# Zagotovite si odpornost na kibernetske grožnje

BMA PARTNERJI

**Skoraj vsako podjetje lahko označimo kot tehnološko, kot tako pa je izpostavljeno tudi kibernetskim tveganjem. Kibernetski vdori lahko povzročijo prekinitve v poslovanju in dobavni verigi, težave z izdelki in še več. To lahko vpliva tudi na zunanje deležnike, kot so stranke, pacienti, gostje ali dobavitelji. Čeprav gre za eno glavnih poslovnih tveganj, s katerimi se soočajo organizacije, večina ni primerno pripravljena na kibernetske vdore oziroma druge varnostne dogodke.**

Statistika na tem področju je strašljiva, saj analitiki predvidevajo, da bodo do leta 2021 letne škode zaradi kibernetskih vdorov po vsem svetu dosegle kar 6 bilijonov USD1. Vlaganje v kibernetsko varnost pa bo v štiriletnem obdobju do leta 2021 preseglo 1 bilijon USD2. Uprave organizacij se teh groženj zavedajo, ampak ali so nanje tudi dobro pripravljene? Imajo pripravljena orodja za obravnavo kibernetskih napadov takoj, ko se zgodijo? Kibernetski vdor (incident), ne glede na vrsto ali javno razkritje, lahko katastrofalno vpliva na poslovne izide organizacij.

## Kako začeti?

Za začetek vzpostavljanja kibernetske odpornosti je treba upoštevati nekaj pomembnih korakov:

1. **Prepoznavanje** (razumeti morate svoje okolje in splošno kibernetsko tveganje),
2. **Zaščita** (izvesti morate primerne varovalne ukrepe za zamejitev škode ob kibernetskem vdoru ali drugem varnostnem dogodku),
3. **Zaznavanje** (vzdrževati morate preglednost svojega omrežja, da lahko zaznate vdore),
4. **Odzivanje** (predpostaviti morate, da bo prišlo do vdora, in pripraviti ustrezen načrt) in
5. **Reševanje** (največje tveganje je prekinitev poslovanja; obrnite se na strokovnjake, ki vam bodo pomagali hitro rešiti situacijo).

## Izvedite oceno kibernetskih tveganj

Zelo učinkovit in celosten način izvedbe teh korakov je izvedba ocene kibernetskih tveganj po metodologiji samostojnega sprotnega vrednotenja kibernetske izpostavljenosti Cyber Quotient (CyQu) družbe Aon, ki uporablja vodilno podatkovno analitiko za vrednotenje izpostavljenosti organizacije kibernetskim tveganjem, odkrivanje najbolj ranljivih točk in poenostavljanje strategij za zmanjšanje tveganj. Rezultat je ocena zrelosti na področju kibernetskih tveganj, primerjalni rezultat glede na podobne organizacije in jasna pot do ocenjevanja ter razumevanja izvedljivih popravnih strategij.

CyQu vam lahko pomaga prepoznati ranljivosti – razumeti, kakšna je vaša izpostavljenost v devetih kritičnih domenah: varovanje podatkov, nadzor dostopa, končne točke in sistemi, varnost omrežij, fizična varnost, varnost aplikacij, drugi deležniki, odpornost poslovanja in delo na daljavo.

Ta nagrajena metodologija vam zagotovi avtomatizirano oceno in pregled zrelosti družbe na področju kibernetskih tveganj in izpostavljenosti v (najmanj) devetih varnostnih domenah, označi ranljiva območja in določi potencialna kibernetska tveganja za organizacijo. Vašo organizacijo primerja s podobnimi organizacijami v vaši panogi po vsem svetu.

Zavarovalnice že nudijo rešitve za zavarovanja kibernetskih tveganj. Postopek sklenitve takega zavarovanja je lahko precej zapleten, saj zahtevajo kakovostne podatke in je lahko s tem povezana izpostavljenost zelo visoka, vse to pa vpliva na postopek pravilnega vrednotenja stroškov zavarovanja. Če torej načrtujete prenos tega tveganja na zavarovalnico, lahko to orodje uporabite kot pomoč sebi in zavarovalnici pri zagotavljanju boljšega pregleda in razumevanja svojega položaja in izpostavljenosti.

Za več informacij smo vam na voljo na naslovu: bma.partnerji@bmap.si

PROMO

[1,2] *Cybersecurity Facts, Figures, Predictions, And Statistics For 2019 To 2021, Sausalito, Calif, 2019*