TIETOTURVAPALVELUT

SISÄLLYS

Tietoturvapalvelut yleisesti

Asiakkaan vastuulla on huolehtia sovellustensa, laitteistonsa ja henkilöstönsä tietoturvasta ja tietoturvakoulutuksesta. TNNet Oy tarjoaa kattavasti erilaisia tietoturvaan liittyviä lisäpalveluita, joita voi hankkia joko omina palveluinaan tai yhdessä muiden TNNetin palveluiden kanssa. Palveluiden skaala on hyvin laaja aina käyttäjien koulutuksesta tietoverkon tekniseen tietoturvaan asti.

Organisaation tietoturva on aina yhtä vahva kuin sen heikoin lenkki. Tyypillisesti on voitu ajatella, että riittää, kun käyttäjillä on antivirus asennettuna. Tietoturva ei kuitenkaan ole mikään yhden palvelun tai tuotteen kokonaisvaltainen ratkaisu, vaan tärkeintä on ns. kerrossuojautuminen.

Tietototurvapalveluissa hyödynnetään usein kolmannen osapuolen tuotteita (esimerkiksi Sophos, Symantec, Checkpoint, Netscout, Tenable), joissa myös osa datasta on kolmannen osapuolen hallussa. Huolehdimme oman tietoturvapolitiikkamme mukaisesti, että kaikki käytettävät kolmannet osapuolet vastaavat TNNetin tietoturvavaadetta. Kaikki data säilytetään mahdollisuuksien mukaan omassa laitesalissamme tai vähintään Euroopan sisällä. Jos data poistuu TNNetin laitesalista, tarkemmat ja ajankohtaiset tiedot datan sijaintiin ja tietoturvaan liittyen löytyvät tapauskohtaisesti valmistajan omilta sivustoilta tai palvelukuvauksista.

Laitteiden tietoturva (EDR ja XDR)

Laitteiden tietoturvapalvelut sisältävät tietoturvasovelluksia niin käyttäjien laitteille kuin palvelimillekin. Käyttäjän laitteilla tarkoitetaan henkilökohtaisia työkoneita (Windows ja Mac) sekä tabletteja ja puhelimia (Android ja iOS). Palvelimilla tarkoitetaan kaikkia palvelinkäyttöjärjestelmiä, kuten Windows Serverit ja Linux-jakelut. Myös käyttäjien tietokoneilla olevat Linuxit lasketaan palvelimiksi, vaikka ne olisivat työpöytäkäytössä.

Miten palvelu toimii

Huolehdimme siitä, että jokaisella asiakkaalla on tietoturvalliset politiikat, joita ylläpidämme säännöllisesti. Kun tuotteisiin tulee uusia ominaisuuksia, huolehdimme siitä, että ne tulevat käyttöön sellaisille laitteille, jotka ovat TNNetin määrittämien politiikkojen piirissä.

Asiakkaan ylläpitäjien on mahdollista tehdä TNNetin määrittämistä politiikoista klooneja, joihin voidaan asettaa yrityskohtaisia erityissääntöjä. Erityissäännöt voidaan erillispyynnöstä tehdä myös meidän toimestamme, mutta erityispolitiikkojen ylläpitäminen on aina asiakkaan vastuulla. TNNet vastaa siis vain omien keskitettyjen politiikkojensa ajantasaisuudesta.

Asiakkaan ylläpitäjillä on mahdollisuus käyttää itsepalveluportaalia kokonaisvaltaisesti lisenssien ja laitteiden hallintaan. Ongelmatilanteissa TNNetin tuki on aina saatavilla. Ratkaisemme useimmat ongelmat suoraan itse, mutta mikäli ongelma on laadultaan sellainen, että tarvitaan valmistajan tukea (esimerkiksi bugi sovelluksessa), hoidamme asioinnin veloituksetta valmistajan suuntaan.

Jos laitteella havaitaan tietoturvauhka, ohjelmistot pyrkivät poistamaan uhan automaattisesti ja jättävät siitä ilmoituksen asiakkaan ylläpitäjälle sekä tuotteen hallintaportaaliin. Ilmoitusten huomaaminen ja niihin reagoiminen on kuitenkin asiakkaan vastuulla. TNNet auttaa erillisillä työpyynnöllä myös laitteiden jälkitarkastuksessa ja ilmoitusten tulkitsemisessa, mikäli niihin tarvitaan apua. Tietoturvauhkien löytäminen, havaitseminen ja reagointi on mahdollista myös ostaa erillisenä lisäpalveluna. TNNetillä on siihen erikseen oma palvelunsa (MDR), joka on kuvattu myöhemmin tässä palvelukuvauksessa.

Lisensointi

Palvelu lisensoidaan tapauskohtaisesti joko laite- tai käyttäjäkohtaisesti. Jos kyseessä on laitekohtainen lisensointi, lisenssi kuluu jokaisesta laitteesta, jolle tuote on asennettu. Mikäli kyseessä on käyttäjäkohtainen laite, lisensointiperuste on palvelun piirissä olevalle laitteelle kirjautuneiden eri käyttäjätunnuksien lukumäärä kuitenkin niin, että käyttäjiä ei voi olla koskaan enempää kuin laitteita, mutta laitteita voi olla enemmän kuin käyttäjiä. Sovellettava lisensointimalli on kerrottu palvelun tarjouksella ja/tai sopimuksella.

TNNetin laskutusperuste on aina valmistajan hallintaportaalin raportoima lisenssimäärä. Kun lisensoitavia kohteita lisätään, lisenssimäärä päivittyy automaattisesti järjestelmään. Vastaavasti jos lisensoitava kohde on poistunut (esimerkiksi virtuaaliserveri poistetaan), kohde poistuu automaattisesti lisensoinnista, kun laite on ollut 30 vuorokautta offline-tilassa valmistajan pilven suuntaan.

Käyttöönotto

Palvelun käyttöönottoon sisältyy tietoturvapolitiikkojen luominen sekä asennuspaketin luovuttaminen asiakkaalle. Aluksi ohjelmisto luovutetaan vain skannaustilassa, jossa noin viikon ajan tarkkaillaan ympäristöä. Noin viikon kuluttua TNNetin asiantuntijat katsovat näkyykö lokeissa jotakin, joka vaatii erillisen sallinnan. Tämän jälkeen politiikka vaihdetaan estävään moodiin asiakkaan valinnan mukaan (Joustava tai Kovennettu). Asiakkaan tulee tutustua vaihtoehtoihin ja valita sopiva moodi erillisestä dokumentaatiosta.

Asiakkaan vastuulla on ohjelmiston asennus haluamilleen laitteille. Asiakas vastaa myös siitä, että ohjelmisto on asennettuna kaikille tarvittaville laitteille. Tarvittaessa ohjelmistojen asennus ja huolehtiminen siitä, että se on asennettuna kaikille, on ostettavissa myös palveluna TNNetiltä IT-tuen palveluiden kautta.

MDR

Tuotamme MDR-palvelua 24/7 yhdessä eri valmistajien kanssa. Palvelussa kyberasiantuntijat valvovat yhteistyössä ympäristöä usealla eri aikavyöhykkeellä niin, että 24/7 valvonta toteutuu vuoden jokaisena päivänä virkeiden työntekijöiden toimesta. Ellei toisin sovita, toimii MDR-palvelu niin, että hälytyksen tultaessa MDR-tiimi tekee ensimmäisen arvion tilanteesta, jonka jälkeen he ovat yhteydessä TNNetiin. Jos tilanne vaatii välittömiä toimia, eikä MDR-tiimi saa TNNetin työntekijöitä kiinni, yrittää MDR-tiimi vielä mahdollisuuksien mukaan soittaa suoraan loppuasiakkaalle, ja viimeisenä vaihtoehtona tiimi voi itse tehdä tarvittavat toimenpiteet ympäristössä. Huomionarvoista on kuitenkin se, että TNNetillä on 24/7 vikapäivystys, josta saa aina jonkun kiinni. Kun MDR-tiimi on saanut kontaktin TNNetiin, teemme tarvittavat toimenpiteet parhaalla katsomallamme tavalla joko loppuasiakkaan kanssa yhteistyössä tai kriittisessä tilanteessa omatoimisesti. Edellä kuvattu toimintatapaa on mahdollista myös muokata asiakkaan tahtomalla tavalla: on mahdollista antaa MDR-tiimille suoraan lupa toimia parhaalla katsomallaan tavalla tai antaa ehdoton kielto, että he eivät missään tilanteessa saa tehdä muutoksia ympäristöön. **Hälytyksen vastaanottaminen ja kyberuhan torjuminen sisältyvät palvelun hintaan, joten tästä ei tule asiakkaalle lisäkustannuksia missään tilanteessa.** Tilanteen rauhoituttua ja välittömän uhan poistuttua tulee tapahtumista suorittaa vielä erillinen juurisyyanalyysi, joka on erikseen laskutettavaa työtä käytetyn ajan mukaan.

MDR-tiimillä on oma SLT (Service Level Target), joka tarkoittaa sitä, että tavoitteena on muodostaa ensimmäinen hyökkäystä torjuva toimenpide 30 minuutin sisään ensimmäisestä hälyttävästä havainnosta. Tähän aikaan siis sisältyy jo havainnon analysointi ja korjaustoimenpiteiden suunnittelu. Historiallisesti MDR-palvelussa kyberhyökkäykset on torjuttu 38 minuutissa ensimmäisestä havainnosta koko casen sulkemiseen asti.

Integroitavat järjestelmät

MDR palvelu vaatii toimiakseen integraatioita asiakkaan käyttämiin kolmannen osapuolen järjestelmiin, jotta saadaan tarvittavaa tietoturvadataa ja mahdollisuus suorittaa ehkäiseviä toimenpiteitä hyökkäyksen sattuessa. Mahdolliset integraatiot vaihtelevat hieman lopullisen ratkaisun mukaan, mutta geneerisesti yleisimmät palomuurivalmistajat, M365 ja Sophoksen sekä Checkpointin eri järjestemät ovat täysin tuettuja ja integroitavissa.

Jos asiakkaalla on käytössä esimerkiksi sellainen EDR palvelu, joka ei ole integroitavissa, suosittelemme erittäin vahvasti vaihtamaan EDR:n sellaiseen tuotteeseen, joka on tuettuna myös MDR:n puolesta.

Käyttöönotto

Käyttöönotossa asiakkaalle luodaan MDR profiili, johon kerätään tieto sisäiseistä IP-verkoista ja luodaan integraatiot kaikkiin mahdollisiin teknologioihin. Tämän jälkeen ympäristöä tarkkaillaan muutaman viikon ajan, jonka jälkeen esitetään välittömät parannusehdotukset siten, että MDR:n piiriin saadaan tarpeeksi eri datapisteitä palvelun tuottamiseksi. Tämän jälkeen sovitaan yhteiset pelisäännöt, joilla hälytyksiin reagoidaan ja aletaan näiden perusteella tuottamaan palvelua täysimääräisesti.

Käyttöönoton kustannuksiin vaikuttaa ympäristön laajuus ja suoritettavien integraatioiden määrä. Hinnoittelu on projektikohtainen ja arvioidaan aina jokaiseen ympäristöön erikseen.

Sähköpostin tietoturva

Yli 90% hyökkäyksistä organisaatioita vastaan alkaa haitallisesta sähköpostista, ja 75% kiristyshaittaohjelmahyökkäyksistä (ransomware) tulee sähköpostin kautta organisaation sisään. Koska sähköpostihyökkäykset yleensä liittyvät ihmistekijään, eli ihmisen tekemään virheeseen, Microsoft 365 ja Google Workspace -ympäristöt ovat organisaatioiden heikoin lenkki. Onnistuneet phishing- ja ransomwarehyökkäykset voivat aiheuttaa merkittävää taloudellista vahinkoa. Tämän tietoturva-aukon sulkeminen vaatii suojausta montaa eri uhkaa vastaan: tietojenkalastelua, haittaohjelmia sekä datan ja tunnusten varastamista.

Tekninen kuvaus

Sähköpostin tietoturva toimii API-rajapinnalla sähköpostitarjoajan (Google tai M365) ja sähköpostiturvan välillä. Kun sähköposti menee sähköpostipalvelimelle, sähköpostiturva ”kaappaa” viestin välistä omaan palveluunsa, jossa viestin tietoturva tutkitaan läpi. Viestistä voidaan AI:ta hyödyntäen tulkita esimerkiksi käytettyä kieltä (näyttääkö huijausviestiltä), skannata liitetiedostot virusten tai haitallisen ohjelmien varalta sekä tarkastella muita sähköpostiin liittyviä teknisiä parametrejä, kuten SPF ja DKIM -tietueiden oikeellisuus.

Järjestelmän käyttöönotto vaatii Microsoftilla Global Admin -rooliin kuuluvan tilin, jonka jälkeen tilin oikeudet voidaan rajata Exchange-adminiin. Vikatilanteissa kuitenkin Global Adminin olemassaolo voi helpottaa vian löytämistä. Googlen käyttöönotto vaatii integraatiotilille oman Googlen workspace-lisenssin ja Administrator-tason käyttäjän.

Kun sähköpostiturva on tarkistanut viestin, se joko välitetään sellaisenaan alkuperäiseen kohteeseen, tai viestiä voidaan muokata. Sisään tuleville viesteille voidaan laittaa esimerkiksi varoitus käyttäjälle, että viestissä oli jotakin epäilyttävää, mutta se päästettiin kuitenkin läpi. Viesti voidaan myös laittaa sähköpostiturvan karanteeniin, josta ylläpitäjä voi käydä viestin tarkastamassa ja vapauttamassa. Jos viesti on tarpeeksi varmasti haitallinen, se voidaan estää kokonaan. Estetytkin viestit ovat kuitenkin saatavilla jälkikäteen järjestelmästä, ja niiden avulla voidaan järjestelmää kouluttaa kunkin organisaation omiin tarpeisiin.

Käyttöönotto

Käyttöönotossa TNNet integroi asiakkaan sähköpostijärjestelmän tietoturvan piiriin nk. Read Only tilassa, ja järjestelmän annetaan pyöriä näin noin viikon ajan. Viikon kuluttua järjestelmän havaintoja käydään yhdessä läpi asiakkaan kanssa ja sen perusteella tehdään tarvittavia poikkeuksia.

Asiakkaan vastuulla on sitoutua osallistumaan läpikäyntipalaveriin noin viikon sisällä aloituksesta. Käyttöönoton jälkeen asiakkaan vastuulla on seurata sähköpostiliikennettä ja halutessaan vapauttaa viestejä loppukäyttäjille.

Lisensointi

Microsoftin sähköposteissa ei tarvitse lisensoida jaettuja ryhmälaatikoita, aliaksia tai muita Microsoftille lisensoimattomia sähköposteja. Nämä ovat kuitenkin saman suojan piirissä kuin normaalitkin käyttäjät. Hyvä nyrkkisääntö on, että jos Microsoft vaatii laatikosta lisenssin, niin lisenssi vaaditaan myös sähköpostiturvaan. Minimilisenssi, jota voidaan suojata, on Exchange Online plan 1. Jos Microsoftilta halutaan suojata ja tarkastella tietoja myös muissa sovelluksissa (Teams, Sharepoint, OneDrive), tulee käyttäjillä olla vähintään Microsoft E5 -lisenssi.

Googlen tapauksessa ryhmälaatikoita ei lisensoida tai suojata, vaan ainoastaan ryhmään kuuluvien jäsenien laatikot suojataan. Jos käyttäjä siis menee suoraan ryhmälaatikkoon lukemaan viestejä, ei viesti ole suojattu. Suojattavilla käyttäjillä tulee olla Googlelta sähköpostia varten mikä tahansa lisenssi, paitsi Essentials tai Business Starter. Google Driven suojaaminen vaatii vähintään Googlen Business Standard -lisenssin.

Molemmissa sähköpostipalveluissa käyttäjiä on mahdollista suojata myös ryhmä- tai jopa käyttäjäkohtaisesti, jolloin koko organisaation ei tarvitse olla suojattuna. Kannattaa kuitenkin aina muistaa, että tietomurtoon riittää yksikin suojaamaton laatikko, jos hyökkääjä onnistuu lähettämään suojaamattomalle henkilölle haittaohjelman.

Tietoturvakoulutus ja hyökkäyssimulaatio

Suurin osa kyberhyökkäyksistä saa alkunsa loppukäyttäjän tekemästä virheestä. Virheitä voidaan yrittää paikata erilaisilla teknologiaratkaisuilla, mutta varmin keino välttyä kyberhyökkäykseltä on kouluttaa käyttäjiä. Teknologiset ratkaisut ja koulutus eivät kuitenkaan ole toisiaan poissulkevat vaihtoehdot, vaan toisiaan erittäin hyvin tukevia. Mitä jos käyttäjä tekee koulutuksesta huolimatta virheen, tai mitä jos teknologiaratkaisu kohtaakin entuudestaan tuntemattoman hyökkäyksen eikä osaa torjua sitä?

Keskimäärin 18% haitallisista sähköposteista tulee klikatuksi, eli käytännössä joka viides työntekijä klikkaa huijaussähköpostissa olevia linkkejä. Vain kolmen kuukauden palvelun käytön jälkeen tämä prosentti saadaan laskettua alle kahteen. Vastaavasti jos palvelun käyttö lopetetaan, paluu alkuperäisen 18% lukemaan tapahtuu noin parissa kuukaudessa, eli jatkuva ja säännöllinen koulutus on äärimmäisen tärkeää.

Miten palvelu toimii

Toteutamme loppukäyttäjiin kohdistuvia hyökkäyssimulaatioita, eli huijaussähköpostikampanjoita, sekä käyttäjien mikrokoulutuksia tietoturvaan liittyen Nimblr:n järjestelmää hyödyntäen. Järjestelmä on monikielinen, mutta esimerkiksi Suomi, Ruotsi ja Englanti ovat täysin tuettuja kieliä.

Palvelussa organisaation käyttäjille lähetetään siis kalasteluviestejä, jotka ovat AI:n kustomoimia hyödyntäen esimerkiksi loppukäyttäjän titteliä tai organisaation toimialaa. Näin hyökkäykset ovat realistisia ja verrattavissa jokapäiväisiin kalasteluviesteihin. Viestejä lähetetään säännöllisen epäsäännöllisesti, jotta käyttäjä ei voisi ajankohdasta päätellä, onko viesti aito vai tämän palvelun viesti.

Hyökkäyssimulaation lisäksi käyttäjälle luodaan muutaman minuutin mittaisia mikrokoulutuksia tietoturvaan liittyen. Koulutukset ovat kokonaisvaltaisesti tietoturvaan liittyviä, eli kyseessä ei ole pelkästään huijaussähköpostien tunnistamista, vaan myös ihan perinteistä fyysistä tietoturvaa, haittaohjelmia, webin käyttöä ja ajankohtaisia pinnalla olevia kyberuhkia. Koulutusten aiheet muokkautuvat organisaatio- ja käyttäjäkohtaisesti sen mukaan, kuinka ihmiset katsovat koulutuksia ja toimivat hyökkäyssimulaatioissa.

Jos käyttäjät eivät syystä tai toisesta tee heille määrättyjä koulutuksia, käyttäjille menee kerran viikossa muistutusviesti koulutuksesta. Lisäksi organisaation pääkäyttäjä pääsee portaalista näkemään, miten käyttäjät ovat käyneet koulutuksia ja suoriutuneet hyökkäyssimulaatioista.

Palvelu sisältää TNNetin toimesta palvelun käyttöönoton yhdessä asiakkaan kanssa ja asiakkaan pääkäyttäjän koulutuksen portaaliin sekä tuen mahdollisissa ongelmatilanteissa. Käyttöönotossa tyypillisesti pitää sähköpostipalveluntarjoajalle sallia Nimblr:n käyttämät IP-osoitteet, jotta viestit eivät mene roskapostiin. TNNet voi tehdä tämän, jos tarvittavat oikeudet omaava käyttäjätunnus on saatavilla. Käytännössä palvelu ei vaadi asiakkaan pääkäyttäjältä käyttöönoton jälkeen toimenpiteitä, vaan oikein käyttöönotettuna palvelu havaitsee itse uudet ja poistuneet työntekijät tarpeen mukaan.

Kaikki palvelun data on Nimblr:n konesalissa (Hetzner), joka sijaitsee Euroopassa.

Käyttöönotto

Käyttöönottoon sisältyy asiakkaan toimittaman listan mukaisesti käyttäjien lisääminen ja ryhmittely, sekä ensimmäiset ryhmäasetukset ja ylläpitotunnuksen luominen asiakkaan ylläpitäjille.

Asiakkaan vastuulle jää tehdä tarvittavat whitelistaukset omiin sähköpostisuodatuksiinsa. Jos sähköpostit ovat TNNetin hallinnassa, voidaan whitelistauksien tekeminen myös tilata erillistyönä TNNetiltä.

Lisensointi

Palvelu lisensoidaan käyttäjäkohtaisesti. Käyttäjät voidaan määritellä erikseen, ja kaikkia organisaation käyttäjiä ei tarvitse lisensoida. Palvelu on aluksi vuoden määräaikainen, ja jatkuu sen jälkeen toistaiseksi voimassa olevana yhden kalenterikuukauden irtisanomisajalla, ellei toisin ole sovittu asiakaskohtaisessa sopimuksessa.

DDoS-suojaus

TNNetin verkkoyhteyksiä hyödyntäviin palveluihin on mahdollista ostaa lisäpalveluna DDoS-suojauspalvelu. Palvelu vaatii toimiakseen TNNetin IP-osoitteen, eli käytännössä palvelulla voidaan suojata palvelinympäristöjä, palomuureja ja nettiliittymiä. Kaikissa Hosting-tuotteissa palvelu on oletuksena päällä.

Palvelu toteutetaan Arborin Sightline with Sentinel -tuotteella, johon myös asiakkaalle on mahdollista antaa oma pääsy joko hallinta- tai raportointiportaaliin. Hallintaportaalista on mahdollista jopa itse suorittaa hyökkäyksen torjuntatoimenpiteitä, jos niin haluaa. Raportointiportaalista on mahdollista koostaa itselleen kattavia raportteja verkon liikenteestä niin normaali- kuin poikkeustilanteissakin. Portaalinäkymä vaatii, että suojattavat IP-osoitteet ovat omasta verkkoblokista eikä jaetusta IP-verkosta. Näin ollen esimerkiksi tavallisella julkisella IP-osoitteella olevaa Openstack-virtuaalipalvelinta ei voida näyttää raportoinnin puolelta. Jaetuissa IP-verkoissa olevat palvelutkin voidaan kuitenkin suojata DDoS-suojauspalvelulla, mutta ilman portaalinäkymää.

DDoS-suojaus toimii BGP Flowspec-teknologialla siten, että Sentinel pyrkii tunnistamaan DDoS-hyökkäyksiä erilaisilla parametreilla kuten liikenteenmäärä, tunnetusti haitalliset lähdeosoitteet ja liikenneprofiili. Tämän jälkeen BGP Flowspeciä hyödyntäen voidaan TNNetin reitittimille kertoa, että liikennettä ei vastaanoteta TNNetin reunalta sisään kohdistuen suojattuun palveluun. Sentinel on maailman johtava

tuote hyökkäysten tunnistamisessa, mutta se ei kuitenkaan takaa kaikkien hyökkäyksien havaitsemista. Mikäli asiakas kokee hyökkyäksen, jota Sentinel ei tunnista, voidaan vastaavat torjuntatoimenpiteet tehdä asiantuntijan analyysin perusteella joko asiakkaan itsensä toimesta hallintaportaalista tai asiantuntijoidemme avulla.

Kun TNNet havaitsee hyökkäyksen, hyökkäys pestään ensi tilassa pois, jotta mahdollinen häiriö palveluille loppuu. Hyökkäyksen loppumisen jälkeen, tai tarvittaessa jo hyökkäyksen aikana, asiakasta raportoidaan tapahtumien kulusta. Jos hyökkäys kohdistuu sellaiseen palveluun, joka ei ole suojauksen piirissä, ja hyökkäys haittaa TNNetin muiden asiakkaiden palveluita, laitamme kaiken palveluun kohdistuvan liikenteen mustaan aukkoon. Tämä tarkoittaa sitä, että hyökkäys käytännössä loppuu, mutta palveluun ei myöskään pääse ulkopuolelta edes luvallinen liikenne. Hyökkääjä on siis saavuttanut tavoitteensa. Jos hyökkäys on niin pieni, että TNNetin muut palvelut eivät siitä koe haittaa, ei hyökkäykselle tehdä mitään.

Jos halutaan suojata yksittäinen laite, joka on sellaisen palomuurin takana, jonka takana on myös muita laitteita, tulee suojata koko palomuuri ja kaikki sen takana olevat laitteet. Jos näin ei toimittaisi, voisi suojattavan palvelun kaataa hyökkäämällä vierekkäiseen palveluun, joka sivuvaikutuksena kaataisi myös palomuurin. Sama analogia pätee myös muissa palveluissa, joissa suojattava palvelu on riippuvainen muista palveluista.

Käyttöönotto

Käyttöönotto ei aiheuta palvelukatkoksia eikä vaadi asiakkaalta erityisiä toimenpiteitä. Käyttöönotossa TNNet konfiguroi omaan DDoS-pesuriinsa asiakkaan verkon IP-osoitteet, seuraa liikennettä ja asettaa pesupolitiikat paikalleen.

Verkkoskannaus

Verkkoskannauspalvelussa TNNet skannaa julkiverkkoon näkyviä IP-osoitteita pyrkien löytämään tunnettuja haavoittuvuuksia ja liian avoimia palomuurin sallintasääntöjä. Tyypillisesti mikään ei ole yhtä pysyvää, kuin hetkellinen muutos. Hetkellinen muutos voi olla esimerkiksi huoltotoimenpiteen vuoksi avattu pääsy palomuurille tai testimielessä asennettu lisäosa kotisivuille. Skannauspalvelua voi yksinkertaisuudessaan hyödyntää siihen, että säännöllisesti testataan, onko palomuurin rajaukset sellaisessa kunnossa kuin on kuviteltu niiden olevan tai onko verkkosivujen kaikki komponentit päivitetty haavoittuvaisista versioista uusimmaksi.

Palvelussa skannaamme turvallisesti erikseen määritetyt palvelut siten, että skannauksesta ei koidu muuta haittaa skannattavalle ympäristölle. Liian aggressiivinen testaus voisi aiheuttaa esimerkiksi palvelunestohyökkäyksen kaltaisen tilanteen skannattavaan ympäristöön. Skannaukset voidaan tehdä aina täsmällisesti sovittuun aikaan, jolloin skannattavassa ympäristössä on mahdollista valmistautua skannaukseen. Asiakkaan on myös hyvä ilmoittaa omalle palveluntarjoajalleen skannauspalvelun käyttöönotosta, mikäli palveluntarjoaja on joku muu kuin TNNet, sillä palveluntarjoajalla saattaa olla omia sääntöjä verkkoskannauksen osalta.

Asiakas saa jokaisesta skannauksesta yksityiskohtaisen raportin löydetyistä laitteista, avoimista porteista ja niistä löydetyistä haavoittuvuuksista. Raportin lukeminen on aina asiakkaan vastuulla, mutta erillisestä lisäpyynnöstä on mahdollista pyytää apua raportin tulkintaan ja havaintojen korjaamiseen asiantuntijoiltamme.

Skannaus suoritetaan Tenablen Nessus -työkalua hyödyntäen, mutta palvelu on toimintaperiaatteeltaan on-premin tapainen, eli kaikki skannaukset ja datan säilöntä tapahtuvat TNNetin ylläpitämällä laitteistolla.

Käyttöönotto

Käyttöönottoon sisältyy verkkoskannauspolitiikkojen luominen ja testaaminen.

Asiakkaan vastuulla on ilmoittaa halutut IP-osoitteet, joita skannataan, sekä varmistaa, että palomuuri sallii skannaukset. Asiakkaan vastuulla on myös ilmoittaa mahdollisille kolmansille osapuolille ostamastaan skannauspalvelusta, jotta se ei aiheuta häiriötä muiden palveluntarjoajien jaetuissa ympäristöissä.

Lisäprojektina on myös mahdollista skannata ja testata autentikoinnin takana olevia palveluita, joissa asiakkaan vastuulla on luoda ja luovuttaa tarvittavat autentikointitunnukset.

Lisensointi

Palvelu lisensoidaan asset-määrän mukaan. Assetilla tarkoitetaan joko verkkosivua (FQDN) tai IP-osoitetta. Jos verkkosivu sijaitsee samassa IP-osoitteessa kuin mikä on jo määriteltynä asseteihin, lisensoidaan kaksi assetia. Jos skanneriin määritetään esimerkiksi kokonainen IP-verkko, niin asseteiksi lasketaan koko verkon koko (/28 maskilla laskutetaan 16 assetia).

SASE

SASE (Secure Access Service Edge) on kattotermi usealle teknologialle tai tavalle toimia. Tärkeimmät komponetit ovat ZTNA ja SWG, jotka on tarkemmin eritelty seuraavissa kappaleissa.

ZTNA (Zero Trust Network Access)

ZTNA ei ole yksittäinen teknologia, vaan tapa toimia. ZTNA:lla tarkoitetaan yleisesti sitä, että verkkoon päästääkseen käyttäjän tulee olla teknologisesti tunnistettu, käyttäjällä on mahdollisimman vähän pääsyjä ja käyttäjän mahdolliset oikeudet tehdä muutoksia ovat mahdollisimman vähäiset. Tämän lisäksi edellä mainittuja ehtoja tarkkaillaan jatkuvasti, ja mikäli tilanne muuttuu, voidaan pääsy estää.

ZTNA toimii teknisesti siten, että muurin taakse asennetaan ZTNA-connectori, joka soittaa HTTPS-yhteyden ZTNA-pilveen. Myös palomuuri itse voi toimia ZTNA-connectorina IPSec tunnelia hyödyntäen. Vastaavasti käyttäjä ottaa HTTPS-yhteyden ZTNA-pilveen, jossa nämä yhteydet yhdistetään. Yhteyttä monitoroidaan koko ajan ja se voidaan katkaista heti, kun käyttäjä lopettaa applikaation käytön tai tietoturva sitä vaatii. Jokaisesta ZTNA:n läpi kulkevasta liikenteestä jää kattavat lokitiedot talteen, jotta jälkikäteenkin on mahdollista tarkastella, kuka on käyttänyt sovelluksia miten ja milloin. Havainnollistava kuvaus toiminnasta on kappaleen lopussa olevassa kuvassa.

ZTNA-portaali tukee käytännössä kaikkia TCP-protokollia, jos käyttäjällä on asennettuna SASE agentti, joka mahdollistaa esimerkiksi tietokantayhteydet konesaliin erillisillä ohjelmistoilla. Jos käyttäjän ei ole mahdollista asentaa SASE agenttia koneelleen, ZTNA tukee selaimen kautta käytettäväksi seuraavia applikaatioita:

- Web-applikaatio (HTTP ja HTTPS, TCP -porttia voidaan muuttaa)
- SSH-applikaatio tai SSH-gateway (Porttia voidaan muuttaa, salasana ja avainkirjautuminen)
- RDP-applikaatio (Porttia voidaan muuttaa)

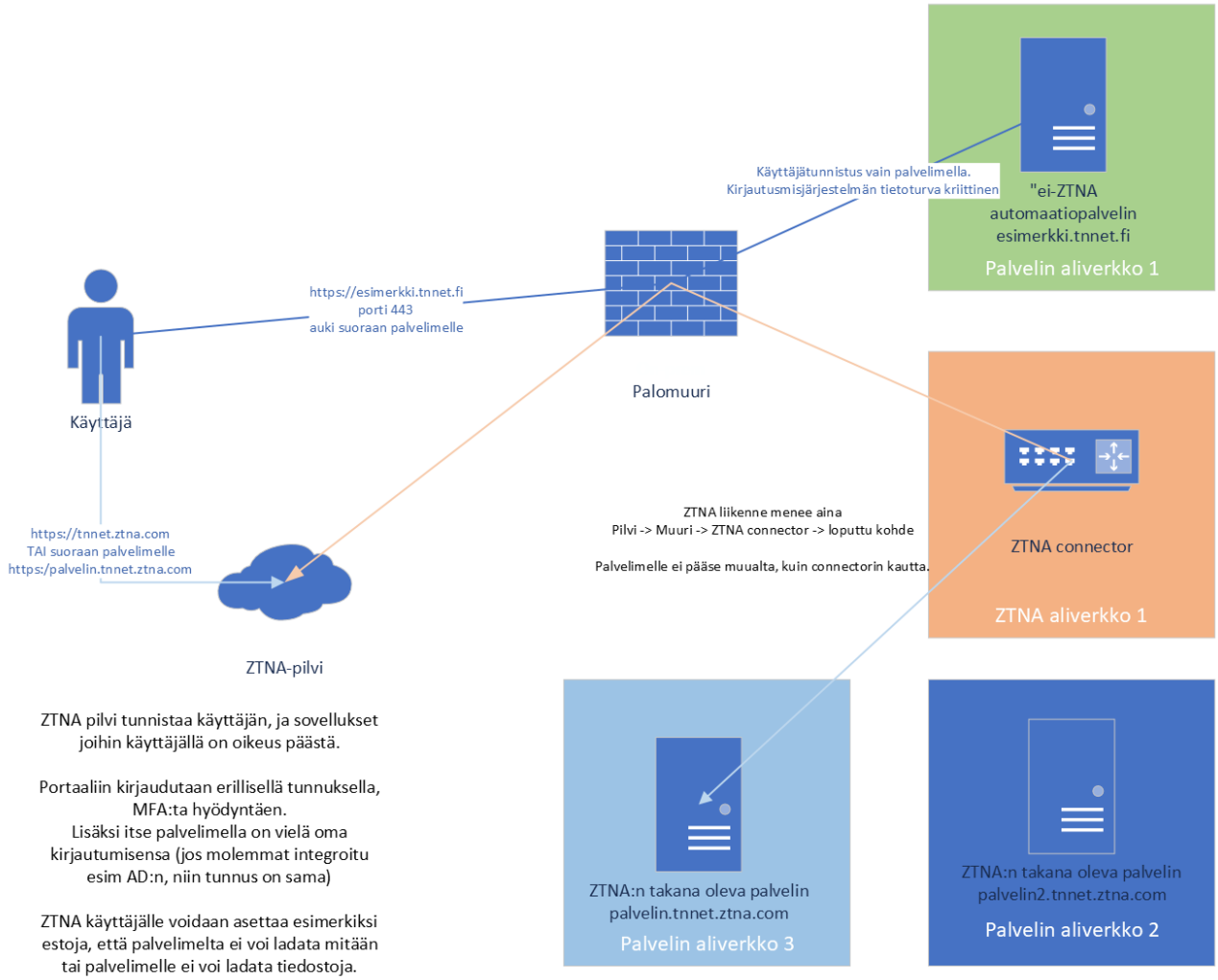
ZTNA-palveluun on mahdollista määrittää sovelluksille lisävaateita tietoturvan osalta. Esimerkkejä tällaisista rajoituksista:

- Mistä lähdeosoitteesta yhteydet sallitaan.
- Mistä GeoIP:stä yhteydet sallitaan, esimerkiksi vain Suomesta, vain Euroopasta, kaikkialta paitsi Aasiasta.
- Pitääkö käyttäjällä olla MFA päällä ZTNA-pilveen.
- Mihin vuorokauden aikaan palvelua voi käyttää.

- Onko laitteen tietoturva halutulla tasolla

Lisäksi on saatavilla applikaatiokohtaisia erityissääntöjä. Esimerkiksi Web-applikaatiolle voidaan määrittää, voiko palveluun tehdä ainoastaan GET-requesteja, vai sallitaanko esim POST ja PUT -requestit, jolloin voitaisiin estää palveluun tiedostojen lataaminen tai palvelusta tiedostojen lataaminen. SSH-applikaatiossa taas voidaan estää tiettyjen käyttäjänimien käyttäminen kokonaan.

Asiakkaalla on mahdollisuus saada ZTNA-portaaliin omat ylläpitäjätunnukset, joilla portaalia pystyy hallinnoimaan täysin itsenäisesti. Palveluun sisältyy TNNetin toimesta palvelun käyttöönotto ja tapauskohtaisesti sovittujen asetusten ja politiikkojen määrittäminen yhdessä asiakkaan kanssa. Portaali on varsin yksinkertainen, joten jos muutoksia on tulevaisuudessa tarve tehdä, on käyttöönoton jälkeen itsenäinen ylläpito helppoa. Erillisestä työpyynnöstä voimme myös auttaa myöhempien asetusten tekemisessä.



1 Periaatekuva ZTNA:n toiminnasta palomuurin kanssa.

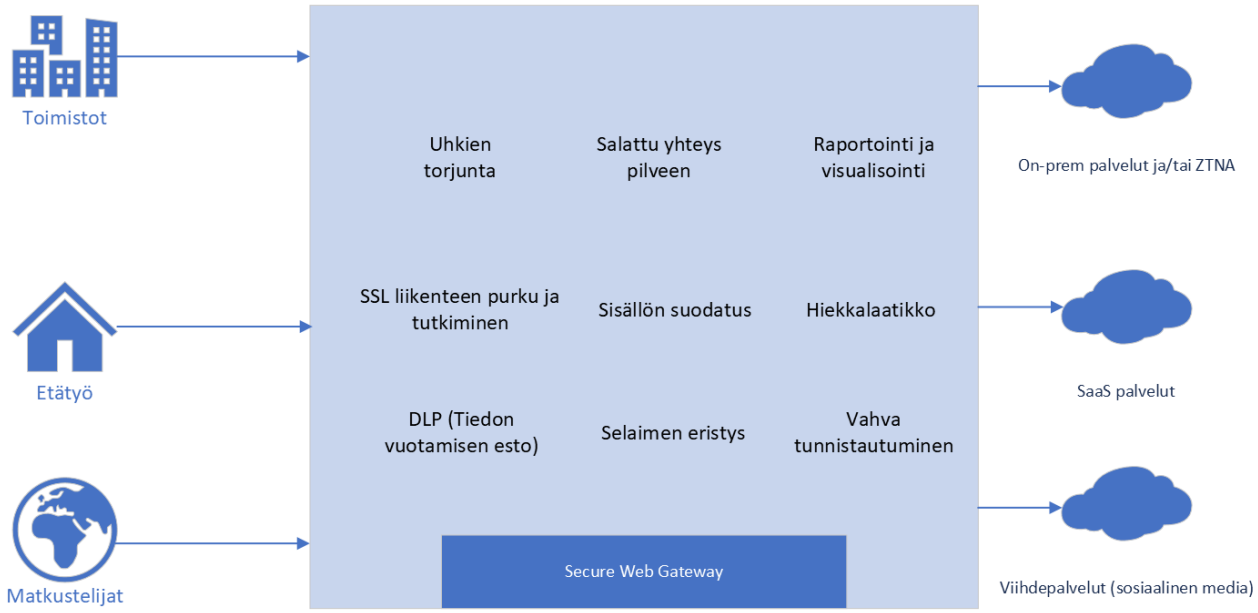
Portaalin käyttäjät on mahdollista integroida useita eri auth-providereita vasten (esimerkiksi Okta, AD, ja EntraID). Kaikkia integroituja käyttäjiä ei tarvitse lisensoida, vaan ainoastaan palvelua käyttäneet aktiiviset käyttäjät lisensoidaan.

Secure Web Gateway (SWG)

SWG:t toimivat yrityksen työntekijöiden ja Internetin välissä, suodattavat epävarman sisällön verkkoliikenteestä, estävät kyberuhkia ja tietomurtoja, ja estävät riskialttiin tai luvattoman käyttäjäkäyttäytymisen. SWG:tä voisi ajatella eräänlaisena käyttäjäkohtaisena palomuurina, joka toimii pilvessä käyttäjän sijainnista riippumatta.

SWG:t ovat erityisen hyödyllisiä etätyöntekijöiden hallinnassa. Vaatimalla etätyöntekijöitä käyttämään Internetiä turvallisen verkkoyhdyskäytävän kautta, voivat yritykset, jotka luottavat hajautettuun työvoimaan, estää paremmin tietomurtoja. Tämä onnistuu, vaikka heillä ei olisi suoraa hallintaa työntekijöidensä laitteista tai verkoista, tai käyttäjiä ei voida suojata yrityksen omilla palomuurilaitteilla.

Kun asiakaslaitteelta lähetetään pyyntö verkkosivustolle tai sovellukseen Internetissä, pyyntö kulkee ensin SWG:n kautta. Porttina toimiva SWG todentaa käyttäjän ja tarkastelee pyyntöä varmistaen, että se ei riko hyväksyttäviä käyttöpolitiikkoja. SWG sallii pyynnön jatkua vain, jos se on todettu sopivaksi ja turvalliseksi. Havainnollistava kuva tästä toimintaperiaatteesta on tämän kappaleen lopussa.



2 Periaatekuva SWG:n toiminnasta.

Miten tuote toimii

SWG:n voi yksinkertaistaa pilvessä toimivaksi palomuuriksi, jonka läpi pakotetaan käyttäjän kaikki selainliikenne (HTTP, HTTPS). Pilven kautta toteutuvat tietoliikennenopeudet ovat maksimissaan noin 500 Mbps, mutta vaihteluväli on ruuhkan mukaan 100 – 500 Mbps.

Alla vielä listattuna tärkeimmät ominaisuudet, jotka SWG mahdollistaa:

- Uhkien torjunta – Tunnistetaan sivuilta ja ladattavista tiedostoista mahdollisia haittaohjelmia tai muita tietoturvauhkia ja reagoidaan niihin.
- Salattu yhteys pilveen – Käyttäjällä on aina salattu yhteys pilveen.
- SSL liikenteen purku ja tutkiminen – Voidaan purkaa HTTPS-liikenteestä salaus, jotta liikenne pystytään tarkistamaan tietoturvauhkien varalta.

- Sisällön suodatus – Tunnistetaan sivustolla näytettävä sisältö ja voidaan asettaa sen mukaisia tietoturvapolitiikkoja.
- Tiedon vuotamisen esto (DLP)– Nettiin ladattavista tiedostoista pystytään tunnistamaan erilaisia merkintöjä, esim. Salainen tai Julkinen, ja niiden mukaan tiedoston lataus voidaan estää.
- Selaimen eristys[1] – Halutut sivut, joko kaikki tai tietyt kriteerit täyttävät, voidaan ajaa todellisuudessa pilvessä ja käyttäjälle näytetään vain ”videokuvaa” sivusta. Näin sivuston tietoturvauhkat eivät vaikuta käyttäjään.
- Hiekkalaatikko[1] – Nettisivuilta ladattavat tiedostot ajetaan ”hiekkalaatikossa” ennen kuin ne päätyvät käyttäjille. Näin voidaan varmistua ladattavien tiedostojen tietoturvallisuudesta.
- Vahva tunnistautuminen – Integroitavissa useaan eri auth-provideriin, MFA-mahdollisuus.
- Raportointi ja visualisointi – Kattavat raportit ja muokattavat visuaaliset kuvaajat tietoturvatapahtumista.

SASE käyttöönotto

Käyttöönottoon sisältyy SASE ympäristön luominen ja asiakkaan ylläpitotunnuksien tekeminen. Kaikki muu asiakaskohtainen hienosäätö on erikseen laskutettavaa tuntiyötä, joka voidaan myös projektoida kiinteähintaiseksi, jos TNNetillä on riittävän kattava käsitys asiakkaan ympräistöstä ja vaateista.

Tavanomaisiin tehtäviin kuuluu ainakin (suluissa arvio tavanomaisesta työajasta):

- SASE-verkon luominen, ei saa mennä päällekkäin asiakkaan nykyisten verkkojen kanssa, 15-30min
- Connectorien yhdistäminen (joko erillinen sovellus tai IPSec-tunneli asiakkaan muureille), 15min per connectori
- Käyttäjätilien luominen tai muun SSO:n integrointi, 30min
- Asiakaskohtaisten erityissallintojen luominen, esim Yle Areenaan tms., 30min
- Oletusarvoisten palomuurisääntöjen tekeminen, 15min

Asiakkaan vastuulle jää SASE agenttien asentaminen haluamilleen laitteille. Asennuksen voi ostaa myös erillisenä palveluna TNNetin IT-Tuen palveluiden kautta.

SASE Lisensointi

SASE lisensoidaan sekä yhdyskäytävien (peruspalvelu) että käyttäjien mukaan. Normaalisti yritykselle riittää yksi yhdyskäytävä, joka sijoitetaan Helsinkiin, mutta jos kuormaa halutaan ajaa globaalisti myös esimerkiksi muista Euroopan maista, tulee jokaista maata kohden olla oma yhdyskäytävänsä.

Lisäksi lisensoidaan jokainen palvelusta löytyvä käyttäjä. Erityishuomiona se, että TNNet varaa itselleen kaksi ylläpitokäyttäjää, joista menee myös lisenssimaksu. Todellinen käyttäjämäärä siis on N+2 (N = palvelua käyttävein asiakastilien määrä)

Lisätietoja

Lue myös TNNet yleinen palvelukuvaus. Suosittelemme lukemaan myös muut TNNetin palvelukuvaukset, sillä tietoturvapalvelut ovat liitettävissä käytännössä kaikkiin TNNetin tuottamiin palveluihin.