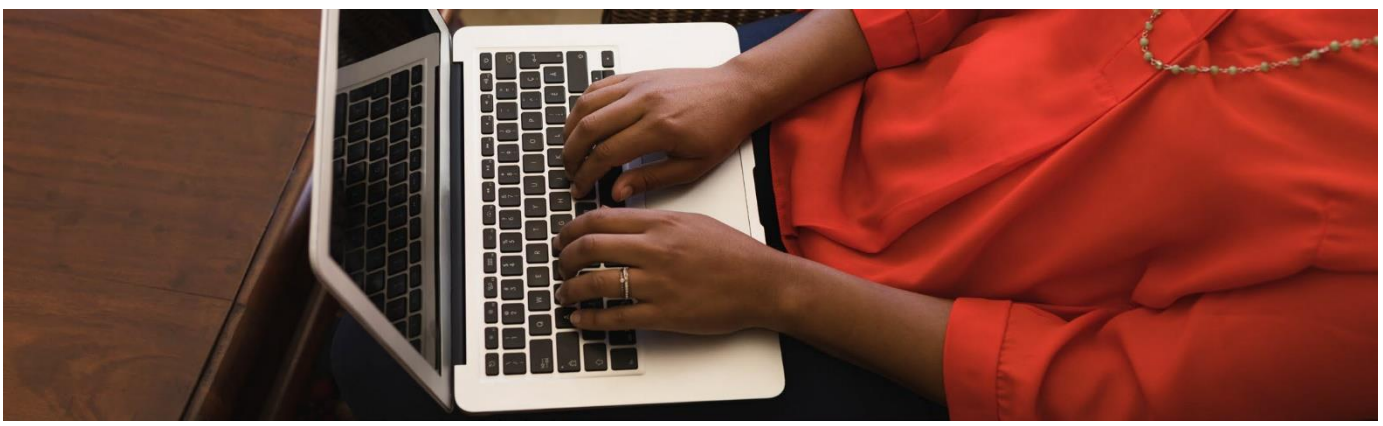
Vzpostavite kibernetsko upravljanje

Vzpostavite upravljanje kibernetske varnosti na način, da ta opredeljuje vloge in odgovornosti, tudi uprave in pristojnih za upravljanje. Sprejmite jasne in dosledne politike, standarde in postopke za upravljanje kibernetskih tveganj ter spremljanje, poročanje in ukrepanje na področju skladnosti.

06

Izvajajte redne revizije in ocene

Izvajajte stalno ocenjevanje ukrepov kibernetske varnosti in ukrepov za odkrivanje in odpravljanje ranljivosti.



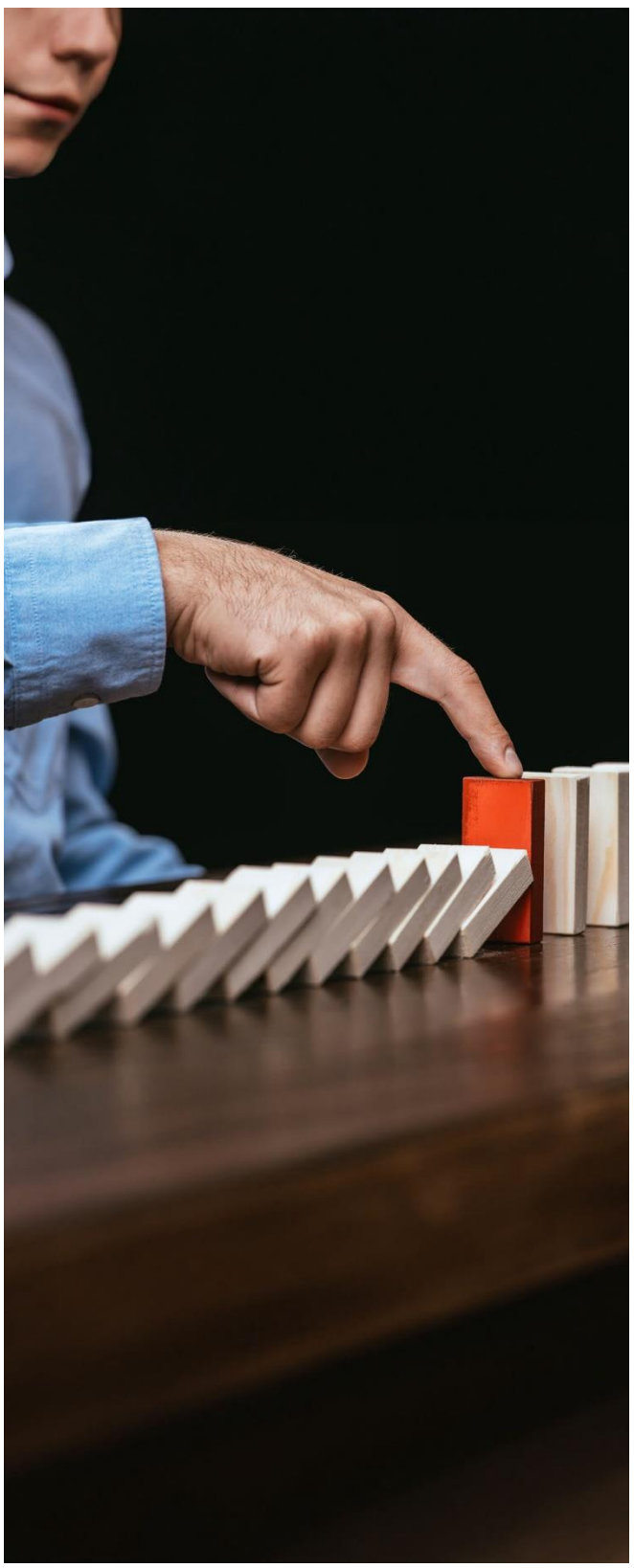
Zaključek

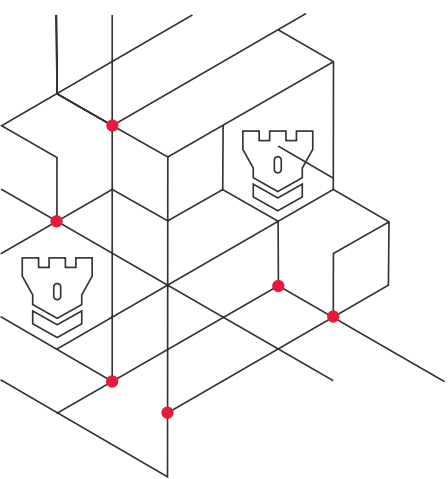
Vedno večji razkorak med organizacijami, ki obvladujejo kibernetska tveganja in tistimi, ki na tem področju niso najbolj uspešne, kaže na to, da je treba kibernetsko varnost nujno postaviti na prvo mesto in jo vključiti med ključne poslovne cilje.

Z razumevanjem njenega pomena, izkoriščanjem globalnih spoznanj in izvajanjem strateških ukrepov lahko organizacije zavarujejo svoja sredstva, ohranijo neprekinjeno delovanje in gradijo zaupanje v vse bolj digitalnem svetu.

Ne gre več za vprašanje ali, temveč kdaj bo vaša organizacija ogrožena. Kibernetski kriminal ne bo prizanesel nobeni državi ali organizaciji, zato je ključnega pomena, da čim prej poskušate zapolniti vrzeli, ki jih identificirate na področju zagotavljanja kibernetske varnosti.

Kibernetske grožnje se stalno razvijajo, zato se mora stalno razvijati tudi naš pristop obvladovanja teh groženj, tako da bomo na področju kibernetske varnosti vedno korak pred drugimi.





Kako lahko BDO pomaga?

Temelji, ki so jih vzpostavili strokovnjaki za kibernetsko varnost, delujejo. BDO-jevo globalno prakso kibernetske varnosti sestavljajo strokovnjaki iz različnih področij, vključno z izkušenimi svetovalci za IT, varnost podatkov ter strokovnjaki za forenzično tehnologijo, poslovno svetovanje in računovodstvo.

Ustvarjeni smo tako, da vsaki stranki zagotavljamo celovite in prilagojene storitve, pri čemer se osredotočamo na vsako stranko posebej, njene tehnične zahteve, regulatorno okolje in dinamiko panoge.

Ne glede na to, ali gre za finančne storitve, zdravstvo, trgovino, naravne vire ali katero koli drugo panogo, razumemo vaše potrebe. Naš globalni odtis sega v vse kotičke sveta, prav tako kot kibernetski kriminal.

Dovolite nam, da vaši organizaciji, ne glede na to, kje ste, pomagamo zmanjšati kibernetska tveganja, s katerimi se soočate.

Manuela Šribar
manuela.sribar@bdo.si

9,22 bilijonov USD

stroški kibernetske kriminalitete po svetu v letu 2023

Svetovni stroški kibernetskega kriminala naj bi do leta 2027 narasli na

23,84 bilijonov USD

do leta 2027,

v primerjavi z 8,44 bilijona dolarjev leta 2022 (Statista).

46%

predstavlja delež organizacij, ki po napadu z izsiljevalsko programsko opremo plačajo odkupnino.

1,9 milijonov

globalno število edinstvenih groženj, o katerih so poročali končni uporabniki v letu 2023