Leiliruum külmkapis: küberründajad keerasid Selveri ja Euroopa poodide külmikud 50-kraadisesse leitsakusse

1 nädal tagasi - 02.11.2026 Autor: AM

Sel esmaspäeval tabas küberrünnak Selveri keti (üht) toidukauplust, kus ründajad pääsesid ligi poe külmasüsteemi kaugjuhtimise arvutile ning kruttisid külmleti temperatuuri 50 soojakraadini.

Külmasüsteemide tehnoloogiatarnija Kitman Coldtechi tegevjuht Jann Mutso kinnitas rahvusringhäälingule juhtunut,konkreetset poeketi poodi aga osapooled turvalisuse kaalutlustel ei nimetanud. Väidetavalt oli see viimane uuendamata süsteemiga kauplus.

Eesti polnud selles kuumalaines aga sugugi üksi – samal päeval anti sarnastest rünnakutest teada ka Soomes, Rootsis, Belgias, Luksemburgis ja Iirimaal.

Öine kuumalaine muutis külmletid prügikastideks

Rootsi jaekettide ICA ja Coop töötajad avastasid esmaspäeva varahommikul tööle jõudes, et nende külmikud ja sügavkülmikud huugavad täistuuridel sooja toota. Üks Rootsi ICA pood teatas sotsiaalmeedias otsekoheselt, et nende seadmed olid öösel "ära häkitud" ja seatud 50 soojakraadi peale. Stockholmis asuva ICA Baroneni kaupluse müügijuhi sõnul toimus rünnak kohaliku aja järgi kell kaks öösel, kuid jaole saadi sellele alles pool kuus hommikul.

ICA pressiesindaja kommenteeris olukorda uudisteagenbtuuridele e-kirja teel: "Me oleme teadlikud, et piiratud hulka kauplusi mõjutas öine intsident, mis avaldas mõju nende jahutus- ja külmutussüsteemidele."

Sarnaseid rünnakuid kinnitas kuues oma poes ka Rootsi teine suur jaekett Coop.

Belgia ja Luksemburgi poodides rullus lahti täpselt sama stsenaarium, kui jaeketid Ahold Delhaize ja Colruyt avastasid kümnetes kauplustes ootamatud temperatuuritõusud. Ahold Delhaize'i süsteeme haldava Belgia külmutusettevõtte Sabcobel tegevjuht Stephan Moelans kinnitas, et tegu oli küberrünnakuga, mille käigus lülitati seadmete aurustid sulatusrežiimile. Colruyt Grupi pressiesindaja teatas viie poe ründamisest ning Iirimaal said pihta 13 SuperValu kaupluse

jahutussüsteemid.

See pole esimene kord, kui toidupoed sellise "kuumarabanduse" saavad. Ahold Delhaize teatas juba oktoobris politseile "kahtlasest tegevusest" oma taristus ning 12. oktoobril tabas veelgi rängem rünnakulaine Prantsusmaad. Seal võtsid häkkerid Taani tootja Danfossi juhtimissüsteemide kaudu üle sadade supermarketite külmutusseadmed, kütsid need 50 kraadini ning põhjustasid lisaks riknenud toidule ka reaalseid tulekahjusid.

Kuidas küberkurjategija kodumasinasse või autosse poeb?

Kõige levinumad sihtmärgid on internetti ühendatud ja mõne nutika äpi kaudu kaugjuhitavad seadmed: turvakaamerad, video-uksekellad, valvesüsteemid, nutilukud, termostaadid ja keskküttesüsteemid. Ohus on ka internetti ühendatud külmikud, ahjud, pesumasinad ja nutikad hambaharjad.

Turvatööstuse andmetel on üle kolmveerandi kõigist võrguseadmete rünnakutest suunatud aga hoopis ruuterite, mitte kodumasinate endi vastu. Kehvasti turvatud koduruuter on küberkurjategijale nagu lahtine välisuks, kustkaudu jalutatakse otse elutuppa ja võetakse üle kõik, mis elektrit tarbib ja võrgus suhtleb.

Kui kurjategija on kord seadmesse sisse pääsenud, saab ta teha kahte asja: koguda infot või võtta seadme juhtimine üle. Kaamera näitab kodus toimuvat, mikrofon kuulab pealt ning ülevõetud ruuter paljastab kogu võrguliikluse. Juhtimise haaranud ründaja saab seadmeid sisse ja välja lülitada, seadeid muuta, kasutajaid kontodelt välja lukustada või kasutada nutiseadet hüppelauana samas võrgus asuva sülearvuti sisu ja isiklike andmete vaatamiseks.

Kas transport ja veevärk on järgmised?

Kas see tähendab, et homme võtab keegi üle autod, elektrivõrgu või veevärgi?

Küberturvalisuse teadlased on võrku ühendatud sõidukite haavatavusi korduvalt tõestanud. Juba 2015. aastal võtsid teadlased internetti ühendatud meelelahutussüsteemi kaudu kaugjuhtimisega üle liikuva Jeepi, mis sundis tootjat tagasi kutsuma umbes 1,4 miljonit sõidukit. Peaaegu kümme aastat hiljem paljastati turvaauk, mis võimaldas jälgida, avada ja käivitada teatud Kia mudeleid, aga õnneks parandas tootja vea mõne kuuga ja päriselus seda teadaolevalt ära ei kasutatud.

Sõidukid ning igasugune muu taristu, nagu elektri- ja veevõrgud, on siiski ehitatud mitmekihiliste turva-, seire- ja varusüsteemidega. Need ei ole

küberrünnakute suhtes küll täiesti immuunsed, kuid on kodusesse Wi-Fi-võrku ühendatud mõnedest seadmetest märksa kõvemad pähklid.

Kuidas oma nutikodu kaitsta?

Selleks, et sinu kodused seadmed võõrastele kuuletuma ei hakkaks, soovitavad küberturvalisuse eksperdid järgida selliseid reegleid:

- Vaheta kohe oma seadmetel vaikimisi paroolid ja võta võimalusel kasutusele kaheastmeline autentimine.
- Paigalda regulaarselt tarkvarauuendusi nii ruuterile, nutikõlaritele kui ka teistele seadmetele.
- Ühenda võrgust lahti või vaheta välja vanad seadmed, mis enam tootjalt turvauuendusi ei saa.
- Hoia seadmeid kohalikus võrgus ja ühenda need "laia" internetti vaid siis, kui selleks on selge ja reaalne vajadus.

Kõige lihtsam reegel on sageli kõige tõhusam: mida vähem võrku ühendatud seadmeid sul on, seda vähem on ründajatel potentsiaalseid sissepääsupunkte.

- Uudised

- Turvalisus
- Võrguseadmed

Pilt

DANONE
DANONE