Check Point Softwaren kyberturvallisuusennusteet vuodelle 2023

Check Point Softwaren vuoden 2023 kyberturvallisuusennusteen mukaan muun muassa haktivismi, syvävääreennökset ja hyökkäykset yritysten yhteistyötyökaluihin nousevat organisaatioiden kyberturvallisuushaasteiden kärkeen ensi vuonna.

ESPOO – 24. marraskuuta 2022 – Maailman johtava tietoturvayhtiö Check Point Software Technologies on julkaissut uusimman kyberturvaennusteensa, jossa tarkastellaan organisaatioiden ensi vuoden tärkeimpiä tietoturvahaasteita.

Kyberhyökkäykset lisääntyivät 28 % kaikilla toimialoilla vuoden 2022 kolmannella neljänneksellä vuoteen 2021 verrattuna. Check Point ennustaa jyrkän nousun jatkuvan maailmanlaajuisesti, mikä johtuu kiristysohjelmien lisääntymisestä ja kansainvälisten konfliktien aiheuttamasta valtioiden mobilisoimasta haktivismista. Samaan aikaan organisaatioiden tietoturvatiimeihin kohdistuu kasvava paine, kun globaali 3,4 miljoonan työntekijän kybertyövoimakuilu kasvaa entisestään ja hallitusten odotetaan ottavan käyttöön uusia kyberturvallisuussäädöksiä kansalaisten suojelemiseksi tietovuodoilta.

Vuonna 2022 kyberrikolliset ja valtioihin sidoksissa olevat toimijat jatkoivat organisaatioiden hybridityötapojen hyväksikäyttöä, eikä näiden hyökkäysten lisääntyminen osoita hidastumisen merkkejä Ukrainan sodan ja sen maailmanlaajuisten vaikutusten jatkuessa. Organisaatioiden on vahvistettava ja automatisoitava tietoturvainfrastruktuuriaan, jotta ne voivat paremmin valvoa ja hallita hyökkäyspintojaan ja estää kaikentyyppisiä uhkia yksinkertaisemmin ja pienemmillä henkilöstöresursseilla.

Check Pointin kyberturvallisuusennusteet vuodelle 2023 jakautuvat neljään osaan: haittaohjelmat ja tietojenkalastelu, haktivismi, hallitusten sääntely ja kyberturvallisuuden vahvistaminen.

Haittaohjelmien ja hakkeroinnin nousu

● **Ei hengähdystaukoa kiristysohjelmilta**: Kiristyshaittaohjelmat olivat organisaatioiden suurin uhka vuoden 2022 ensimmäisellä puolikkaalla. Kiristysohjelmien ekosysteemi kehittyy ja kasvaa edelleen, kun rikollisryhmät muotoutuvat aiempaa pienemmiksi ja ketterämmiksi pyrkiessään välttelemään lainvalvontaa.
● **Ongelmalliset yhteistyötyökalut**: Vaikka henkilökohtaisiin ja yritysten sähköpostitileihin kohdistuvat tietojenkalasteluyritykset ovat jokapäiväinen uhka, vuonna 2023 rikollisten tietojenkalasteluhyökkäysten kohteina ovat myös yritysten yhteistyötyökalut, kuten Slack, Teams, OneDrive ja Google Drive. Ne sisältävät runsaasti arkaluontoisia tietoja, koska useimpien organisaatioiden työntekijät tekevät edelleen usein etätöitä.

Haktivismi ja syvävääreennökset kehittyvät

● **Valtioiden mobilisoima haktivismi**: Viime vuoden aikana haktivismissa on tapahtunut siirtymä henkilösuhteisiin perustuvista, tavoitteiltaan vaihtelevista ryhmistä (kuten Anonymous) kohti valtion tukemia ryhmiä, jotka ovat organisoidumpia, jäsennellympiä ja kehittyneempiä. Tällaiset ryhmät ovat viime aikoina hyökänneet kohteisiin Yhdysvalloissa, Saksassa, Italiassa, Norjassa, Suomessa, Puolassa ja Japanissa, ja nämä ideologiset hyökkäykset jatkavat kasvuaan vuonna 2023.
● **Syvävääreennökset aseina**: Lokakuussa 2022 levisi laajalti deepfake-video Yhdysvaltain presidentti Joe Bidenista laulamassa Baby Shark -laulua kansallislaulun sijaan. Oliko se vitsi vai yritys vaikuttaa tärkeisiin Yhdysvaltain välivaaleihin? Deepfake-teknologiaa käytetään yhä enemmän mielipiteiden ohjailuun ja manipulointiin tai käyttöoikeuksien huijaamiseen työntekijöiltä.

Hallitukset tehostavat toimia kansalaisten suojelemiseksi

● **Tietovuotoja koskevat uudet lait**: Australialaisen televiestintäyhtiö Optusin tietovuoto on saanut maan hallituksen ottamaan käyttöön uusia tietovuotoja koskevia säädöksiä, joita muiden puhelinyhtiöiden on

©2022 Check Point Software Technologies Ltd. All rights reserved

noudatettava asiakkaiden suojelemiseksi petoksilta. Vuonna 2023 tulemme näkemään, etteivät olemassa olevat säädökset, kuten GDPR, riitä muillekaan hallituksille, vaan ne noudattavat Australian esimerkkiä.
● **Uudet kansalliset kyberrikollisuustyöryhmät**: Useat hallitukset seuraavat Singaporen esimerkkiä ja perustavat kiristyshyökkäysten ja kyberrikollisuuden torjumiseksi yhteistyöryhmiä, joissa on mukana valtion virastoja, yrityksiä ja lainvalvontaviranomaisia. Näin pyritään torjumaan kauppaan ja kuluttajiin kohdistuvaa kasvavaa uhkaa. Ponnistukset ovat osittain seurausta pohdinnasta, voidaanko kybervakuutusalaan luottaa turvaverkkona kyberturvallisuuden pettäessä.
● **Suunniteltu tietoturva ja yksityisyys**: Autoteollisuus on jo ryhtynyt ottamaan käyttöön toimenpiteitä ajoneuvojen omistajien tietojen suojaamiseksi. Muiden tietoja tallentavien ja käsittelevien kuluttajatuotteiden valmistajat alkavat seurata autoalan esimerkkiä, koska valmistajia pidetään vastuullisina tuotteidensa haavoittuvuuksista.

Konsolidaatiolla on väliä
● **Monimutkaisuuden vähentäminen riskien pienentämiseksi**: Globaali kybertaitojen osaajavaje kasvoi yli 25 % vuonna 2022. Silti organisaatioilla on pandemian vuoksi käytössä enemmän monimutkaisia hajautettuja verkkoja ja pilvipalveluita kuin koskaan ennen. Tietoturvatiimien on vahvistettava IT- ja tietoturvainfrastruktuuriaan parantaakseen puolustustaan ja keventääkseen työtaakkaansa, jos ne aikovat pysyä uhkien edellä. Yli kaksi kolmasosaa tietoturvajohtajista totesi, että heidän yrityksensä kyberturvallisuus paranisi, jos käytössä olisi ratkaisuja nykyistä pienemmältä joukolta toimittajia.

Check Pointin johtajien ennusteet:

Maya Horowitz, VP of Research, Check Point Software
”Olemme astumassa uuteen haktivismin aikakauteen, jossa poliittisista ja sosiaalisista syistä johtuvat hyökkäykset lisääntyvät. Uhkatoimijat muuttuvat yhä röyhkeämmiksi ja kiinnittävät huomionsa kriittiseen infrastruktuuriin.”

Deryck Mitchelson, EMEA CISO, Check Point Software
”Tulemme näkemään paljon enemmän keskustelua kyberturvallisuussääntelystä ja painostusta sen edistämiseksi, koska nykyinen keppi ja porkkana -lähestymistapa ei ole toiminut.”

Jeremy Fuchs, Research Analyst, Avanan, Check Point -yhtiö
”Vaikka sähköposti ja tietojenkalastelu kulkevat käsi kädessä, ovat yhä vaarallisia ja leviävät nopeasti, vuonna 2023 kyberrikolliset hyödyntävät entistä enemmän yritysyhteistyökaluja ja tekevät tietojenkalasteluhyökkäyksiä päästäkseen käsiksi esimerkiksi uhrin Slackiin, Teamsiin, OneDriveen ja Google Driveen. Työntekijät jakavat usein huolettomasti dataa ja henkilökohtaisia tietoja näitä yrityssovelluksia käyttäessään, mikä tekee niistä tuottoisan tietolähteen hakkereille.”

Jony Fischbein, CISO, Check Point Software
”Monihybridiympäristössä monet tietoturvajohtajat pyrkivät rakentamaan kattavan tietoturvaohjelman useiden toimittajien ratkaisuista. Vuonna 2023 tietoturvajohtajat vähentävät tietoturvaratkaisujen määrää ja suosivat yhtä kokonaisvaltaista ratkaisua kompleksisuuden vähentämiseksi.”

Oded Vanunu, Head of Products Vulnerability Research, Check Point Software
”Digitaaliset huijaukset lisääntyvät dramaattisesti globaalista talouden hidastumisesta ja inflaatiosta johtuen. Kyberrikolliset tekevät yhä useammin sosiaalisen median kampanjoita Telegramin, WhatsAppin ja muiden suosittujen viestisovellusten avulla. Myös Web3-lohkoketjualustoihin kohdistuu enemmän kyberhyökkäyksiä, pääasiassa alustojen ja niiden käyttäjien kryptovarallisuuden kaappaamiseksi.”

Lue Check Point Softwaren vuoden 2023 kyberturvaennuste kokonaisuudessaan osoitteessa https://blog.checkpoint.com/.

©2022 Check Point Software Technologies Ltd. All rights reserved

Lisätiedot:
Viivi Tynjälä, Country Manager, Finland and Baltics, Check Point Software Technologies, viivit@checkpoint.com, p. 0400 411 530.
Haastattelupyynnöt: Päivi Savolainen, viestintäkonsultti, OSG Viestintä, paivi.savolainen@osg.fi, p. 050 441 6068.

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

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. Check Point Infinityn ratkaisuportfolio suojaa yrityksiä ja julkisia organisaatioita 5. sukupolven kyberhyökkäyksiltä alan johtavalla haittaohjelmien, kiristysohjelmien ja muiden hyökkäysten kiinnijäämisprosentilla. Infinity koostuu neljästä peruspilarista: Check Point Harmony etäkäyttäjille; Check Point CloudGuard pilven automaattiseen suojaamiseen; ja Check Point Quantum tietoverkkojen ja datakeskusten suojaamiseen. Näitä kaikkia hallitaan alan kattavimmalla ja intuitiivisimmalla yhtenäisellä hallintajärjestelmällä; Check Point Horizonilla, joka on tietoturvapoikkeamien ennaltaehkäisyyn tähtäävä ohjelmisto- ja palvelukokonaisuus. Check Point huolehtii yli 100 000 ison ja pienen yrityksen ja yhteisön tietoturvasta.

©2022 Check Point Software Technologies Ltd. All rights reserved