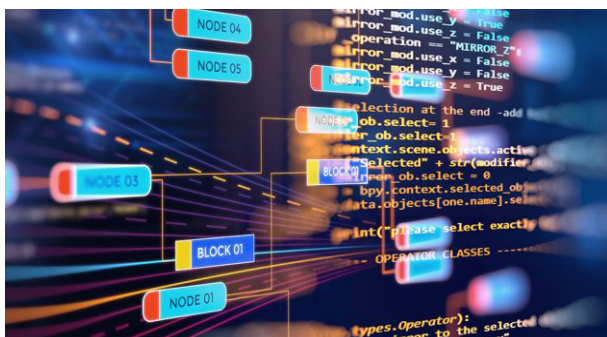


## Ebben a négy pontban benne van a távmunka minden biztonsági nyűge

*Nem általában a távmunkáé, hanem a mostani tipikus távmunka-helyzeteké. A szervezetek arra nem voltak felkészülve, hogy mindenki otthonról dolgozik.*



A járvány egyre nagyobb tömegeket kényszerít távmunkára. Diákok és tanárok, főnökök és alkalmazottak, értékesítők és ügyfelek lógnak naphosszat a neten, és próbálják csinálni közösen ugyanazt, amit néhány hete még az irodában/iskolában, személyesen intéztek. (Aki számára ez továbbra sem járható út, itt olvashatnak egy csokorra való jó tanácsot:

<https://bitport.hu/nem-opcio-az-otthoni-munka-akkor-erre-erdemes-figyelni.>)

A távmunkára kényszerített szervezetek IT-ja csak kapkodja a fejét, mert nap mint nap rendkívüli esetekkel, szituációkkal szembesülnek, és szinte a kivételek váltak a sztenderddé.

Am az üzletnek mennie kell(ene)... A gyors, előkészítetlen átállás azonban még azoknál a szervezeteknél is komoly biztonsági kockázattal jár, melyeknek már volt gyakorlata a távmunkában, írja az IDC egy friss tanulmányában

[\(https://blogs.idc.com/2020/03/30/cyber-resiliency-will-be-another-covid-19-tragedy-if-precautions-are-not-taken/\)](https://blogs.idc.com/2020/03/30/cyber-resiliency-will-be-another-covid-19-tragedy-if-precautions-are-not-taken/). Ezek a biztonsági kockázatok paradox módon épp arra jelentik a legnagyobb ve-

szélyt, amiért a vállalat egyik napról a másikra átállt a távmunkára: az üzletmenet-folytonosságra.

A helyzeten javítani csak a szituáció tervszerű elemzésével lehet, éppen ezért érdemes azt is pontosan számba venni, hogy milyen új kockázatok jelentek meg. Ezeket helyzetérzékenyen prioritizálva lehet napról napra javítani a biztonsági szintjét.

## A négy kulcsterület

Az IDC a kockázatok rendszerezéséhez készített tanulmányában négy fő területet azonosított. Meg kell vizsgálni a felügyeleti területeket, az IT uniformizáltságát, valamint a láthatóságot és a támogatást.

A **felügyeleti területen** az okozza a legnagyobb kihívást, és erre is kell az IT-nak a leggyorsabban megoldást találnia, hogy olyan végfelhasználói eszközök kapcsolódnak – sokszor akár magas jogosultságokkal – a vállalati hálózathoz, amelyek fölött az IT-nak nincs semmiféle kontrollja. Hogy csak a legegyszerűbbet mondjuk: a legtöbb otthoni wifi routeren távolról lényegében lehetetlen érvényesíteni a vállalati biztonsági házirendet (ha érvényesíthetik, akkor esetleg a munkavállaló be sem jut a vállalati rendszerbe). Eközben ezeken az eszközökön folynak üzletkritikus és amúgy is magas biztonsági kockázatú műveletek.

A másik fontos terület, amire valamiféle megoldást kell találni, hogy egyszerre nagyon **sokféle eszköz jelenik meg a vállalati hálózaton**. Ez ott is probléma, ahol korábban már bevezették a távmunka lehetőségét. Általában ezzel a lehetőséggel együtt járt az is, hogy az eszközmenedzsment hatékonyabbá tételéhez, a biztonsági szint emeléséhez specifikációk alapján egységesítették a végfelhasználói eszközöket és a hálózati összetevőket. Ha volt is ilyen szisztéma, akkor most az valószínűleg teljesen felborult. Bár az ilyen egységes rendszerekben is volt lehetőség kivételek alkalmazására, most lényegében csak kivételek vannak. Ide tartozik az IDC szerint az is, hogy a korábban

kialakított szerepköralapú biztonsági szisztéma fenntarthatatlanná válik.

A **láthatóság** elsősorban az incidenskezelésnél jelent komoly kihívásokat. A biztonsági elemzők lényegében meg vannak fosztva a szenzoraiktól. Korlátozottan tudnak támaszkodni olyan telwmetriai adatokra, melyek alapján például többlépcsős támadások lehetőségei vagy az egyes rendszerek kockázatai elemezhetők. Emiatt lelassul mind a támadások detektálása, mind az azokra adott válasz.

És végül, de nem utolsósorban **romlik az IT-támogatás minősége**. Ennek egyik oka, hogy az informatikai csapatok jellemzően szintén otthonról dolgoznak, így nem támaszkodhatnak a hagyományos munkakörnyezetükre és rutinjaikra. Sokkal nehezkesebbé válnak például az olyan rutinfeladatok, mint az eszközök karbantartása, biztonsági ágensek, javítócsomagok, frissítések telepítése,

sérülékenységek keresése, biztonsági beállítások konfigurálása stb.

### **Ne dőljön be a CISO vagy a CIO minden ingyenes ajánlatnak**

Mindezekre a problémákra gyors megoldás kell, mindenekelőtt a végponti védelmet kell kiterjeszteni a hálózaton megjelent eszközökre. A végponti védelmeket kínáló szállítók most elhalmozzák a cégeket különféle ingyenes ajánlatokkal. Az IDC szerint azonban ne a jelenlegi ingyenesség legyen a döntő választási szempont, hanem érdemes hosszabb távra tervezni, és meghatározni a követelményeket a fenti négy terület alapos áttekintése után. És ha ez megtörtént, akkor már valóban jöhet a választás.

Forrás: <https://bitport.hu/ebben-a-negy-pontban-benne-van-a-tavmunka-minden-biztonsagi-nyuge>

Válogatta: Fonyó Istvánné