KISKAPUK NÉLKÜL

A biztonságos távmunkához a munkatársak oktatása is szükséges


RÓZSA ROLAND, 4iG

FORRÁS: 4iG

Az információbiztonságot sokkal komolyabban kell venni a járvány miatt távmunkára átállt szervezeteknek. Ezzel együtt felül kell vizsgálni az üzletmenet-folytonossági terveket és szükség szerint módosítani, hogy a mostani helyzethez alkalmazkodva szolgálja a vállalkozás érdekeit.

A digitalizációban élen járó vállalkozások korán átálltak a részleges távmunkára. A szervezetek többségénél, ahol ezt meg lehet tenni, elkerülhetetlen lesz az átállás és várható, hogy egyre szélesebb körben részesítik előnyben a munkavégzés e módját. A megváltozott körülmények az IT-biztonság tekintetében is új szemléletet igényelnek. „Ha a korábban 5-10 százalékos távmunka hirtelen felugrik 60-70 százalékra, jelentősen megnő a szervezet biztonsági kitettsége”, figyelmeztet Rózsa Roland, a 4iG stratégiai tanácsadója.

A biztonság ára

A vállalkozás rendszereihez távolról hozzáférő dolgozók számával a kockázat is megnő, ezzel tisztában vannak a biztonsági rések kihasználói, akik valóságos aranybányát látnak ebben. Nagyon gyorsan kellemetlen helyzetben találják magukat azok a vállalatok, ahol nem gondoskodtak saját infrastruktúrájuk megfelelő védelméről.

Rózsa Roland szerint, még ha „túlélő” üzemmódban is van most egy cég, akkor is abszolút minimumnak számít az IT-biztonság kiemelt kezelése, mert felfokozottak a kockázatok. Ezért, amikor gyorsan kell kialakítani a távmunka-rendszert, különösen fontos, hogy betartsák a gyártói ajánlásokat és a biztonsági szabványokat.

A biztonság erősítését akkor is meg kell lépni, ha az némi kényelmetlenséget okoz a dolgozóknak. A kétfaktoros azonosítás több felhasználói interakciót és odafigyelést igényel, de kulcsfontosságú. „Meg is lehet találni azt az egyensúlyt, ahol anélkül nyújtunk megfelelő biztonságot, hogy kiskapuk keresésére ösztönöznénk a felhasználókat”, teszi hozzá a 4iG szakértője.

Gondoskodni kell arról, hogy a csoportmunka továbbra is biztosított legyen a dolgozóknak. Ehhez a vállalkozás által felügyelt földi vagy felhős megoldásokat kell alkalmazni, biztosítva az adatok megfelelő védelmét.

Kiemelt fontosságú a munkatársak oktatása, tájékoztatása, hogy a megváltozott munkakörülmények során jól tudják használni a számukra új megoldásokat. Ezzel minimalizálható az a lehetőség, hogy kockázatos saját megoldásokkal dolgozzanak.

Ez egy másik katasztrófa

A legtöbb nagyvállalatnál vannak üzletmenet-folytonossági (BCP) és katasztrófa-elhárítási (DRP) tervek, ám azok többnyire olyan természeti katasztrófákra és komolyabb technológiai zavarokra készültek, mint egy árvíz, földrengés, vagy ha hosszabb időre kimarad egy közmű-szolgáltatás. „Az, hogy a dolgozóknak otthonról kell dolgozni, még nem katasztrófa. Ám ha a dolgozóink fele a fertőzés miatt munkaképtelen, az már mindenképpen katasztrofális. Egy ilyen helyzetre valószínűleg nagyon kevesen készültek fel előre”, mondja Rózsa Roland. Az így megváltozott körülményekre is kell valamilyen választ adni. Az egyik lehetőség a vállalati működés tartalékra kapcsolása lehet, ahol csak a legszükségesebb területek folytatják a tevékenységet, azok is csak visszafogottan.

Meg lehet találni azt az egyensúlyt, ahol anélkül nyújtunk megfelelő biztonságot, hogy kiskapuk keresésére ösztönöznénk a felhasználókat

Emellett a 4iG stratégiai tanácsadója a BCP/DRP tervek egy másik aspektusára is felhívja a figyelmet. Ezek a tervek az informatikai infrastruktúra vagy szolgáltatások kiesésének idejére általában papíralapú működésre való visszatéréssel számolnak. Jellemzően ezek a tervek nincsenek felkészítve arra, ha az infrastruktúra olyankor válik elérhetetlenné, amikor a többség otthonról dolgozik. Ráadásul az infrastruktúra bizonyos részeit gyakran külső szolgáltatók üzemeltetik – tehát a cégünk üzletmenet-folytonossága partnereink, beszállítóink felkészültségétől is függ. A tervek ellenőrzésével és módosításával csökkenthetők a nem tervezett események okozta károk. ■