Covid-19 vaikutti kyberturvallisuuteen

Microsoftin vuoden 2020 digitaalisen turvallisuuden raportin mukaan vuosi 2020 tullaan muistamaan sekä COVID-19 viruksesta ja sen luomista häiriöistä sekä fyysiseen, että digitaaliseen maailmaan. Se on näkynyt ja näkyy edelleen myös kyberturvallisuuden tilassa.

Tietoverkkorikolliset löytävät haavoittuvia kohteita uusien kanavien kautta hyödyntäen COVID-19 viruksen vaikutuksia etenkin etätyöhön. Microsoftin raportti keskittyi kolmeen huipputason alueeseen: tietoverkkorikollisuus, kansallisvaltioiden uhat ja etätyövoima.

Raportin mukaan verkkorikollisia löytyy maailmanlaajuisesti ja heillä on erilaisia taitoja ja motiiveja. Osa verkkorikollisista on riippumattomia taloudellisista, poliittisista tai yhteiskunnallisista muutoksista, osa taas hyödyntää näitä muutoksia.

Tietoverkkorikolliset oppivat vuoden 2020 aikana hyödyntämään COVID-19-pandemiaa esimerkiksi jäljittelemällä Maailman terveysjärjestöä saadakseen käyttäjät klikkailemaan haitallisia liitteitä tai linkkejä.

Verkkorikollisuus on julkisen ja yksityisen sektorin jatkuva ja kasvava haaste ympäri maailman. Tietoverkkorikollisuutta voidaan pitää suurena ja monipuolisena yrityksenä, joka on usein myytävänä ja joka tekee erilaisia hyökkäyksiä, kuten petoksia, varkauksia ja vakoilua. Se voi olla taloudellisesti motivoitunut tai kansallisvaltion tukema tai molempia.

Lisäksi tietoverkkorikollisuus on lakiteknisesti haastavaa, sillä se on rajat ylittävää.

Uhkaympäristömme kehittyy jatkuvasti ja verkkorikolliset ovat luovia, hyvin resursoituja, organisoituja ja innovatiivisia sekä nopealiikkeisiä löytääkseen uusia haavoittuvaisuuksia, käyttääkseen uusia hyökkäyksiä ja reagoimaan uusiin puolustuksiin.

Hyökkääjät päivittävät "teemojaan" globaalien uutisten mukaisesti. Vaikka COVID-19-aiheiset hyökkäykset edustavat pientä osaa haittaohjelmista, ne kuitenkin osoittavat, kuinka nopeasti tietoverkkorikolliset liikkuvat mukauttaakseen syöttinsä, kuten linkit ja liitteet, päivän aiheisiin.

Aiemmin kyberhyökkäyksiä pidettiin tiettyihin teollisuudenaloihin kohdistuvina, kehittyneinä toimina, mikä jätti loput alat uskomaan, etteivät ne kuulu tietoverkkorikollisuuden piiriin, Siten ei tiedetty, mihin kyberturvallisuusuhkiin näiden yritysten olisi varauduttava. Lunnasohjelmat, ransomware, ovat tehneet kyberhyökkäyksistä todellisen ja kaikkialla läsnä olevan vaaran kaikille.

Monille organisaatioille ransomware hyökkäyksestä tulevat kustannukset lunnasohjelmatilanteen jälkeen ovat paljon suurempia kuin alkuperäiset vaaditut lunnaat.

Usein lunnaiden maksaminen näyttää helpolta vaihtoehdolta palata liiketoimintaan. Todellinen vahinko kuitenkin tapahtuu vasta silloin, kun tietoverkkorikollinen vuotaa tai myy tiedostoja ja jättää takaovet verkkoon tulevaa rikollista toimintaa varten. Nämä riskit säilyvät riippumatta siitä, maksetaanko lunnaat vai ei.

2000-luvun digitaalitalouden tunnusmerkki on työntekijöiden kyky työskennellä mistä tahansa, infrastruktuurin, mobiilipäätelaitteiden ja viestintäsovellusten merkittävien innovaatioiden innoittamana. Vaikka viime vuosina on tullut yhä enemmän mahdollisuuksia etätyöhön, koronapandemia katalysoi näitä ponnisteluja ja pakotti merkittävän osan työvoimasta työskentelemään kotona. Kahden vuoden digitaalinen muutos tapahtui kahden kuukauden aikana keväällä 2020.

Ismo Turve

Kirjoittaja on kyberturvallisuus orientoitunut heinolalainen ja Tietojenkäsittelyn lehtori Hämeen ammattikorkeakoulusta.