Varuhi kibernetske varnosti

Mesec kibernetske varnosti

Kako lahko uprave izboljšajo svoje znanje o kibernetski varnosti:

6 strategij za zaščito organizacije pred kibernetskimi grožnjami

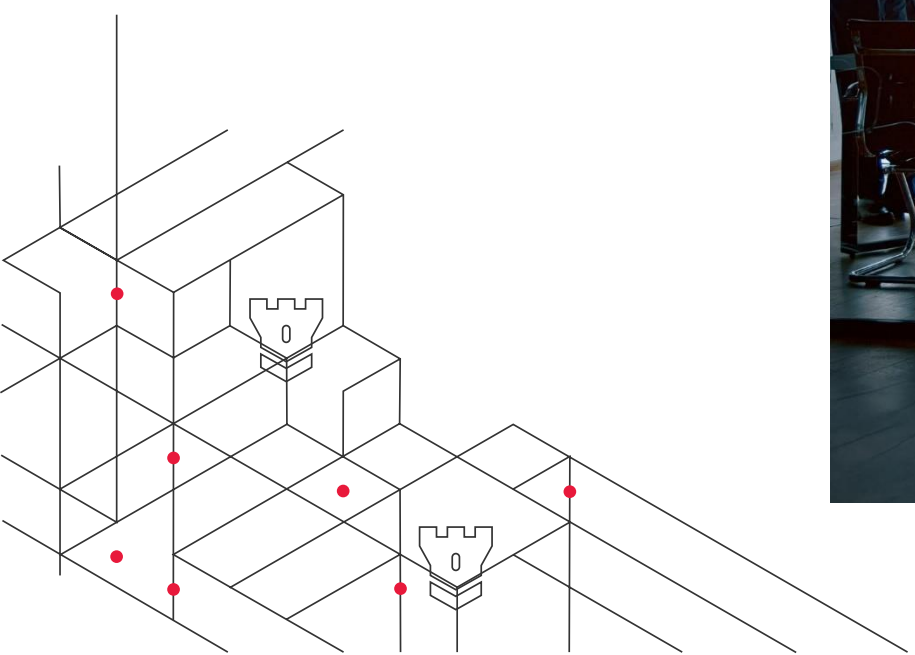
BDO

Kako lahko uprave izboljšajo svoje znanje o kibernetski varnosti: šest strategij za zaščito organizacije pred kibernetskimi grožnjami

Incidenti kibernetske varnosti niso le vse pogostejši, ampak tudi vse dražji: povprečni stroški ene kršitve varnosti podatkov (incidenta) v letu 2024 znašajo 4,88 mio USD, kar je 10 % več kot v letu 2023. Gre za najvišje stroške v zgodovini na tem področju. Seveda finančne posledice niso edini strošek, s katerim se organizacije soočajo ob kibernetskih incidentih – pogosto sta posledica tudi izguba ugleda in operativna škoda.

Člani uprav morajo imeti aktivno vlogo pri zmanjševanju in preprečevanju kibernetskih napadov. Uprava je odgovorna za vzpostavitev takšnega kontrolnega okolja, ki zagotavlja znižanje tveganj na vseh področjih poslovanja na sprejemljivo raven – IT področje ni izjema. Zanimivo je, da ima le 12% družb iz skupine S&P 500 sedanjega ali nekdanjega člana uprave, ki je strokovnjak za kibernetsko področje. Vrzel v znanju na tem področju lahko škoduje vaši organizaciji - zdaj in v prihodnosti.

Kako lahko zagotovite, da se vaša organizacija ne bo znašla v zadnjem krogu novic o kršitvah kibernetske varnosti? Začnite s postavljanjem pravih vprašanj.



Kako naj uprava pripomore k zagotavljanju obvladovanja kibernetskih tveganj oz. kibernetske varnosti?

Tehnološke zmogljivosti so se v zadnjih letih močno povečale, kar organizacijam omogoča učinkovitejše delovanje. Ker je tehnologija vse bolj prepletena s poslovnimi cilji, morajo člani uprav tehnološke odločitve obravnavati na enak način kot strateške poslovne odločitve. Tehnologija je del poslovnih odločitev vsake organizacije.

Uprava je dolžna upravljati z IT tveganji na enak način kot z ostalimi poslovnimi tveganji s katerimi se srečuje organizacija. To doseže s/z:

01

strateškim usklajevanjem:
zahteve/potrebe po kibernetski varnosti naj bodo usklajene s poslovnimi in tehnološkimi cilji organizacije. Uprava naj bo proaktivna, na način, da zagotovi in upošteva tudi prihodnje trende in tveganja na tem področju;

02

zagotavljanjem skladnosti s predpisi:
uprava naj zagotovi nadzor nad skladnostjo organizacije z ustreznimi predpisi in zakoni. Samo v letošnjem letu je za finančni sektor začela veljati Uredba DORA (Digitalna operativna odpornost za finančni sektor), v oktobru letos pa naj bi v veljavo vstopil tudi nov Zakon o informacijski varnosti (ZInfV-1), ki udejanja zahteve Direktive o ukrepih za visoko skupno raven kibernetske varnosti v EU (NIS 2). Ta močno razširja obseg zavezancev. Ključno je, da uprava razume stopnjo skladnosti z zakonodajo in tveganja, ki jim je organizacija zaradi morebitne neskladnosti izpostavljena;

03

upravljanjem in nadzorom:
uprava mora razumeti postopke naslavljanja IT tveganj: načine identifikacije, ocenjevanja in njihovega zmanjševanja;

04

spremljanjem in poročanjem:
uprava naj redno prejema najnovejše informacije o kibernetskem stanju organizacije, vključno z napredkom pri ključnih pobudah za kibernetsko varnost, ključnimi metrikami in ključnimi kazalniki uspešnosti;

05

sodelovanjem strokovnjakov:
v kolikor še ni, naj uprava razmisli o vzpostavitvi funkcije varnostnega inženirja (angl. okrajšava: CISO). Če organizacija nima internih resursov za opravljanje teh nalog, si seveda na tem področju lahko pomaga z zunanjimi pogodbenimi partnerji;

06

odzivanjem na kibernetske incidente:
organizacija mora imeti vzpostavljen sistem za ustrezno odzivanje na incidente. Sistem je potrebno redno testirati in posodabljati. Za upravo je v primeru nastopa incidenta ključno tudi kako organizacija komunicira z javnostjo in zainteresiranimi stranmi.

Kako lahko izboljšate ozaveščenost in znanje na področju kibernetske varnosti?

Uprava bo lahko imela dober nadzor nad sistemom upravljanja kibernetskih tveganj, če bo imela na tem področju osnovna znanja, ki ji bodo pomagala razumeti situacijo, v kateri se organizacija nahaja.

Kako lahko to dosežete?

01

Vzpostavite redna izobraževanja o kibernetski varnosti.
Zagotovite si redno posodabljanje informacij o kibernetski varnosti. Seznanite se z največjimi kibernetskimi tveganji v vaši panogi in z izkušnjami obvladovanja tveganj na tem področju v podobnih organizacijah. Pridobite informacije o tem kaj vaša organizacija počne, da bi zmanjšala ali preprečila incidente na tem področju oz. kako se odziva na ta tveganja. Odgovori, ki jih dobite, so lahko ključni za okrepitev obrambnega sistema vaše organizacije.

02

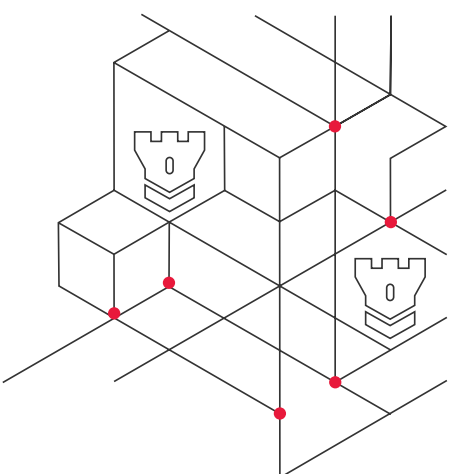
Preusmerite metrike in uporabite panožna merila.
Pomembno je, da ne upoštevate samo tehničnih metrik in parametrov, ampak tudi organizacijski del. Vključite različne segmente poslovanja organizacije: tehnični del, ekipo za odzivanje, pravno podporo. Razmislite o zavarovanjih iz tega naslova. Uporabite panožna merila za primerjavo svoje organizacije z drugimi
v svoji panogi, kar vam bo pomagalo razumeti, kje je organizacija in katere izboljšave so potrebne.

03

Povabite zunanje strokovnjake za kibernetsko varnost.
Z vključitvijo zunanjih strokovnjakov za kibernetsko varnost lahko člani uprave ne le izboljšajo svoje znanje o kibernetski varnosti, temveč tudi dobijo pomoč pri "prevajanju" informacij, osredotočenih na tehnologijo, v spoznanja in strategije, osredotočene na tveganja. To upravi omogoči reden dostop do potrebnega strokovnega znanja, ki dopolnjuje ekipe za upravljanje tveganj, varnost in tehnologijo v vaši organizaciji.

04

Izvedite kibernetske simulacije.
Če želite bolje razumeti dejanske kibernetske grožnje in način odzivanja nanje, razmislite o organizaciji simulacij incidentov. To vam bo pomagalo razumeti vašo vlogo člana uprave med kibernetskim napadom, morebitne vplive na poslovanje organizacije ter identificirati področja za izboljšave v primeru nastanka incidenta.



05

Zagotavljanje nadzora med incidentom.

V primeru kibernetskega napada morajo člani uprave aktivno sodelovati z varnostnimi strokovnjaki in ekipami za odzivanje na incidente ter od njih prejemati najnovejše informacije. Če so obveščeni o poteku in rezultatih incidenta, lahko zagotovijo neodvisen nadzor in znajo postavljati vprašanja z namenom, da bi odkrili morebitna preostala tveganja. Prav tako je pomembno, da uprava razume kje in na kakšen način so potrebne prilagoditve aktivnosti, ki so vezane na odzivanje na incidente.

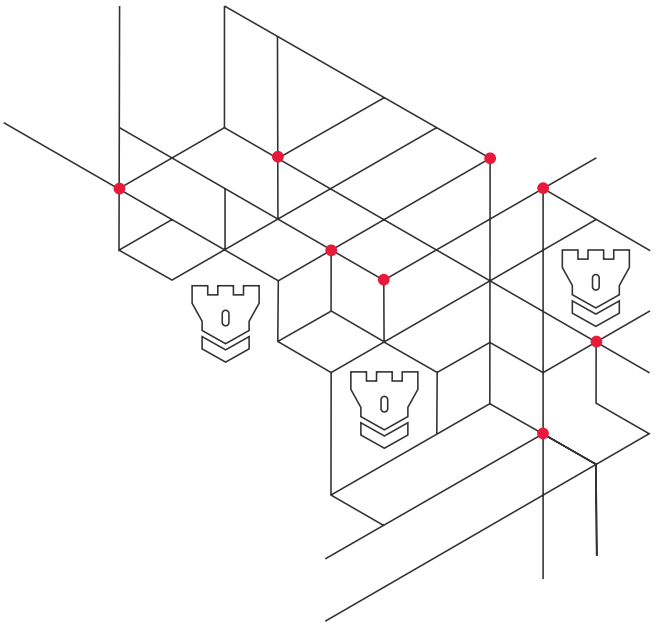
06

Ozrite se nazaj.

Lep slovenski pregovor pravi, da je "v vsaki slabi stvari tudi nekaj dobrega". Če se je incident vam ali vašemu sosedu že zgodil, se skušajte iz tega čim več naučiti. Poskusite z izkušnjami zmanjšati tveganja na tem področju.

Kaj je ključna vloga uprave pri upravljanju kibernetskega tveganja?

V nedavni Gartnerjevi študiji je 88 % uprav navedlo, da kibernetsko varnost obravnavajo kot poslovno tveganje. Tako je prav, saj so kibernetska tveganja le eno področje tveganj, s katerimi se organizacije srečujejo. Gre za vse pomembnejša tveganja, ki jih mora uprava primerno obvladati. Gre za dolžnost in obvezo uprave, ki je ne more delegirati drugim.



Kako lahko pomaga BDO?

Naš pristop h kibernetski varnosti je poslovno usmerjen pristop k obvladovanju kibernetskih tveganj.

Ponujamo izobraževanja za različne segmente zaposlenih in zunanjih pogodbenih partnerjev organizacij, seveda tudi uprav in pristojnih za upravljanje. Na teh srečanjih članom uprav pokažemo, kako pogovor, osredotočen na tehnologijo, preusmeriti v pogovor o poslovnem tveganju. Cilj je, da uprava lahko zagotavlja učinkovito raven nadzora in svojim kolegom, tudi tistim s tehničnega področja, postavlja prava vprašanja. Naša izobraževanja zajemajo tudi predstavitev najnovejših kibernetskih tveganj, s katerimi se organizacije soočajo in priporočila kako ta tveganja obvladovati.

POVEŽITE SE Z NAŠO EKIPO ZA KIBERNETSKO VARNOST ŠE DANES

Povežite se z našo ekipo za kibernetsko varnost še danes in tako izboljšajte svoje znanje o kibernetski varnosti, da boste pripravljeni na prihajajoče grožnje.