információbiztonsági tudnivalók – zsarolóvírus

Kedves Imre!

A K&H vállalati biztonságtudatosság program részét képező hírlevelekben megismerheti a leggyakoribb vagy az aktuálisan legnagyobb veszélyt jelentő támadási formákat, valamint ezek kivédési módjait. A vállalatokat érintő támadások sok esetben specifikusabbak, mint azok, amelyeknek elsősorban a magánszemélyek a célpontjai, azonban a vállalatok esetén is elég egyetlen óvatlan kolléga és már meg is történik a baj. Hírlevél sorozatunkban abban próbálunk segíteni, hogy a kollégák megértsék a veszélyt, ami rájuk – és rajtuk keresztül a vállalatra leselkedik.

Mi az a zsarolóvírus?

A zsarolóvírus (ransomware) olyan rosszindulatú programkód, mely **titkosíthatja az adatokat, vagy zárolhatja az eszközt** annak érdekében, hogy támadók pénzt csikarjanak ki az áldozattól. A támadás után jellemzően váltságdíj követelő képernyő jelenik meg, melyen a támadók - mindenféle garancia nélkül - az ígérik, hogy a megadott összeg kifizetése után visszaállítják az adatokhoz, gépekhez történő hozzáférést.
A zsarolóvírusokat az esetek **többségében anyagi haszonszerzésre használják** a támadók, azonban a felhasználás módja a támadó szándékaitól függően sokféle lehet. A teljesség igénye nélkül: hacktivizmus, “csak” rombolás/károkozás, az áldozat piaci szerepének meggyengítése, más - szofisztikált támadás - leplezése. A ransomware-támadás bizonyos bűnözői csoportok “specialitása”, melyre önálló szolgáltatás is épült már: RaaS (Ransomware as a Service).

a védelem rétegei

A zsarolóvírusok ellen három rétegben érdemes leginkább védekeznünk:

1. a megelőzés során gondoskodunk arról, hogy a zsarolóvírus ne kerülhessen be informatikai rendszereinkbe:

- privilegizált szerepkörök (pl. rendszergazda, aki telepítheti a szoftvereket) kialakításával
- vírusvédelmi szoftverek alkalmazásával, tartalomszűréssel, rendszeres teljeskörű vizsgálattal, a szoftverek beállítását pedig erős jelszóval, vagy többfaktoros autentikáció beállításával védjük,
- az operációs rendszer, böngésző, alkalmazások frissítésével,
- mellékletek, csatolmányok körültekintő megnyitásával
- kettős kiterjesztésű fájlok megnyitásának tiltásával, a kiterjesztés megjelenítésével
- makrók futtatásának és a futtatható állományok tiltásával,
- linkek vizsgálatával kattintás előtt
- automatikus lejátszás funkció kikapcsolásával,
- a nem használt vezeték nélküli kapcsolatok kikapcsolásával

2. a már bekerült kártevő esetén a legfontosabb, hogy ne terjedjen tovább, a lehető legkevesebb fájlt fertőzze meg:

- a szegmentált hálózat egyik előnye, hogy a kártevő nem terjed el a teljes belső hálózaton, csak az adott szegmenst fertőzik meg,
- a konténerek alkalmazása (ami az iPhone készülékek esetén alapértelmezett), szintén azt biztosítja, hogy a kártevő ne szabaduljon el
- a hálózati kapcsolat azonnali megszakításával elérjük, hogy a kártevő és vezérlőszervere ne kommunikálhasson
- semmilyen perifériát, adathordozót ne csatlakoztassunk és semmilyen vezetékes vagy vezeték nélküli módon ne próbáljunk bármilyen más eszközt csatlakoztatni a gépre, mert ezzel kockáztatjuk a fertőzés elterjedését.

3. készüljünk fel a helyreállításra:

- határozzunk meg visszaállítási pontokat
- készítsünk rendszeresen mentéseket, amiket lehetőség szerint offline tárolunk és rendszeresen ellenőrizzük, hogy egy esetleges támadás esetén a rendszerek helyreállíthatóak-e a mentésből

banki támogatás a védekezéshez

A K&H Vállalati API szolgáltatásunk lehetővé teszi, hogy Ön egy integrált, automatizált folyamaton keresztül kapjon képet cége aktuális pénzügyi helyzetéről és biztonságos módon kezdeményezhessen átutalásokat.

Ezzel a megoldással saját könyvelői vagy vállalatirányítási rendszeréből közvetlenül intézheti a mindennapi banki tevékenységét: elkerülhető az internetbanki felület

használata és a manuális adatbevitel, így jelentősen nő az adat- és információbiztonság, illetve csökken a manuális munkavégzésre fordított idő. Az utalási és számlainformációs adatok titkosított, zárt, két végpont között kerülnek átadásra a rendszerek között, így nem szükséges harmadik feles szolgáltatók bevonása, rendszerek telepítése.

kapcsolódó tartalmak

- eszközbiztonság – podcast epizód
- kiberbiztonsági hírlevelek korábbi részei
- általános információkat a K&H Bank Biztonság a pénzügyekben oldalán találhat

Üdvözlettel:
K&H Bank

Vállalati Ügyfélszolgálat +36 1 468 7777 » kh.hu » bank@kh.hu a KBC Csoport tagja