Tietoturva ja kyberturvallisuus

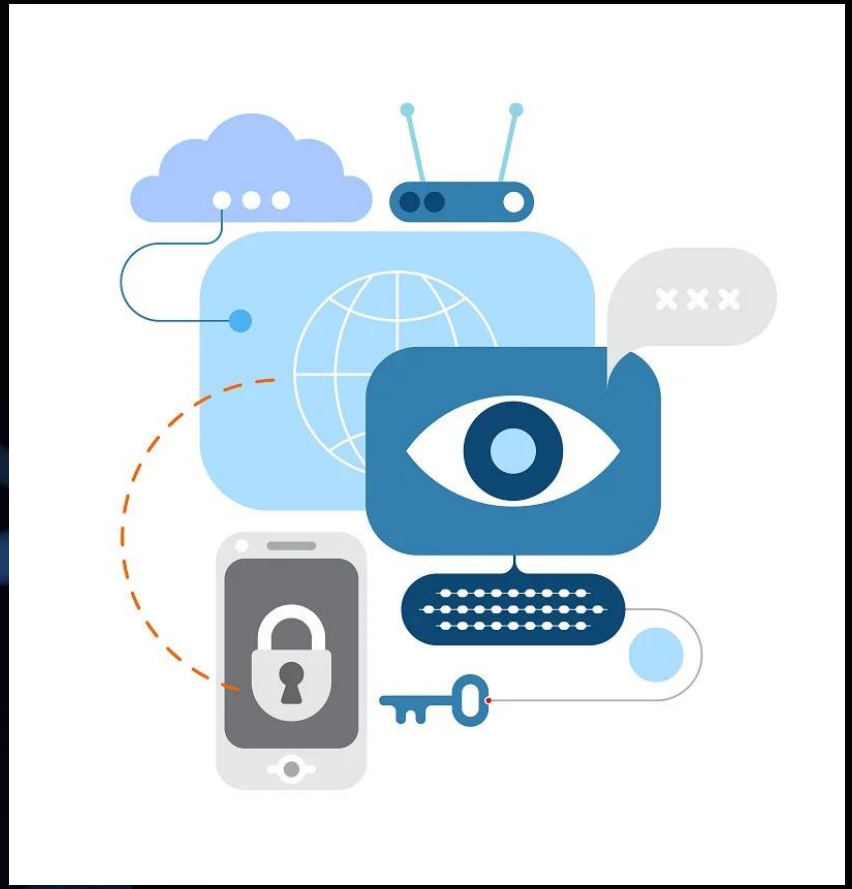
Johdanto

Tietoturva, tietosuoja, palomuuri, virustorjuntaohjelma, kyberturvallisuus. Hikeä nostattavia sanamörköjä?

Ei huolta, yksinkertaisuudessaan näissä on kyse sinun turvallisuudestasi ja maalaisjärjen käytöstä.

Virustorjunta

- Ohjelmisto, jonka tarkoituksena on suojata tietokonetta, mobiililaitetta tai muuta digitaalista laitetta haittaohjelmilta, kuten viruksilta, troijalaisilta, madoilta, vakoiluohjelmilta ja muilta haitallisilta ohjelmistoilta.
- Sen päätavoite on estää näiden ohjelmien pääsy järjestelmään ja poistaa ne, jos ne ovat jo päässeet tunkeutumaan laitteeseen.
- Virustorjuntaa käytetään erityisesti:
  - Suojaamaan henkilökohtaisia tietoja ja yksityisyyttä.
  - Varmistamaan laitteen turvallinen ja vakaa toiminta.
  - Suojaamaan laitteita ja verkkoja hyökkäyksiltä, jotka voivat johtaa esimerkiksi tietojen varastamiseen tai kiristysohjelmien käyttöön.
- On olemassa sekä kaupallisia että ilmaisia ohjelmistoja
  - Kaupalliset tarjoavat myös usein ilmaista versiota, jossa ei ole niin kattava suojaus.



McAfee

F-Secure

Norton by Symantec

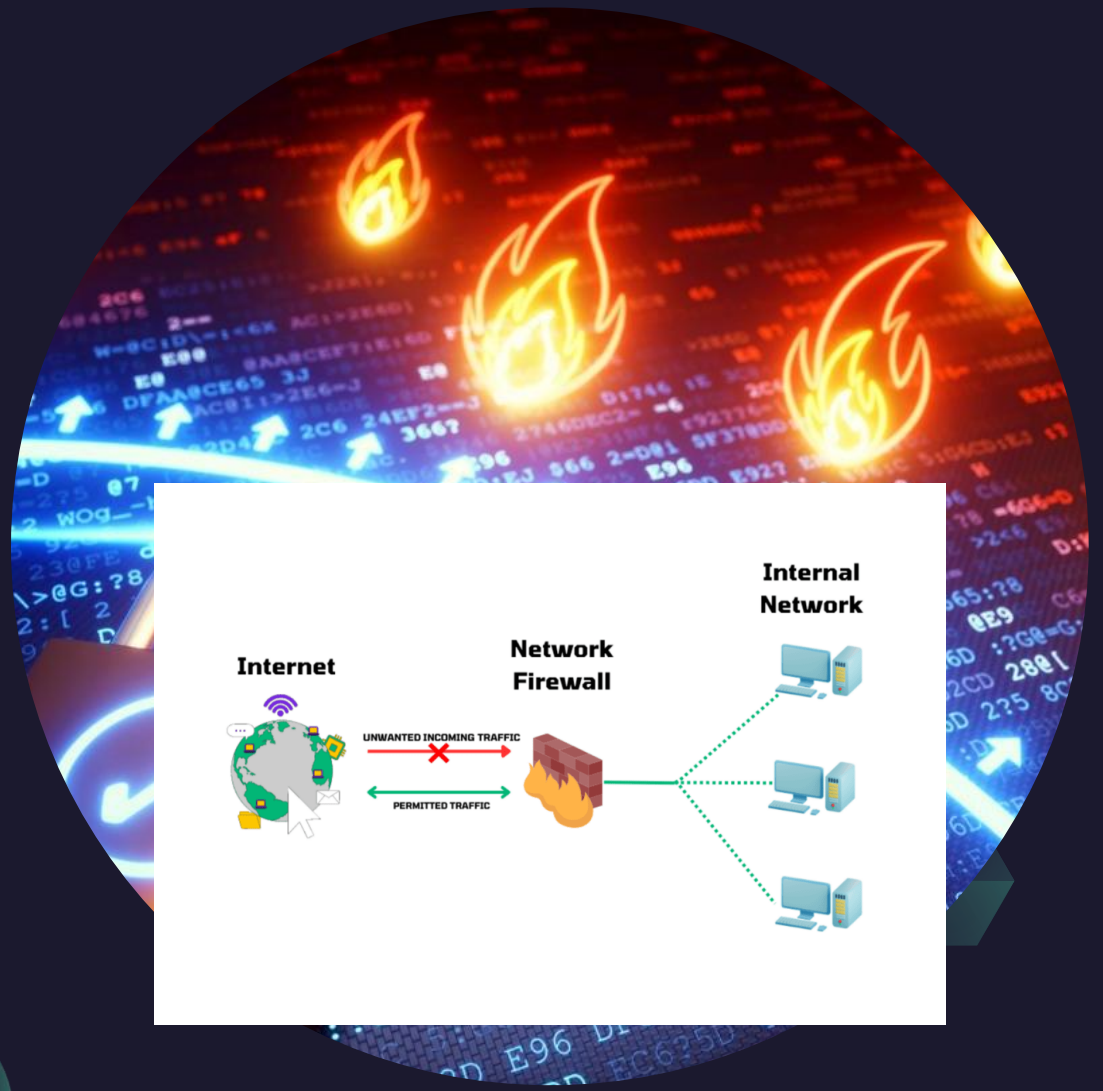
Avast

Palomuuri

- On tietoturvalaite tai ohjelmisto, joka toimii suodattimena lähiverkon ja internetin välillä.
- Sen päätehtävänä on estää luvaton tai haitallinen liikenne pääsemästä lähiverkkoon ja suojata näin tietokoneita ja verkkoa hyökkäyksiltä.

Palomuurien tyypit:

- Laitteistopalomuuri: Fyysinen laite, joka sijoitetaan sisä- ja ulkoverkon välille. Sopii yrityksiin ja organisaatioihin.
- Ohjelmistopalomuuri: Ohjelmisto, joka asennetaan yksittäiseen tietokoneeseen tai palvelimeen. Suojaa kyseistä laitetta estämällä luvattoman liikenteen. Sopii parhaiten yksityishenkilölle.
- Pilvipohjainen palomuuri: Verkkopohjainen palomuuri, jotka toimii pilvipalveluissa. Soveltuu erityisesti yrityksille, jotka käyttävät hajautettuja ja pilvipohjaisia IT-järjestelmiä.



Palomuuri on olennainen osa minkä tahansa tietoverkon tai yksittäisen tietokoneen tietoturvaa, ja sitä tarvitaan estämään ulkoiset uhat ja hallitsemaan verkkoliikennettä turvallisuuden varmistamiseksi.

Kyberturvallisuus

- Eli digitaalinen turvallisuus tarkoittaa tapoja, joilla voit suojata digitaalisia tietoja, laitteita ja resursseja. Tämä sisältää henkilökohtaiset tiedot, tilit, tiedostot, valokuvat ja jopa henkilökohtaiset varat.

- Vaikka suojaussovellukset ja -laitteet, kuten virustorjuntaohjelmat ja palomuurit, ovat ehdottoman tärkeitä, ei riitä, että otat käyttöön kyseiset työkalut ja oletat, että kaikki on hyvin. Yksilön toimiva kyberturvallisuus edellyttää myös, että käytössä on joukko harkittuja käytäntöjä:

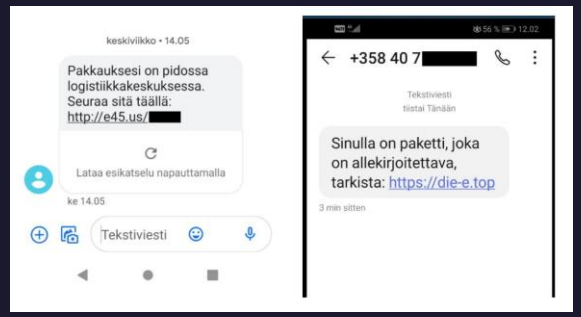
    - Älä avaa outoja linkkejä tai liitteitä, joita saatat saada sähköpostitse tai tekstiviestinä, vaikka ne näyttäisivät olevan peräisin luotettavalta lähettäjältä.

    - Pidä käyttöjärjestelmä, ohjelmisto ja selaimet ajan tasalla valmistajan uusimpien päivitysten ja korjausten kanssa.

    - Käytä vahvoja ja yksilöllisiä salasanoja. Muista joka tilille eri salasana!

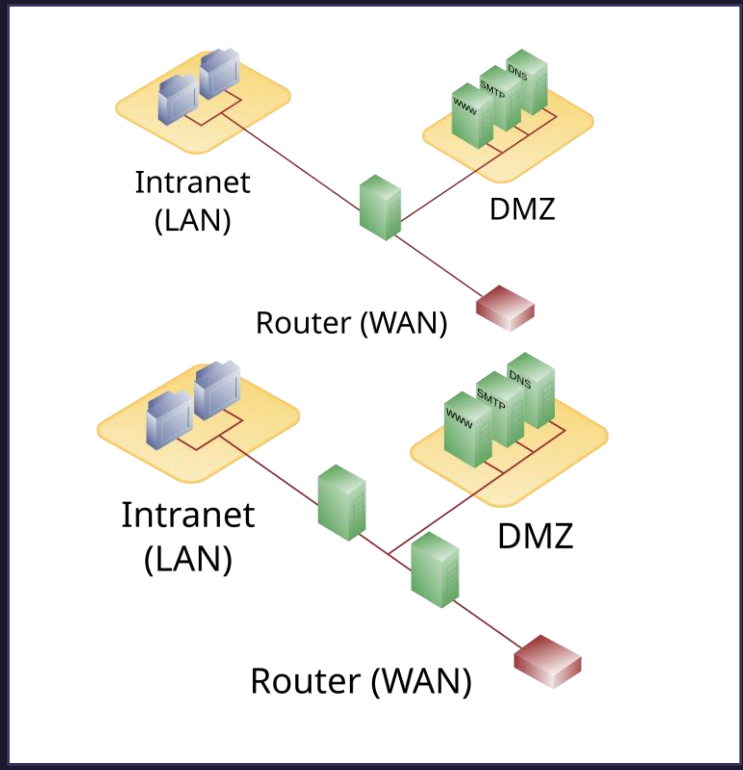
    - Varmista, että laitteesi vaativat salasanan, PIN-koodin tai biometrisen todennuksen, kuten sormenjäljen tai kasvontunnistuksen sisäänkirjautumiseen.

    - Ota käyttöön monivaiheinen tunnistautuminen aina kun mahdollista.



DMZ-alue

- DMZ (engl. Demilitarized Zone) on tietokoneverkon osa joka sijoittuu sisäverkon ja julkisen verkon väliin. Se suojaa yrityksen tietokoneet ja palvelimet suoralta Internet-yhteydeltä
- Se toimii ylimääräisenä tietoturvatasona, ”puskurivyöhykkeenä” jossa yritys voi pitää julkisia palvelimia, kuten verkkosivustoja tai sähköpostipalvelimia.
- DMZ on alue johon ulkopuoliset käyttäjät voivat päästä, mutta jos esim. yrityksen palvelimeen, joka on DMZ:lla, kohdistuu kyberhyökkäys, niin se estää hyökkäyksen suoran pääsyn yrityksen sisäverkkoon.
- DMZ-alue voidaan toteuttaa joko yhdellä tai kahdella palomuurilla. Näistä jälkimmäinen on kalliimpi mutta turvallisempi.



GDPR, tietosuoja

- GDPR (General Data Protection Regulation) on Euroopan Unionin asettama tietosuoja-asetus, joka astui voimaan toukokuussa 2018.
- Sen tarkoituksena on suojella yksilöiden henkilötietoja ja vahvistaa heidän oikeuksiaan tietojen hallintaan.
- GDPR velvoittaa yritykset ja organisaatiot käsittelemään henkilötietoja vastuullisesti ja läpinäkyvästi sekä varmistamaan tietojen turvallisuuden.
- Yksinkertaisesti sanottuna, GDPR asettaa säännöt siitä, miten organisaatiot voivat kerätä, tallentaa ja käyttää henkilötietoja, ja se antaa kansalaisille enemmän valtaa omiin tietoihinsa