AVOKI

● Perusopas kyberturvallisuuteen

Mikä on kyberhyökkäys?

Sisältö

● Perusopas kyberturvallisuuteen

Digitalisaation aikakausi

Maailmassa, jossa digitalisaatio kiihtyy, kyberturvallisuuskysymykset tulevat yhä ajankohtaisemmiksi. Lähes päivittäin kohtaamme uutisia kyberhyökkäyksistä yritysten ja viranomaisten IT-järjestelmiin. Joudumme epäsuorasti kärsimään esimerkiksi siitä, että ruokakauppojen kassajärjestelmät eivät toimi, elokuvalippuja ei voi ostaa, verkkokauppa ei toimi ja yritysten verkkosivut ovat saavuttamattomissa. Pian vain mielikuvitus asettaa rajat sille, kuinka haavoittuva yhteiskuntamme on digitalisaation levitessä toimintoihimme.

Mutta mitä näiden tapausten taustalla oikeastaan on?

Miten kyberhyökkäys toteutetaan?

Tässä oppaassa käymme läpi yleisimmät syyt kyberhyökkäyksiin ja näytämme vaihe vaiheelta, kuinka hyökkääjä pääsee käsiksi tietokoneeseesi ja verkkoosi hyvin vähäisellä ajalla ja resursseilla, laajentaen sitten pääsyään ja ottaen haltuunsa koko IT-ympäristösi.

Käytämme sanaa kyberhyökkäys kattoterminä eri menetelmille, joita kyberrikolliset – tai hakkerit – käyttävät, yleensä tietokoneen ja Internetin avulla. Tämän oppaan tavoitteena on antaa sinulle, lukijalle, yleiskuva siitä, miten kyberhyökkäykset toteutetaan ja mitä toimenpiteitä voidaan tehdä niiden estämiseksi. Toivomme, että tämän oppaan luettuasi olet informoitu ja ajan tasalla siitä, miten kyberhyökkäys tapahtuu ja miten voit toimia välttääksesi sellaisen.

Tärkeä askel organisaatiosi suojaamisessa on asettaa oikeat vaatimukset IT-toimittajallesi. Aloitetaan matka kohti turvallisempaa digitaalista tulevaisuutta.

82%

kaikista tunkeutumisyrityksistä ihmistekijä on mukana

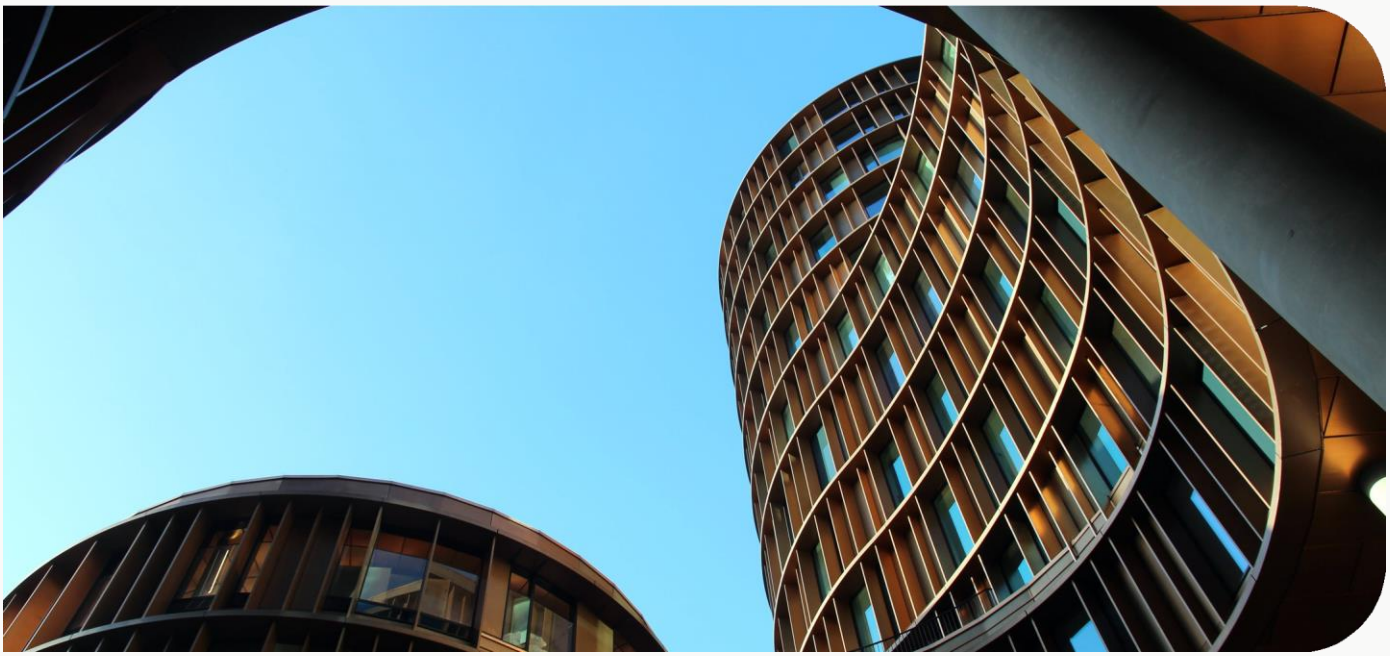
Sääntelyvaatimukset

EU-direktiivi — NIS2

EU:n NIS2-direktiivi otti keskeisen roolin kyberuhkien torjunnassa. 18. lokakuuta 2024 vaatimukset yritysjohtoa kohtaan tiukentuivat ja heidän vastuunsa kasvoi kyberhyökkäysten riskin proaktiivisessa tunnistamisessa, arvioinnissa ja vähentämisessä. Direktiivi teki selväksi, että yritysjohtajat ovat henkilökohtaisesti vastuussa monimutkaisten ja jatkuvasti muuttuvien kyberuhkien hallinnasta

Jos näitä vaatimuksia ei täytetä, seurauksena voi olla huomattavia sakkoja tai sanktioita. Tämä korostaa entisestään sitä, kuinka tärkeää on saada yritysten kyberturvallisuusstrategia nopeasti esityslistalle ja mukauttaa strategia uuteen sääntelyyn.

Johtajilta vaaditaan korkeaa sitoutumista ja ymmärrystä yrityksen tehokkaaseen suojaamiseen, mikä tarkoittaa laajempaa vastuuta ulkoisten kyberuhkien hallinnassa. Tämä direktiivin noudattaminen pitäisi asettaa yritysten strategisen suunnittelun kärkeen.



● Kyberhyökkäyksen toteuttamistavat

Yleisimmät hyökkäysmenetelmät

USA:n kyberturvallisuus- ja infrastruktuuriturvallisuusviraston (CISA) mukaan on viisi pääasiallista menetelmää, joita kyberrikolliset käyttävät saadakseen aluksi pääsyn IT-ympäristöön. Näihin kuuluvat:

Yleisten sovellusten hyödyntäminen

Löytämällä ja hyödyntämällä yleisten toimisto-ohjelmistojen haavoittuvuuksia

Ulkopuolisten IT-palveluiden käyttö

Missä kolmannen osapuolen tarjoamat palvelut muodostavat riskipisteen, esimerkiksi pilvipalvelut

Kelvollisten tilien käyttö

Usein varastettujen tai murrettujen kirjautumistietojen avulla hakkeroiduista verkkosivustoista

Luottamuksen hyväksikäyttö

Hyökkääjä pääsee sisään tutun kautta, esimerkiksi kumppanin, jolla on pääsy yrityksen IT-järjestelmään tai -verkkoon

Verkkokalastelu

Hyvin yleinen tekniikka, joka tarkoittaa harhaanjohtavien sähköpostiviestien lähettämistä

- Inhimillinen tekijä

Sosiaalinen manipulointi

Verizonin Data Breach Investigation -raportin mukaan verkkourkinta on yleisin menetelmä alkuperäisissä kyberhyökkäyksissä, joissa 82 % murroista sisältää inhimillisen tekijän.

Näistä 60 % on verkkourkinnan tulosta, kuten sosiaalista manipulointia (ihmisten psykologista manipulointia, jotta he suorittavat toimia tai paljastavat luottamuksellista tietoa) saadakseen ihmiset paljastamaan arkaluonteista tietoa.

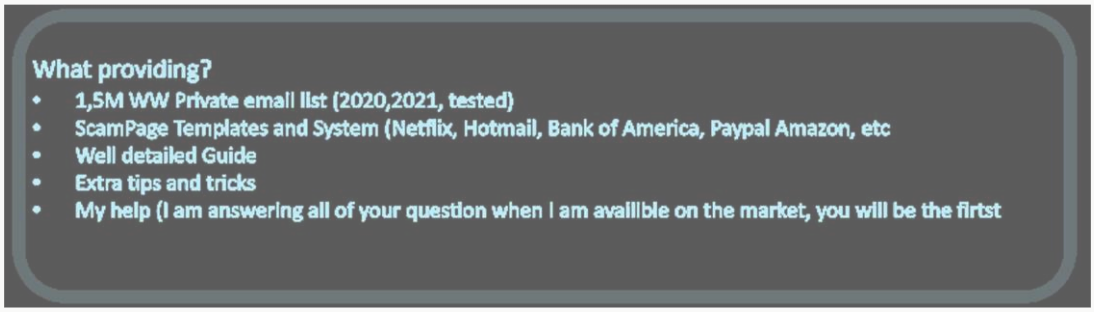
Taitava hakkeri voi suhteellisen helposti luoda haitallisen sovelluksen, joka asentuu käyttäjän tietokoneen taustalle huomaamattomasti sähköpostilinkin klikkauksen kautta ja luo niin sanotun takaoven. Tämä takaovi mahdollistaa hakkerin ottaa järjestelmän hallintaansa huomaamattomasti.

Nykyään kyberrikollisten ei tarvitse edes nähdä erityistä vaivaa näissä hyökkäyksissä.

"Dark Webissä", internetin osassa, joka vaatii erityisiä ohjelmia pääsyyn, on markkinapaikkoja, joissa rikolliset voivat ostaa valmiita verkkokalastelupaketteja.

Nämä paketit sisältävät kaiken väärennetyistä sähköpostiviesteistä harhaanjohtaviin maksusivuihin, joita voidaan käyttää tiedon varastamiseen.

Nämä paketit, jotka usein sisältävät väärennettyjä maksusivuja tunnetuille brändeille, ovat halpoja ja tekevät haitallisen kampanjan aloittamisesta helppoa. Alla on todellinen mainos Dark Webistä. (kuva 1)



Kuva 1

● Inhimillinen tekijä

Joitakin yleisimpiä menetelmiä

Tiedoston lataus

Haitallisen koodin luojat käyttävät usein temppuja saadakseen sinut lataamaan haitallisia tiedostoja. Tämä voi tapahtua sähköpostiviestin liitteen tai linkin kautta, joka näyttää olevan kuitti, maksuvahvistus tai lasku. Sinua voidaan pyytää avaamaan liitetiedosto toimituksen viimeistelemiseksi tai maksun vastaanottamiseksi.

Sähköpostihuijaukset

Sähköposti on nykyään työväline, jota käytetään organisaatioissa ympäri maailmaa – mutta se on myös hyökkäysvektori kyberrikollisille. Jotkut haitalliset sähköpostiviestit on helppo tunnistaa huonon oikeinkirjoituksen tai tuntemattomien lähettäjäosoitteiden vuoksi. Nykyään kyberrikolliset käyttävät generatiivista tekoälyä luodakseen uskottavia, täydellisesti muotoiltuja ja uskottavia viestejä, jotka lähetetään tuhansille vastaanottajille sähköpostitse. On myös yleistä, että nämä sähköpostiviestit väärennetään näyttämään siltä, että ne tulevat tunnetulta ja luotettavalta yritykseltä tai tutulta henkilöltä. Haittaohjelmat voivat myös hakkeroida sähköpostitilejä ja käyttää niitä roskapostin lähettämiseen koko yhteystietoluetteloon. Deloitten mukaan 91 % kyberhyökkäyksistä alkaa sähköpostin kautta, jossa haitallisia linkkejä ja liitetiedostoja käytetään avaamaan takaovia kyberrikollisille.

Microsoft Office -tiedostot

Microsoft Office, joka on tunnettu tuottavuustyökalujen paketti, sisältää tehokkaan ohjelmointikielen, jonka avulla käyttäjät voivat luoda edistyneitä toimintoja. Rikolliset voivat kuitenkin käyttää tätä ohjelmointikieltä väärin kehittääkseen haitallisia skriptejä, jotka asentavat haittaohjelmia tai suorittavat muita vahingollisia toimintoja. Näitä avattaessa saa yleensä varoituksen.

Siirrettävät tallennuslaitteet

Toinen menetelmä haittaohjelmien levittämiseen on siirrettävien tallennuslaitteiden, kuten USB-muistien ja ulkoisten kiintolevyjen kautta. Kun nämä saastuneet laitteet liitetään tietokoneeseesi, haittaohjelma voi asentua automaattisesti.

Sovelluksen asennus

Joskus haittaohjelma voi livahtaa järjestelmääsi muiden ohjelmien mukana, joita lataat, erityisesti verkkosivustoilta, jotka eivät ole sovellusten virallisia toimittajia tai tiedostoista, joita jaetaan yksityisissä niin sanotuissa P2P-verkoissa (peer-to-peer).

Verkkosivustot ja selaimet

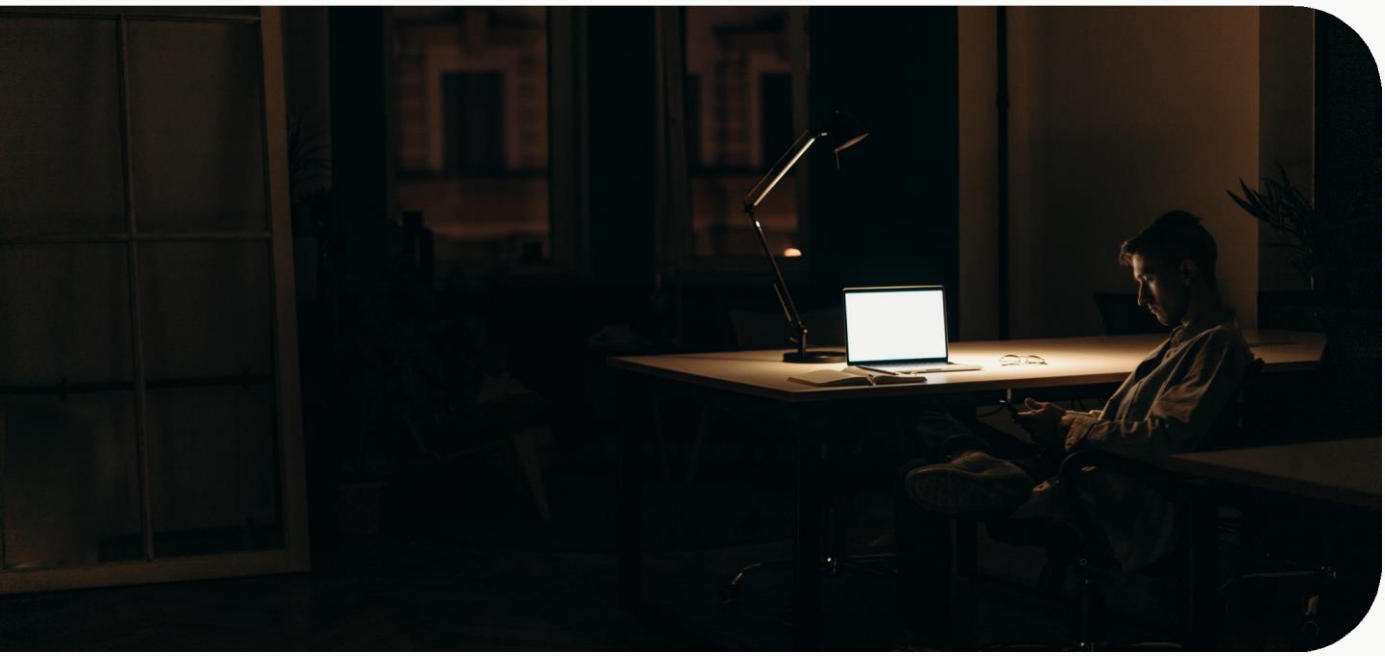
Vierailu tietyillä verkkosivustoilla voi johtaa kyberhyökkäyksiin, joko siksi, että verkkosivusto itsessään on haitallinen tai siksi, että laillinen sivusto on hakkeroitu. Nämä hyökkäykset hyödyntävät selaimesi haavoittuvuuksia. Siksi on erittäin tärkeää päivittää kaikki ohjelmistot uusimpaan versioon, erityisesti selain ja poistaa käyttämättömät selaimen lisäosat.

Näiden menetelmien ymmärtäminen on tärkeä askel tietokoneesi ja henkilökohtaisten tietojesi suojaamisessa kyberuhkia vastaan. Säännölliset päivitykset, varovaisuus latauksissa ja sähköpostiviesteissä sekä siirrettävien laitteiden ja sovellusten turvallinen käsittely ovat perusta tehokkaalle suojaukselle.

● Miten kyberhyökkäys tapahtuu?

Eri vaiheet

Tarkoituksenamme on valaista, miten yksi yleisimmistä tunkeutumisista voi tapahtua ja miten se toteutetaan. Käymme läpi tavallisen hyökkäyksen eri vaiheet ja miten hakkeri voi tunkeutua tietokoneeseesi ja IT-ympäristöösi. Antaaksemme käsityksen siitä, miten hyökkäys tapahtuu, selitämme alla, miten yksi yleisimmistä kyberhyökkäyksistä tapahtuu ja miten hakkerit pääsevät tietokoneeseesi ja IT-ympäristöösi.



Vaihe 1: Vekkokalasteluhyökkäys

Yleinen ensimmäinen askel hakkerille on suorittaa verkkokalasteluhyökkäys. Tämä tarkoittaa usein sähköpostiviestien lähettämistä, jotka näyttävät "aidoilta", sisältäen houkuttelevia tarjouksia tai kehotuksia, jotka herättävät vastaanottajan uteliaisuuden. Kun vastaanottaja klikkaa viestissä olevaa linkkiä tai liitettä, aktivoituu pieni ohjelma, joka ilman vastaanottajan tietämystä käynnistää useita prosesseja tietokoneessa ja luo takaoven käyttäjän tietokoneeseen. Muutaman sekunnin kuluessa klikkauksesta hakkerille muodostuu pysyvä pääsy.

Vaihe 2: Sisäisen IT-ympäristön tutkiminen

Kun hakkeri on saanut pääsyn tietokoneeseen ja järjestelmään, hän käyttää käyttäjän käyttöoikeuksia etsiäkseen muita tietokoneita verkosta. Tämä voi tarkoittaa erilaisten digitaalisten työkalujen avulla jaettujen tiedostojen, sovellustietokoneiden, tietokanta- ja verkkopalvelimien etsimistä ja joskus jopa tulostimen verkkokäyttöliittymän tutkimista, mikä voi antaa arvokasta tietoa lisätunkeutumisia varten.

Vaihe 3: Tulostimen hyväksikäyttö

Tulostimet ovat usein haavoittuvia kohtia, jotka jäävät huomiotta. Hakkeri voi hyödyntää tulostimen turvallisuuspuutteita, kuten oletussalasanoja tai salasanan puuttumista, saadakseen pääsyn korkeampiin käyttöoikeuksiin. Hakkeri voi selata tulostimen verkkosovellusta ja päästä käsiksi kokoonpanoasetuksiin.

Manipuloimalla tulostimen asetuksia hakkeri voi olla vuorovaikutuksessa muiden verkon järjestelmien kanssa ja käyttää digitaalisia työkaluja siepatakseen sähköpostiosoitteita, salasanoja ja käyttäjätilejä sekä muita verkon tietoja, jotka voivat olla arvokkaita jatkotunkeutumisia varten.

Monien tulostimien oletusasetuksena on sallia pääsy verkkosovellukseen ilman salasanaa ja jos salasana on olemassa, monet käyttäjät unohtavat vaihtaa oletussalasanan, joka on helposti löydettävissä käyttöoppaista verkossa. Jos hakkeri saa pääsyn tulostimeen, jolla on toiminto skannata asiakirjoja ja lähettää niitä sähköpostitse, tätä voidaan käyttää haitallisiin tarkoituksiin.

Jotta tulostin voisi lähettää sähköpostiviestejä, se on ehkä konfiguroitu käyttäjätilillä, jolla on korkeammat käyttöoikeudet kuin keskimääräisellä käyttäjällä. Hakkerit, joilla on digitaalisia työkaluja tämän tilin salasanan selvittämiseksi, voivat sitten käyttää sitä väärin suorittaakseen lisätunkeutumisia verkkoon tai kerätäkseen luottamuksellista tietoa.

Vaihe 4: Laajentaa pääsyä

Päästyään korkeampiin käyttöoikeuksiin hakkeri alkaa tutkia IT-ympäristöä perusteellisemmin. Tämä voi tarkoittaa tiedostojen ja arkaluonteisten tietojen etsimistä sekä järjestelmänvalvojatilejä, joita voidaan käyttää IT-ympäristön täydelliseen hallintaan.
Järjestelmällisesti ja metodisesti hakkeri etsii kaiken saatavilla olevan tiedon ja ennemmin tai myöhemmin löytää tietoja, usein vanhoista varmuuskopioista tai vanhoista jaetuista tiedostoista, järjestelmänvalvojan tilin ja siihen liittyvän salasanan.

Nykyisen IT-ympäristön yleiskuvan puute ja se, mitä aikaisemmat IT-järjestelmänvalvojat loivat ja eivät koskaan poistaneet, tekee organisaatiosta haavoittuvan kyberhyökkäyksille. Varastetun järjestelmänvalvojan salasanan avulla hakkeri saa nyt täyden pääsyn koko IT-ympäristöön, tiedostoihin, tileihin, taloustietoihin ja paljon muuhun..

Vaihe 5: Täydellinen haltuunotto

Viimeisessä vaiheessa hakkerilla on täysi hallinta IT-ympäristöstä ja hän voi tehdä mitä haluaa. Tätä pääsyä voidaan käyttää tietojen salaamiseen niin sanotussa kiristyshyökkäyksessä, mikä pakottaa yrityksen maksamaan lunnaat saadakseen takaisin pääsyn tietoihinsa.

Hakkeri voi myös käyttää IT-ympäristön resursseja laittoman tiedon levittämiseen tai jakamiseen internetissä sekä haittaohjelmien levittämiseen.

Nyt hakkerilla on täysi pääsy ja hän voi kirjautua sisään hallinnollisilla oikeuksilla koko organisaatioon ja salata koko IT-ympäristön tai osia siitä.

Tämä osoittaa, kuinka kehittyneitä ja haitallisia kyberhyökkäykset voivat olla ja korostaa ennakoivien turvatoimien tärkeyttä IT-ympäristön suojaamiseksi.

Täydellisen pääsyn avulla koko IT-ympäristöön ja tietokoneeseen, joka hallitsee turvallisuutta, hakkeri voi tehdä käytännössä mitä tahansa, esimerkiksi käyttää työkalua ladatakseen kaikki käyttäjä- ja tilitiedot. Kaikki salatut salasanat murretaan työkalulla, joka tekee miljardeja arvauksia sekunneissa.

● Miten suojaudun?

Miten voin ennaltaehkäistä?

IT-ympäristön suojaaminen kyberhyökkäyksiltä on yksi kriittisimmistä haasteista, joita organisaatiot kohtaavat nykyajan digitaalisessa aikakaudessa.

Kyberuhkien määrän jatkuvasti kasvaessa on yhä tärkeämpää toteuttaa vahvoja turvatoimia herkän tiedon suojaamiseksi. Tehokas strategia sisältää edistyneen teknologian, kuten palomuurien ja virustorjuntaohjelmien käytön, jotka ovat avainasemassa mahdollisten uhkien tunnistamisessa ja torjumisessa.

Verkon jatkuva valvonta on ratkaisevan tärkeää epäilyttävien toimintojen nopeaan havaitsemiseen ja niihin reagointiin. On myös tärkeää olla aliarvioimatta käyttäjien koulutuksen arvoa. Informoimalla käyttäjiä uusimmista kyberuhkista ja niiden välttämisestä voidaan monet turvallisuusongelmat estää jo alkuvaiheessa. Näiden menetelmien yhdistelmä tarjoaa vahvan perustan herkän tiedon tehokkaalle suojaamiselle ja tietomurtojen sekä muiden turvallisuuteen liittyvien tapausten riskin minimoimiselle.

Alla on joitakin erilaisia järjestelmiä ja ratkaisuja sekä toimenpiteitä, jotka varmistavat organisaation kyberturvallisuuden. Tietysti toiminnan koko on merkityksellinen sen suhteen, minkä tyyppiseen järjestelmään tai ratkaisuun katsotaan olevan varaa, mutta kyberuhkilta suojautumisen tarkastelu ja pohdinta on tärkeää kaikille.

Järjestelmät ja ratkaisut

Microsoft 365

Microsoft 365 tarjoaa kattavan suojan kyberuhkien ennaltaehkäisyyn, havaitsemiseen ja hallintaan. Tähän suojaan sisältyvät edistyneet tietojenkalastelun estotoiminnot Microsoft Defenderissä, jotka varoittavat mahdollisista sähköpostihuijauksista ja epätavallisista merkeistä lähettäjän osoitteissa.

Microsoft Defender for Office 365 toimii yhtenäisenä turvallisuusalustana, joka havaitsee automaattisesti haitallisen ja epäilyttävän sisällön useissa sovelluksissa, mukaan lukien sähköposti ja Microsoft Teams. OneDrive for Business tarjoaa suojan kiristyshyökkäyksiä vastaan sallimalla tiedostojen aiempien versioiden palauttamisen. Nämä turvallisuustoiminnot ovat ratkaisevan tärkeitä organisaatioiden suojaamiseksi monenlaisilta kyberuhkilta.

Verkon segmentointi Verkon segmentointi on tehokas strategia organisaation kyberturvallisuuden parantamiseksi. Tämä menetelmä tarkoittaa verkon jakamista pienempiin osiin tai segmentteihin. Näin tekemällä voidaan tehokkaasti rajoittaa kyberturvallisuushyökkäyksen aiheuttamia vahinkoja, koska hyökkääjän, joka onnistuu tunkeutumaan yhteen osaan verkkoa, on vaikea levitä muihin osiin. Jokaisella verkon segmentillä voi olla omat turvallisuussäännöt ja pääsynvalvonta. Tämä mahdollistaa turvallisuustason räätälöinnin verkon jokaiselle osalle sen herkkyyden ja tarpeiden mukaan.

Riippumatta siitä, miten hakkerit pääsevät tietokoneeseesi, verkon segmentointi on yksinkertainen mutta erittäin tehokas tapa rajoittaa sitä, kuinka paljon verkostasi hakkeri voi päästä käsiksi, jos he pääsevät ympäristöösi.

Asenna EDR- ja XDR-tekniikkaa EDR- (Endpoint Detection and Response) ja XDR-tekniikka (Extended Detection and Response) ovat järjestelmiä, jotka valvovat paljon enemmän kuin perinteiset virustorjuntaohjelmat ja tarjoavat kehittyneitä toimintoja kyberuhkien torjumiseksi.

EDR-tekniikka keskittyy yksittäisten laitteiden, kuten tietokoneiden, palvelimien ja mobiililaitteiden, valvontaan ja suojaamiseen. Järjestelmä valvoo jatkuvasti jokaista laitetta reaaliajassa, kerää ja analysoi tietoja tunnistaakseen ja reagoidakseen epäilyttävään käyttäytymiseen ja haitalliseen toimintaan. Se pystyy nopeasti löytämään ja käsittelemään epäilyttävät toiminnot sekä pysäyttämään tietoturvaongelmat.

XDR-tekniikka kattaa laajemman näkemyksen kyberturvallisuudesta integroimalla tietojen keräämisen, siirron ja mittaamisen tietokoneista, mobiililaitteista, verkoista ja pilviympäristöistä. XDR:n kyky kerätä, yhdistää ja analysoida tietoja eri tietoturvakerroksista mahdollistaa nopeamman kehittyneiden kyberuhkien havaitsemisen ja niihin reagoinnin. Järjestelmä tarjoaa keskitetyn näkyvyyden tietoturvatilanteesta ja erilaisten ennaltaehkäisevien turvatoimien automatisoinnin.

Jokaisen organisaation tulisi harkita EDR- ja XDR-tekniikoiden käyttöä. Molemmat tekniikat ovat välttämättömiä tehokkaan kyberturvallisuusstrategian kehittämiseksi. Molemmat käyttävät mukautettua kyberuhkien havaitsemista ja tekoälyteknologiaa tunnistaakseen ja vastatakseen uhkiin automaattisesti ennen kuin ne voivat vahingoittaa organisaatiota.

“91%

kaikista kyberhyökkäyk-sistä alkaa sähköpostin kautta, jossa haitallisia linkkejä ja liitetiedostoja käytetään takaovien avaamiseen kyberrikollisille.

Lähde: Deloitte

Käytä verkon havaitsemis- ja reagointityökaluja

Network Detection and Response (NDR) on erittäin tehokas järjestelmä kyberturvallisuuden alalla. Järjestelmä toimii valvomalla verkkoliikennettä kyberturvallisuusuhkien tunnistamiseksi ja niihin reagoimiseksi. NDR-ratkaisut käyttävät edistyneitä analyyttisiä menetelmiä, kuten tekoälyä (AI) ja koneoppimista (ML), rakentaakseen malleja normaalista verkkokäyttäytymisestä. Jatkuvan verkkoliikenteen analyysin avulla nämä järjestelmät voivat havaita poikkeavaa tai haitallista liikennettä, jonka muut turvallisuustyökalut voivat jättää huomiotta. Järjestelmä tunnistaa erilaisia uhkia, mukaan lukien tuntematon haittaohjelma, kohdennetut hyökkäykset, sisäpiirihyökkäykset ja jopa käyttäjien riskialtis käyttäytyminen.

Käytä vähimpien oikeuksien periaatetta

Vähimpien oikeuksien periaatteen toteuttaminen on olennainen osa tehokasta kyberturvallisuusstrategiaa. Tämä periaate tarkoittaa, että jokaisella käyttäjällä, prosessilla tai ohjelmalla on pääsy vain niihin resursseihin ja oikeuksiin, jotka ovat ehdottoman välttämättömiä heidän tehtäviensä tai toimintojensa suorittamiseksi. Rajoittamalla pääsyä vain välttämättömään vähennetään tahattomien tai tahallisten tietomurtojen ja kyberhyökkäysten riskiä.

Jotta tämä voitaisiin toteuttaa tehokkaasti, organisaatioiden tulisi suorittaa perusteellinen analyysi käyttäjärooleista ja niiden pääsytarpeista määrittääkseen sopivan pääsytason jokaiselle käyttäjälle tai roolille. Vähimpien oikeuksien periaate on kulmakivi Zero Trust -tietoturvamallissa, jossa jokainen pääsypyyntö tarkistetaan ja vahvistetaan riippumatta siitä, mistä se tulee.

AVOKI

Vahvista ja rajoita pääsyä kriittiseen järjestelmäkonfiguraatioon

Vahvistaa ja rajoittaa pääsyä kriittiseen järjestelmäkonfiguraatioon on tärkeä askel kyberturvallisuuden parantamiseksi. Tämä tarkoittaa useiden toimenpiteiden toteuttamista luvattoman pääsyn riskin vähentämiseksi ja arkaluonteisten tietojen suojaamiseksi.

1. Vaadi vahvaa todennusta

Käytä vahvoja todennusmenetelmiä, kuten monivaiheista todennusta (MFA), suojataksesi verkkokäyttöliittymät ja muut kriittiset järjestelmät. Tämä on erityisen tärkeää palveluille, jotka ovat käytettävissä ulkoisesti, kuten VPN-palvelut.

2. Sammuta tarpeettomat palvelut ja segmentoi verkko

On tärkeää poistaa käytöstä tarpeettomat palvelut ja segmentoida verkko rajoittaaksesi pääsyä kriittisiin järjestelmiin. Jakamalla verkon pienempiin osiin voit luoda hyviä tietoturvakäytäntöjä ja -kontrolleja jokaiselle segmentille, mikä estää hyökkääjiä liikkumasta vapaasti verkossa.

3. Ohjelmistojen säännölliset päivitykset

Jatkuvat ohjelmistopäivitykset ja parannukset ovat välttämättömiä tunnettujen haavoittuvuuksien suojaamiseksi. Säännöllinen tietoturvapäivitysten asennus auttaa sulkemaan tietoturva-aukkoja, joita hyökkääjät voivat hyödyntää.

4. Rajoita fyysistä pääsyä verkkoliitäntöihin

On tärkeää rajoittaa fyysistä pääsyä verkkoliitäntöihin estääksesi luvattoman pääsyn ja mahdolliset tunkeutumiset.

5. Käytä tiedostojen ja laitteiden salausta

Tietojen salaaminen sekä levossa että siirron aikana suojaa arkaluonteisia tietoja luvattomalta lukemiselta.

6. Asenna ja käytä tietoturvaohjelmistoja

On tärkeää, että sinulla on ajan tasalla oleva tietoturvaohjelmisto, kuten virustorjunta ja palomuurit, suojautuaksesi erilaisilta kyberhyökkäyksiltä.

7. Lokitus ja valvonta

Ota käyttöön lokitus- ja valvontatyökaluja, jotta voit seurata ja analysoida järjestelmän epäilyttäviä toimintoja. Näiden toimenpiteiden toteuttaminen voi auttaa organisaatioita luomaan turvallisemman ja kestävämmän IT-ympäristön, joka on paremmin varustettu kestämään ja reagoimaan kyberuhkiin.

Käytä monivaiheista todennusta (MFA)

Monivaiheisen todennuksen (MFA) käyttö on tärkeä strategia kyberturvallisuuden vahvistamiseksi. MFA käyttää monikerroksista menetelmää tietojen ja sovellusten suojaamiseksi vaatimalla käyttäjää esittämään yhdistelmän kahta tai useampaa todennuskertaa henkilöllisyytensä vahvistamiseksi kirjautumisen yhteydessä. Tämä lisää turvallisuutta merkittävästi, koska vaikka yksi todennuskerta, kuten salasana, tulisi hakkerin tietoon, luvaton käyttäjä ei pysty täyttämään toista todennusvaatimusta eikä näin ollen pääse fyysiseen tilaan, laitteeseen, verkkoon tai IT-ympäristöön.

MFA on erityisen tehokas suojaamaan erilaisilta kyberhyökkäyksiltä, mukaan lukien tietojenkalastelu, sosiaalinen manipulointi ja salasanojen arvaushyökkäykset. Se suojaa myös hyökkääjien kirjautumisilta, jotka hyödyntävät heikkoja tai varastettuja tietoja.

Kolme yleistä todennuskertaa, joita käytetään MFA:ssa, ovat jotain, jonka tiedät (esim. salasana tai PIN-koodi), jotain, joka sinulla on (esim. älypuhelin tai turvatunniste) ja jotain, mikä olet (esim. biometriset tiedot, kuten sormenjälki tai kasvojentunnistus).

Vaatimalla todisteita kahdesta tai useammasta näistä kategorioista luodaan vahvempi turvallisuuseste.

On tärkeää ottaa MFA käyttöön organisaatiossasi, ei vain ulkoisille palvelimille, vaan myös sisäiselle järjestelmänvalvojan pääsylle. Rajoittamalla pääsyä kriittisiin järjestelmiin MFA:n avulla voit tehokkaasti vähentää riskiä, että hakkerit pääsevät käsiksi arkaluonteisiin tietoihin tai kriittisiin järjestelmiin.

Toteuta kalastelutestit

Kalastelutestit, joita suorittavat eettiset hakkerit, ovat erittäin tehokas menetelmä yrityksen IT-infrastruktuurin heikkouksien tunnistamiseen ja korjaamiseen. Tämä prosessi sisältää simuloidun kyberhyökkäyksen, jolla löydetään haavoittuvuuksia verkostoista ja järjestelmistä. Tunnistamalla proaktiivisesti heikkoudet, joita hakkerit voivat hyödyntää, yritys voi vähentää onnistuneiden tietomurtojen tai -tapahtumien riskiä.

Kalastelutestit antavat objektiivisen arvion järjestelmän turvallisuusvalvonnasta ja paljastavat usein vakavia haavoittuvuuksia, jotka automaattiset skannaukset ovat saattaneet ohittaa. Testit voidaan luokitella eri lähestymistapoihin, jotka tarjoavat erilaisia näkemyksiä riippuen siitä, kuinka paljon tietoa eettisellä hakkerilla on järjestelmästä.

Testit eivät ole pelkästään tekninen tarkastus, vaan prosessi, jota on kehitettävä ja jatkuvasti parannettava ajan myötä.

Tunkeutumistestit ovat välttämättömiä kypsälle kyberturvallisuusstrategialle, eikä yritysten, jotka haluavat suojata kriittistä infrastruktuuriaan kyberuhilta, tulisi laiminlyödä niitä.

Microsoft Secure Score

Microsoft Secure Score on työkalu, jolla mitataan organisaation turvallisuustilannetta. Tulokset vertaavat organisaation turvallisuustasoa alan standardeihin ja Microsoftin turvallisuussuosituksiin. Korkeampi pistemäärä osoittaa paremman turvallisuuden, ja pisteet auttavat mittaamaan edistystä ajan myötä. Työkalu antaa suosituksia organisaation turvallisuuden parantamiseksi, keskittyen heikkouksien tunnistamiseen ja korjaamiseen parannettavissa olevilla alueilla. Työkalu auttaa arvioimaan turvallisuutta eri alueilla, kuten identiteetti, laitteet, tiedot, sovellukset ja infrastruktuuri.

> Jopa **70%** kyberhyökkäysten riskeistä voidaan vähentää kouluttamalla käyttäjiä.

Lähde: Aberdeen Group

Vertaamalla organisaation tilannetta ajan myötä ja muihin organisaatioihin voidaan luoda suunnitelma tietoturvan parantamiseksi. Microsoft Secure Score -pisteet voivat toimia perustana nykyisen tietoturvatilanteen raportoinnille sekä parannuksille liiketoimintajohdolle ja toimia pohjana tietoturvastrategian muutoksille.

Työkalu on integroitu muihin Microsoft-tuotteisiin ja voi myös ottaa huomioon, kun kolmannen osapuolen ratkaisua on käytetty suositeltujen toimenpiteiden hallintaan. Tämä mahdollistaa edistymisen selkeyttämisen, jotta organisaation IT-ympäristöä voidaan suojata paremmin.

Käyttäjien koulutus

Vaikka laitteisto- ja ohjelmistosuojaukset ovat tärkeitä kybertietoturvan osa-alueita, ne eivät yksinään pysty estämään kaikkia tietojenkalasteluhyökkäyksiä.

Aberdeen Groupin tutkimuksen mukaan tietoturvatietoisuuden koulutus voi vähentää riskejä 45–70 %, mikä korostaa säännöllisen ja tehokkaan koulutuksen merkitystä kybertietoturvan lisäämisessä käyttäjien keskuudessa.

Toinen Proofpointin tutkimus osoitti, että yritykset, jotka toteuttivat tietoturvatietoisuuden koulutusta, näkivät jopa 40 %:n vähennyksen käyttäjien klikkaamien haitallisten linkkien määrässä.

Tämä korostaa käyttäjien jatkuvan muistuttamisen riskeistä sekä kuukausittaisen koulutuksen tai kyberturvallisuustiedon tarjoamisen merkitystä työntekijöille.

Palomuuri

Palomuuri on olennainen osa organisaation verkkotietoturvaa ja toimii esteenä suojaten verkkoa luvattomalta pääsyltä ja kyberuhkilta.

Se voi olla joko fyysinen laite (laitteistopalomuuri) tai ohjelmisto (ohjelmistopalomuuri) ja on suunniteltu valvomaan ja hallitsemaan saapuvaa ja lähtevää verkkoliikennettä ennalta määriteltyjen tietoturvasääntöjen perusteella.

Palomuurit sijoitetaan usein Internetin ja yksityisen verkon väliin, yleensä reitittimen yhteyteen tai sisäänrakennettuna. Ne valvovat liikennettä verkkojen välillä ja soveltavat tietoturvasääntöjä estääkseen ei-toivotun tai haitallisen liikenteen pääsyn sisäisiin järjestelmiin. On olemassa ohjelmistopalomuureja, jotka asennetaan suoraan tietokoneisiin tai laitteisiin tarjoamaan suojaa yksilöllisellä tasolla.

Palomuurin päätehtävä on suodattaa verkkoliikennettä ja estää luvattomat yritykset päästä järjestelmään tai verkkoon. Tämä sisältää tiettyjen tietojenkalasteluhyökkäysten ja muiden kyberuhkien estämisen.

Mutta palomuureilla voi olla rajoituksia, erityisesti kun on kyse kehittyneemmistä tietojenkalasteluyrityksistä, jotka kohdistuvat suoraan käyttäjiin saadakseen heidät paljastamaan arkaluonteisia tietoja.

Säännöllinen palomuurisääntöjen ja -kokoonpanojen tarkistus ja päivittäminen on avain tehokkaan verkkotietoturvan ylläpitämiseen.

Backup – Varmuuskopiointi

Varmuuskopiointistrategian toteuttaminen, joka kattaa useita varmuuskopioiden sukupolvia, on kriittinen osa vahvaa kybertietoturvastrategiaa.

Kyberuhat, kuten kiristysohjelmat ja virukset, muodostavat vakavia riskejä tietojen eheydelle, ja varmuuskopiot toimivat ratkaisevana turvatoimena organisaation arvokkaan tiedon suojaamiseksi. Kun kyberhyökkäys tapahtuu, vaikutukset voivat olla katastrofaalisia, jolloin kriittinen tieto joko lukitaan tai tuhotaan.

Varmuuskopion, eli backupin, avulla organisaatio voi tehokkaasti palauttaa digitaalisen tietonsa ajankohdasta ennen hyökkäystä. Tämä on erityisen arvokasta tilanteissa, joissa myös viimeisin varmuuskopio on vaarantunut.

Useiden sukupolvien varmuuskopiointistrategian omaksuminen ei ole pelkästään vakuutus tietojen menettämistä vastaan kyberhyökkäysten vuoksi, vaan myös ratkaiseva osa liiketoiminnan jatkuvuuden ja operatiivisen vakauden ylläpitämisessä.

Se on erittäin tärkeä toimenpide, joka varmistaa, että organisaation digitaaliset omaisuudet pysyvät suojattuina ja saatavilla, jopa yhä kehittyneempien kyberuhkien maailmassa.

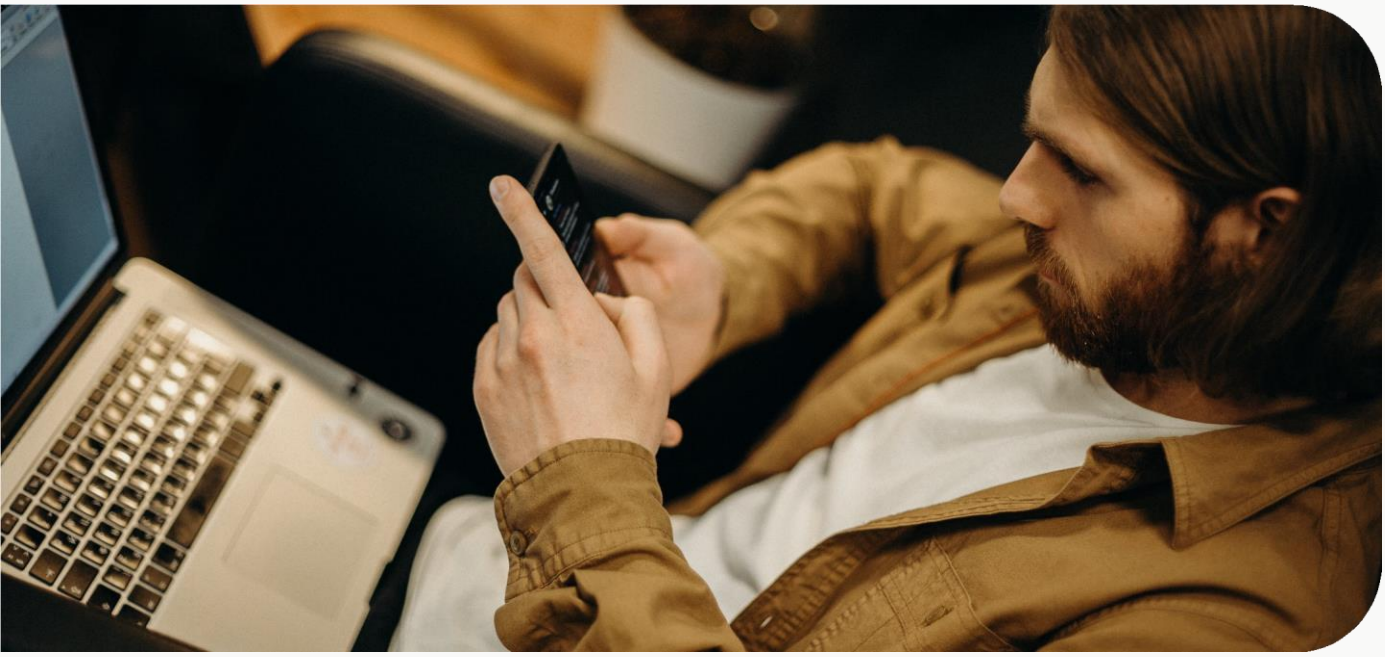
> Kyberhyökkäyksen vaikutukset voivat aiheuttaa suuria seurauksia yhteiskunnan kannalta tärkeille toiminnoille ja kriittisille IT-järjestelmille ja kyberhyökkäysten suorat ja epäsuorat kustannukset arvioidaan olevan miljardiluokkaa.

Lähde: SUPO - Suojelupoliisi

● **Meidän ainutlaatuinen tarjontamme**

Miten ratkaisumme suojaa kyberuhkilta

Vastauksena kyberturvallisuuden monimutkaisuuteen olemme kehittäneet kaksi palvelua, jotka yhdessä hyödyntävät Microsoftin XDR-ratkaisua (Extended Detection and Response).



Microsoft XDR on tietoturvajärjestelmä, joka tarjoaa kattavan ja integroidun kuvan tietoturvauhkista koko organisaation IT-ympäristössä.

Tämä sisältää verkot, laitteet, sovellukset ja pilvipalvelut. Yhdessä Microsoft XDR:n kanssa olemme vieneet kyberhyökkäysten valvonnan askeleen pidemmälle. Tekoälyn ja älykkäiden raportointi- ja analysointityökalujen avulla IT-ympäristöäsi valvotaan.

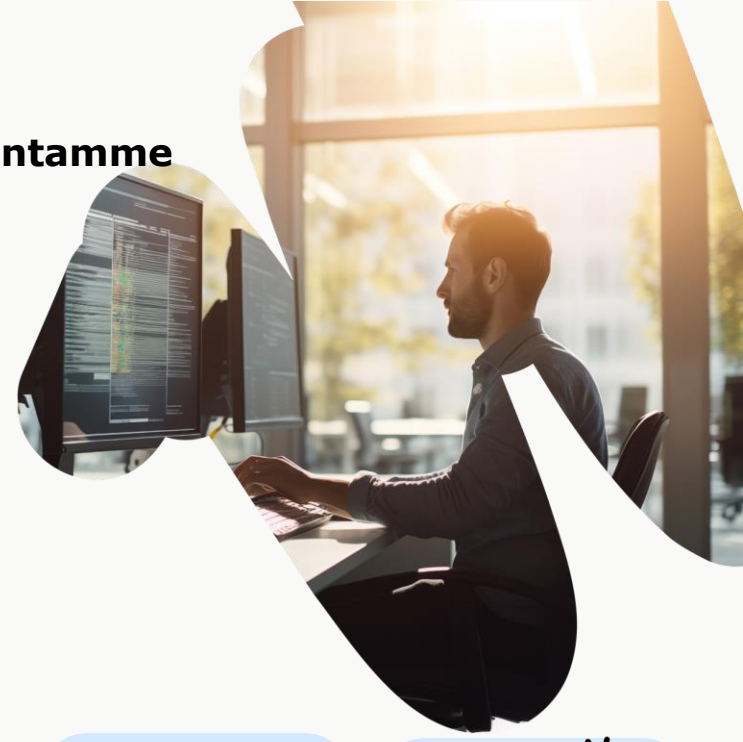
Microsoft XDR tarjoaa monia toimintoja, mutta tavalliselle käyttäjälle se voi tuntua melko vaikealta navigoida. On paljon asetuksia, joita voidaan tehdä ja joskus ei ehkä ole varma, mitä kaikki tekee tai mihin ne on tarkoitettu.

Palvelumme tarjoaa tehokkaan ratkaisun tähän, ja olemme kehittäneet kaksi palvelua, joita tarjoamme asiakkaillemme. Hoidamme asetukset Microsoft-ympäristössänne ainutlaatuisten tarpeidenne ja käyttötapojenne perusteella.

AVOKI

● **Meidän ainutlaatuinen tarjontamme**

X-One Cloud Security (Ruotsissa)



Tällä ainutlaatuisella ratkaisulla takaamme paitsi räätälöidyn tietoturvan yrityksesi erityistarpeiden perusteella, myös automaattisen valvonnan, joka pitää käyttäjäsi ja tietosi suojattuina.

Tietoturva tekoälyn avulla: Apex Insight

Oma kehittämämme valvonta-agentti turvaa yrityksesi ja käyttäjäsi tekoälyn avulla. Kehittyneiden algoritmien avulla Apex Insight tunnistaa riskialttiit ja uhkaavat käyttäytymismallit ja estää käyttäjätilit. Kun asetettu riski- tai uhkakynnys ylittyy, X-ONE Cloud Security hälyttää tietoturva-asiantuntijan ja asiakkaana saatte analyysin jälkeen täydellisen analyysiraportin tapahtuneesta.

Yrityksesi digitaalisten käyttötapojen ja käyttäytymismallien analyysi

Varmistaa yrityksesi eheyden ja käyttäytymismallit tarkistamalla kirjautumistiedot ja luomalla ehdollisia käyttöoikeussääntöjä. Riippuen siitä, miten tietoturvataso asetetaan, voidaan sallia, rajoittaa tai estää pääsy. Estosäännöt päivitetään dynaamisesti ajankohtaisen ympäristötiedon perusteella.

Palveluiden tilan valvonta Tennant Healthin avulla

Valvomme Microsoft-pilvipalveluiden tilaa, mukaan lukien Office verkossa, Microsoft Teams, Exchange Online ja Microsoft Dynamics 365. Jos pilvipalvelussa on ongelmia, ilmoitamme siitä teille ja voimme selvittää, onko kyseessä tunnettu ongelma, johon on jo ratkaisu työn alla, ennen kuin soitatte tukeen tai käytätte aikaa vianmääritykseen.

Yksityiskohtaiset näkemykset, räätälöity IT:lle ja päätöksentekijöille kvartaaleittain

Tarjoamme jatkuvia analyysejä, päivityksiä ja muutoksia uusien uhkien ja ohjeiden valossa. Tämä siksi, että asiakkaana voit tuntea olosi turvalliseksi suojauksen toimivuuden suhteen ja saada perustan päätöksille, jos jotain tarvitsee muuttaa lisääntyneen uhkakuvan tai yrityksen IT-ympäristön käyttöoikeuksia koskevan IT-politiikan päivityksen vuoksi.

X-ONE 365 Cloud Security yhdistää Microsoftin Secure Scoren Xiten kokemukseen ja asiantuntemukseen luodakseen vahvan 365-ympäristön. Tarjoamme jatkuvia analyysejä, päivityksiä ja muutoksia uusien uhkien ja ohjeiden valossa.

Esimerkkejä asetuksista, jotka sisältyvät:
Safe attachment policy: liitetiedostojen tarkistus sähköposteissa ja Teamsissa, **Safe links policy:** suojaus haitallisilta linkeiltä vähentääkseen tietojenkalastelun riskiä, **Antimalware policy**: epäilyttävien tiedostojen ja koodin karanteeni, **Antiphishing policy:** suojaus identiteettivarkauksilta ja tietojenkalastelulta, **Mobile policy:** mobiililaitteiden tietoturva ennen kuin saatu pääsy 365-ympäristöön.

X-One Endpoint Security / Premium (Ruotsissa)

X-ONE 365 Endpoint Security (EDR), edistynyt tietoturvapalvelu, joka perustuu Microsoft XDR:ään ja tarjoaa yrityksille uuden tason proaktiivista suojaa. Kattavan valvonnan ja reagoinnin sekä digitaalisten laitteiden, kuten tietokoneiden, matkapuhelimien ja tablettien, tehokkaan hallinnan avulla voit tuntea olosi turvalliseksi.

Yksityiskohtaisten tietoturvaraporttien ja Microsoft Defender for Endpoint -integraation avulla tämä palvelu tarjoaa kattavan suojamekanismin IT-järjestelmillenne. X-ONE 365 Endpoint Security tarjoaa jatkuvasti päivitetyn, proaktiivisen tietoturvaratkaisun.

Proaktiivinen suoja

Suojaa laitteesi proaktiivisella suojauksella

Valvonta

Jatkuva haitallisten toimintojen valvonta laitteilla

Näkemykset

Yksityiskohtaiset näkemykset, räätälöity IT:lle ja päätöksentekijöille kvartaaleittain

Sofistikoitu valvonta

Valvomalla Microsoft Defenderiä, X-ONE 365 Endpoint Security (Ruotsissa) tunnistaa tietokoneet, joilla on riskialtista käyttäytymistä ja mahdollisia viruksia, sekä varmistaa proaktiivisen suojauksen.

Automaattiset hälytykset

Kun palvelu havaitsee riskin tai uhan, hälytetään tietoturvateknikko, joka voi ryhtyä asianmukaisiin toimenpiteisiin. Kun palvelu havaitsee riskin, se hälyttää vastuullisen teknikon ja eristää automaattisesti altistuneen laitteen vähentääkseen leviämisriskiä.

Endpoint Security Premium -lisäosan avulla lisätään useita automaattisia toimenpiteitä leviämisen vähentämiseksi, kuten laitteiden eristäminen ja deaktivointi sekä SMS-hälytykset vastuuhenkilöille.

Defender Endpoint Hardening

X-ONE 365 Endpoint Securityn (Ruotsissa) käyttöönoton yhteydessä tehdään analyysi Microsoftin Exposure Scoren ja Xiten oman asiantuntemuksen perusteella. Tämän pohjalta asetetaan säännöt, jotka ovat tarpeen turvallisen ja käyttökelpoisen asiakas/palvelinympäristön saavuttamiseksi. Asetusten analysointi ja säätäminen on jatkuvaa työtä, joka sisältyy X-ONE 365 Endpoint Securityyn. Kun uusia uhkia ja ohjeita ilmenee, päivitämme myös ympäristöänne näiden edellytysten mukaisesti.

Tietoanalyysi

Jokaisen vahvistetun uhan kohdalla suoritetaan perusteellinen tietoanalyysi. Yksityiskohtainen raportti lähetetään asiakkaalle ja se sisältää tärkeitä tietoja, kuten tietokoneen nimen, riskin tunnistamisajankohdan, riskin tyypin ja tason sekä tietokoneen tilan.

Kvartaaliraportti

Kvartaaleittain saat raportin, joka sisältää yksityiskohtaista tietoa ympäristösi turvallisuudesta. Tämä raportti sisältää yrityksen altistuspisteet, mahdolliset heikkoudet käyttöjärjestelmissä ja sovelluksissa sekä yksityiskohtaiset asiakas/palvelintiedot.

● Lopuksi

Digitalisaation aikakausi

Lopuksi on tärkeää korostaa, että yrityksen tulisi olla tietoinen IT-ympäristönsä suojaamisen tärkeydestä kyberhyökkäyksiltä.

On ratkaisevan tärkeää toteuttaa vahvoja tietoturvatoimia. Tarkista suojauksenne tänään ja harkitse edistyneen teknologian, kuten EDR- ja XDR-tekniikan käyttöönottoa, jos niitä ei vielä ole IT-ympäristössänne.

Älä unohda, että säännöllinen tietoturvatietoisuuden koulutus ja kalastelutestit ovat tärkeitä riskien minimoimiseksi ja heikkouksien havaitsemiseksi ennen kuin hakkeri tekee sen. Ajattelutapaa, että se tapahtuu muille eikä minulle, on kyseenalaistettava ja kyse ei ole siitä, JOS minulle tapahtuu jotain, vaan MILLOIN. Varmista, että tietosi on suojattu ennen kuin on liian myöhäistä.