Tietoturvan vuosi: Korona- ja kyberpandemia käsi kädessä – kyberhyökkäykset terveydenhuoltoon hakkereiden suosiossa

Check Point Software Technologiesin uusi tietoturvaraportti osoittaa globaalin kyberpandemian laajuuden ja kertoo, miten organisaatiot voivat kehittää immuniteettiaan kyberuhkille vuonna 2021. Se valottaa, kuinka hakkerit hyödynsivät koronaviruspandemiaa kaikilla liiketoiminta-alueilla viime vuonna ja tuo esiin heidän yleisimmät taktiikkansa pilvihyökkäyksistä tietojenkalasteluun ja kiristysohjelmiin.

• Yritysmaailmassa kohdataan päivittäin yli 100 000 haitallista verkkosivustoa ja 10 000 haitallista tiedostoa.
• Viime vuonna 46 prosentissa organisaatioista vähintään yksi työntekijä on ladannut haitallisen mobiilisovelluksen.
• Kyberhyökkäykset sairaaloihin ja muihin terveydenhuollon organisaatioihin olivat hakkereiden suosituimpia trendejä.
• 87 prosenttiin yritysverkoista on kohdistunut jo tunnetun, olemassa olevan haavoittuvuuden hyödyntämisyritys.

ESPOO – 25. helmikuuta 2021 -- Maailman johtava tietoturvaratkaisujen toimittaja Check Point Software Technologies on julkaissut vuoden 2021 tietoturvaraporttinsa. Check Point 2021 Security Report valottaa menetelmiä, joilla kyberrikolliset hyökkäsivät viime vuonna organisaatioihin eri toimialoilla ympäri maailmaa hyödyntäen COVID-19-pandemiaa. Raportti antaa tietoturva-ammattilaisille ja yritysjohtajille eväitä viidennen sukupolven kyberuhkilta suojautumiseksi.

Check Pointin tutkijoiden viime vuonna havainnoimista kyberrikollisuuden ilmiöistä merkittävimpiä:

- **Pilvipalveluiden käyttöönotto tietoturvan edellä**: Pandemia vauhditti vuonna 2020 organisaatioiden digitaalisen transformaation suunnitelmia yli viidellä vuodella, mutta julkisen pilven tietoturva on edelleen suuri huolenaihe 75 prosentille yrityksistä. Lisäksi yli 80 prosenttia yrityksistä havaitsi, että niiden nykyiset tietoturvatyökalut eivät toimi lainkaan tai toimivat vain rajoitetusti pilvessä. Tämä osoittaa, että pilvipalvelujen tietoturvaongelmat jatkuvat vuonna 2021.
- **Kohteena etätyö**: Hakkerit tehostivat hyökkäyksiä etätyöntekijöiden keskustelujen kaappaamiseksi tarkoituksena varastaa tietoja tai tunkeutua yritysverkkoihin. Tähän käytettiin Emotet- ja Qbot-troijalaisia, joita esiintyi 24 prosentissa yritysverkoista maailmanlaajuisesti. Hyökkäykset etäkäyttöjärjestelmiin, kuten RDP:hen ja VPN:ään, lisääntyivät myös huomattavasti.
- **Kaksinkertaiset kiristyshyökkäykset lisääntyvät:** Vuoden 2020 kolmannella neljänneksellä lähes puoleen kiristystapahtumista liittyi kohdeorganisaatiolta varastetun tiedon julkaisun uhka. Kiristyshaittaohjelmien uhriksi joutuu uusi organisaatio keskimäärin 10 sekunnin välein maailmanlaajuisesti.
- **Hyökkäykset terveydenhuoltoon yltyvät epidemiaksi**: Vuoden 2020 viimeisellä neljänneksellä Check Point Research raportoi, että sairaaloihin kohdistuvat kyberhyökkäykset (erityisesti kiristyshyökkäykset) olivat lisääntyneet 45 % maailmanlaajuisesti. Rikolliset uskovat sairaaloiden suostuvan muita aloja helpommin kiristysvaatimuksiin COVID 19:n aiheuttamien paineiden vuoksi.
- **Mobiililaitteet ovat liikkuvia kohteita**: 46 prosentissa organisaatioista vuonna 2020 ainakin yksi työntekijä oli ladannut haitallisen mobiilisovelluksen, mikä vaarantaa niiden verkot ja datan. Mobiililaitteiden lisääntynyt käyttö globaalien rajoitusten aikana on lisännyt myös mobiilitroijalaisten määrää.

”Yritykset ympäri maailmaa yllättivät itsensä digitaalisten aloitteidensa nopeudella vuonna 2020: Digitaalisen transformaation arvioidaan edenneen jopa seitsemällä vuodella. Samaan aikaan kyberrikolliset muuttivat taktiikoitaan hyötyäkseen näistä muutoksista ja pandemiasta lisäten hyökkäyksiä kaikilla sektoreilla. Meidän on toimittava nyt lopettaaksemme kyberpandemian leviämisen. Organisaatioiden on rokotettava hyperkytketyt verkkonsa estääkseen nämä vahingolliset kyberhyökkäykset", sanoo Check Pointin **Dorit Dor**, vice president of products.

Check Pointin Security Report 2021 perustuu Check Pointin globaalin ThreatCloud-verkoston ajantasaisesti keräämiin hyökkäystietoihin, Check Pointin viime vuoden aikana tekemiin tutkimuksiin sekä kyselyyn, jonka Check Point teetti IT-ammattilaisten ja yritysjohtajien parissa. Raportti kertoo, millaisia ovat uusimmat uhat eri toimialoilla ja käy perusteellisesti läpi haittaohjelmien, tietovuotojen ja valtiollisten kyberhyökkäysten trendit. Check Pointin omat asiantuntijat analysoivat raportissa tämän hetken ja huomisen monitahoista uhkamaisemaa, jotta se tulisi ymmärretyksi yrityksissä ja organisaatioissa.

*Lataa **koko raportti** ja lue **blogi** Check Pointin sivustolla.*

Lisätietoja:
Maajohtaja Sampo Vehkaoja, Check Point Software Technologies, sampov@checkpoint.com.
Tietoturva-asiantuntija Rami Rauanmaa, Check Point Software Technologies, ramira@checkpoint.com.
Haastattelupyynnöt: Viestintäkonsultti Päivi Savolainen, OSG Viestintä, paivi.savolainen@osg.fi, p. 050 441 6068.

Seuraa Check Pointia:
Twitter: http://www.twitter.com/checkpointsw
Facebook: https://www.facebook.com/checkpointsoftware
Blog: http://blog.checkpoint.com
YouTube: http://www.youtube.com/user/CPGlobal
LinkedIn: https://www.linkedin.com/company/check-point-software-technologies

Julkaisijasta:

Check Point Research
Check Point Research (research.checkpoint.com) huolehtii siitä, että Check Pointin asiakkailla ja laajemmalla tietoturvayhteisöllä on käytettävissään paras mahdollinen tieto kyberturvallisuuden riskeistä. Tutkijaryhmä kerää ja analysoi ThreatCloud-verkkopalvelun tallentamat maailmanlaajuiset kyberhyökkäystiedot, jotta hakkerit pysyvät kurissa ja kaikki Check Pointin tuotteet pystytään päivittämään uusimmilla suojauksilla. Tutkijaryhmä koostuu yli 100 analyytikosta ja tutkijasta, jotka tekevät yhteistyötä muiden tietoturvayhtiöiden ja viranomaisten kanssa.

Check Point Software Technologies Ltd.
Check Point Software Technologies Ltd. (www.checkpoint.com) on johtava yritysten ja valtionhallinnon kyberturvallisuusratkaisujen tarjoaja globaalisti. Sen ratkaisut suojaavat 5. sukupolven kyberhyökkäyksiltä alan johtavalla haittaohjelmien, kiristysohjelmien ja muiden hyökkäysten kiinnijäämisprosentilla. Check Pointin monitasoinen tietoturva-arkkitehtuuri, ”Infinity” Total Protection sisältää 5. sukupolven (Gen V) edistyneen uhkientorjunnan, joka suojaa yrityksen pilvi-, verkko- ja mobiililaitteissa sijaitsevan tiedon. Check Point tarjoaa myös alan kattavimman ja intuitiivisimman yhden kontrollipisteen ohjausjärjestelmän. Check Point huolehtii yli 100 000 ison ja pienen yrityksen ja yhteisön tietoturvasta.

