R*

CGI

*RATKAISU 3.2018

Jyväskylän Energia turvaa elämää

Ajokortti tuli puhelimeen

LähiTapiola valjasti hakkerit yhteistyöhön

HAKKEREITA TARJOLLA

MÅRTEN MICKOS

Ennakoiva kyberturva | Jatkuva riskien valvonta

Pääkirjoitus

Näe tosiasiat

NYKYPÄIVÄN turvallisuusriskit edellyttävät tehokasta valvontaa, jossa hyödynnetään sekä teknologiaa että inhimillistä asiantuntemusta. Silti monet luottavat kybersuojautumisessaan liikaa pelkkiin teknisiin ratkaisuihin.

Toinen yleinen ongelma on epärealistinen luottamus kykyyn välttää ja havaita kyberturmat. Valitettavan usein ongelmat havaitaan liian myöhään ja ulkopuolisen tahon vinkkaamana.

Kyberturvallisemman tulevaisuuden rakentamiseksi kokosimme tähän numeroon tarinoita ja esimerkkejä siitä, miten kaikkien tulisi huolehtia turvallisuudestaan.

Kyberturvallista syksyä!

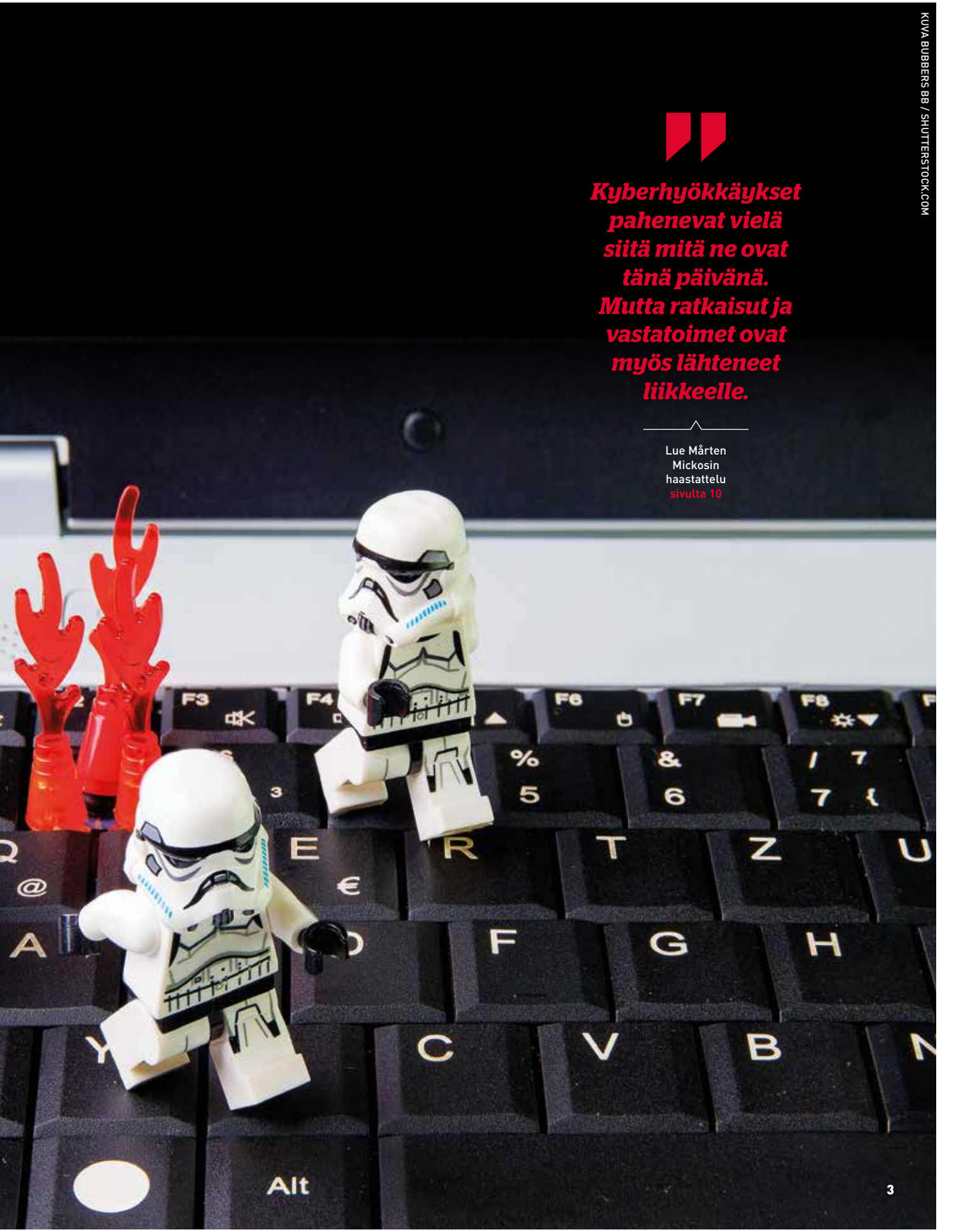
Leena-Mari Lähteenmaa
toimitusjohtaja, CGI Suomi

CGI

CGI on globaali IT-palveluyritys, jonka palveluksessa on 74 000 asiantuntijaa yli 40 maassa. Ratkaisu on CGI:n asiakaslehti Suomessa. Lisätietoja cgi.com, cgi.fi

Päätoimittaja Teea Hurme-Rintala, teea.hurme-rintala@cgi.com, **Toimituspäällikkö** Esa Luoto, esa.luoto@cgi.com, **Toimitus** yhteistyössä Legendium Oy:n kanssa. **AD** Laura Ylikahri, **Osoitteenmuutokset** myynti.fi@cgi.com, ISSN-L 1455-1934, ISSN 1455-1934 (Painettu), ISSN 2323-153X (Verkkojulkaisu)

YMPÄRISTÖMERKKI MILJÖMÄRKT
4041 0750
Painotuote



Kyberhyökkäykset pahenevat vielä siitä mitä ne ovat tänä päivänä. Mutta ratkaisut ja vastatoimet ovat myös lähteneet liikkeelle.

Lue Mårten Mickosin haastattelu
sivulta 10

KUVA BUBBERS BB / SHUTTERSTOCK.COM

SOC TORJUU KYBERUHKIA

”Vain kuusi prosenttia organisaatioista on riittävän kyvykkäitä suojautumaan hyökkäyksiä vastaan.”

TEKSTI ESA LUOTO KUVAT ANTTI KIRVES GRAAFI LAURA YLIKAHRI

Uutiset kyberuhista ovat tulleet osaksi arkipäivää. Siitä huolimatta niihin varautuminen on monissa yrityksissä ja organisaatioissa vaillinaista. CGI:n kyberturvallisuusjohtaja **Jan Mickos** kertoo esimerkin.

”Peräti 94 prosenttia kyberhyökkäyksen kohteena olevista organisaatioista kuulee hyökkäyksestä oman organisaationsa ulkopuolelta. Vain kuusi prosenttia organisaatioista on riittävän kyvykkäitä suojautumaan hyökkäyksiä vastaan.”

Jan Mickos korostaa, etteivät perinteiset virustorjunnat ja verkkopalomuurit eikä edes kyvykäs henkilöstö enää riitä uhkien torjuntaan. Erityiseksi haasteeksi on muodostunut se, miten yhdistää ympäristön eri tapahtumat yhtenäiseksi ja ajantasaiseksi tilannekuvaksi kokonaisuudesta ja kuinka hyvin sen perusteella osataan tunnistaa monimutkaiset haittatapahtumat sekä reagoida niihin.

360 asteen näkyvyys kyberturvallisuusuhkiin

Suomessa CGI on markkinoiden ainoa kyberturvallisuuden kokonaistoimittaja. Keskeinen osa CGI:n kyberturvallisuuspalveluja tuotetaan kyberturvallisuuskeskuksista (Cyber Security Operations Center – SOC). Suomen oman keskuksen lisäksi yhtiöllä on seitsemän SOC-yksikköä eri puolilla maailmaa. Verkoston ansiosta CGI:llä on erittäin kattava uhkatilannekuva sekä globaalisti että Suomessa.


Jan Mickos

”Asiakkaillemme tämä tarjoaa mahdollisuuden ennakoivampaan ja kokonaisvaltaisempaan tieto- ja kyberturvaan. Kansainvälinen SOC-verkosto valvoo ja puolustaa kumppaneiden kyberturvallisuutta ympäri vuorokauden ja yli maarajojen. Tarjoamme 360 asteen näkyvyyden niin teknologisiin kuin liiketoiminnallisiin kyberturvallisuusuhkiin. Seuraamme maailmanlaajuisesti kyberuhkia, suodatamme väärät hälytykset sekä tosipaikan tullen otamme ohjat, valmistaudumme seuraavaan hyökkäykseen ja teemme forensista tutkintaa”, Mickos kuvailee.

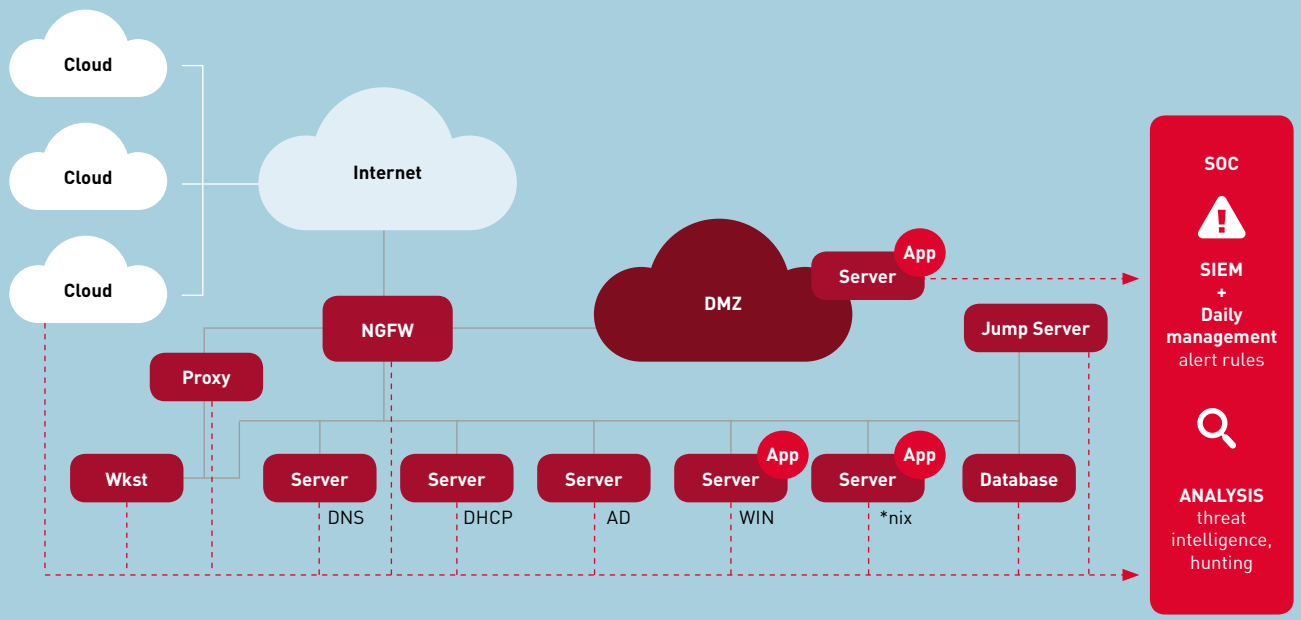
Jatkossa CGI:n Suomeen perustama kyberturvallisuuskeskus alkaa tarjota jatkuvaa tietoturvan valvontaa asiakkailleen myös muissa Pohjois-Euroopan maissa. *

ESIMERKKEJÄ CGI CYBER SECURITY CENTERIN PALVELUISTA

Jatkuvia kyberturvallisuuspalveluja:
- Jatkuva tietoturvan valvontapalvelu – Continuous Security Monitoring
- Liiketoimintasovelluksen jatkuva tietoturvavalvonta
- Tietoturvatapahtumien hallinta (Security Incident Response)
- Forensinen tutkimus ja proaktiivinen uhkien metsästäminen
- Jatkuva haavoittuvuuksien hallinta

Konsultatiivisia kyberturvallisuuspalveluja:
- Health Check -terveystarkastukset
- Murtotestaus ja Red Team -harjoitukset
- Tietoturvapäällikköpalvelut sekä turvallisuusjohtamisen ja hallinnan kehittäminen
- Kyberturvallisuuden kehityshankkeet

HERÄSIKÖ KYSYMYKSIÄ?
Jan Mickos
+358 40 847 8740
jan.mickos@cgi.com



Suomen oman keskuksen lisäksi yhtiöllä on seitsemän SOC-yksikköä eri puolilla maailmaa. Verkoston ansiosta CGI:llä on erittäin kattava uhkatilannekuva sekä globaalisti että Suomessa.

#CGInside

Aamupuuroa Afrikassa

TEKSTI JAAKKO LIIKANEN KUVA ANNEMARI UURTIMO

YHTEISKUNTAVASTUU on projektipäällikkö **Annemari Uurtimolle** tärkeä osa yritysten toimintaa.

”Yritysten pitää toimia vastuullisesti myös ympäristössään. Minusta on hienoa, että myös CGI ymmärtää roolinsa yhteiskunnassa pelkkää työllistäjää suuremmaksi.”

Uurtimolla on ollut jo pitkään halu auttaa konkreettisesti tavalla, joka liittyisi huono-osaisten, erityisesti lasten auttamiseen.

”Ystäväni vinkkasi minulle lasten hyvinvoinnin ja oikeuksien puolesta Keniassa työskentelevän Home Street Home ry:n. Yksi tapa auttaa oli lähteä vapaaehtoistyöhön. Siitä se lähti.”

Palvelumuotoiluun, varhaiskasvatuksen käyttöönottoprojekteihin ja sivistyspuolen hankkeisiin työssään syventynyt Uurtimo työskenteli heinäkuun ajan Keniassa Makongenin kylässä. CGI:llä jokainen työntekijä on oikeutettu käyttämään työpäivän vuodessa valitsemaansa vapaaehtoistyöhön. Uurtimo hyödynsi oikeutensa ja muut joustovaransa liittämällä ne kesälomaansa.

Työnantajaltaan hän vielä pyysi ja sai mukaansa myös kyniä, viivoittimia ja paperia lahjoitettavaksi kylään. Ne liittyivät osin varhaiskasvatukselliseen projektiin.

Keniassa hän asui paikallisten luona, keitti ja tarjoili koulussa puuroa aamuisin sekä auttoi rakennustöissä kottikärryt, kuokka ja metallihara työkaluinaan.

Mieleisintä oli puuronkeitto.

”Sain tutustua paikalliseen alakouluun. Ja HSH Feeding -projektin merkitys lapsille on valtava. Monet heistä tulevat kouluun pitkien matkojen päästä ja aamupuuro auttaa keskittymään. Monille aamupuuro on myös syy siihen, että he ylipäänsä tulevat kouluun.”

DATAHUB VIE ENERGIA-ALAN ALUSTATALOUTEEN

FINGRID DATAHUB OY hankkii sähkön vähittäismarkkinoiden keskitetyn tiedonvaihtojärjestelmän CGI:ltä. Huhtikuussa 2021 käyttöön otettavaan Datahubiin tallennetaan tietoja Suomen 3,5 miljoonasta sähkönkäyttöpaikasta.

Järjestelmällä nopeutetaan ja tehostetaan tiedonvaihtoa sähkön vähittäismarkkinoilla. Datahub parantaa osaltaan tiedon laatua ja edistää markkinatoimijoiden tasapuolista ja syrjimätöntä kohtelua tiedon saannissa. Kuluttajille datahub mahdollistaa erilaisia alan palveluita.

Datahub vastaa tulevan lainsäädännön, toimialan ja Fingridin yhdessä määrittelemiin tiedon käsittelyn, tietosuojan ja -turvan, tuen ja ylläpidon sekä synkronisten sähkön vähittäismarkkinaprosessien tarpeisiin.

”Olemme matkalla kohti puhdasta ja varmaa markkinaehtoista sähköjärjestelmää”, toteaa Datahub Oy:n toimitusjohtaja **Asta Sihvonen-Punkka.**

NUORI POLVI PANKISSA

MILLENIAALIT odottavat yksilöllistä palvelua ja asiakasuskollisuutensa palkitsemista, kertoo CGI:n tuore, suomalaisten nuorten aikuisten pankkipalveluille asettamia vaatimuksia kartoittava tutkimus. Vuoteen 2020 mennessä yli puolet työikäisistä edustaa milleniaaleja.

Digipalveluiden hyödyntämisestään huolimatta milleniaalit arvostavat henkilökohtaista palvelua. Kasvokkain kohtaamista ei välttämättä tarvita – myös puhelinpalvelua ja uusia chat-kanavia pidetään riittävinä henkilökohtaisen palvelun muotoina. Tärkeää kuitenkin on, että kanavan toisessa päässä on ihminen.

Ratkaisu-lehden tehtävänä on tarjota kiinnostavaa ja hyödyllistä sisältöä juuri sinulle.

Jotta lehtemme palvelee sinua parhaalla tavalla, pyydämme palautettasi. Mitä mieltä olet lehdestä nyt ja miten toivoisit meidän sitä kehittävän: **viestinta.fi@cgi.com**

Murrettakin ymmärtävä keinoäly

HELSINGIN ja Uudenmaan sairaanhoitopiiri ottaa käyttöön puheentunnistusratkaisun, jonka keinoäly oppii tunnistamaan jopa lääkärien murteet. CGI:n HUS:lle toimittama CGI OMNI360 puheentunnistus ja puheohjaus -ratkaisu integroidaan Apotti-järjestelmään.

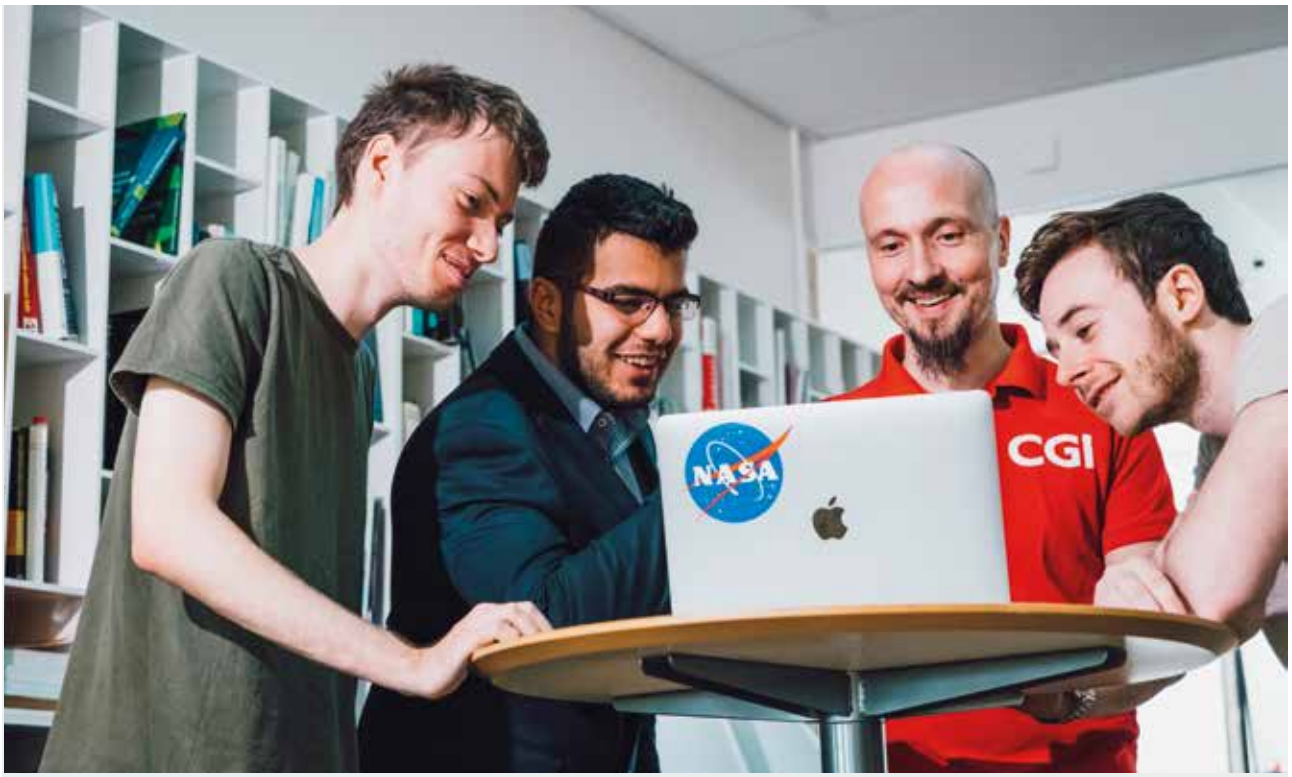
Puheentunnistus tulee muuttamaan merkittävästi HUSin työkäytäntöjä, sillä arkisin tehdään noin 7 000 sanelua vuorokaudessa. Vuositasolla saneluja kertyy lähes pari miljoonaa.

Puheentunnistamisen ansiosta asiakirjojen laatu paranee ja niiden valmisteluminen nopeutuu.

57 %

SUOMALAISYRITYKSISTÄ ARVIOI TODENNÄKÖISEKSI, ETTÄ ORGANISAATIO ON JOSKUS OLLUT TUNNISTAMATTA JÄÄNEEN TIETOMURRON TAI -VUODON KOHTEENA.

Lähde: CGI Finland



KUVA ANTTI KIRVES

AVARUUSDATA PARANTAA MAAILMAA

OTANIEMESSÄ käy kuhina, kun eri puolilta maailmaa saapuneet nuoret kehittävät YK:n World Challenge -kilpailussa maailmaa parantavia innovaatioita. Skaala on lavea, hyönteisruoasta siitepölyn leviämisen seurantaan sekä liikennetukosten avaamiseen.

Jo kuudennen kerran järjestettävän kilpailun finaali kisattiin elokuun lopulla. CGI oli toista kertaa mukana sponsorina ja mentorina.

Tänä vuonna World Challengen voiton vei kolmen Yorkin yliopiston opiskelijan Wildfire Aware -projekti, joka nimensä mukaisesti ennustaa maastopaloja ja vähentää niiden aiheuttamia vahinkoja.

ESAn ja NASAn mukanaolo kielii siitä, että kilpailussa on kyse avaruuteen liittyvistä teknologian sovellutuksista. Vaikka World Challenge on kilpailu eikä varsinainen hackathon, joihin CGI osallistuu aktiivisesti, näkee CGI:n mentori **Petteri Verronen** näissä paljon samaa.

”Kummassakin yhdistyvät oman firman pitkä kokemus, osaaminen ja asiantuntijuus opiskelijoiden ja nuorten yritysten tuoreisiin näkökulmiin. Kokeilukulttuurin tuloksena syntyy uudenlaisia ratkaisuja ja näkökulmia oman liiketoimintamme ja asiakkaidemme konkreettisiin haasteisiin.”

5x lyhyesti

1. Taitoalle valjastettin tekoäly tehostamaan ostolaskujen käsittelyä.
2. Someron sote-henkilöstön työvuorosuunnittelusta tehtiin yhteisöllistä Titania-pilven avulla.
3. Väre Energialle ja KSS Energialle uusi Kolbiri-asiakastietojärjestelmä.
4. CGI osallistuu elinkeinoministeri Lintilän luotsaamaan tekoälyohjelmaan.
5. CGI jatkaa LS Retailin ainoana Diamond-tason kumppanina Suomessa.

7 KOHTALOKASTA KYBERSYNTIÄ

Organisaation tietoturvasta huolehtimiseen vaikuttavat monet inhimilliset syyt.

TEKSTI PAULIINA NIKKO-TAKALA

1. KIELTÄMINEN

+ Yrityksillä on luja usko henkilöstönsä kykyihin puolustautua kyberrikollisia vastaan. Jopa kolme neljästä organisaatiosta* uskoo pystyvänsä havaitsemaan kyberhyökkäykset itse.
+ OPETUS: Usein kyberhyökkäykset havaitaan vasta ulkopuolelta saadun vihjeen tai tiedon perusteella. Tunnusta todellinen uhka. Jos olit eilen suojattu, se ei riitä tänään.

2. PUUTTEELLINEN JOHTAMINEN

+ Suuri osa suomalaisyrityksistä luottaa verkkotason valvontaan, vaikka vain 40 prosenttia haittaohjelmista jää viruksentorjuntaohjelmistoihin ja palomuureihin.
+ OPETUS: Nimitä ylimpään johtoon tietoturvasta vastaava henkilö. Tietoturvaa johdetaan strategisesti.

3. VAJAVAINEN RISKIENHALLINTA

+ Tyypillisesti kyberhyökkääjät etsivät arvoketjun heikoimman lenkin pyrkien näin arvokkaimpaan toimijaan. Vakavan tietomurron myötä voi pörssiyrityksen arvo laskea jopa 15 prosenttia.**
+ OPETUS: Kyberturvallisuus on liiketoimintariski. ”Oman tontin” suojaus ei riitä. Vaadi myös palveluntarjoajia noudattamaan tietoturvavaatimuksianne.

4. HUONO KYBERHYGIENIA

+ 83 prosenttia tietoturvatapahtumista johtuu huonosta kyberhygieniasta eli perusasioiden puutteellisesta hallinnasta.
+ OPETUS: Tietoturvakulttuuri vaatii pitkäjänteistä työtä. Kouluta henkilöstöä, harjoittele ja testaa. Määritä tietoturvalle tavoitteidesi mukaiset resurssit ja hanki tueksi kumppani, joka auttaa teknologiavalinnoissa sekä konsultoi ja kouluttaa.

5. SOKEA USKO TEKNOLOGIAAN

+ Teknologian kehittyessä vauhdilla voi iskeä vauhtisokeus ja usko teknologian kaikkivoipaisuuteen. Todellisuudessa kyberturvallisuusriskejä ei voi hallita pelkällä teknologialla.
+ OPETUS: Turvallisuusriskit edellyttävät älykästä teknologiaa, relevanttia ja ajantasaista uhkatietoa sekä inhimillistä asiantuntemusta.

6. HEIKKO REAGOINTIVALMIUS

+ Varotoimista huolimatta noin 10 prosenttia hyökkäyksistä onnistuu. Jos kyberhyökkäys osuu – kenties keskellä yötä – miten nopeasti saat tilanteen hallintaan?
+ OPETUS: Varmista toimintakyky poikkeustilanteissa. Kouluta, harjoittele ja testaa. Tee varautumissuunnitelma ja perusta tietoturvapoikkeamien hallintatiimi.

7. JATKUVAN KEHITTÄMISEN UNOHTAMINEN

+ Kyberturvallisuus ei ole yksittäinen hanke.
+ OPETUS: Tunnista kehitystarpeet, luo tiekartta ja suunnitelma jatkuvaan seurantaan, mittaamiseen ja kehittämiseen. Seuraa tietoturvan toteutumista myös arvoketjussa.

* Kyberturvallisuuden tila suomalaisissa organisaatioissa 2018 tutkimus, CGI Suomi
** The Cyber-Value Connection survey, CGI UK

Puolustajien kannattaa jakaa tietoa ja tehdä yhteistyötä.

TEKSTI SAMI LAAKSO KUVAT HACKERONE JA SHUTTERSTOCK

Kyberriski ei ole koskaan nolla prosenttia.
Oleellista on keskittyä yrityksissä sen minimointiin.

KYBERTURVAA

VALKOHATUISTA JA TOSIASIOIDEN TUNNUSTAMISESTA

NotPetya-kyberhyökkäys aiheutti Maerskille 240 miljoonan euron tappiot, Facebook-palvelun tietovuoto vaarantanut yli 50 miljoonaa käyttäjätunnusta, ulkoministeriön tietoverkossa vakoilua, verkkopankissa häiriöitä, nettikäyttäjät saaneet kiristysviestejä…

Kyberrikoksista kertovista uutisista on runsaudenpulaa, vaikka merkittävä osa tapauksista jää julkisuudelta piiloon. **Mårten Mickos** on vakuuttunut, että lisää uutisia on luvassa. Pahinta ei ole vielä nähty.

”Kyberhyökkäykset pahenevat vielä siitä mitä ne ovat tänä päivänä. Mutta ratkaisut ja vastatoimet ovat myös lähteneet liikkeelle”, hän sanoo.

Mårten Mickosilla on perspektiiviä näkemyksiinsä. Tällä hetkellä hän toimii Piilaaksossa HackerOne -yhtiön toimitusjohtajana. Aiemmasta työhistoriasta löytyy näyttävä polku työtehtäviä ja yrityksiä, muun muassa MySQL, Sun Microsystems, Eucalyptus Systems sekä Hewlett-Packard.

KUKA?
Mårten Mickos

TYÖ
HackerOne-yhtiön toimitusjohtaja

URA
Johtotehtävissä useissa teknologiayrityksissä, muun muassa MySQL, Sun Microsystems, Eucalyptus Systems, Hewlett-Packard

KOULUTUS
Diplomi-insinööri

Konkreettisia toimia tarvitaan nyt

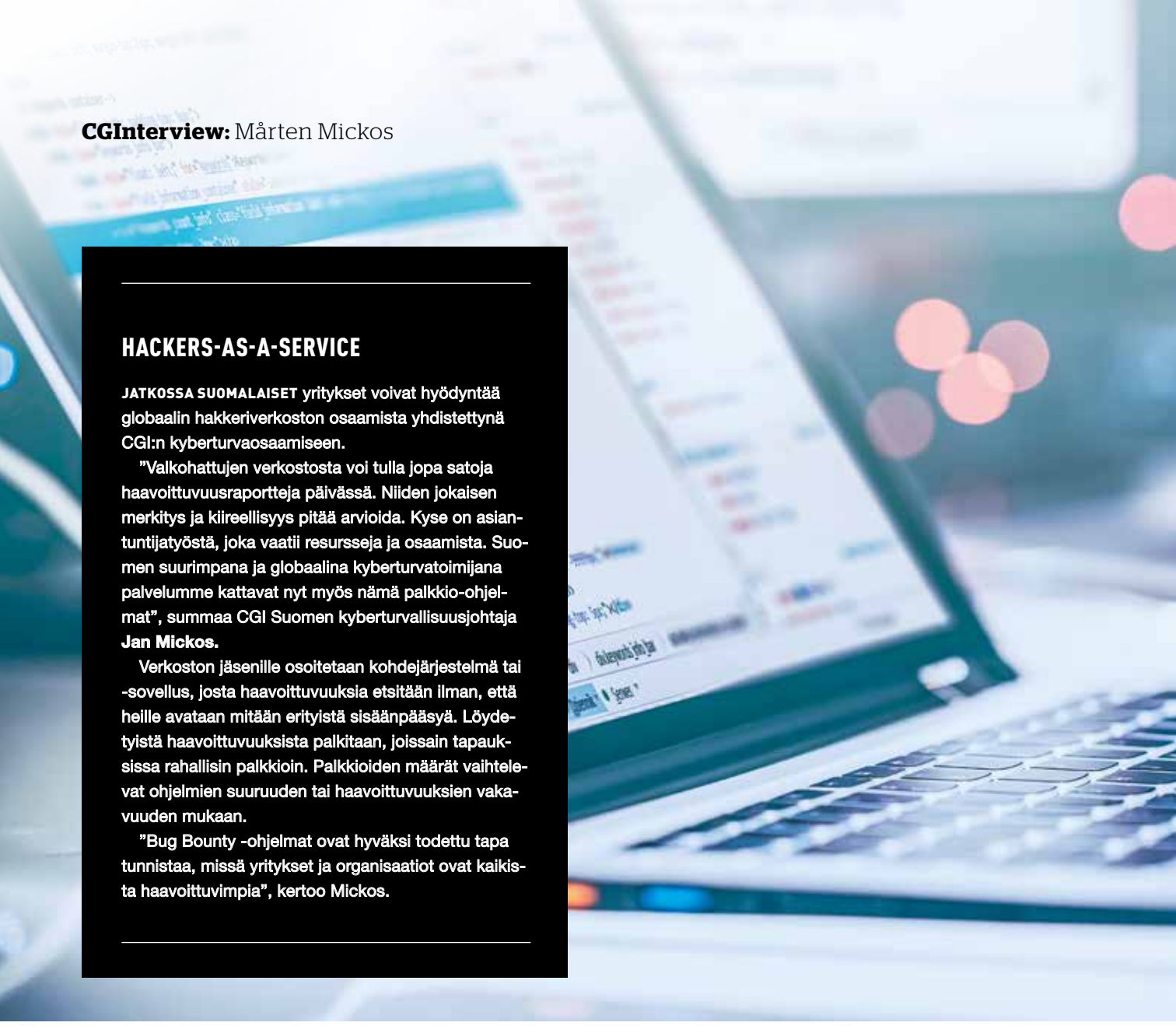
Kuten julkitulleet tapaukset karusti osoittavat, kyberuhkien kirjo on pelottavan laaja. Huonoja skenaarioita rajoittaa oikeastaan vain mielikuvitus.

”Kyberuhkia on paljon ja on mahdotonta arvioida mikä niistä olisi pahin. On hirvittävää, jos luottokortti- tai pankkitietoja varastetaan. Mutta on pahempaa, jos yhteiskunnan tietojärjestelmät menevät nurin. Vieläkin pahempaa on energian saannin tai terveyshuollon pysähtyminen. Ehkä on olemassa vieläkin kammottavampia skenaarioita, joiden seuraukset olisivat hyvin kalliit”, MIckos pohtii.

Hänen mukaansa pahimmassa tapauksessa kyberhyökkäys voi horjuttaa kansalaisten uskoa yhteiskuntaan.

”Sen tuloksena voi olla sekasorto ja yhteiskuntajärjestyksen järkkyminen”, Mickos maalailee.

Synkistä sävyistä huolimatta hän kuitenkin korostaa, että pahimmat vaihtoehdot eivät ole väistämättömiä. Paljon on kiinni kyvystämme puolustautua ja aktiivisuudestamme tilanteen parantamiseksi.



HACKERS-AS-A-SERVICE

JATKOSSA SUOMALAISET yritykset voivat hyödyntää globaalin hakkeriverkoston osaamista yhdistettynä CGI:n kyberturvaosaamiseen.

”Valkohattujen verkostosta voi tulla jopa satoja haavoittuvuusraportteja päivässä. Niiden jokaisen merkitys ja kiireellisyys pitää arvioida. Kyse on asiantuntijatyöstä, joka vaatii resursseja ja osaamista. Suomen suurimpana ja globaalina kyberturvatoimijana palvelumme kattavat nyt myös nämä palkkio-ohjelmat”, summaa CGI Suomen kyberturvallisuusjohtaja **Jan Mickos.**

Verkoston jäsenille osoitetaan kohdejärjestelmä tai -sovellus, josta haavoittuvuuksia etsitään ilman, että heille avataan mitään erityistä sisäänpääsyä. Löydetyistä haavoittuvuuksista palkitaan, joissain tapauksissa rahallisin palkkioin. Palkkioiden määrät vaihtelevat ohjelmien suuruuden tai haavoittuvuuksien vakavuuden mukaan.

”Bug Bounty -ohjelmat ovat hyväksi todettu tapa tunnistaa, missä yritykset ja organisaatiot ovat kaikista haavoittuvimpia”, kertoo Mickos.

”Onneksi yhteiskunta ja sen toimijat ovat jo nähneet nämä riskit ja ryhtyneet vastatoimiin. Edistyneimmät organisaatiot näkevät tietoturvan riskienhallintatoimintana. Monet ymmärtävät, että puolustajien kannattaa keskenään jakaa tietoa ja tehdä yhteistyötä. Tiedetään, että ulkoa tulevat haavoittuvuusraportit ovat arvokkaita. Nyt on enää vain kyse siitä, miten nopeasti – tai hitaasti – laiva kääntyy”, Mickos sanoo.

Laivassa – tai oikeastaan lukemattomissa laivoissa – riittää kääntämistä. Sillä pelkkä organisaatioiden tietoisuus ja toimenpiteet eivät riitä, kun usein kyberturvallisuuden heikon lenkki on ihminen. Varomaton käyttäjä voi avata oven vilpintekijöille.

Mickos korostaakin, että kyberturvallisuuden ongelmat ovat niin laajoja ja merkittäviä, että jokaisen pitää olla niistä tietoinen.

”Varovaisuudella ja kurinalaisella tietokoneen käytöllä voi jokainen pienentää kyberhyökkäyksen riskiä. Ota varmuuskopioita. Älä avaa liitetiedostoja, äläkä klikkaa sähköpostissa olevia linkkejä”, Mickos muistuttaa perusasioista.

Tervetuloa hakkerit

Millä taktiikalla kyberuhkia sitten pitäisi lähteä kampittamaan? Vaikka täydellinen turva uhkia vastaan olisi tietysti paras vaihtoehto, Mickos kehottaa realismiin. Hänen mukaansa puolustustaistelussa ei olla etsimässä teknologiaa, joka

> ***On hyvä tiedostaa, että kyberriski ei ole koskaan nolla prosenttia. Siksi ei keskitytä riskin poistamiseen vaan sen minimointiin.***

pysäyttäisi kaikki hyökkäykset, vaan pyritään minimoimaan riskitekijöitä.

”On hyvä tiedostaa, että kyberriski ei ole koskaan nolla prosenttia. Siksi ei keskitytä riskin poistamiseen vaan sen minimointiin. Tällä tavalla tulokset ovat merkittäviä ja kustannukset siedettäviä.”

Tätä riskien vähentämisen filosofiaa toteuttaa myös Mårten Mickosin johtama HackerOne -yhtiö, jolla on takanaan peräti 250 000:n niin sanotun valkohatun verkosto.

Nämä valkohatut ovat hakkereita, jotka käyttävät osaamistaan vastuullisesti kyberturvallisuuden ja luottamuksen edistämiseen. Usein he saavat palkkion kohdejärjestelmästä tai -sovelluksesta löytämistään haavoittuvuuksista.

Yrityksille ja organisaatioille kyse on ennalta varautumisesta, kun ohjelmistojen ja sovellusten haavoittuvuuksia pyritään tunnistamaan samankaltaisin menetelmin kuin kyberrikolliset käyttävät.

”Kun yritys korjaa löydetyn vian, tietomurron riski pienenee. On huomattu, että tämä menetelmä on tehokkaampi ja edullisempi kuin kaikki muut tavat etsiä ja löytää tietoturvahaavoittuvuuksia”, Mickos listaa etuja.

Valkohattujen verkostosta voi niin kutsuttujen Bug Bounty -ohjelmien yhteydessä tulla jopa satoja haavoittuvuusraportteja päivässä. Niiden jokaisen merkitys ja kiireellisyys pitää arvioida.

”Kyse on asiantuntijatyöstä, joka vaatii resursseja ja osaamista. Harvalla yrityksellä on niitä riittävästi omasta takaa. Mutta työhön voi ja yleensä kannattaakin valjastaa haavoittuvuuksien analysointiin ja hallintaan erikoistunut kumppani”, muistuttaa Mickos.

3x

keinot pienentää kyber-hyökkäyksen riskiä

1. **Minimoi riskitekijät, sillä kaikkia hyökkäyksiä ei voi estää.**
2. **Varaudu ennakkoon ja testauta tietoturvasi taso eettisillä hakkereilla.**
3. **Ihminen on usein heikoin lenkki. Ylläpidä henkilöstön tietotaitoa aktiivisesti.**

HERÄSIKÖ KYSYMYKSIÄ?
Jan Mickos
+358 40 847 8740
jan.mickos@cgi.com

Kaikki eivät ole heränneet

Millainen tilanne sitten on Suomessa? CGI:n selvityksen mukaan viimeisen kahden vuoden aikana joka viides organisaatio on jo ollut kiristyshaittaohjelman ja joka kolmas muun haittaohjelman kohteena. Vain 13 prosenttia organisaatioista kertoo tapahtuneen kyberhyökkäyksen tai -vahingon tulleen julkisuuteen. Jopa 70 prosenttia organisaatioista arvioi todennäköisesti joutuvansa hyökkäyksen kohteeksi seuraavan vuoden aikana.

Mårten Mickosin mielestä tilanne on kaksijakoinen.

”Suomessa on toisaalta maailman parasta tietoturvaosaamista, mutta toisaalta esiintyy myös yleisesti ongelman kieltämistä.”

Mickos kannustaa organisaatioita nostamaan tietoturvan ydinprioriteetikseen. Se tarkoittaa, että turvallisuuslähtöisen sovelluskehittämisen lisäksi järjestelmille pitää järjestää jatkuva tietoturvahoito, ja organisaatioiden on myös varauduttava mahdollisiin hyökkäyksiin ja muihin häiriötilanteisiin.

Hänen mukaansa modernit toimijat myös ymmärtävät avoimuuden tärkeyden. Jakamalla tietoa ja kuuntelemalla ulkopuolisia asiantuntijoita, mahdollisuudet kyberriskien vähentämiseen moninkertaistuvat.

Vaikka kyberuhat voivat tuntua valtavilta, Mickos sanoo, ettei tilanne niiden suhteen sinänsä ole sen kummempi kuin minkään muunkaan merkittävän uhan osalta.

”Tosiasiat pitää nähdä ja myöntää. Korjaaviin toimenpiteisiin pitää ryhtyä. Täydelliseen turvaan ei saa uskoa. Kyse on riskien tietoisesta ja järjestelmällisestä hallinnasta”, hän summaa. ✱

PERUSASIAT *kuntoon*

Valmetin IT-infrapalvelujen tietoturvapäällikön Sakari Koikkalaisen mukaan riskiarvioon pohjautuva kyberturvanhallinta auttaa pitämään tietoturvan perusasiat kustannustehokkaasti kunnossa.

TEKSTI ARI RYTSY KUVAT KRISTIINA KONTONIEMI JA SHUTTERSTOCK

”Ympäristöt, jotka eivät aiemmin olleet tietoteknisen maailman kanssa tekemisissä, ovat sitä nykyään ja tulevaisuudessa. Tämä luo uusia liiketoimintariske- jä muun muassa kyberturvan osalta. Se tarkoittaa, että kyberturvallisuuden vaikutus liiketoimintaan kasvaa koko ajan”, sanoo Valmetin IT-infrapalvelu- jen tietoturvapäällikkö Sakari Koikkalainen.

Uusien haasteiden myötä kyberturvallisuus on ulotettava operatiivista toimintaa pidemmälle. Riittävä kyberturvan taso saavutetaan kun kyberturvan uhat otetaan mukaan liiketoiminnan ohjaukseen ja päätöksentekoon. Kyberturvastrategia ja -hallintamalli sekä tekniset ja hallinnolliset kontrollit kannattaa rakentaa tukemaan liiketoimintaa ja toimimaan osana riskien- hallintaa. Turvakontrollien lisäksi käyttäjien tietoisuus kyberturvasta ja

CGI TARJOAA HUOLETTOMIA HALLINTAPALVELUJA

KYBERTURVALLISUUDEN KONSULTOINTIPALVELUJEN johtaja **Stefan Anderson** tunnistaa Koikkalaisen esille nostamat kyberturvan perusasiat, joista huolehtiminen ei ole läheskään kaikissa yrityksissä arkipäivää. Puutteet ovat usein seurausta siitä, että asioita ei ole vastuutettu riittävän selkeästi tai ne vain yksinkertaisesti unohtuvat. Tilanteeseen joudutaan helposti esimerkiksi silloin, kun organisaatiossa ei ole dedikoitua henkilöä, joka huolehtii kyberturvallisuuden hallinnasta ja hankinnoista, vaan päädytään hankkimaan yksittäisiä palomuureja ja muita tietoturvalaitteita ja -ratkaisuja.

”Monet asiakkaat ovat ratkaisseet ongelman ulkoistamalla perusasioista huolehtimisen meille joko palvelusopimuksina tai osana laajempaa infra- tai sovellusulkoistusta. Näihin sopimuksiin voidaan kattavasti sisällyttää kyberturvallisuuden hallintaan liittyviä kokonaisuuksia”, sanoo Anderson.

HERÄSIKÖ KYSYMYKSIÄ?
Stefan Anderson
+358 40 841 0105
stefan.anderson@cgi.com

Riskiarvioon pohjautuva kyberturvanhallinta tuottaa kustannustehokkaimman tuloksen.

SAKARI KOIKKALAINEN
IT-infrapalvelujen tietoturvapäällikkö, Valmet

-turvauhista on avainasemassa hyvää tietoturvakulttuuria luotaessa.

”Kybersuojaus vaatii aina rahallista panostusta. Tämän vuoksi riskiarvioon pohjautuva kyberturvanhallinta tuottaa kustannustehokkaimman tuloksen”, muistuttaa Koikkalainen.

Pitkään tietoliikenteen ja tietoturvallisuuden hallinnan kehitystehtävissä toiminut Koikkalainen aloitti uransa vuonna 1997 teleoperaattorisektorilla ja siirtyi vuonna 2006 Metson kautta Valmetin tietohallinnon palvelukseen. Koikkalaisen nykyiset työtehtävät kohdistuvat Valmetin IT-tietoturvan kehittämiseen.

Päivitykset ja paikat ajallaan

Kyberturvanhallinnan kannalta on aina tärkeää ymmärtää, mitä suojataan ja miltä. Valitut ratkaisut eivät itsessään saa luoda kyberuhkia, joten ne on toteutettava turvallisesti ja pidettävä ajan tasalla.

”Kyberturvallisuudessa pitää paneutua identiteettien ja datan suojaamiseen. Ennaltaehkäisevinä kontrolleina haavoittuvuuksien hallinta on tärkeää sekä teknisessä että hallinnollisessa mielessä”, sanoo Koikkalainen.

Kun riskiarviot on tehty ja strategiat laadittu, on huolehdittava, että kyberturvallisuuspolitiikkaa toteutetaan kaikilla alueilla valitulla tasolla – keittiön ovea ei jätetä huolimattomuuden takia auki kyberrotille. Jos jossain on reikä, on vain ajan kysymys, milloin hiiret ja rotat löytävät siitä tiensä sisään. Kun esimerkiksi ohjelmistojen ja sovellusten kehittäjä julkaisee päivityksiä ja paikkauksia, tulee niiden asentamisen tapahtua ilman turhia viiveitä.

Oman mausteensa kyberturvan hallintaan tuovat jatkuvasti yleistyvät pilvipalvelut. Niiden hyödyntämisessä on noudatettava samaa tietoturvastrategiaa ja -politiikkaa yrityksen sisäisten järjestelmien ja sovellusten kanssa. Siksi ennen pilvipalveluiden käyttöönottoa on syytä käyttää riittävästi aikaa ja osaamista suunnitteluun sekä riskiarviointiin. Pilvipalvelujen hyödyntämistä on mietittävä myös liiketoiminnan jatkuvuuden ja riskienhallinnan, ei pelkästään kustannussäästön tai ketteryysominaisuuksien kannalta.

Parempaa hallintaa ja havainnointia

Koska resurssien rajallisuus on usein arkea myös IT-hallinnossa, resurssien järkevä allokointi on

4
vinkkiä kyberturvassa onnistumiseen

1. **Huomioi kyberuhat liiketoiminnan ohjauksessa ja päätöksenteossa.**
2. **Lisää käyttäjien tietoisuutta kyberturvasta.**
3. **Hallitse haavoittuvuuksia sekä teknisesti että hallinnollisesti.**
4. **Tee IT-ulkoistukset suunnitelmallisesti ja liiketoimintalähtöisesti.**

keskeinen osa kustannustehokasta kyberturvaa. Siksi hallintapalvelujen ulkoistus ammattilaisille on Koikkalaisen mukaan kannatettava asia, kun se on tehty liiketoimintalähtöisesti ja suunniteltu riittävän tarkasti. Näin yritys voi kohdistaa omat IT-ammattilaiset, joita on usein rajatusti, suunnittelemaan ratkaisuja liiketoiminnalle ja varmistamaan laadukkaan palvelun tuoman lisäarvon yritykselleen.

”Tänä päivänä yksi tärkeimpiä kyberturvapalveluja ovat mielestäni SOC-palvelut. Niiden avulla varmistetaan ajantasainen näkyvyys kyberturvan tilannekuvaan. Sitä kautta saadaan myös arvokasta tietoa kyberturvan tehokkaaseen kehitykseen ja ohjaukseen”, sanoo Koikkalainen.

Ulkoistamisen osalta suomalaiset yritykset ovat menneet merkittävästi eteenpäin. Palveluiden ostamiseen on opittu ja hallinta- sekä muiden palveluiden hankkiminen oman talon ulkopuolelta on arkipäiväistynyt.

”Tulevaisuudessa suurimmat uudistukset kyberturvapalveluissa tulevat näkymään poikkeamien havainnoinnissa big dataan ja keinoälyyn pohjautuvien kyberturvapalvelujen avulla”, arvioi Koikkalainen. *

ENERGIAN *ja elämän turvaaja*

Jos veden, sähkön tai lämmön jakelu katkeaa, se näkyy välittömästi ja koskee lähes kaikkia.

TEKSTI VESA KAARTINEN JA ESA LUOTO KUVAT SHUTTERSTOCK JA KRISTIINA KONTONIEMI

Onnistunut isku energiahuoltoon lamauttaisi nopeasti koko yhteiskunnan. Ja tekisi elämästä hyvin kylmää, pimeää, likaista ja vaikeaa. Kirjaimellisesti.

Ei siis ihme, että kyber- ja tietoturvariskit ovat nousseet avainpuheenaiheiksi myös energia-alalla.

”Yhä olennaisempaa on tietoturvauhkien havaitseminen mahdollisimman aikaisessa vaiheessa. Se mahdollistaa nopean reagoinnin ja minimoi vahingot”, korostaa tietohallintopäällikkö **Marko Metiäinen** Jyväskylän Energiasta.

Yritykset kohtaavat keskimäärin useita kyberhyökkäyksiä kuukaudessa. Pääosa hyökkäyksistä jää havaitsematta tai niistä luetaan vasta otsikoissa. Yleensä kyberhyökkäys huomataan vasta kuukausien, jopa vuosien kuluttua sen alkamisesta.

Perushaasteet ovat Marko Metiäisen mukaan energiayhtiöillä samat kuin minkä tahansa muun alan yrityksillä, mutta vastuualue vielä paljon laajempi ja kokonaisvaltaisempi.

> ***Tehtäväkenttämme edellyttää jatkuvaa hälytysvalmiutta.***
>
> **MARKO METIÄINEN**
> tietohallintopäällikkö,
> Jyväskylän energia

”Lähtökohtana on sekä alueen energiatuotannon että oman liiketoimintamme häiriöttömyyden ja jatkuvuuden varmistaminen. Loppupelissä kyse on kuitenkin toimialueemme jokaisen asukkaan ja organisaation arjen turvaamisesta. Tehtäväkenttämme edellyttää jatkuvaa hälytysvalmiutta”, Metiäinen summaa.

Digitalisaatio asiantuntijuuden renessanssina

Digitalisaation ja IoT:n edetessä keskustelujen painopiste on siirtynyt fyysisistä laitteista koko infrastruktuuriin tuotanto- ja jakelu- ja automaatiojärjestelmineen. Kyberriskejä lisää se, että pirstoutuvissa toimintaketjuissa vastuu riskeistä helposti hämärtyy.

”Perinteiset virustorjunnat ja verkkopalomuurit eivät enää riitä pitämään tietojärjestelmiä, verkkoja ja niissä olevia tietoja yritysten hallussa. Kun tietoturvauhkien ja -riskien määrä ja kirjo kasvaa, tarvitaan koko ajan uusia työkaluja niiden torjumiseen sekä kokonaiskuvaa ymmärtäviä asiantuntijoita”, analysoi Metiäinen.

Aiempien kertaluonteisten auditien sijaan pystymme nyt ennakoimaan tieto- ja kyberturvatilannetta aiempaa kokonaisvaltaisemmin.

Jyväskylän Energian ratkaisuna on tietoturvan valvonta- ja hallintapalvelujen ulkoistaminen CGI:n kyberturvallisuuskeskuksen asiantuntijoille. Sopimus avaa Jyväskylän Energialle myös pääsyn CGI:n globaaliin uhkatieto- ja palveluverkostoon.

Kun normaalista poikkeavaa toimintaa havaitaan Jyväskylän Energian verkoissa tai järjestelmissä, CGI:n Cyber Security Operations Centerin (SOC) asiantuntijat analysoivat hälytyksen aiheuttaneet löydökset ja ehdottavat jatkotoimia niiden kriittisyysasteen perusteella.

”Palvelu tuo reaaliaikaisen tilannekuvan verkkoon ja tietojärjestelmiimme. Aiempien kertaluonteisten auditien sijaan pystymme nyt ennakoimaan tieto- ja kyberturvatilannetta aiempaa kokonaisvaltaisemmin. Samalla parannamme häiriötilanteisiin liittyviä valmiuksiamme”, Metiäinen kertoo.

Valtioneuvoston vuonna 2017 valmistuneen kyberturvaselvityksen mukaan yhteiskunnan kaikkia elintärkeitä toimintoja ja huoltovarmuuskriittisiä yrityksiä ei ole tällä hetkellä suojattu riittävällä tavalla erilaisia kyberuhkia vastaan. Myös häiriötilanteiden sietokyvyssä on puutteita.

Metiäinen vertaa SOC-palvelun tuomaa tukea vakuutusturvaan. ”Ensisijainen tavoitteemme on Jyväskylän seudun toiminta- ja huoltovarmuus. Emme voi ottaa sitä riskiä, että luottaisimme vain teknologiaan.” ✱

LISÄTIETOA:
Mika Heino
040 777 0370
mika.heino@cgi.com
SOC-palvelut, CGI

CGI:N CYBER SECURITY CENTER TARJOAA KYBERTURVALLISUUDEN JAETTUJA PALVELUITA

CGI:N CYBER SECURITY CENTER tarjoaa asiakkailleen laajasti kyberturvallisuuden palveluita aina kyberturvallisuuden riskien kartoittamisesta jatkuviin SOC (Security Operations Center) -palveluihin asti. SOC-palvelu tarkoittaa asiakasympäristössä mukaan lukien pilvipalveluissa tapahtuvien kyberturvaherätteiden jatkuvaa valvontaa ja niihin reagoimista tarkoituksena varmistaa mahdollisimman häiriötön ja turvallinen toiminta. Asiakas saa käytännössä, yhden henkilön kustannuksella, kymmenen kyberosaajan tietotaidon. Tämä perustuu resurssien ja prosessien tehokkaaseen jakamiseen asiakkaiden kesken.

”Nimeämme asiakkaalle nimikkoanalystin, joka perehtyy asiakkaan henkilöihin, prosesseihin ja tekniseen ympäristöön ja pystyy sitä kautta tuottamaan aitoa lisäarvoa asiakkaalle”, sanoo CGI:n Cyber Security Centerin johtaja **Mika Heino.**

HERÄSIKÖ KYSYMYKSIÄ?
Julia Heiskanen
+358 40 841 0105
julia.heiskanen@cgi.com

MOBIILI-AJOKORTTIA KELPAA SUOMEN NÄYTTÄÄ

Suomessa pian käyttöön tuleva ensimmäinen täysin digitaalinen mobiiliajokortti parantaa ajokortin käyttömahdollisuuksia merkittävästi, sanoo Trafin pääjohtaja. Mielenkiinto on jo herännyt ulkomaita myöten.

TEKSTI JA KUVAT ANTTI KIRVES

”Mobiiliajokortti on digitalisaation hyötyjen ulosmittaamista. Ihmisillä on aina kännykkä mukana eikä lompakkoa tai erillistä luottokorttia kohta enää tarvita, vaan kännykässä todella on kaikki tarvittava. Mobiiliajokortti on tässä kehityksessä yksi keskeinen elementti. Arjesta tulee entistäkin helpompaa ja parempaa”, sanoo liikenteen turvallisuusviraston Trafin pääjohtaja **Mia Nykopp.**

Mobiiliajokortti on Suomessa kehitetty iOS- tai Android-puhelimeen ladattava sovellus, jolla voidaan osoittaa käyttäjän henkilötiedot ja ajo-oikeus helposti ja luotettavasti. Mobiiliajokortti on osa Trafin Autoilija-sovellusta.

> ***Kännykässä todella on kaikki tarvittava.***
>
> **MIA NYKOPP**
> pääjohtaja,
> liikenteen
> turvallisuusvirasto
> Trafi

Nykoppin mielestä mobiiliajokortti on erittäin merkittävä hanke niin Suomen sisällä kuin kansainvälisestikin – etenkin kun on kyse viranomaispalvelusta, joka viedään oikeasti ja konkreettisesti mobiiliin käyttökelpoisena appina eikä pelkkänä selainversiona.

Hän ei halua sanoa Suomen versiota maailman ensimmäiseksi mobiiliajokortiksi, koska muissakin maissa erilaisia hankkeita vastaavista viranomaispalveluista on joko osittain tarjolla tai kehitteillä. Mutta Suomi on aivan globaalia kärkeä. Muualla tullaan selvästi perässä.

”Suomi on ensimmäinen Euroopan maa, jossa otetaan käyttöön täysin digitaalinen ajokortti. Kyllä tässä tehdään uraa uurtavaa työtä. Suomalaiset ovat muutenkin ottaneet sähköiset viranomaispalvelut hyvin vastaan. Mobiiliajokortti on luontainen

Suomi ottaa ensimmäisenä Euroopassa käyttöön täysin digitaalisen ajokortin. Hanke on herättänyt kiinnostusta kansainvälisestikin, kertovat Trafin Mia Nykopp ja Simo Karppinen.

Mobiiliajokorttia osaa käyttää jokainen, jolla on älypuhelin.

SIMO KARPPINEN
Ajo-oikeudet ja kortit -yksikön päällikkö, Trafi

jatkumo esimerkiksi sähköiselle rekisteröinnille. Samalla se on osoitus julkishallinnon ja poliittisten päättäjienkin ketteryydestä. On lähdetty kokeilemaan, testattu aidosti asiakkaiden kanssa, haettu palautetta ja kehitetty tuotetta aina lainsäädäntöön asti", Nykopp sanoo.

Parempi kuin vanha

Mobiilikortti on ilmainen ja aina matkassa, sen tiedot ovat aina ajan tasalla ja kuva tuore, toisin kuin 20 vuotta vanhassa fyysisessä kortissa. Ruudun kokoinen tuore kuva helpottaa henkilön tunnistamista ja qr-koodilla tiedot saadaan Trafin rekistereistä ajantasaisesti.

"Mobiiliajokorttia osaa käyttää jokainen, jolla on älypuhelin. Tietojen tarkastaminen on yksiselitteisempää, kun tarkastajan ei tarvitse lähteä kortin turvatekijöitä arvioimaan, vaan tiedot saa omalle ruudulle ja tietää että niihin voi luottaa", sanoo Trafin Ajo-oikeudet ja kortit -yksikön päällikkö **Simo Karppinen.**

Autoilija-sovelluksen ensimmäiseen julkaisuun kuuluvat Karppisen mukaan mobiiliajokortti, omat ajoneuvotiedot (ajoneuvojen perustiedot, joiden omistaja tai haltija on) sekä viestipalvelu, joka muistuttaa ajokortin uudistamistarpeesta.

Myöhemmin sovellus täydentyy muilla palveluilla, kuten ajoneuvotietopalvelulla, jossa rekisteritunnuksella voi maksuttomasti hakea ja katsoa Suomessa rekisteröityjen ajoneuvojen teknisiä tietoja.

6x
Mobiiliajokortin hyödyt

1. **Aina mukana.**
2. **Aina ajantasaiset tiedot.**
3. **Luotettava ja turvallinen.**
4. **Helppo käyttää.**
5. **Käyttäjälle ilmainen.**
6. **Liitettävissä uusiin sähköisiin palveluihin.**

Karppinen korostaa, että mobiiliajokortti on vaihtoehto ja lisäarvopalvelu. Perinteinen fyysinen ajokortti ei katoa sen rinnalta vielä aikoihin, mutta lakimuutoksen jälkeen fyysisen kortin kantaminen mukana ei ole enää välttämätöntä.

Trafilla on edustajansa työryhmässä, joka suunnittelee kansainvälistä ISO-standardia sähköisille ajokorteille. Standardin arvioidaan valmistuvan 2020, mutta se ei sinänsä riitä vielä esimerkiksi EU-käyttöön, vaan ensin EU:n ajokorttidirektiiviin täytyy tehdä muutoksia.

TURVALLINEN KORTTI

TIETOTURVA ON mobiiliajokortin kaltaisessa henkilötietoihin liittyvässä viranomaisprojektissa kriittinen asia.

”Mobiiliajokortin tietoturva on huomioitu kokonaisvaltaisesti koko ohjelmistokehitysprosessin ajan. Järjestelmään tehty useita auditointeja, joista saatujen havaintojen perusteella turvaominaisuuksia on tarvittaessa tiukennettu”, sanoo CGI:n mobiiliratkaisuista ja Trafin mobiiliajokortin kehityksestä CGI:llä vastaava johtaja **Tero Laitila.**

Sekä sovelluksessa että tietoliikenteessä käytetään useita eri salaamis- ja suojausmenetelmiä.

”Korttisovelluksessa on useita turvaelementtejä, kuten liikeantureihin perustuva digitaalinen hologrammi, joka liikkuu, kun puhelinta liikuttaa. Animoidun taustakuvan pinta reagoi ikään kuin särkemällä digitaalisen mobiiliajokortin pinnan, kun sitä koskettaa. Nämä ominaisuudet helpottavat viranomaista ja muita eri toimijoita tunnistamaan virallisen digitaalisen mobiiliajokortin esimerkiksi pelkästä kuvakaappauksesta.”

”Ulkomailla autoillessa fyysinen kortti vaaditaan vielä pitkään. Ja Suomessakin voi näin alkuvaiheessa tulla vielä eteen paikkoja, joissa ei ole kuultu mobiilikortista”, Karppinen muistuttaa.

”Mutta testikäyttäjiä on ollut kolmisen tuhatta ja käyttäjäkokemukset ovat olleet hyvin positiivisia. En usko, että pitkään menee ennen kuin mobiiliajokortti on ihan arkipäivää.” *


esc
num
Hacker
shift

LUPA hakkeroida

LähiTapiola hyödyntää valkohattuisia hakkereita tietoturvahaavoittuvuuksien etsinnässä. Tietoturvajohtaja Leo Niemelä sanoo hakkeriyhteistyön hyödyttävän kaikkia osapuolia.

TEKSTI ARI RYTSY KUVAT SHUTTERSTOCK JA SAMPO KORHONEN

LähiTapiolan tietoturvahaavoittuvuuksien etsimiseen kannustava avoin palkinto- eli Bug Bounty -ohjelma sai alkunsa halusta tunnistaa haavoittuvuudet aiempaa tehokkaammin ja ennakoivammin. Vaikka LähiTapiolan ICT-järjestelmien ja sähköisten palveluiden tietoturvallisuutta varmistetaan monipuolisesti, ei perinteisiä keinoja pidetty riittävinä. Niemelä korostaa, että huolellisinkaan testaus ei paljasta jokaista tietoturvahaavoittuvuutta. Mitä vaativammasta koodista on kyse, sitä todennäköisemmin osa virheistä löydetään vasta tuotannossa.

”Digitaalisen murroksen pyörteissä kaikki koodaajat tekevät joskus virheitä. Bug Bounty -ohjelman avulla olemme saaneet lisää silmäpareja niiden etsintään. Tarkoituksena ei ole syyllistää koodaajia, vaan kehittää palveluidemme tietoturvaa”, **Leo Niemelä** toteaa.

Ensimmäisenä pohjoismaisena finanssitalona Bug Bounty -ohjelman aloittanut LähiTapiola ei rynnännyt hakkeriyhteistyöhön suin päin. Puoli vuotta kestäneen suunnitteluvaiheen aikana yrityksessä tehtiin perinpohjaisia riskianalyysejä ja uhkamallinnusta, sillä tarkkaan säännellyssä liiketoiminnassa henkilötietojen luottamuksellisuuteen ja tietosuojaan on kiinnitettävä erityistä huomiota.

Uhkakuvat eivät ole realisoituneet vaan päinvastoin. Kokemukset Bug Bounty -ohjelmasta ovat olleet niin hyviä, että sitä on laajennettu ja yksittäinen palkintosumma on nostettu 20 000 eurosta 50 000 euroon. Käytännössä palkintosumma on sitä suurempi, mitä merkittävämpi haavoittuvuuden liiketoimintavaikutus on. EU:n uuden tietosuoja-asetuksen piiriin liittyvistä löydöistä maksetaan erillinen GDPR-bonus.

”Tähän mennessä suurin maksamamme palkinto on ollut 18 000 euroa. Kyseisestä haavoittuvuudesta ja sen korjaamisesta lähetettiin ilmoitus Viestintäviraston Kyberturvallisuuskeskukseen. Sieltä tieto levisi eteenpäin myös muille yrityksille”, Niemelä kertoo.

> ***Kaikkien yhteisenä tavoitteena on tuottaa mahdollisimman hyvälaatuista koodia.***
>
> **LEO NIEMELÄ**
> Tietoturvajohtaja,
> LähiTapiola

HERÄSIKÖ KYSYMYKSIÄ?
Jan Mickos
+358 40 847 8740
jan.mickos@cgi.com

Hakkerit saavat Bug Bounty -ohjelman kautta itselleen rahaa sekä positiivista tunnustusta taidoistaan. Se on parempi houkutin kuin tehdä jotain laitonta ja vilkuilla jatkuvasti olkansa yli viranomaisia peläten.

Bug Bounty täydentää perinteistä tietoturvaa

Bug Bountyn kaltaiset haavoittuvuusohjelmat ovat yksi keino yritysten verkkopalveluiden tietoturvan parantamiseksi, koska ne joutuvat ei-toivotun hakkeroinnin kohteeksi joka tapauksessa. Pelko siitä, että palveluita luvallisesti hakkeroiva henkilö muuttaisi mielensä ja myisi haavoittuvuudet pimeille markkinoille, ei ole osoittautunut aiheelliseksi.

”Hakkerit saavat Bug Bounty -ohjelman kautta itselleen rahaa sekä positiivista tunnustusta taidoistaan. Se on parempi houkutin kuin tehdä jotain laitonta ja vilkuilla jatkuvasti olkansa yli viranomaisia peläten”, vakuuttaa Niemelä.

Bug Bounty -ohjelman positiivisten kokemusten siivittämänä LähiTapiola on osallistanut hakkereita yhä enemmän esimerkiksi oman Hack Dayn kautta, missä tutkitaan tiimeittäin valitun kohdejärjestelmän turvallisuutta.

Bug Bounty ei korvaa perinteisiä tietoturvapalveluja, vaan täydentää niitä. Sen käyttö on kuitenkin näkynyt LähiTapiolassa esimerkiksi säästöinä tietoturva-auditointien vaatimissa investoinneissa. Ohjelma paikkaa myös tietoturvan katvealueita eri kumppanien kanssa toimittaessa.

”LähiTapiola kehittää jatkuvasti uusia palveluja ja sovelluksia kumppaneidensa kanssa. Kaikessa tekemisessä asiakkaiden tietoturva ja tiedon luottamuksellisuus ovat meille erittäin tärkeitä asioita”, korostaa Niemelä.

LähiTapiolan Bug Bounty -ohjelman saama julkisuus perustuu yrityksen päätökseen toimia asiassa mahdollisimman avoimesti. Vastaavanlaisia hankkeita toteutetaan tälläkin hetkellä suomalaisissa yrityksissä kaikessa hiljaisuudessa, jolloin niistä tietävät vain palveluita testaavat hakkerit. Toteutustavasta riippumatta Niemelä on vakuuttunut Bug Bounty -ohjelman hyödyistä, jotka näkyvät palveluiden parantuneen tietoturvan lisäksi yrityksen turvallisuuskulttuurin kehityksenä ja sisäisen turvallisuuden paranemisena.

”Kaikkien yhteisenä tavoitteena on tuottaa mahdollisimman hyvälaatuista koodia. Siksi löydettyjä haavoittuvuuksia käytetään apuna koodaajien ja tietoturvan testaajien osaamisen kehittämisessä”, hän sanoo.

4x
hakkerit hyötykäyttöön

1. **Aloita suunnittelusta, riskianalyyseistä ja uhkamallinnuksesta.**
2. **Huomioi erityisesti henkilötietojen luottamuksellisuus ja tietosuoja.**
3. **Hyödynnä palkkioita ja hakkereiden osallistamista.**
4. **Käytä löydöksiä koodaajien ja testaajien osaamisen kehittämiseen.**

ICT-kumppanit mukana ohjelmassa

Bug Bounty -ohjelman pyörittämisestä LähiTapiolassa vastaa sitä varten nimetty tiimi, johon kuuluu yrityksen omien tietoturva-asiantuntijoiden lisäksi ICT-kumppaneiden edustajia. Kumppanien mukanaolo on tuonut hankkeeseen laajempaa käsitystä tietoturvasta ja mahdollistanut nopean reagoinnin löydettyihin korjaustarpeisiin.

Pienen alkutunnustelun jälkeen ohjelma on kulkenut tehokkaasti omia raiteitaan. Nykyisin LähiTapiolan ICT-sopimuksissa on maininta siitä, että sen palvelujen ulkoiset rajapinnat kuuluvat Bug Bounty -ohjelman piiriin.

Menestyksekkään haavoittuvuusohjelman kytkeminen osaksi päivittäistä tekemisestä ei ole luonut tarvetta lisärekrytoinneille, sillä helppoutta, nopeutta ja kustannustehokkuutta pystytään lisäämään ulkopuolisten kumppaneiden avulla, jotka tuntevat yrityksessä käytettävät sovellukset.

”Bug Bountyn kaltaisten ohjelmien käyttö tulee pakostakin lisääntymään erityisesti asiakasrajapinnan ratkaisuissa. Siellä hakkerit ovat yksi työkalu lisää tietoturvallisuuden puolesta käytävässä taistelussa”, kiteyttää Niemelä. *

Bug Bounty -ohjelman käyttö on näkynyt säästöinä tietoturva-auditointien vaatimissa investoinneissa, sanoo LähiTapiolan tietoturva-johtaja Leo Niemelä.

TYLSÄ ON YHTÄ KUIN TURVALLINEN

KYBERTURVALLISUUSKESKUKSEN eli SOCin (Security Operations Center) toiminnan ydintä ovat tylsät rutiinit, joiden tarkoitus on pitää huolta asiakkaiden turvallisuushygieniasta.

Kyberturvapoikkeamien havaintoaika ilman SOCin toteuttamia palveluita on tyypillisesti jopa kuukausia – ei minuutteja. Suurin osa tapauksista johtuu kehnosta kyberturvallisuushygieniasta: asiattomat pääsevät käsiksi vakiosalasanoilla suojattuihin järjestelmiin, käyttäjän tekemän virheellisen klikkauksen vuoksi haittaohjelmat pääsevät työasemaan tai pilvipalveluiden kirjautumiseen tarkoitetut käyttäjätunnukset ja salasanat vuotavat väärennettyihin kirjautumissivustoihin.

SOC auttaa organisaatiotasi varmistamaan kyberturvallisuutesi seuraamalla haittaohjelmaskannereitanne, tunkeutumisen havaitsemis- ja estojärjestelmiänne ja muita turvallisuusteknologioistanne saatuja hälytyksiä kyberongelmien varalta. ✱ **MIKA HEINO** www.cgi.fi/blogi/tylsa-on-yhta-kuin-turvallinen-niin-tosielamassa-kuin-kyberturvallisuudessakin

RATKAISEEKO TEKOÄLY KYBERTURVALLISUUDEN HAASTEET?

TEKOÄLYN, KONEOPPIMISEN ja muiden kehittyvien tekniikoiden ympärillä käy kova kuhina. Voisikin kuvitella, että teknologiaratkaisuilla ratkaistaan kaikki kyberturvallisuuden haasteet. Todellisuus on kuitenkin se, ettei teknologia yksin riitä takaamaan kyberturvallisuutta. Nykyisiin ja tuleviin kyberuhkiin vastaaminen edellyttää saumatonta älykkään teknologian ja kyberturvallisuusammattilaisten yhdistelmää, eli tosiälyä. Se yhdistää kehittyvien teknologioiden mahdollistaman potentiaalin, testatut ja hyväksi havaitut prosessit, relevantin uhkatilannetiedon sekä osaavat ja sitoutuneet ihmiset, joiden päämääränä on turvata digitaalinen liiketoimintasi. ✱ **JAN MICKOS** www.cgi.fi/blogi/ratkaiseeko-tekoaly-kyberturvallisuuden-haasteet

Q&A

Tietoturva on suojaamisen arvoinen

Kyberriskit voivat realisoituessaan vaarantaa yrityksen koko olemassaolon. Pk-yrityksille suunnattu kybervakuutus antaa turvaa kybervahingon sattuessa.

1 MILLAISIA OVAT YRITYSTEN TYYPILLISIMMÄT HAASTEET AIHEESEEN LIITTYEN?

Erityisesti pienemmissä yrityksissä on haasteita tunnistaa omaan liiketoimintaan ja toimintaverkostoon liittyviä kyberriskejä. Saattaa olla myös vaikea ymmärtää, miten erilaiset digitaaliset ratkaisut ovat kytkeytyneet yrityksen liiketoimintaan ja kuinka ne vaikuttavat yrityksen tulokseen. Haasteellista voi lisäksi olla uusi tietosuoja-asetus vaatimuksineen ja käytäntöön ottoineen.

2 MITEN TIETOTURVARISKEIHIN KANNATTAISI VARAUTUA?

Olisi syytä laatia tietoturvan ja tietosuojan merkityksen yrityksen liiketoiminnalle kuvaava tietoturvapolitiikka tai -ohjeistus ja koulutettava koko henkilöstö sen noudattamiseen. Tietoturvan osalta vähimmäisvaatimuksena on yrityksen ICT-laitteiden ja tietoverkkojen suojaaminen ajan tasalla olevalla virustorjunnalla, palomuurilla sekä varmuuskopioinnilla.

3 MIKSI KYBERVAKUUTUS KANNATTAISI HANKKIA?

Kyberhyökkäys voi pahimmillaan keskeyttää yrityksen liiketoiminnan pitkäksi ajaksi ja aiheuttaa merkittävät taloudelliset tappiot yritykselle, yhteistyökumppaneille sekä asiakkaille. Perinteiset vakuutusturvat eivät kata tietoturvaloukkauksista, tietojen menettämisestä tai muista vastaavista kyberriskeistä aiheutuneita kustannuksia. Vaarassa on usein toisen osapuolen omistamaa tietoa, kuten asiakastiedot. Ne voidaan menettää tai ne voivat joutua vääriin käsiin.

Kybervakuutuksella yritys varautuu osittain kyberhyökkäyksen ja tietoturvaloukkauksen jälkeisiin vastuisiin ja velvoitteisiin.

4 MITÄ KYBERVAKUUTUS SISÄLTÄÄ?

Se kattaa sovittuun vakuutusmäärään asti välittömät kriisinhallintakustannukset, vakuutuksenottajalle aiheutuneen keskeytysvahingon sekä toiselle osapuolelle tietoturvaloukkauksen seurauksena aiheutuneen taloudellisen vahingon. Kriisinhallintakustannukset sisältävät asiantuntijapalveluista aiheutuneet kulut. Siitä korvataan myös tiedostojen ja ohjelmistojen palautuskustannukset sekä kustannukset, jotka aiheutuvat tietosuoja-asetuksen tiedottamisvelvollisuudesta.

Kybervakuutus ei korvaa henkilövahinkoa, kärsimystä, esinevahinkoa tai sakkoja. Vakuutus ei kata myöskään puutteellisesta palomuurista tai virustorjuntaohjelmistosta tai päivittäisen varmuuskopioinnin laiminlyönnistä aiheutuneita vahinkoja.

Sami Kehusmaa
tiimipäällikkö, OP

RATKAISU19

24.1.2019, Finlandia-talo

ratkaisu.cgi.fi

#Ratkaisu19

+ INNOVATE

RUN
TRANSFORM
GROW

Ratkaisu19-seminaarin teemana on **Design Your Future Business.** Teeman mukaisesti puheenvuoroissa ja työpajoissa pureudutaan seuraavan kaltaisiin kysymyksiin: Miten Suomessa investoidaan digitalisaatioon ja kasvuun? Millaisia strategioita yrityksillä on digiajan kilpailukyvyn kehittämiseen? Mikä on datan ja analytiikan rooli muutoksessa?

Tervetuloa osallistumaan keskusteluun ja muotoilemaan kanssamme tulevaisuuden liiketoimintaa!

Tutustu ohjelmaan ja ilmoittaudu: ratkaisu.cgi.fi

Pääyhteistyökumppanimme

CISCO

HITACHI
Inspire the Next

Microsoft