X, Y, Z ÉS ALFA

Generációs sajátosságok az IT-biztonságban

Négy generáció dolgozik egy időben a munkaerőpiacon. A meg-megismétlődő incidensek során jól körülrajzolódnak az egyes korosztályokra jellemző IT-biztonsági anomáliák. Összegeztük tehát, hogy milyen csapdákba esnek leggyakrabban az X, Y, Z és alfa generáció képviselői, és milyen fenyegetésekre kell felkészülniük a vállalkozásoknak 2022-ben.

CSELEDI SÁNDOR, BALASYS

FORRÁS: BALASYS

SZEKÉR ZOLTÁN, OD&IT

FORRÁS: ITB

A járványhelyzet reflektorfénybe helyezte a virtuális térben tevékenykedő felhasználók IT-biztonsági tudatosságát, és hogy ebben személyenként és csoportonként is óriási különbségek tapasztalhatók. Nem meglepő módon az analóg vagy digitális szocializáció és a technológiai környezet jelenléte is nagyban befolyásolja azt, hogy ki, hogyan áll a kiberbiztonsághoz, és adott generációba tartozó felhasználót melyik típusú támadással lehet a leginkább kelepcébe csalni.

A kibertámadások típusai a kkv-szektorban

A mikro-, kis- és középvállalkozások felét érte már támadás az interneten. A cégek eddig legnagyobb részben adathalász leveleket kaptak (35 százalék), ezt követik a zsarolóvírusok, emailben vagy interneten érkező vírustámadások (29 százalék). A vállalkozások 13 százalékának törték már fel weboldalát, közösségi oldalát, vagy próbálkoztak meg ezzel. Anyagi kárt viszont mindössze a kkv-k tizedének okoztak a támadások – derül ki a K&H kutatásából.
A legnagyobb kkv-k, azaz a 300 millió és 2 milliárd forint közötti árbevételű középvállalkozások ellen irányult messze a legtöbb rosszindulatú támadás, 68 százalékuknak volt már része ilyenben. A 100 és 300 millió forint közötti árbevételű kisvállalkozások esetében ez az arány 48 százalék, a legfeljebb 100 millió forint árbevétellel rendelkező mikrocégeknek pedig éppen felét érte már támadás – áll a K&H Bank kutatásában.

Mi jellemzi egyes korcsoportok biztonságtudatosságát?

„Nagyfokú, negatív előjelű óvatosság jellemzi az X-generáció IT-biztonsági attitűdjét, ami abból fakad általánosságban, hogy egyfajta félelemmel vagy gyanakvással tekintenek a technológiára, mert előfordul, hogy nem értik a működését, vagy nem bíznak benne. Jó példa erre a felhő, amelyet sok esetben azért nem használnak munkavégzés közben, legfeljebb csak mentésre, mert saját fájljaik tárolását a saját számítógépükön érzik a legbiztonságosabbnak. A zsarolóvírusok jelentik a legnagyobb veszélyt az X generációs munkavállalókra, annak ellenére, hogy ismerik, tudják, hogy létezik ez a támadási forma”, mondta *Szekér Zoltán,* az OD&IT CEO-ja.
Az Y generáció ennél tudatosabb. Tagjaikra jellemző, hogy a jól bevált, erős jelszavakat nem szeretik változtatgatni. A gyors ütemű digitalizációnak köszönhetően már „minden is” elintézhető online, ami több tucatnyi különböző jelszó

Az IT és a HR kommunikációja elengedhetetlen ahhoz, hogy a rendszeres frissítésekre felkészüljenek a kollégák

fejben tartását igényelné, erre pedig a millenniumi generáció nem vevő. „Sokszor találkozunk azzal, hogy szinte mindenhol ugyanazt a jelszót használják, a munkahelyi rendszerben és a privát oldalakon is, és ha nem kényszeríti ki a program/rendszer annak megváltoztatását”, mondta el Szekér Zoltán.
A Z és alfa generáció még tudatosabb, változtat jelszót, ugyanakkor a biometrikus azonosítást jobban kedveli. Kifejezetten frusztrálja őket a kétfaktoros autentikáció, és az, ha manuális beavatkozásra van szükség az IT-biztonsági azonosítás során. „Számukra felgyorsítja a kiégési folyamatot egy rosszul működő szoftver, például, amely a biztonság miatt megadott időközönként kiléptet”, tapasztalja Szekér Zoltán.

„A nyugdíjasok az elsődleges áldozati csoport, számukra jellemzően ismeretlen terület az internet. Nem értik a működését, és az alapvető felhasználási módokon túl nem is foglalkoznak vele. A csalók viszont foglalkoznak velük, mert viszonylag könnyen átverhetők, megkárosíthatók.

Új szoftver beszerzésekor az IT-biztonsági oktatást is újra kell gondolni

Veszélyeztetettek még a kisgyermekek, akik egyre korábban kezdenek internetezni, de a szülők sokszor nem készítik fel őket erre megfelelően. Az összes többi korosztályban vannak olyanok, akik hajlamosabbak áldozatul esni a különféle támadásoknak, és olyanok is, akik tudatosságuknak köszönhetően meglehetősen védettnek számítanak”, fogalmazta meg *Cseledi Sándor,* a Balasys CEO-ja.
Ami a generációk biztonságtudatosságát és a pandémia indította digitalizációs hullám arra gyakorolt hatását illeti, romlott és javult is a helyzet. „Társadalmi léptékben egyértelműen magasabb lett a tudatosság, jobban félnek az emberek a rájuk leselkedő netes veszélyektől, jobban is vigyáznak, ezért arányaiban kevesebb embert sikerül átverniük a csalóknak. Ám mivel sokkal többen interneteznek aktívan, és egyre többen tesznek feljelentést, ha átverték őket, ami korábban nem volt jellemző, az abszolút számértékek sokat romlottak”, mondta Cseledi Sándor.

2022-ben leselkedő veszélyek

„Továbbra is a zsarolásos támadás, a ransomware lesz a legelterjedtebb, ám új formában. Míg korábban azért fizettek a cégek, hogy visszakapják a támadó által titkosított adatokat, most már el is lopják az adatokat, így külön kell fizetni azért, hogy azok ne kerüljenek ki az internetre. A védekezéshez nem elég egy vírusirtó és egy tűzfal. Csak egy olyan tudatos stratégia mentén kiépített IT-biztonsági rendszerrel lehet kivédeni a támadásokat, amilyen a »zero trust« modell is, amelynek lényege, hogy a hozzáférés engedélyezése előtt ellenőrizni kell mindent és mindenkit”, mondja Cseledi Sándor.
Az erős jelszavak használata, a szoftverek folyamatos frissítése, a wifi-hálózat biztonságossá tétele vagy az illegális szoftverek elkerülése minimális energiabefektetést igényelnek, ám ezen óvintézkedések már önmagukban is hatékonyan csökkentik a kockázatokat. Emellett érdemes elkerülni azokat az alkalmazásokat, amelyek a számítógép távoli vezérlését teszik lehetővé. Ha ugyanis ezt sikerül feltörniük a támadóknak, teljesen átvehetik az irányítást a készülék felett. Mindezek mellett a munkatársak generációra szabott képzése elengedhetetlen, hiszen lehet bármennyire biztonságos egy rendszer, elég egy rossz kattintás, egy átlépett biztonsági előírás, és máris megtörtént a baj.

Kiss Franciska