A zsaroló programok elleni utolsó védelmi vonal

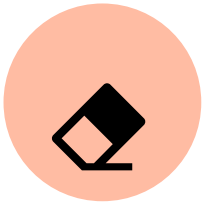
NetApp Ransomware Protection and Recovery

Katona Tihamér
NetApp Business Development Manager
2023.11.06

Az Ön adatai értékesek, és ezt a bűnözők is tudják.

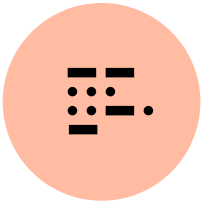
“2025-re a vállalatok 40%-a fogja megkövetelni, hogy az adattárolási termékek integrált zsarolóvírus elleni védelmi mechanizmusokkal rendelkezzenek, szemben a 2021-es 10%-kal.”[1]

1. Gartner. “Innovation Insight for Cyberstorage Solutions to Protect Unstructured Data Against Ransomware”, 2021



Törlés

A hackerek törlik a biztonsági mentési adatokat, hogy megakadályozzák az adatok helyreállítását.



Titkosítás

A támadók titkosítják az adatokat, és váltságdíjat kérnek a kulcsért.

Kiszivárogtatás

A hackerek azzal fenyegetőzhetnek, hogy nyilvánosságra hozzák az ellopott adatokat, hacsak nem fizet egy második váltságdíjat.

Mekkora veszélyben vagyunk?

66%

a szervezeteknek érte ransomware támadás az előző évben[2]

76%

a támadásonak az adatok titkosítását eredményezte[2]

24%

egy és hat hónap közötti időbe telt, mire felépültek a támadásból[2]

2. Sophos, “The State of Ransomware 2023.”

Mennyibe kerül a zsarolóvírus?

$12B

Éves szinten 20-30%-kal növekvő biztosítási díjak[3]

$1.54M

Az átlagos váltságdíj 2023-ban ($812 380 2022-ben)[4]

$1.82M

A zsarolóvírus-támadások átlagos helyreállítási költsége 2023-ban a váltságdíj nélkül ($1,4M 2022-ben)[4]

3. Standard and Poor's report.
4. Sophos, "The State of Ransomware 2023."

NetApp

11 másodpercenként történik zsarolóvírus támadás[5]

Felkészült?

54%

A vállalkozások 54%-a szerint a zsarolóvírus-támadások túl fejlettek ahhoz, hogy az informatikai csapatuk egyedül kezelni tudja őket. [6]

8%

Az áldozatok 8%-a szerzi vissza az összes adatát egy zsarolóvírus-támadás után.[7]

50%

Az informatikai szakemberek fele úgy gondolja, hogy szervezete nincs felkészülve a zsarolóvírus-támadások elleni védekezésre.[7]

35%

Az adatok 35%-a elveszik egy átlagos zsarolóvírus áldozatnál.[8]

5. Cybercrime Magazine, “Global Ransomware Damage Costs Predicted to Reach $20 Billion (USD) by 2021,” by Steve Morgan, October 21, 2019.
6. Sophos, “Ransomware Recovery Cost Reaches Nearly $2 Million, More than Doubling in a Year, Sophos Survey Shows,” April 7, 2021.
7. Sophos, “The State of Ransomware 2023.” May 2023
8. Sophos, “State of Ransomware 2021,” April 2021.

Helyreállítási költség és idő az adat-visszanyerési módszer szerint [9]

Költség

Kifizette a váltságdíjat és visszakapta az adatokat	Biztonsági másolatokat használt az adatok visszaállításához
átlag **$2.6M**	átlag **$1.62M**

Idő

Váltságdíjat fizetett	Biztonsági másolatokat használt
egy héten belül felépült	
39%	**45%**
több mint egy hónapig	
32%	**23%**

9. Sophos, “The State of Ransomware 2023.” May 2023

A helyreállítás költségei és a zsarolóvírus-támadást követő leállási idő, valamint a hírnevet ért károk 10-15-ször nagyobbak lehetnek, mint a váltságdíj.[10]

10. Gartner. “How to Prepare for Ransomware Attacks”.

Zsarolóvírus-ellenálló adatinfrastruktúra

Kritikus adatok

- biztonsága
- elérhetősége
- megbízhatósága
- helyreállíthatósága

NetApp zsarolóvírus elleni védelem

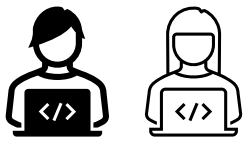
Védje adatait a zsarolóvírus-támadások ellen

Védelem

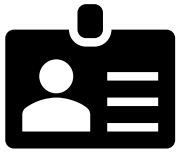
Automatikusan blokkolja az ismert rosszindulatú fájltípusokat

Víruskeresés a fájlhozzáféréskor

Az adatok megsemmisülésének megakadályozása megváltoztathatatlan és kitörölhetetlen másolatokkal



Csaló adminok és rosszindulatú felhasználók blokkolása



Biztonságos adathozzáférés, végponttól végpontig

Növeli az átláthatóságot és optimalizálja az adathozzáférési engedélyeket

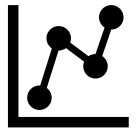
Észlelés

A fájlrendszer és a felhasználói viselkedés anomáliáinak észlelése és az azokra való reagálás

Automatikusan létrehoz helyreállítási pontokat és blokkolja a veszélyeztetett felhasználói fiókokat

Helyreállítás

Az adatok perceken belüli helyreállítása az állásidő minimalizálása érdekében



Fejlett kriminalisztika és elemzések alkalmazása a NetApp segítségével vagy vezető SIEM eszközökkel

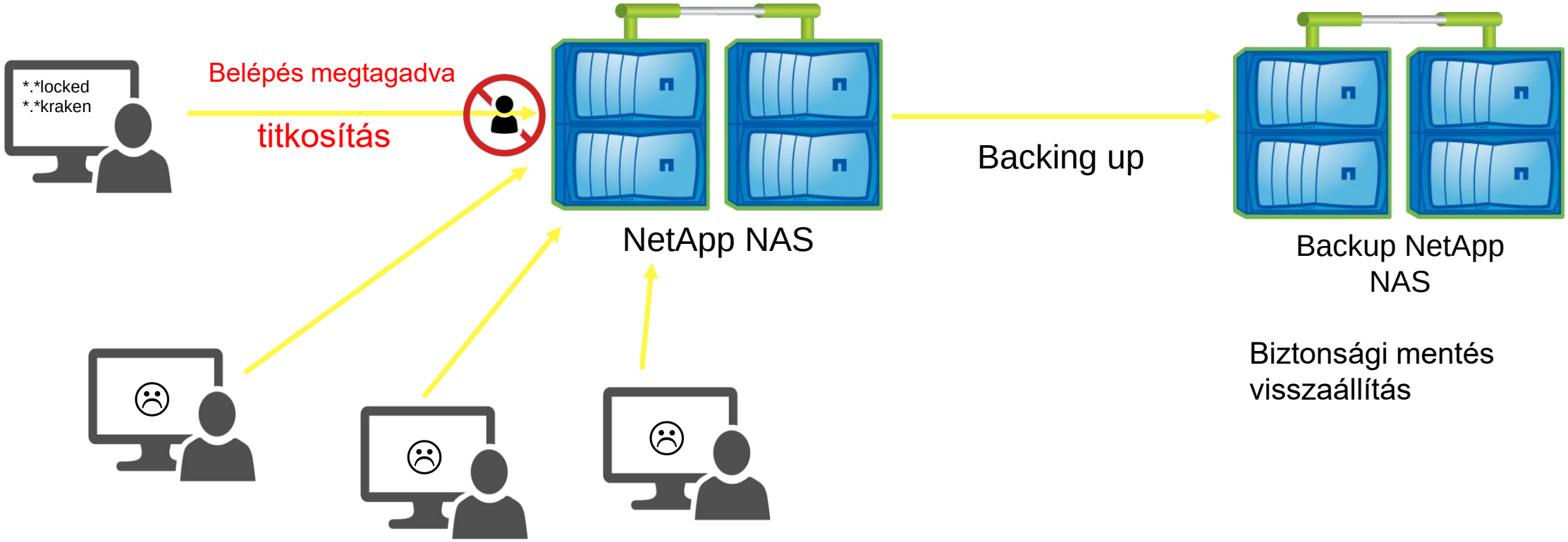
NetApp

Ransomware támadások felismerése és csökkentése NetApp ARP-vel

NetApp NAS környezet

Azonosítani tudom a titkosított fájlokat a beépített anti-ransomware funkció segítségével (entropy detection). A NAS az észlelés után azonnal helyi snapshot felvételeket hoz létre.

Biztonsági mentések védelme SnapLock segítségével



A Cloud Insights (Cloud Secure) képes észlelni az anomáliákat a felhasználói viselkedésben, blokkolja a támadó munkamenetét és jelentést készít.

NetApp®

Az egyetlen olyan vállalati tárolóeszköz-gyártó, amelyet szigorúan titkos adatok tárolására hitelesítettek.

Commercial Solutions for Classified (CSfC) Program Component List

FIPS 140-2

U.S. Department of Defense Information Network (DoDIN) Approved Products List (APL)

Common Criteria

A legfontosabb megállapítások

- A támadásokkal kapcsolatos költségek és adatvesztés fedezéséhez több kell, mint kiberbiztonsági biztosítás. A legjobb védekezés jó támadás: ügyeljen arra, hogy a bevált gyakorlatok, a biztonság és az adatvédelem a helyén legyen, mielőtt támadás történik.
- A zsarolóvírusra való felkészülés a lehetséges kockázatok és biztonsági hiányosságok feltárásával, valamint azok orvoslásának legjobb módjának meghatározásával kezdődik.
- A szükséges NetApp® szoftverek és eszközök megfelelő implementálása, konfigurálása és kezelése növeli a zsarolóvírusokkal szembeni ellenálló képességet.
- A zsarolóvírus-támadások utáni túlélés kulcsa annak biztosítása, hogy az üzleti szempontból kritikus adatok teljesen helyreállíthatók és sértetlenek legyenek.

Köszönöm a figyelmet