KIBERNETSKA VARNOST: VODIČ ZA DELO OD DOMA

SAMOOCENJEVALNI KONTROLNI SEZNAM

UVOD

COVID-19 in posledično nacionalna zapiranja so prekinila konvencionalnost na področju kje in kako delati. Delo izven dejanskega delovnega okolja kot so delo od doma, delo iz skupnih prostorov ali delo od kjerkoli, je postalo trend, ki smo se mu morali prilagoditi. V zadnjih osmih mesecih je bila večina prilagoditvenih izzivov kot so, povezljivost, načini dela, težave povezane z medsebojnim sodelovanjem, rešenih z ustvarjanjem sprejemljivosti fenomena dela od kjerkoli. Medtem ko veliko podjetij navija za vrnitev na fizična delovna mesta, ti novi postopki delovanja ostajajo in se bodo sčasoma le še povečevali.

Zato morajo organizacije dati prednost kontinuiteti svojih kritičnih funkcij in ostati fleksibilne v svojem delovanju. Z dolgoročne perspektive je tako nujno, da delo od doma ali delo od kjerkoli, postane bolj zanesljivo, varnejše in stabilnejše.

Za lažji razmislek k temu smo znotraj mreže BDO pripravili kratek kontrolni seznam, ki bo pomagal organizacijam oceniti in obvladovati tveganja kibernetskih incidentov. Ta kontrolni seznam služi le kot pripomoček za ocenitev razumnih ukrepov za izboljšanje dela od doma.

POVEZLJIVOST

VARNOST

SODELOVANJE

ODZIVI NA INCIDENTE

POVEZLJIVOST

V mnogih organizacijah, ki uvajajo delo od doma, se je obremenjenost domačih internetnih povezav verjetno povečala.

Če postane domača internetna povezava počasna ali preobremenjena, bi morali imeti zaposleni, ki opravljajo ključne funkcije, nadomestni vir internetne povezave. Učinkovit komunikacijski načrt bi opredelil primarna sredstva za povezovanje (na primer domača internetna povezava) in izredna sredstva za povezovanje (na primer mobilna dostopna točka 4/5G).

Če zaposleni obdelujejo občutljive podatke, ki jih na daljavo ni morejo varno shranjevati, je treba razmisliti, da bi zaposlenim zagotovili alternativno možnost varnostnega kopiranja kritičnih podatkov, na primer šifrirani USB ali trdi disk.

KONTROLNI SEZNAM

Ste razmišljali o potrebni količini podatkov in o potrebni pasovni širini internetnih povezav za vaše zaposlene?

Ali imajo zaposleni, ki opravljajo ključne funkcije, nadomestna sredstva za internetno povezovanje?

Ste opozorili zaposlene, naj varnostno kopirajo in shranijo svoje delo, če se povezava izgubi, prekine in/ali se ne odzove?

Ali ste zaposlenim zagotovili način za delo brez povezave in za ustrezno varnostno kopiranje podatkov?

Ali ste preizkusili sposobnost ključnega osebja, da opravlja svoje funkcije doma v času največje uporabe omrežja in v daljšem obdobju?

Ali ste zaposlenim naročili, naj izvajajo večje posodobitve (npr. operacijskega sistema) izven obdobja največje uporabe omrežja (npr. čez noč)?

Ali ste vzpostavili jasno verigo odločanja, s katero v primeru izgube povezljivosti zagotavljate sprejemanje ključnih poslovnih odločitev?

VARNOST

ODDALJEN DOSTOP

Domače okolje (omrežje) ni vedno varno. Izvajanje ustreznih kontrol za dostop na brezžičnem usmerjevalniku in konfiguriranje najnovejšega brezžičnega varnostnega šifriranja zmanjšuje varnostna tveganja. Če dovolite osebnim napravam dostop do organizacijskih sistemov/omrežij, pomeni, da dovolite neznanim napravam dostop do podatkov družbe.

Če zaposleni dela z osebne naprave, je potrebno nujno zagotoviti ustrezen nadzor varnosti in stalno posodobljeno programsko opremo. Napadi za zavrnitev storitve – DoS in DDoS napadi – so med pandemijo COVID-19 vse bolj razširjeni. Mehanizmi za preprečevanje tovrstnih napadov so še bolj kritični, če osebje, ki vzdržuje te sistema, dela od doma.

KONTROLNI SEZNAM

Ali bodo zaposleni uporabljali osebne naprave za delo od doma? Če da, kako so osebne naprave skladne z vašimi varnostnimi zahtevami?

Ali se zaposleni od doma povezujejo v vaš sistem preko varne povezave, kot je npr. VPN povezava?

Ste že preizkusili, ali lahko zaposleni dostopajo do službenega okolja z osebnimi napravami?

Ste opozorili zaposlene, naj blokirajo svoje spletne kamere, kadar je to mogoče, ko jih ne uporabljajo?

Ste opozorili zaposlene, naj za oddaljeno izvajanje delovnih nalog ne uporabljajo privilegiranih (admin) računov?

Ste pripravili smernice v zvezi z varnostjo makrov v Officeovih aplikacijah Word in Excel?

Ali imate nameščeno tehnologijo za odkrivanje in opozarjanje na grožnje ali prijave uporabniških računov?

V kolikor uporabljate oddaljeni dostop (RDP), kako so ti dostopi zavarovani?

Ste zaposlene opomnili na pravilnik o sprejemljivi uporabi sredstev družbe?

Ste zaščitili svoje spletno mesto oz. kritične spletne funkcije pred napadi DoS / DDoS?

VARNOST nadaljevanje

GESLA

Pomembno je, da delovne naprave zaščitite z močnimi gesli. Ljudje pogosto uporabljajo isto geslo v več sistemih, aplikacijah in računih. Uporaba močnega gesla in orodja za upravljanje z gesli znatno zmanjša tveganje za številne vdore, ki temeljijo na geslih.

Zagotovitev, da bodo zaposleni spremenili privzeta skrbniška gesla za ključne račune, bo pomagalo ublažiti tveganje vdorov. Zaposleni naj zaklenejo svoje delovne postaje, kadar jih ne uporabljajo, tudi ko so doma.

KONTROLNI SEZNAM

Ste potrdili, da so uporabniški računi ločeni od skrbniških računov?

Ali so vaše naprave oz. osebne naprave zaposlenih šifrirane?

Če zaposleni uporabljajo službeni telefon, je le-ta šifriran in ali je zagotovljen ustrezen nadzor dostopa?

Ali uporabljate več nivojsko avtentikacijo v vseh poslovnih aplikacijah v oblaku (npr. O365, XERO, DropBox, Google Drive, SharePoint itd.)?

Če morajo zaposleni za delo od doma uporabljati svoj osebni mobilni telefon, ste razmišljali o upravljanju mobilnih naprav?

Ali ste zagotovili, da so naprave, ki se uporabljajo za delo, zaščitene z geslom in/ali drugim avtentikacijskim sredstvom?

Ste zaposlenim svetovali uporabo orodja za upravljanje gesel?

Ali so morali zaposleni potrditi, da pri domačem internetnem usmerjevalniku ne uporabljajo privzetega gesla?

VARNOSTNO KOPIRANJE

Organizacije morajo imeti vzpostavljeno strategijo varnostnega kopiranja, da se zagotovi redno varnostno kopiranje pomembnih podatkov in programskih rešitev.

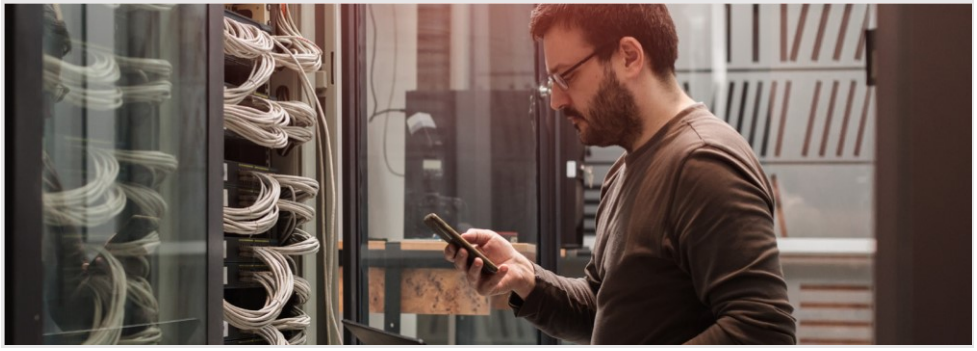
KONTROLNI SEZNAM

Ali imate izvajanje varnostnih kopij standardizirano in tudi kje zapisano?

Ali imajo zaposleni varnostne kopije za podatke na katerih so delali na svojem osebnem računalniku?

Ste opozorili zaposlene, naj varnostno kopirajo in shranijo svoje delo, če se povezava izgubi ali prekine in/ali se ne odzove?

Ste od zaposlenih zahtevali, da svojih delovnih naprav ne posojajo družinskim članom ali prijateljem?



VARNOST nadaljevanje

EPOŠTA IN PHISHING

Med pandemijo COVID-19 kibernetski napadalci nenehno ciljajo na različne organizacije z uporabo tehnik lažnega predstavljanja (phishing), povezanih s situacijo COVID-19. Velika verjetnost je, da bodo tudi vaši zaposleni postali žrtev uspešnih phishing napadov. Če/ko se to zgodi morajo vedeti, da je ključnega pomena, da o dogodku takoj opozorijo vašo IT-ekipo.

Izobrazite zaposlene o različnih tehnikah lažnega predstavljanja. Testirajte obnašanje zaposlenih v takšnih okoliščinah.

KONTROLNI SEZNAM

Ali ste zaposlene opozorili, da morajo biti pazljivi na sumljiva e-poštna sporočila, zlasti na e-poštna sporočila v povezavi s COVID-19?

Ali vaša organizacija izvaja programe ozaveščanja o lažnem predstavljanju (phishing)?

Ali ste v obdobju dela od doma posebno pozornost namenili izobraževanju na področju odobravanja plačil?

Ste zaposlene seznanili s politiko družbe o vzpostavitvi večnivojske avtentikacije?

SODELOVANJE

Orodja za sodelovanje so ključnega pomena pri zagotavljanju produktivnosti zaposlenih. Ta orodja omogočajo organizacijam, da vzpostavijo varna okolja, v katerih lahko zaposleni dostopajo do podatkov, ne da bi jim bilo te potrebno prenašati prek nezaščitene povezave.

Če zaposleni uporabljajo osebne naprave, lahko to povzroči povečano tveganje, če morajo dostopati do osebnih ali občutljivih podatkov brez vzpostavljenega ustreznega nadzora.

KONTROLNI SEZNAM

Ste razmislili, kako bodo vaši zaposleni sodelovali na sestankih in pri delu na skupnih dokumentih?

Ali se za sodelovanje zanašate samo na e-pošto? Če je odgovor pritrdilen, ste razmišljali o tem, kako boste komunicirali, če bodo e-poštne storitve vaše organizacije postale nedostopne?

Ste razmislili o varnosti e-pošte?

Ste pomislili, kako lahko delo od doma vpliva na sodelovanje s strankami?

Ali so bila vzpostavljena okolja za sodelovanje, da je mogoče dostopati do vseh kritičnih datotek, informacij in drugih podatkovnih sredstev?

Ste prepoznali kakšne kritične informacije, do katerih ni mogoče dostopati zunaj poslovnih prostorov?

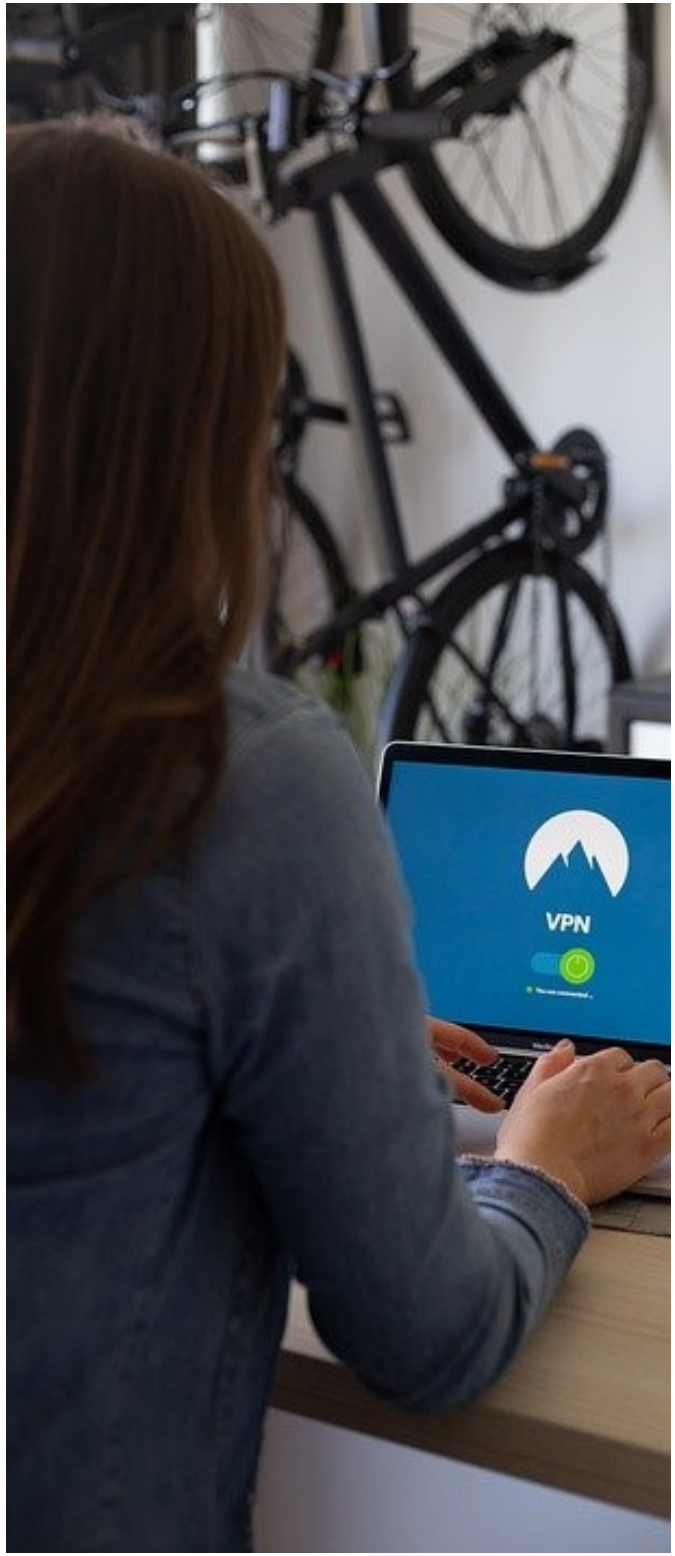
Ali so bili zaposleni usposobljeni za uporabo orodij za sodelovanje?

Ali ste upoštevali ustrezno zakonodajo o varovanju osebnih podatkov (npr. GDPR)?

Ste pripravili nabor izjem, ki jim je potrebno slediti v primeru dela od doma?

Ste zaposlene pozvali, naj službenih podatkov ne shranjujejo na osebne naprave, če je to le mogoče?

Ste zaposlene opozorili na njihove obveznosti glede varovanja zasebnosti in zaupnosti podatkov vaše družbe in podatkov strank?



ODZIVI NA INCIDENTE

Ko pride do incidenta, je potrebno razmisliti o sledečem:

- kako se odzvati,
- koga poklicati,
- kaj se je zgodilo,
- kdaj se je zgodilo,
- kje se je zgodilo (na katerih napravah),
- na katere informacije vpliva.

KONTROLNI SEZNAM

Ali ima vaša organizacija načrt odzivanja na varnostne incidente vseh vrst, ki bi ji pomagali pri obvladovanju in okrevanju v primeru njihovega nastanka?

Ali načrt upošteva delo od doma ali dogovore o delu na daljavo?

Je bil načrt testiran?

Imajo vsi zaposleni dostop do vsakokratne verzije načrta odzivanja na varnostne incidente? Imate vzpostavljen sistem posodabljanja in obveščanja o posodobitvah tega načrta?

Ste razmišljali, kako boste zaposlenim zagotavljali tehnično podporo v obdobjih dela od doma?

NAŠA KIBERNETSKA FILOZOFIJA

V BDO verjamemo, da je zagotavljanje kibernetske varnost pot, na katero bi se, z namenom varnega doseganja poslovnih ciljev, morala odpraviti vsaka organizacija.

Gre za strateško odložitev vsak organizacije. Ko ta doseže želen nivo informacijske varnosti, jo mora vzdrževati, kar zahteva veliko truda – po drugi strani pa zadovoljstva tako zaposlenih kot tudi strank.

NAŠ PORTFELJ ZA KIBERNETSKO VARNOST

Naša skupina strokovnjakov z bogatimi izkušanj iz različnih industrij, globalnega strokovnega znanja in sodobnih tehnologij ponuja vrsto celostnih storitev kibernetske varnosti, zasnovanih za zagotovitev varnega okolja, ki ščiti pred ranljivostmi in blaži nastajajoča tveganja.

O BDO

BDO je vodilna revizijsko-svetovalna organizacija, ki je prisotna v 167 državah, zaposluje več kot 91.000 ljudi po vel kot 1.600 pisarnah. Trudimo se zagotoviti resnično izjemne storitve za stranke s pomočjo pristopa po meri, hkrati pa sodelujemo z našimi zaposlenimi in strankami po vsem svetu.

BDO V SLOVENIJI

BDO v Sloveniji ponuja revizijske storitve, storitve na področju davčnega, finančnega, računovodskega in drugega poslovnega svetovanja tako za domača, kot mednarodna podjetja iz vseh sektorjev. Po višini prihodkov smo peta revizijsko – svetovalna družba v Sloveniji.

STOPITE V KONTAKT Z NAMI

MANUELA ŠRIBAR
Pooblaščena revizorka, CISA
031 617 379
manuela.sribar@bdo.si

BOŠTJAN PATE
IT svetovalec
031 338 112
bostjan.pate@bdo.si

BDO Revizija d.o.o.

Cesta v Mestni log 1
1000 Ljubljana

www.bdo.si