Check Pointin tietoturvaennuste 2020: Varautukaa uuteen kylmään sotaan!

*Tietoturvayhtiö ennustaa, että valtioiden tukemat kyberhyökkäykset hallituksia, kriittistä infrastruktuuria ja korkean profiilin yrityksiä vastaan yleistyvät, kun kansainväliset jännitteet kasvavat.*

**ESPOO — 5.11.2019** – Tietoturvayhtiö Check Point® Software Technologiesin vuoden 2020 kyberturvallisuusennusteet jakautuvat kansainvälisiin trendeihin ja teknisiin ennusteisiin.

Check Pointin kansainvälisten kyberturvallisuusennusteiden kolmen kärki:

1. **Kybermaailman kylmä sota kiihtyy** – Lännen ja idän suurvaltojen ajautuminen erilleen jatkuu, mistä selvä merkki on Yhdysvaltojen ja Kiinan välinen kauppasota. Lännen ja idän teknologiat eriytyvät, ja kybermaailman kylmä sota kiihtyy. Isot valtiot rahoittavat pienten valtioiden välisiä kyberhyökkäyksiä vahvistaakseen ja laajentaakseen vaikutusvaltaansa. Vastaavaa on jo nähty [Iraninvastaisissa kyberhyökkäyksissä](https://uk.reuters.com/article/uk-usa-iran-military-cyber-exclusive/exclusive-u-s-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-say-idUKKBN1WV0EM), joita seurasivat Saudi-Arabian öljylaitoksiin kohdistuneet hyökkäykset.
2. **Valeuutiset 2.0 Yhdysvaltain vaaleissa** – Yhdysvaltain vuoden 2016 vaalit tunnetaan tekoälypohjaisen valeuutisten levityksen alkupisteenä. Kampanjoinnin tueksi perustettiin tuolloin erityisiä valeuutisryhmiä, jotka loivat ja levittivät valheellisia tarinoita vastustajan kampittamiseksi. Ulkopuoliset tahot toteuttavat todennäköisesti jo nyt suunnitelmia, joiden tarkoituksena on manipuloida äänestäjiä vuoden 2020 vaaleissa.
3. **Sähköverkkoihin ja muuhun kriittiseen infraan kohdistuvat hyökkäykset yleistyvät** – Sähköverkkoihin kohdistettiin päättyvänä vuonna kyberhyökkäyksiä ainakin [Yhdysvalloissa](https://www.eenews.net/stories/1061111289) ja [Etelä-Afrikassa](https://www.bbc.co.uk/news/technology-49125853). Kriittinenkin energia- ja vesi-infrastruktuuri perustuu monin paikoin ikääntyneeseen tekniikkaan, joka on altista hyökkäyksille. Päivitykset on voitu jättää tekemättä esimerkiksi jakelun keskeytysten pelossa. Monet valtiot joutuvat nyt harkitsemaan kriittisen infrastruktuurinsa kybersuojauksen huomattavaa vahvistamista.

Check Pointin teknisten tietoturvaennusteiden kolmen kärki:

1. **Kohdistetut kiristyshaittaohjelmat yleistyvät** – Jo tänä vuonna on nähty tarkasti yrityksiin, viranomaisiin ja terveydenhuollon organisaatioihin kohdennettuja kiristyshaittaohjelmahyökkäyksiä. Hyökkääjät ovat käyttäneet aikaa tietojen keruuseen kohteista varmistaakseen toimintahäiriön laajuuden ja lunnaiden sopivan tason. Hyökkäyksistä on tullut niin vahingollisia, että [FBI on pehmentänyt kantaansa lunnaiden maksamiseen](https://www.theregister.co.uk/2019/10/03/fbi_softens_stance_on_ransomware/): se myöntää nyt, että joissakin tapauksissa yritysten kannattaa harkita maksamista suojatakseen omistajiaan, työntekijöitään ja asiakkaitaan.
2. **Kalastelua tapahtuu muuallakin kuin sähköpostissa** – Sähköposti säilyy kyberrikollisten suosituimpana hyökkäysmenetelmänä, mutta he käyttävät myös monia muita menetelmiä houkutellessaan potentiaalisia uhreja luovuttamaan henkilötietoja tai salasanoja ja jopa lähettämään rahaa. Yhä useammin kalastelussa käytetään [tekstiviestejä](https://research.checkpoint.com/advanced-sms-phishing-attacks-against-modern-android-based-smartphones/), sosiaalista mediaa ja pelialustoja.
3. **Mobiililaitteiden riskit kasvavat** – Tämän vuoden ensimmäisellä vuosipuoliskolla [mobiililaitteiden pankkihaittaohjelmien hyökkäysmäärä kasvoi 50 prosenttia](https://www.checkpoint.com/press/2019/check-point-research-from-supply-chain-to-email-mobile-and-the-cloud-no-environment-is-immune-to-cyber-attacks/) verrattuna vuoteen 2018. Nämä haittaohjelmat voivat varastaa maksutietoja, käyttöoikeustietoja ja rahaa uhrin pankkitililtä. Uusia ohjelmaversioita on verkossa myytävänä kenelle tahansa, joka on valmis maksamaan kehittäjille. Myös mobiililaitteissa tapahtuvista kalasteluyrityksistä tulee entistä hienostuneempia ja tehokkaampia. Niissä uhri houkutellaan klikkaamaan linkkiä, joka johtaa haitalliselle verkkosivulle.

Check Pointin perustaja ja toimitusjohtaja **Gil Shwed** kommentoi: ”Mitä vahvemmin luotamme jatkuvaan ja saumattomaan yhteydenpitoon, sitä enemmän tilaisuuksia tarjoamme rikollisille ja valtiollisille toimijoille, joiden tavoitteena on vaikuttaa vaalien tuloksiin tai aiheuttaa häiriötä ja tuhoa, joka vaarantaa ihmiselämiä. Hyökkäysten määrä kasvaa jatkuvasti: kuluneen vuoden aikana ThreatCloud-palvelumme pysäytti lähes 90 miljardia hyökkäysyritystä päivässä. Googlessa tehtiin samaan aikaan kuusi miljardia hakua.”

”Emme pysty enää puolustautumaan perinteisillä, haittaohjelmien havaitsemiseen perustuvilla tietoturvan malleilla: siihen mennessä, kun havaitsemme uhan, se on jo aiheuttanut vahingon. Näitä uudentyyppisiä, viidennen sukupolven hyökkäyksiä vastaan tarvitaan viidennen sukupolven tietoturva, joka yhdistää reaaliaikaisen uhkientorjunnan ja tietojen jakamisen sekä kattavan suojauksen verkoissa, pilvessä ja mobiilisovelluksissa”, Schwed jatkoi.

Pidemmät ennusteet ovat luettavissa  [Check Pointin blog](https://blog.checkpoint.com/2019/10/24/2020-vision-check-points-cyber-security-predictions-for-the-coming-year/)issa.

**Lisätietoja:**

Rami Rauanmaa, Head of Security Engineering, Finland and Baltics, Check Point Software Technologies, ramira@checkpoint.com, p. 050 382 6694

Maija Rauha, viestintäkonsultti, OSG Viestintä, maija.rauha@osg.fi, p. 0400 630 065

**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

**Check Point Software Technologies Ltd.**

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://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.