Check Pointin kyberturvaennuste 2021 – Seuraavaa normaalia turvaamassa

Check Point ennustaa, että tietoturvasta vastaavien päänvaivaksi tulee ensi vuonna lisää koronapandemiaan liittyviä kyberhyökkäyksiä, entistä kehittyneempiä haittaohjelmia sekä uusia 5G- ja IoT-uhkia.

ESPOO – 16. marraskuuta 2020 – Maailman johtava tietoturvayhtiö Check Point Software Technologies on julkaissut uusimman kyberturvaennusteensa, joka listaa yritysten ja organisaatioiden ensi vuoden tärkeimmät tietoturvahaasteet.

Check Pointilta kerrotaan, että COVID-19-pandemian aiheuttamat työtapojen muutokset ovat organisaatioiden IT- ja tietoturvatiimien tärkeä painopistealue ensi vuonnakin. 81 % yrityksistä on siirtynyt pääosin etätyöhön ja 74 % suunnittelee tekevänsä etätyöstä mahdollista pysyvästi.

”Pandemia suisti lähes kaikkien organisaatioiden toiminnan radaltaan. Se pakotti yrityksest siirtämään tavallisen liiketoimintansa ja strategiset suunnitelmansa syrjään ja keskittymään turvallisten yhteyksien ja uusien toimintatapojen luomiseen etätöihin siirtyvälle henkilöstölle. Hakkerit pyrkivät hyödyntämään pandemian aiheuttamaa häiriötilannetta, mikä lisäsi tietoturvatiimien kiirettä. 71 % tietoturva-alan ammattilaisista on raportoinut kyberhyökkäysten yleistyneen etätyöhön siirtymisen jälkeen”, kommentoi Check Pointin Suomen maajohtaja **Sampo Vehkaoja.**

”Yksi varmimmin ennustettavista asioista tietoturvassa on se, että hakkerit pyrkivät aina hyödyntämään koronapandemian tai 5G:n tulon tapaisia isoja tapahtumia ja muutoksia omaksi edukseen. Heitä edellä on mahdollista pysyä ainoastaan ennakoivalla toiminnalla ja pitämällä kaikki hyökkäykselle alttiit pinnat suojattuina ja valvottuina. Muuten yrityksestä tulee taitavasti rakennettujen kohdennettujen hyökkäysten seuraava uhri”, hän jatkaa.

Check Pointin tietoturvaennuste 2021 jakaantuu kolmeen osaan: Koronapandemiaan liittyviin riskeihin, haittaohjelmiin, yksityisyyteen ja kyberkonflikteihin sekä kehittyviin 5G- ja IoT-alustoihin.

Pandemiaan liittyvät riskit

- **Uuden normaalin tietoturva:** Covid-19 vaikuttaa vuonna 2021 edelleen ihmisiin, yrityksiin ja yhteiskuntiin, mutta vaikutusten muoto muuttuu ajan kuluessa. Joudumme sopeutumaan kokonaiseen sarjaan ”seuraavia normaaleja”. Yrityksillä on edelleen tehtävää etätyöhön siirtymisen jälkitoimissa, kun ne varmistavat, että hajautettujen verkkojen ja pilvipalvelujen tietoturva on kunnossa. Uhkientorjuntaa tulee vahvistaa ja se pitää automatisoida verkon kaikissa pisteissä työntekijän puhelimesta ja kannettavasta tietokoneesta pilvipalveluihin ja IoT-laitteisiin saakka. Vain tällä tavoin voidaan estää kyberhyökkäysten nopea eteneminen organisaatiossa heikkouksia etsien. Ennaltaehkäisyn automatisoiminen on kriittistä, koska 78 % organisaatioista kokee pulaa kybertaidoista.

- **Pandemiaa hyödyntäviin huijauksiin ei ole lääkettä:** Niin kauan kuin COVID-19 pysyy otsikoissa, ei rokotekehitystä tai uusia rajoituksia hyödyntäville kalastelukampanjoille näy loppua. Rokotteita kehittävät lääkeyritykset ovat hyökkäysten kohteena, kun rikolliset tai valtiolliset toimijat pyrkivät käyttämään tilannetta hyväkseen.

- **Etäoppimisympäristöt eivät ole turvassa:** Koulut ja yliopistot ovat ottaneet laajamittaiseen käyttöön etäoppimisalustoja, joten ei ehkä yllätä ketään, että tällä sektorilla koettiin elokuussa 30 prosentin nousu viikottaisten kyberhyökkäysten määrässä. Hyökkäykset häirisevät edelleen etäopetusta tulevana vuonna.

Haittaohjelmat, yksityisyys ja kybersodankäynti

- **Kaksinkertainen kiristys voittaa alaa:** Tämän vuoden kolmannella neljänneksellä havaittiin jyrkkä nousu kaksinkertaisten kiristysten määrässä. Näissä hyökkäyksissä hakkerit kopioivat ensin itselleen suuria määriä arkaluontoista dataa ja lukitsevat sen jälkeen uhrin tietokannat salausohjelmalla. Sitten hyökkääjät uhkaavat julkaista datan, ellei lunnaita makseta. Näitä tapahtumakulkuja nähdään ensi vuonna lisää.

- **Bottiverkkojen armeija kasvaa:** Hakkerit ovat muokanneet useista haittaohjelmaperheistä bottiverkkoja, joiden avulla voi koota tahdottomia hyökkäysarmeijoita tartunnan saaneista tietokoneista. Emotet, vuoden 2020 yleisimmin käytetty haittaohjelma, oli ensin pankkitroijalainen, mutta siitä on kehitetty yksi sitkeimmistä ja monipuolisimmista bottiverkoista. Se pystyy käynnistämään useita vahingollisia hyökkäystyyppejä kiristysohjelmasta tietovuotoihin.

- **Valtiot käyvät valtiota vastaan:** Valtiolliset toimijat käyttävät enenevässä määrin kyberhyökkäyksiä muihin valtioihin kohdistuvan vakoilun ja vaikuttamisen välineinä. Microsoft raportoi, että 89 % valtiollisen tason hakkeroinneista tapahtui viime vuonna kolmen valtion toimesta. Viime vuosina keskiössä on ollut kansallisen kriittisen infrastruktuurin suojaaminen, ja vaikka se onkin edelleen olennaista, on tärkeää tunnistaa myös muihin valtiollisiin toimijoihin kohdistuvat hyökkäykset. Näihin kuuluvat terveydenhuollon toimijat ja ministeriöt, esimerkkinä maaliskuussa 2020 tapahtunut, koronapelkoa hyödyntävä Vicious Panda -kampanja, jonka kohteena oli Mongolia.

- **Deepfake-videot aseina:** Videokuvan ja äänen väärentämisen tekniikat ovat nyt niin pitkälle kehittyneitä, että niitä on mahdollista käyttää muun muassa mielipiteiden ja pörssikurssien manipuloimiseen. Aiemmin tänä vuonna belgialainen poliittinen ryhmittymä julkaisi deepfake-videon, jossa Belgian pääministeri yhdisti puheessaan COVID-19-pandemian ympäristövahinkoihin ja jossa vaadittiin toimia ilmastonmuutoksen hillitsemiseksi. Monet pitivät videota aitona. Myös ääntä voi manipuloida pahat mielessä – esimerkiksi yrityksen toimitusjohtajan ääni voitaisiin väärentää käytettäväksi tunnistautumisessa.

- **Yksityisyys, mitä se on:** Puhelin kertoo jo nyt ulkopuolisille paljon enemmän kuin moni ymmärtää. Kiitos tästä kuuluu sovelluksille, jotka pyytävät pääsyä muun muassa käyttäjien puhelinluetteloihin ja viesteihin. Uudempi ongelma ovat heikkotasoiset koronajäljitysohjelmat, jotka vuotavat käyttäjien tietoja. Varsinaisten mobiilihaittaohjelmien tavoitteena on useimmiten napata käyttäjän pankkitunnistustiedot tai houkutella klikkaamaan mainosta, josta lähtee pyörimään maksullinen tilaus. Myös nämä petokset ovat lisääntymään päin.

Uudet 5G- ja IoT-alustat

- **5G:n hyödyt ja haasteet:** 5G lupaa kytkeytynyttä ja nopeaa maailmaa, mutta se tarjoaa myös rikollisille mahdollisuuden käynnistää hyökkäyksiä verkon kautta ja aiheuttaa häiriötä verkon toimintaan. Digitaaliset terveydenhoitoon liittyvät laitteet keräävät tietoa potilaiden voinnista, liikennepalvelut tarkkailevat ajajien liikkeitä ja älykkäät kaupunkisovellukset keräävät tietoja käyttäjien elämäntavasta. Jatkuvasti toimivat laitteet keräävät valtavan määrän dataa. 5G-laitteet on suojattava tietomurtoja, varkauksia ja peukalointia vastaan, jotta yksityisyys ja tietoturva voidaan taata.

- **IoT – uhkien internet**: Kun 5G-verkot laajentuvat, niihin kytkeytyneiden IoT-laitteiden määrä kasvaa massiiviseksi – mikä puolestaan tekee laitteista entistä haavoittuvampia suuren mittakaavan kyberhyökkäyksille. IoT-laitteet ja niiden yhteydet verkkoihin ja pilviin ovat yhä tietoturvan heikko lenkki, koska laitteisiin on vaikea saada täyttä näkyvyyttä ja niiden tietoturvavaatimukset ovat monimutkaiset. Lähestymistavan IoT-tietoturvaan tulee kehittyä nykyistä kokonaisvaltaisemmaksi. Näitä yli kaikkien toimialarajojen kasvavia verkkoja on mahdollista valvoa vain yhdistämällä perinteiset ja uudet keinot.

Lisätiedot:
Sampo Vehkaoja, Country Manager, Finland and Baltics, Check Point Software Technologies, sampov@checkpoint.com, p. 050 555 5500.
Haastattelupyynnöt: Päivi Savolainen, viestintäkonsultti, OSG Viestintä, paivi.savolainen@osg.fi, p. 050 441 6068.

Seuraa Check Point Researchia:
Blog: https://research.checkpoint.com/
Twitter: https://twitter.com/_cpresearch_
Podcast: https://research.checkpoint.com/category/cpradio/
Facebook: https://www.facebook.com/checkpointresearch

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.

