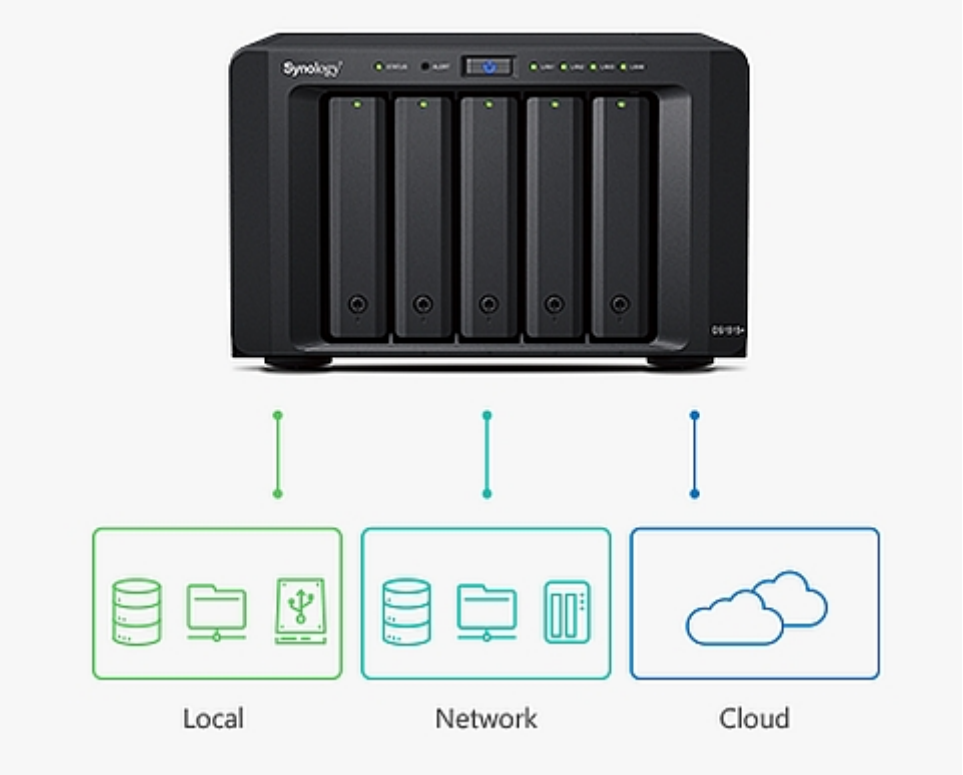
Synology soovitab: kuidas kaitsta krüptoviiruse eest oma võrgusalvestusseadet

9 aastat tagasi - 24.04.2016 Autor: AM



Krüptoviirus on vastik nuhtlus ka neile, kes hoiavad asju turvalises võrguserveris RAID-iga kaitstud kõvaketastel. Kui krüptorviirus möllab, siis kirjutab see üle ka võrguketastel asuvad failid, krüoteerides need ära ja käisdes lahtitegemise eest lunaraha. Ning kui ettenägelik kasutaja on teinud automaatse varunduse, siis ühel hetkel kirjutatakse üle ka tema eemal asuvad kaitstud varundusfailid, sest arvutis on krüptoiirus asunud kõiki olulisi faile üle krüpteerima ja need varundatakse ka arhiivi. Mida siis teha? Võrgusalvestusseadmete tootja Synology annab nõu, kuidas selliste pahalaste vastu saab ja mida tuleks teha oma andmete kaitsmiseks.

Synology on pahavara plahvatusliku leviku vastu oma salvestusseadmetes kasutusele võtnud kaks turvapaketti: Security Advisor ja Qualysguard Security Scan. Kuid lisaks tuleb andmeid kaitsta ka nakatunud arvutitest ründava krüptoviiruse vastu, mis ähvardab faile salvestusseadmes.

Mis on lunavara ja krüptoviirus?

Krüpteeriv pahavara - CryptoWall, CryptoLocker, TorrentLocker jt krüpteerib kasutaja failid, mis asuvad arvutis või ligipääsetavatel võrguketsatsel ja kui see on tehtud, küsib lunaraha, et failid uuesti tagasi saaks. Ilma paroolita pole võimalik neid niisama lihtsalt lahti krüpteerida.

Mida krüptovara vastu ette võtta?

Selleks, et pahavara isiklikke tähtsaid andmeid luku taha ei paneks, on neli ennetavat võimalust:

1. Uuenda oma arvuti operatsionisüsteemi. Installi alati vajalikud turvauuendused ja loobu platvormidest, mida tootja enam ei toeta.

2. Installi arvutisse hea antiviirus ja turvapakett, mis aitab kahjulikke tarkvarasid avastada ja ennetada nende ründeid.

3. Ära ava kahtlasi faile. Mõtle alati mitu korda, kui klikid e-posti lisanditel, mille päritolus kindel pole. Ka süütu laiendiga falid võivad peita endas käivitatavat viirust.

4. Lülita kaughaldus välja. Thti võib pahavara saabuda RDP kaudu (Remote Desktop Protocol). Hoia RDP teenus väljas, kui kaughaldust pole vaja.

Mitme versiooni varundus on parim kaitse

Krüpteeriv pahavara võib ilmsiks tulla alles sis, kui on juba hilja - paljud olulised failid on parooliga krüpteeritud. Parooli saamiseks tuleb aga lunaraha maksta. Kui avastamisega jäädi hiljaks, võib juhtuda, et ka varundusse on jõudnud juba krüpteeritud failidega üle kirjutatud sisu.

Selleks, et oma andmed siiski ka hiljem avastatud pahavarajuhtumi järel kätte saada, aitab vaid mitmeversiooniline varundus. See tähendab, et taastada saab lisaks viimasele versioonile ka eelnevaid versioone andmetest, mis võivad olla veel pahavarast puutumata.

Synology Cloud Station Backup võib näiteks alles hoida kuni 32 eelmist versiooni varundusest, seega võib üsna kindel olla, et mingist seisust õnnestub oma vanad andmed kätte saada - kasvõi mitme päeva või nädala tagusest seisust ja kõik pole jäädavalt kadunud.

Varunda ka kaugemale

Võrgukettale varundamine ei anna siiski veel täit kindlust, et pahavara andmetele ligi ei saa. Viirus võib võrgukettale ligi saada arvuti teenuste kaudu. Abiks on lisa-turvalisus, mis tähendab, et võrgusalvestusseadmest tehakse varukoopia ka mõnesse eraldiseisvasse serverisse, kuhu puudub kasutaja arvutitel otseligipääs.

Siis liiguvad andmed järgmiselt: kohalik arvuti - võrguketas - pilveteenus. Kohalikust arvutist otse pilveteenusele ligi ei saa, sinna saab varundada vaid võrgusalvestusseade.

Mida teha, kui lunavaraviirus juba möllab?

Kui pahavara on juba arvuti ja andmete kallal, siis tuleb käituda järgmiselt:

1. Lülita välja WiFi ja/või eemalda arvuti küljest võrgukaabel.

2. Puhasta võrgust väljas olev arvuti viirusetõrjevahenditega ja veendu, et see ei ole enam nakatunud.

3. Taasta andmed varukoopiast, mis pole nakatunud.

- Uudised
- Turvalisus