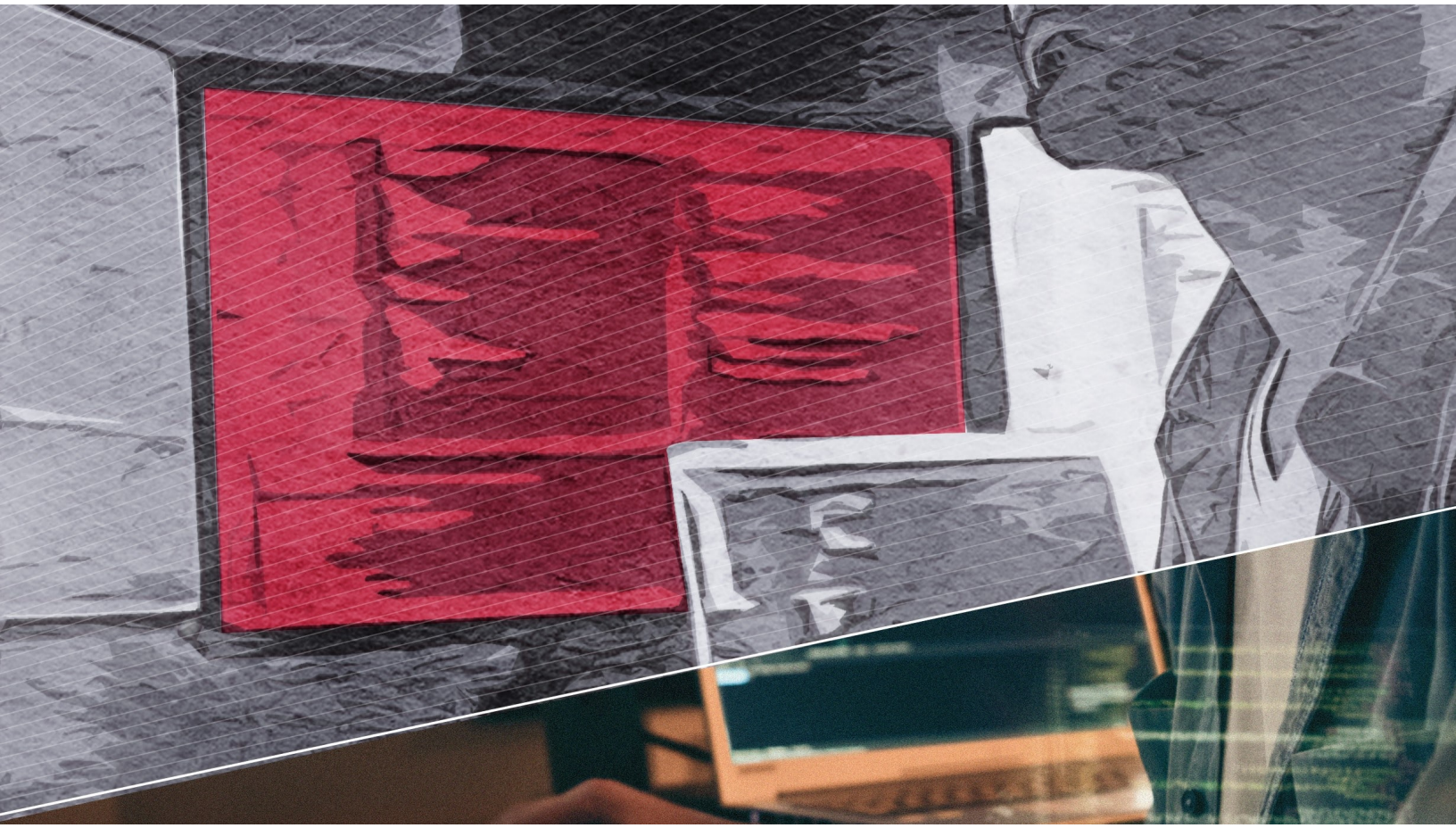

2020-12-08 15:00 EET

Kyberturvallisuus vuonna 2021 nojaa käyttäjien koulutukseen, pilviturvaan ja uhkien laajennettuun havainta- ja vastauskykyyn

Trend Micro ennustaa pilvijärjestelmien joutuvan ensi vuonna rajuun pommitukseen

Trend Micro ennustaa, että kotiverkot, etätyöohjelmistot ja pilvijärjestelmät ovat vuoden 2021 kyberhyökkäysten ykköskohteita. Trend Micro arvioi

Turning the Tide -raportissaan, että vuonna 2021 verkkorikolliset kohdistavat toimenpiteitä erityisesti kotiverkkoihin etsiessään hyökkäysreittejä yritys- ja IoT-verkkoihin.

– Etätyöskentely tulee todennäköisesti jäämään ”uudeksi normaaliksi” pandemian jälkeisessä maailmassa. Sen myötä luvassa on entistä enemmän aggressiivisia hyökkäyksiä yritysten tietoja ja –verkkoja vastaan, kertoo Trend Micron kyberturva-asiantuntija Kalle Salminen. Tietoturvavastaavien on panostettava jatkossa erityisen paljon käyttäjien kouluttamiseen, hyökkäysten tehokkaampaan tunnistamiseen ja hyökkäyksiin reagointiin. Siinä samalla tarvitaan nykyistä mukautuvampaa käyttöoikeuksien valvontaa. Tämä vuosi on ollut yhtä selviytymistaistelua, joten nyt on aika päästää yritysten luovuus valloilleen ja suunnata menestymisen polulle kattavan pilvitietoturvan tukemana.

Raportti varoittaa, että arkaluontoisia tietoja säännöllisesti käsittelevät henkilöt (kuten työntekijöiden tietoja käsittelevät henkilöstövastaavat, asiakastietoja käsittelevät myyntipäälliköt tai yritysten luottamuksellisia sisäisiä tietoja käsittelevät johtajat) ovat suurimmassa vaarassa. Heitä vastaan kohdennetuissa hyökkäyksissä hyödynnetään todennäköisimmin verkon kautta toimivien ryhmätyö- ja tuottavuusohjelmistojen tunnettuja haavoittuvaisuuksia, eikä niinkään nollapäivähaavoittuvaisuuksia.

Access-as-a-service-murtopalveluja tarjoava verkkorikollisuus kasvaa ja kohdistuu etenkin tärkeiden työntekijöiden koti-, yritys- ja IoT-verkkoihin. IT-ylläpitäjien on päivitettävä kotoaan käsin työskentelevien etätyöntekijöiden käytännöt ja suojausjärjestelmät pärjätäkseen monimutkaisten hybridiympäristöjen tuomien haasteiden kanssa. Esimerkiksi kotikoneellaan etätöitä tekevän henkilön kautta päästään käsiksi sekä henkilökohtaisiin että yritysten tietoihin, mikä tekee hänestä houkuttelevan kohteen verkkorikollisille. Tästä johtuen tulevaisuudessa käytetään yhä enemmän Zero Trust -suojausmallia työntekijöiden ja yritysten suojaamiseen.

Trend Micro varoittaa myös API-rajapintojen uhasta kolmansien osapuolten ratkaisujen integrointien määrän kasvaessa. Huonosti suojatuista rajapinnoista tulee uusi suosittu hyökkäysvektori, jonka kautta on mahdollista päästä kiinni arkaluontoisiin asiakastietoihin, lähdekoodiin ja taustapalveluihin.

Kyberuhat kohdistuvat jatkossakin pilvijärjestelmiin. Potentiaalisia uhkia ovat

muun muassa käyttäjien tahattomat virheet, konfigurointivirheet ja hyökkääjät, jotka yrittävät vallata pilvipalvelimia asentaakseen niille omia haittaohjelmia sisältäviä konttejaan.

Trend Micro suosittelee organisaatioille seuraavia toimenpiteitä, joilla uhkia voidaan vähentää merkittävästi vuonna 2021:

- **Kouluttakaa loppukäyttäjiä** yritystietoturvasta, parhaista etätyökäytänteistä ja ohjeistakaa välttämään henkilökohtaisten laitteiden käyttämistä työtehtäviin
- **Rajoittakaa käyttöoikeuksia** sekä yritysverkossa että kotitoimistoissa. Noudattakaa Zero Trust –suojausmallia
- **Panostakaa parhaisiin tietoturvakäytänteisiin ja päivitystenhallintaan**
- **Tehostakaa uhkavalvontaaasiantuntijoiden avulla**, jotta pilvipalvelujen työkuormat, sähköpostit, päätelaitteet, verkot ja palvelimet ovat suojattuja kellon ympäri

Kyberrikolliset suuntaavat jatkossakin helpon rahan perään, hakien hyökkäyksillään suurinta mahdollista taloudellista hyötyä. Niinpä kaikkien organisaatioiden ja niiden tietoturvavastaavien on oltava valppaina ja valmiina pysyäkseen pahisten edellä.

Lisätietoja ja koko raportti alla.

Trend Micro
Japanilainen vuonna 1988 perustettu Trend Micro on yksi kyberturvan globaaleista pioneereista. Kolmessa vuosikymmenessä yrityksestä on kasvanut maailman suurin riippumaton tietoturvaratkaisujen valmistaja. Trend Micro toimii 50 maassa ja työllistää yli 6000 tietoturva-alan asiantuntijaa. Yhtiön valmistamat innovatiiviset tietoturvaratkaisut suojaavat tehokkaasti hybridipilviympäristöt ja tietoverkot sekä modernit työympäristöt päätelaitteineen ja palveluineen. Lisätietoja osoitteesta: www.trendmicro.com.

Yhteyshenkilöt

Natalie Majerski
Lehdistökontakti
Press contact
stockholmtrendmicro@archetype.co
+46 76-103 2010

Kalle Salminen
Lehdistökontakti
Cyber Security Expert, CISSP, CCSP, CEH - Trend Micro Suomi
Kalle_Salminen@trendmicro.com