Zsarolóvírusok: amikor nemcsak az adatok, hanem egy szervezet működése is veszélybe kerül

Egyetlen sikeres kibertámadás elegendő lehet ahhoz, hogy egy vállalat, intézmény vagy akár egy egészségügyi szolgáltató informatikai rendszerei részben vagy teljesen működésképtelenné váljanak. A zsarolóvírusok ma már nem csupán az adatok titkosításával okoznak károkat: a támadók egyre gyakrabban bizalmas információk nyilvánosságra hozatalával is fenyegetőznek. A védekezés ezért nem kizárólag informatikai kérdés, hanem a szervezeti működés, a felkészültség és a válságkommunikáció próbája is.

A zsarolóvírusos támadások módszerei az elmúlt években jelentősen megváltoztak. A bűnözők sok esetben már nem elégednek meg az adatok titkosításával, amellyel megakadályozzák az érintett dokumentumok és rendszerek használatát. Előbb megszerzik és lemásolják a bizalmas információkat, majd azzal is fenyegetik az áldozatot, hogy fizetés hiányában közzéteszik azokat. Ezt a módszert kettős zsarolásnak nevezik.

Rés a pajzson

A támadások egyik gyakori kiindulópontja továbbra is az emberi figyelmetlenségre építő megtévesztés. Egy hitelesnek tűnő elektronikus levél, egy hamis bejelentkezési oldal vagy egy fertőzött melléklet elegendő lehet ahhoz, hogy a támadók hozzáférjenek egy felhasználói fiókhoz vagy eszközhöz.

Ugyanakkor nem minden zsarolóvírus-támadás vezethető vissza egy rossz kattintásra. A bűnözők kihasználhatják az elavult szoftvereket, a nem megfelelően védett távoli hozzáféréseket, a gyenge jelszavakat vagy az informatikai rendszerek biztonsági hiányosságait is.

Miután bejutottak egy szervezet hálózatába, megpróbálhatnak további rendszerekhez hozzáférni, magasabb jogosultságokat szerezni, illetve megakadályozni az adatok egyszerű visszaállítását. A tényleges zsarolás sokszor csak ezután kezdődik.

Támadás az adatainkért

Az Európai Unió Kiberbiztonsági Ügynöksége (ENISA) 2026 szeptemberében közzétett jelentésében a zsarolóvírusokat továbbra is a legsúlyosabb rövid távú hatásokkal járó kibertámadások közé sorolta. A jelentés szerint a vizsgált, pénzügyi haszonszerzésre irányuló események 40 százalékában zsarolóvírus telepítése is szerepelt.

A károk messze túlmutathatnak az informatikai eszközök helyreállításának költségein. Egy támadás miatt leállhat a termelés, akadozhat az ügyfélkiszolgálás, sérülhetnek üzleti kapcsolatok, és hosszú időre megrendülhet az ügyfelek bizalma.

Különösen nagy a tét az egészségügyben. Egy kórházban vagy szakrendelőben az informatikai rendszerek kiesése nemcsak adminisztratív nehézséget jelenthet. Az egészségügyi dokumentáció, az időpontfoglalás, a diagnosztikai rendszerek vagy az ellátást támogató alkalmazások elérhetetlensége közvetlenül befolyásolhatja a betegellátás folyamatosságát.

Nem elég a technológiai védelem

A zsarolóvírusok elleni védekezéshez elengedhetetlen a rendszeresen frissített informatikai környezet, a többtényezős azonosítás, a megfelelő jogosultságkezelés és a biztonsági mentések alkalmazása. Utóbbiaknál különösen fontos, hogy a mentések a támadók számára ne legyenek egyszerűen elérhetők, és azokból a rendszerek helyreállítását rendszeresen teszteljék.

Legalább ilyen fontos azonban, hogy a munkatársak felismerjék a gyanús helyzeteket, és tudják, kihez kell fordulniuk, ha rendellenességet tapasztalnak.

Egy kibertámadás ugyanis nem akkor kezd igazán komoly szervezeti problémává válni, amikor az első számítógép működésében hiba jelentkezik, hanem amikor a bizonytalanság miatt az érintettek nem tudják, mit tegyenek.

Ki jogosult döntést hozni? Kit kell értesíteni? Hogyan tájékoztatják a munkatársakat? Milyen információkat kaphatnak az ügyfelek, a betegek vagy a partnerek? Ezekre a kérdésekre egy súlyos incidens közben már sokkal nehezebb megfelelő válaszokat találni.

A felkészülés tehát nem merülhet ki a biztonsági szoftverek beszerzésében. Világos felelősségi körökre, előre kidolgozott eljárásokra, rendszeres gyakorlatokra és megfelelő válságkommunikációra is szükség van.

Az egészségügyi kiberbiztonság emberi oldala a Hétpecsét Egyesület Fórumán

A kiberbiztonsági válsághelyzetekből történő helyreállítás is napirendre kerül a Hétpecsét Információbiztonsági Egyesület 2026. novemberi Információvédelem Menedzselése Szakmai Fórumán.

Farkas János, a Bács-Kiskun Vármegyei Oktatókórház Informatikai osztályvezető-helyettese „Felkészülni egy zsarolóvírus másnapjára - esettanulmány” címmel tart beszámolót.

Az előadás témája különösen aktuális, hiszen egy egészségügyi intézményben az informatikai biztonság, a dolgozók felkészültsége és a betegellátás folyamatossága szorosan összefügg. Egy megfelelően felépített helyreállítási stratégia nemcsak a bizonytalanság csökkentését segítheti, hanem azt is, hogy a munkatársak kritikus helyzetben gyorsabban és tudatosabban cselekedjenek, így az ellátás folyamatos maradhasson.

A Hétpecsét Információbiztonsági Egyesület szakmai fórumainak célja, hogy az információvédelem és a kiberbiztonság területén dolgozó szakemberek megosszák egymással tapasztalataikat, bemutassák a gyakorlati megoldásokat, és hozzájáruljanak a hazai információbiztonsági kultúra fejlődéséhez.

További információ: www.hetpecset.hu

Sajtókapcsolat:

- Gasparetz András
- Hétpecsét Egyesület
- +36 20 4349 000
- elnok@hetpecset.hu

Eredeti tartalom: Hétpecsét Információbiztonsági Egyesület

Továbbította: Helló Sajtó! Üzleti Sajtószolgálat

Ez a sajtóközlemény a következő linken érhető el:
https://hellosajto.hu/?p=34025