VERKOSSA

Eläintalous herättää joissain ihmisissä vahvoja tunteita. En pidä mahdottomana, että sen harjoittajiin kohdistettaisiin iskuja myös verkossa. **TIETOTURVA-ASIANTUNTIJA ILARI KARINEN, KYBERTURVALLISUUSKESKUS**

Onko sinun ovesi raollaan verkon hiippareille?

Sähköposti on yleisin keino tunkeutua pienyritysten ja kotien tietokoneille. Useille verkkorikollisille se on myös ainoa, mitä ne hakevat.

Tietoturva on yhtä tärkeä kuin lukittu ulko-ovi, vertaa tietoturvayritys D-Fencen toimitusjohtaja **Jani Pajari**.

”Kummastakaan et halua kutsumattomia vieraita.”

D-Fencen kokemuksien mukaan moni pieni yrittäjä ajattelee hyväuskoisesti, etteivät hänen yrityksensä asiat ketään kiinnosta.

Se on sinänsä useimmiten totta: verkkorikollisten toiminta ei perustu pienten yritysten vakoiluun.

Se, mikä soluttautujia kiinnostaa, on mahdollisuus varastaa käyttäjien henkilöllisyys. Siis esimerkiksi urkkia käyttäjän nimissä tämän sähköpostilla tietoja.

Toinen yleinen tavoite on käyttää vastaanottajan koko konetta esimerkiksi jonkin verkkopalvelun kaatamiseen.

”Sähköposti on helpoin ja halvin tapa lähestyä ihmisiä. Aina niitä viestejä joku klikkaa - jos ei tarkoituksella niin vaikka vahingossa kiireessä.”

Päälle tulevat luonnollisesti myös suoranaiset huijausviestit, joilla käytetään suoraan hyväksi vastaanottajien hyväuskoisuutta.

”Tietoturvaa” ja tietoturvaa

Pajarin mukaan suuri osa sähköpostin ”tietoturvasta” on hoidettu puutteellisesti, koska suodatus vain siirtää oletetut haittapostit roskapostilaatikkoon mutta ne eivät poistu järjestelmästä.

Pajarin mielestä tämä vanhentunut roskapostin suodatusmalli on paitsi hukkaan heitettyä aikaa myös riski.

”Sähköpostin käyttäjä on kuitenkin vastuussa viesteistä. Se myös jättää mahdollisuuden avata haitallisia posteja.”

D-Fencen tavoitteena on, ettei tietoturva söisi käytettävyyttä saati aiheuttaisi käyttäjilleen lisää töitä.

Yrityksen kehittämä palvelu tutkii sähköpostia ja sen kulkemaa reittiä Pajarin mukaan sen lähettäjälle asti.

Jos lähettäjää pidetään epäluotettavana, viesti palautuu takaisin hänelle.

Siten saapuvia tilauksia tai muuta tärkeää ei voi päätyä roskapostiksi lähettäjän tai vastaanottajan huomaamatta.

”Ainoa vaatimus palvelumme käytölle on, että on oma domain”, Pajari toteaa.

Jos käyttää jotain yleistä sähköpostipalvelua, on ensin vaihdettava omaan sähköpostipalveluun.

Avoin saa olla muttei huoleton

Toinen ilmiö, joka mietityttää tietoturvayrittäjää, on ihmisten huolettomuus sosiaalisessa mediassa.

”Ethän sinä kaupassa tai kadullakaan kerro tuntemattomille henkilökohtaisia asioitasi”, hän sanoo.

”Vaikka some on tärkeä myös yritysten markkinoinnissa, niin on hyvä muistaa, että kaikkea, minkä sinne laitat, voidaan käyttää myös väärin.”

D-Fence aloitti sähköpostin suojauksella mutta työ on laajentunut tunnistamaan asiakkaiden tietoverkosta myös muita mahdollisia haittoja. Tavoite on, että yrittäjien ei tarvitse miettiä tietotekniikan riskejä vaan he voivat keskittyä siihen, mitä he tekevät ja myyvät.

Jatkuvaa kilpajuoksua

Verkkohuijarien toiminta on entistä ammattimaisempaa, joten tietoturva on jatkuvaa kilpajuoksua.

”Lääkettä on vaikea kehittää ennen kuin tauti on todettu, mutta sitä yritetään.”

D-Fence tekee Pajarin mukaan jatkuvaa yhteistyötä viranomaisten ja alan muiden yritysten kanssa, jotta tietoturva parantuisi kansallisesti.

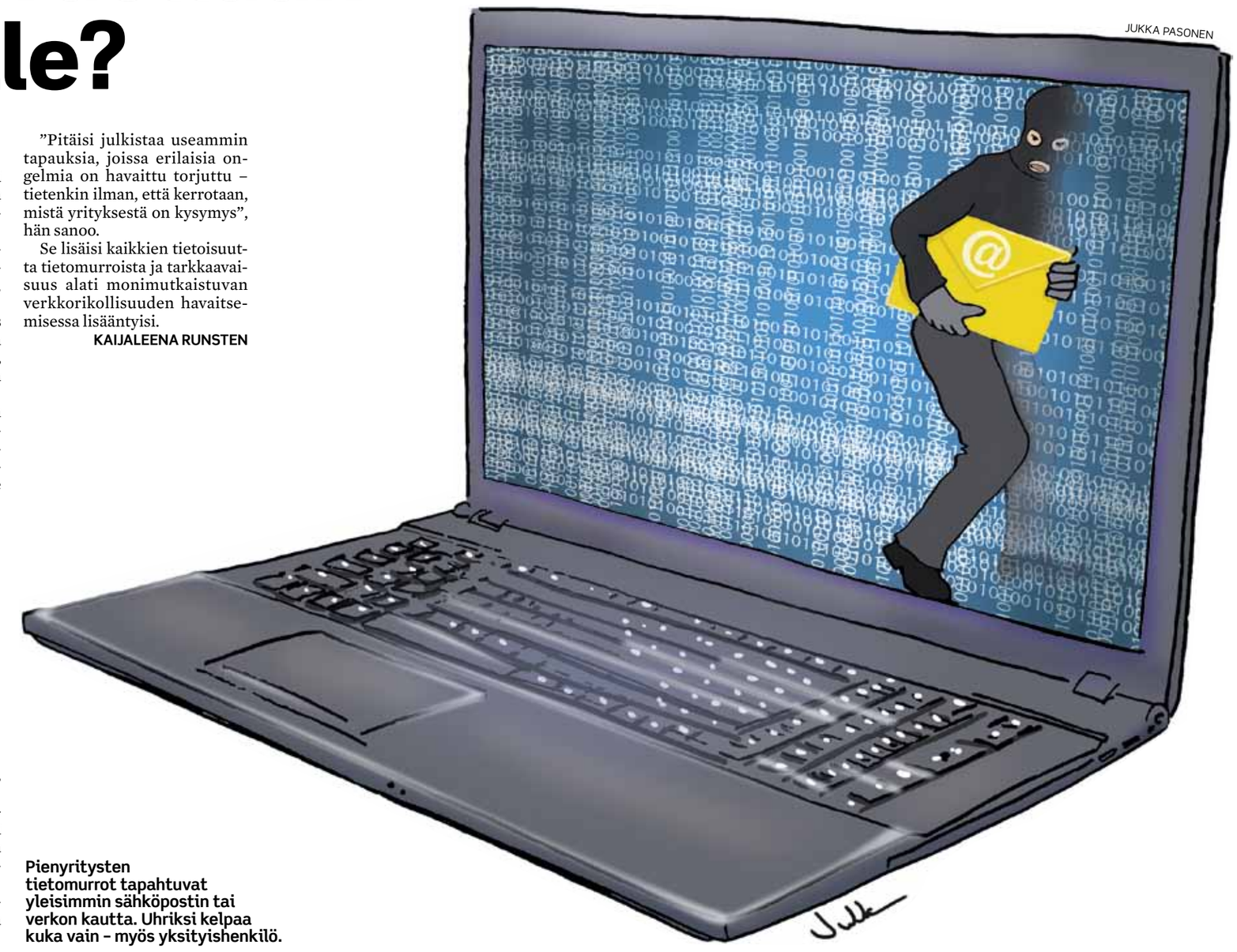
Vaikka tietoturvasta puhutaan paljon mediassa, suurin osa tapauksista jää kertomatta.

”Pitäisi julkistaa useammin tapauksia, joissa erilaisia ongelmia on havaittu torjuttu – tietenkin ilman, että kerrotaan, mistä yrityksestä on kysymys”, hän sanoo.

Se lisäisi kaikkien tietoisuutta tietomurroista ja tarkkaavaisuus alati monimutkaistuvan verkkorikollisuuden havaitsemisessa lisääntyisi.

KAIJALEENA RUNSTEN

JUKKA PASONEN



Pienyritysten tietomurrot tapahtuvat yleisimmin sähköpostin tai verkon kautta. Uhriksi kelpaa kuka vain – myös yksityishenkilö.

MIKÄ?

Tietoturvayritys D-Fence

D-Fence on Avainlippua kantava kotimainen tietoturvayritys, joka on perustettu 2000.
Tekee tuotekehityksessä yhteistyötä kumppaniverkoston kanssa.
Myynnistä vastaavat jälleenmyyjät eri puolilla Suomea ja ulkomailla.
Palvelu on käytössä erikokoisista pk-yrityksistä järjestöihin ja hallintoon.
Asiakkaita on lähes 5 000 ja määrä kasvaa yrityksen laajentuessa uusiin maihin, erityisesti Eurooppaan ja Afrikkaan.

Oman sähköpostin turvallisuutta voi testata D-Fencen verkkosivulla www.d-fence.fi/tuntest.

KARI SALONEN

Tietoturvan pitää hoitua luotettavasti ilman, että se vaivaa yrittäjää itseään, toimitusjohtaja Jani Pajari sanoo.

Palvelunestohyökkäys tukkii verkkosivut joukkovoimalla

Palvelunestohyökkäys merkitsee keinotekoisen ruuhkan luomista verkkopalveluun sen lamaannuttamiseksi.

Kyseessä ei ole tietomurto, vaan käytön estäminen, korostaa tietoturva-asiantuntija **Ilari Karinen** Viestintäviraston kyberturvallisuuskeskuksesta.

Kaikki hyökkäykset eivät mitenkään voi tulla viranomaisen tietoon, eikä tarkkoja tilastoja niistä ole. Trendi on kuitenkin nouseva. Palvelunestohyökkäykset ovat yhä voimakkaampia ja niitä havaitaan yhä useammin.

”Se tiedetään, että hyökkäyksiä havaitaan päivittäin kaikkien operaattoreiden verkoissa.”

Useimmat palvelunestohyökkäyksistä ovat pieniä. Niiden kohteena voi olla esimerkiksi yksittäinen laajakaistaliittymä.

Suuret hyökkäykset herättävät laajaa huomiota, kuten suomalaisten pankkien verkkopalveluita kaataneet hyökkäykset vuodenvaihteessa.

Maineen tavoittelua ja kiusantekoa

Tekojen taustalla on kaksi yleistä motiivia: maineen niittäminen verkkoaktivistien keskuudessa sekä kiusanteko. Harvinaisempaa on rahan kiristäminen hyökkäyksen uhrilta.

Hyökkäysten tehtailu on myös liiketoimintaa. Verkon karhunpalveluksille vaikuttaa olevan kysyntää.

”Erilaiset verkkorikollisryhmät tarjoavat palvelua, jossa rahaa vastaan voi tilata halutun laajuisen ja kestoisen hyökkäyksen tiettyyn osoitteeseen.”

Hyökkäyksen toteuttaja tarvitsee joukkovoimaa: runsaasti tietokoneita tai muita verkkoon kytkettyjä laitteita, jotka voidaan valjastaa tuottamaan liikennettä samaan aikaan.

Perinteinen keino on bottiverkko eli haittaohjelmien avulla kaapattu tietokoneiden verkosto. Haittaohjelman saastuttama tietokone voi toimia osana verkkohyökkäystä omistajan tietämättä.

Yhä useampi hyökkäys hyödyntää erilaisia internetin avoimia palveluja tai haavoittuvia laitteita.

Esimerkiksi internetin perusrakenteisiin kuuluville nimipalvelimille voi tehdä väärennettyjä kyselyjä, jos palvelin on heikosti suojattu. Väärennetyissä kyselyissä vastaukset lähetetäänkin kyselijän osoitteen sijaan hyökkäyksen kohteeseen.

Intohimoja herättävät kohteet alttiita

Jos verkkopalvelun katkeamisesta aiheutuu yritykselle suurta haittaa, voi olla paikallaan miettiä suojautumista. Ensimmäiseksi Karinen kehottaa pohtimaan riskiä: liittyykö yrityksen toimintaan jotain, joka houkuttaisi verkon aktivisteja?

Tällaisia piirteitä voivat olla tunnettuus tai kiinnostavuus jonkin aatteellisen toimijan näkökulmasta. Maaseudun elinkeinotkaan eivät välttämättä ole turvassa.

”Eläintalous herättää joissain ihmisissä vahvoja tunteita, enkä pidä mitenkään mahdottomana, että sen harjoittajiin kohdistettuja iskuja voitaisiin joskus tehdä myös verkossa.”

Käytännössä palvelunestohyökkäyksiä voi ehkäistä sopimalla varautumisesta oman operaattorin kanssa. Hyökkäyksen torjumiseksi se on estettävä, ennen kuin haittaliikenne pääsee yrityksen tietoverkkoon asti.

Tietoliikenneoperaattorit pystyvät useimmiten erottamaan hyökkäykset tavallisesta tietovirrasta. Niiden torjumiseksi voidaan esimerkiksi tehdä suodatuksia, jolloin haitallinen liikenne ei pääse asiakkaan verkkoon asti.

Toinen keino on katkaista tietoliikenne ulkomailta hyökkäyksen kohteeseen määräajaksi.

Palvelunestohyökkäyksissä käytetään huomattavasti enemmän ulkomailla sijaitsevia tietokoneita kuin kotimaisia. Karisen mukaan tähän on syynä muun muassa Suomen tehokas lainsäädäntö, operaattorien tekniset estomenetelmät sekä yleinen tietoverkkojen puhtaus.

HENRIK SCHÄFER

ILMIÖ

Verkkorikollisuus laajeneva ongelma

Tietojen kalastelu lisääntyy. Uhreja voidaan lähestyä sähköpostin ja verkkosivun lisäksi myös tekstiviestein ja puheluin.
Haittaohjelmatartuntoja voidaan torjua teleoperaattorien toimin.
Kyberturvallisuuskeskus käsittelee tietoturvaloukkaukset luottamuksellisina.
Tiedon salaamiseksi on käytössä vähän luotettavia ja helppokäyttöisiä ohjelmia.
Palveluestohyökkäyksiä voimaltaan yli 100 Gbit/s raportoidaan maailmalla kuukausittain: jo puolta pienemmät johtavat Suomessa internetin runkoverkon ongelmiin.
Viestintäviraston havainnointi- ja varoituspalvelu laajenee tänä vuonna koko valtionhallintoon.
Lista perustuu kyberturvallisuuskeskuksen havaintoihin viime vuodelta.

KUVA: JOHANNES TERVO

VERKOSTA LYHYESTI

Järjestöt: Peruskoulu digitalisoitava

Elinkeinoelämän Keskusliitto, Teknologiateollisuus ja Opetusalan Ammattijärjestö ehdottavat yhteisessä kannanotossaan tulevalle hallitukselle ohjelmaa perusopetuksen digitalisoimiseksi.

Järjestöjen mielestä on tärkeää, että peruskoulussa annetaan kunnon eväät tietoyhteiskuntaan. Se edellyttää tietoteknisten menetelmien painottamista opettajakoulutuksessa.

Järjestöt sallisivat oppilaiden omien laitteiden hyödyntämisen opetuksessa.

Lisäksi ne edistäisivät oppikirjojen sähköistymistä laskemalla digikirjojen arvonlisäveron 10 prosenttiin eli painettujen kirjojen tasolle.

Älypuhelimia kotihoitoon

Tyrnävän kunta kokeilee älypuhelimella toimivaa palvelua vanhusten kotihoidossa.

Älypuhelinsovellus tallentaa ja lähettää kotihoidon mittaustulokset viipymättä jatkohoidosta vastaavalle hoitajalle tai lääkärille. Tarkoitus on vähentää hoitotyöntekijöiden kirjauksiin kuluvaa aikaa sekä kirjausvirheitä.

Tammikuussa alkanut kokeilu kestää puoli vuotta. Se on saanut rahoitusta Tekesin Innovatiiviset kaupungit -ohjelmasta. Kokeilussa käytettävän sovelluksen on kehittänyt oululaisyhtiö Istoc.

Laitteet verkottuvat ensin yrityksissä

Laitteiden verkottuminen etenee yrityksissä nopeammin kuin kuluttajatalouksissa, arvioi konsulttiyhtiö Deloitte.

Kehitystä kutsutaan asioiden internetiksi. Deloitte arvioi tänä vuonna myytävän yli miljardi verkkoon kytkettyä langatonta laitetta, joiden lasketaan kuuluvan asioiden internetiin.

Esimerkkinä ilmiöstä käy kone, joka viestittää huoltotarpeestaan suoraan valmistajalle.

Suomalaiset korttikansaa

Suomalaiset maksavat kortilla melkein kaksi kertaa useammin kuin eurooppalaiset keskimäärin, kertoo maksukorttiyhtiö Visa.

Korttia käytetään Suomessa pieniinkin ostoksiin: keskimääräinen maksu oli viime vuonna 29,5 euroa.

Koko Euroopan keskiarvo oli 48 euroa.

Suomessa on noin seitsemän miljoonaa Visa-korttia. Niitä käytettiin yhteensä yli miljardi kertaa.

Visa ennustaa tälle vuodelle voimakasta kasvua lähimaksupalveluun ja verkkokauppaan.