AZ ÚJRAFOGALMAZOTT MUNKAHELY ÚJRAFOGALMAZOTT IT-BIZTONSÁGOT IGÉNYEL

Így készüljünk fel az állandó hibrid munkavégzésre

A hibrid munkavégzés teljesen új kihívások elé állította a cégvezetőket, a munkavállalókat és a biztonsági szakembereket egyaránt. A koronavírus lecsengését követő, visszarendeződés címkével illetett időszak, pedig egyértelműen bebizonyította, hogy a jövő a hibrid munkavégzésé. Erre viszont nem csak az üzleti és a HR-terület oldaláról, hanem az IT-biztonság oldaláról is alaposan fel kell készülni. Az Invitech IT-Security consultant team leadere, Vaspöri Ferenc azt is elárulta mire érdemes figyelni, és komplett megoldásokat is feltárt a horizonton felbukkanó céges fenyegetések kivédésére.

VASPÖRI FERENC, INVITECH

FORRÁS: INVITECH

Home office, VPN, ransomware, munkavállalói hozzáférések, biztonságtudatossági hiányok, rossz internetkapcsolat – a hibrid munkavégzést akadályozó IT-biztonsággal összefüggő jelenségek leggyakrabban a felsorolt hét jelenség közül kerülnek ki és az is előfordul, hogy egyszerre több tényező is nehezíti ezek közül a cég működését.

„Kiberbiztonsági szempontból számtalan következménye van annak, hogy a megváltozott körülmények miatt otthonról (is) dolgozunk. Az már jól látszik, hogy a home office és az irodából történő munkavégzés összefonódása velünk marad, így ki kell alakítani egy olyan munkakultúrát, amelynek keretein belül a hibrid munkavégzés biztonságosan kivitelezhető”, fogalmazta meg Vaspöri Ferenc. Ehhez az első lépés a dolgozók oktatása, de az internet védelme és a VPN megóvása is kulcsfontosságú.

A már meglévő munkatársak esetén is fennáll annak a veszélye, hogy belefut egy adathalász levélbe, vagy a kollégája nevében küldött emailben található kártékony linkre kattint. Újonnan belépő esetében még nagyobb a rizikó. „Hogy a felhasználók meg- és felismerjék a csaló emaileket és weboldalakat, az Invitech IT-biztonsági tudatosságfejlesztő platformjának keretein belül online tananyagokat biztosítunk a résztvevők számára, illetve szimulált támadásokat is végrehajtunk, hogy »játékos« és vezetett keretek között megtapasztalják, milyen átesni egy adathalász-támadáson, mert azt látjuk, hogy a gyakorlati oktatást követően sokkal jobban odafigyelnek az éles helyzetekben”, mondta Vaspöri Ferenc.

A megfelelő munkakultúra kialakításának másik fontos eleme az internetkapcsolat minősége és folytonos elérhetősége, hiszen, ha stabil netkapcsolat híján a dolgozók nem tudnak élni a távoli elérés előnyeivel, és otthonról elvégezni a szükséges feladatokat, az az üzletmenet leállását eredményezheti, amit a támadók is kihasználnak. „Nagyon megnövekedtek a DDoS támadások, amelyek az üzletfolytonosság megszakítását eredményezik az adott cég internethálózatának túlterhelésével. Ezek nemcsak célzottabbá váltak, hanem már a kisebb vállalkozásokat is érintik”, tette hozzá Vaspöri Ferenc.

Olyan munkakultúrát kell kialakítani, amelyben biztonságos lehet a hibrid munkavégzés

Az ilyen típusú akciók során a támadók megpróbálják a cég összes, publikusan elérhető címét túlterhelni, amivel a teljes hálózatot elérhetetlenné teszik. A munkavállalók nem tudnak dolgozni, több órás kiesés például egy banknál óriási veszteséget okozhat. „Internetszolgáltatóként kiemelten fontos az, hogy magas rendelkezésre állást nyújtsunk az ügyfeleknek, a stabil internet mellé pedig elérhető DDoS-védelmi szolgáltatásunk is, amely a fenti fenyegetettség ellen nyújt védelmet”, hangsúlyozta Vaspöri Ferenc.

A munkavállalói hozzáférések és VPN mellett sem lehet elmenni szó nélkül. „Fontos, hogy a VPN-hozzáférések aktualizálva, rendszerszinten karban legyenek tartva, mert ha a hálózaton kinyitják a hozzáférési pontokat a dolgozóknak, de ezek védtelenek, a támadók azonnal bejutnak a céges munkaállomásra. Az Invitech tűzfalszolgáltatása a távoli hozzáférést és a VPN védelmet is garantálja”, mondta el Vaspöri Ferenc. ■