Sajtóinformáció
2020. június 16.

Egyes országokban ötszörösére nőtt a kiberbiztonsági támadások száma a járvány alatt

A koronavírus-járvány már lecsengőben van, azonban továbbra is sokan dolgoznak otthonról. Ebben a helyzetben jelentősen megnőhet a kiberbiztonsági események száma, a hackerek, a csalók és a kéretlen leveleket küldők igyekeznek kihasználni a biztonsági réseket, és megpróbálnak értékes információkat eltulajdonítani. Az Allianz Global Corporate & Specialty (AGCS) szakértői válaszképpen olyan intézkedésekre hívják fel a figyelmet, amelyek segítségével a munkavállalók hatékonyabban vehetik fel a harcot a kiberbiztonsági kihívások ellen.

A koronavírus következtében megváltoztak, illetve a járványt követően átalakultak az emberek mindennapos munkavégzési és kapcsolattartási szokásai, így számos vállalatnál kellett bővíteni a távmunka-kapacitást, ráadásul igen rövid idő alatt. Bizonyos esetekben enyhítették vagy felfüggesztették az informatikai biztonsági előírások alkalmazását, hogy minél több munkavállaló férhessen hozzá könnyen és gyorsan az operációs rendszerekhez és szoftverekhez, ez a lépés azonban megnövelte a vállalaton belüli kiberbiztonsági kockázatokat.

A lazább biztonság következményeképp a kiberbűnözők és a hackerek könnyebben juthatnak be a korábban hatékonyan védett vállalati rendszerekbe, ezzel adatvédelmi incidenseket, zsarolási célú kiberbiztonsági támadásokat, és az informatikai rendszerek leállását okozva. A vállalati hálózathoz virtuális magánhálózaton (VPN) keresztül csatlakozó, otthonról dolgozó munkavállalók kívánatos célpontjai a kiberbűnözőknek, ezt az elmúlt időszak eseményei is megerősítik.

A koronavírussal kapcsolatos, kártékony hivatkozásokat vagy csatolmányokat tartalmazó adathalász e-mailek vagy WhatsApp-üzenetek 2020 januárjában kezdtek el keringeni, és azóta a számuk csak emelkedik. Az Európai Bizottság szerint a kiberbűncselekmények száma nőtt az EU-ban a járvány kezdete óta, míg az Egészségügyi Világszervezet (WHO) nemrég olyan gyanús e-mail-üzenetekre hívta fel a figyelmet, amelyek a COVID-19 okozta helyzetet kihasználva[1] pénzt és bizalmas információkat próbálnak kicsalni az emberektől. Egyes országokban a megkísérelt kiberbiztonsági támadások száma ötszörösére nőtt február közepe és március közepe között.

Az AGCS egy tippeket és intézkedéseket tartalmazó listát állított, amelyet érdemes betartani az internetes támadások elleni védekezés során. A lista alapját a Német Szövetségi Információbiztonsági Iroda („Bundesamt fur Sicherheit und Informationstechnik”) fő intézkedései, valamint a Charter of Trust – a globális IT-biztonságot segítő vállalatok szövetsége, amelynek az Allianz is tagja – iránymutatásai adják, és minden eszközre, így a munkavállalók által használt vállalati eszközökre is érvényes. Az illetékes helyi szervezt kiegészítő, vagy ettől eltérő útmutatásai elsőbbséget élveznek.

Főbb intézkedések az otthoni iroda informatikai biztonsága érdekében*

Tartsa naprakészen szoftvereit!

Ellenőrizze, hogy az operációs rendszerek és a telepített programok legfrissebb verzióit használja-e! Ha teheti, alkalmazza az automatikus frissítési funkciót – általában ez az alapértelmezett beállítás. Ellenkező esetben minél előbb telepítse a szoftverek, különösen a web böngésző és az operációs rendszer biztonsági frissítéseit.

[1] Egészségügyi Világszervezet: Óvakodjunk a magukat a WHO-nak kiadó bűnözőktől, 2020

Használjon vírusvédelmet és tűzfalat!

Ellenőrizze, hogy be van-e kapcsolva a vírusvédelem és a tűzfal, de ne feledje, hogy ezek a beállítások csak más biztonsági eljárások kiegészítő intézkedéseként lehetnek hatásosak, az alkalmazásuk nem helyettesítheti a listában szereplő többi tanács betartását.

Hozzon létre különböző felhasználói fiókokat!

A rosszindulatú programok ugyanolyan jogokkal rendelkeznek a számítógépen, mint az a felhasználói fiók, amelyen keresztül bejutottak a számítógépre, ezért csak akkor dolgozzon adminisztrátori jogosultságokkal, ha az feltétlenül szükséges.

Legyen óvatos a személyes adatok megosztásakor!

Az online csalók úgy igyekeznek növelni a sikerességüket, hogy testre szabott módon közelítik meg áldozataikat: A bizalom megteremtése érdekében felhasználják a korábban megfigyelt adatokat, például a böngészési szokásokat, vagy a személyneveket. Manapság a személyes adatok pénzt érnek az interneten, a csalók kereskednek velük. Amennyiben lehetséges, nyilvános vezeték nélküli hálózati (WLAN) elérési pontokhoz csatlakozva használja az otthoni hálózathoz csatlakozó VPN-t, máskülönben a titkosítás nélkül továbbított adatokat harmadik felek is láthatják.

További intézkedések az otthoni iroda informatikai biztonsága érdekében:

Csak a feltétlenül szükséges eszközöket és információkat vigye haza!

Az információk és az eszközök védelmének legjobb módja, ha egyáltalán nem távolítjuk el őket a vállalati környezetből, így nem veszhetnek el szállítás közben, vagy keverednek el otthon.

Használjon naprakész web böngészőket!

Ellenőrizze, hogy nem szükséges-e letiltani egyes komponenseket és beépülő modulokat a böngésző beállításaiban! Jó módszer a biztonságos hozzáféréshez, ha előbb kézzel begépeli a biztonsági szempontból különösen fontos webhelyek - például az online bankja - címét a böngésző címsorába, majd az így megadott címet elmenti könyvjelzőként.

Frissítse gyakran jelszavait!

Tartsa titokban a jelszavait és a felhasználóneveit, az esetlegesen kiszivárgott jelszavakat pedig haladéktalanul módosítsa. A különböző alkalmazásokhoz használjon eltérő, felismerhetetlen jelszavakat, és az automatikusan generált jelszavakat az első használat előtt módosítsa. Fontos azonban az is, hogy a jelszó könnyen megjegyezhető legyen. Az általános szabály: minél hosszabb, annál jobb. A jelszó legyen legalább nyolc karakter hosszú, ne legyen szótárban megtalálható szó, és tartalmazzon kis- és nagybetűt, speciális karaktert, és számot is.

Kétfaktoros hitelesítés

Ahol lehetőség van kétfaktoros hitelesítésre, használja azt a fiókjához való biztonságosabb hozzáférés érdekében! A jelszókezelő szoftverek használata megkönnyítheti a különböző jelszavak kezelését. Jelszavait soha ne ossza meg másokkal!

Védje adatait titkosítással!

Védje bizalmas e-mailjeit titkosítással! Amennyiben nyilvános vezeték nélküli helyi hálózatot (WLAN-t) használ, a vállalata információbiztonsági útmutatásait betartva ügyeljen a vezeték nélküli hálózat titkosítására. A routeren válassza ki a WPA3 titkosítási szabványt, vagy a WPA2-t, ha az előbbi még nem támogatott. Természetesen az illetékes információbiztonsági megbízott (ISO) ennél szigorúbb feltételeket is szabhat, amelyeket mindenképpen tartson be! Válasszon bonyolult, legalább 20 karakterből álló jelszót.

Csak megbízható forrásokból töltsön le adatokat!

Legyen óvatos, amikor az internetről tölt le tartalmakat! A programok letöltése előtt győződjön meg a forrás megbízhatóságáról, és amennyiben lehetséges, csak a gyártó weboldaláról töltse le ezeket.

Rendszeresen készítsen biztonsági mentést az adatokról!

Amennyiben a számítógép a biztonsági intézkedések ellenére megfertőződik, fontos adatok veszhetnek el. A kár enyhítése érdekében rendszeresen készítsen biztonsági mentést a fájlokról a helyi információbiztonsági megbízott (ISO) útmutatásai szerint.

Kapcsolja ki a hanggal vezérelt intelligens eszközöket az otthoni irodában, és a takarja le a webkamerát, amikor nem használja!

A hangvezérelt asszisztensek hallják, amit a szobában mondunk, és továbbítják a szolgáltató felé. Nem garantálható, hogy ezek a hangfelvételek nem kerülnek rossz kezekbe. Ezen kívül ne felejtse el letakarni a számítógép webkameráját, ha éppen nem használja, illetve ügyeljen arra, hogy mit oszt meg a videofunkción keresztül.

Ne keverje a személyes és vállalati célú felhasználást!

Egyértelműen különítse el a vállalati és a személyes célú eszközöket és információkat, és ne másoljon át munkával kapcsolatos adatokat a személyes eszközeire, ezzel megelőzheti az információ véletlen kiszivárgását. Ez a gyakorlat pszichológiai szempontból is hatásos, mert segít elkülöníteni a munkaidőt a pihenőidőtől.

Mindenki azonosítsa magát az online megbeszéléseken!

A csatlakozáshoz szükséges adatokat megszerző illetéktelen személyek különösen könnyen kapcsolódhatnak nagyobb, sokszereplős online megbeszélésekhez, ezért fontos, hogy a megbeszélésen részt vevő személyek röviden azonosítsák magukat, különösen bizalmas témák megvitatásakor és a prezentációk képernyőn történő megosztásakor.

Védje az eszközöket, és jelentkezzen ki, ha már nem használja azokat!

Akkor is zárolja a számítógép és a mobileszköz képernyőjét, ha csak rövid szünetet tart, éppúgy, mint ahogyan azt a munkahelyen tenné, hogy mások ne férhessenek hozzá az eszközön lévő tartalmakhoz. A készülékek védelméhez természetesen az is hozzátartozik, hogy megóvjuk őket az illetéktelen fizikai hozzáférés és a lopás ellen.

Tartsa be a bizalmas dokumentumok nyomtatására és kezelésére vonatkozó biztonsági lejárásokat!

Ne tartson az íróasztalán bizalmas nyomtatott anyagokat! Az „illetéktelen hozzáférés” kategóriájába beletartozhat az is, amikor a gyermekei rajzpapírnak használják a munkával kapcsolatos dokumentumokat. Zárja el a bizalmas iratokat egy szekrénybe, amikor éppen nincs rájuk szüksége. A

belső használatú és bizalmas dokumentumokat ne dobja a normál szemétkosárba; használjon iratmegsemmisítőt! Ha nem rendelkezik iratmegsemmisítővel, gyűjtse össze ezeket, és ellenőrizze, hogy biztonságosan megsemmisíthetőek-e majd az irodában.

Legyen rendkívül óvatos a gyanús e-mailekkel és csatolmányokkal, különösen, ha ismeretlen a feladójuk!

Az otthoni iroda barátságos környezetében különösen ügyelnie kell a gyanús e-mailekre. Szánjon időt az e-mailek alapos ellenőrzésére, mielőtt megnyitná őket.

**A javaslatok általános kockázatkezelési szempontú műszaki tanácsok, a hatékony alkalmazásuk előtt személyre szabásuk ajánlott az egyedi igények szerint.*

További információk:

A Charter of Trust, a globális információbiztonságot segítő vállalatok szövetségének útmutatója

https://www.charteroftrust.com/

Szakértői szolgáltatások a vállalatok kiberkockázatainak azonosításához

https://www.agcs.allianz.com/services/cyber-risk-management.html

Kapcsolattartók:

Rishi Baviskar
Vezető kiberbiztonsági szakmérnök, Allianz Risk Consulting
rishi.baviskar@allianz.com

Jens Krickhahn
Kiberbiztosítási menedzser, AGCS CEE
jens.krickhahn@allianz.com

Yogesh Virji
Kiberbiztosítási igazgató, AGCS UK
yogi.virji@allianz.com