

Kyberturvallisuus – näkökohdat

Arvioitu oppijan taitotaso: Aloittelija

Kyberturvallisuutta voidaan pitää käsitteenä, joka koostuu 10 eri näkökulmasta. Nämä on määritelty alla, ja jotkut niihin liittyvät käsitteet on määritelty erillisessä luettelossa ensimmäisen luettelon alla.

Kyberturvallisuuden näkökohdat ovat:

1. **Fyysinen:** palvelimien ja muiden laitteiden suojaaminen varkauksilta, katastrofeilta ja muilta fyysisiltä uhilta. Tekniikoita ovat lukitut ovet, valvontakamerat ja turvalliset tilat.
2. **Verkko:** tietojen suojaaminen, kun ne kulkevat tai niitä käytetään verkkojen kautta. Tämä sisältää palomuurit, verkon jakamisen aliverkkoihin, tunkeutumisen esto- ja havaitsemisjärjestelmät (IPS, IDS) ja virtuaaliset yksityiset verkot (VPN).
3. **Päätepiste:** suojaa päätepelilaitteita, jotka muodostavat yhteyden verkkoon. Toimenpiteisiin kuuluvat virustentorjuntaohjelmisto, säännölliset päivitykset (sekä ohjelmistot että laitteistot) ja salaus.
4. **Sovellus:** varmistetaan, että sovellukset ovat turvassa uhilta. Tämä sisältää säännölliset päivitykset, turvalliset koodauskäytännöt, haavoittuvuusarvioinnit, tunkeutumistestauksen ja sovellusten asentamisen vain luotettavista lähteistä.
5. **Pilvi:** pilvessä isännöityjen tietojen, sovellusten ja palveluiden suojaaminen. Tämä kattaa turvallisen pilvi-infrastruktuurin, käyttöoikeuksien hallinnan ja määräysten noudattamisen. Tekniikoita ovat salaus, identiteetin hallinta ja tietoturvan valvonta.
6. **Käyttöoikeuksien hallinta:** varmistetaan, että vain valtuutetuilla henkilöillä on pääsy tiettyihin resursseihin ja että heillä on vain tarvitsemansa oikeudet. Tähän liittyvät prosessit sisältävät käyttäjän todentamisen, valtuutuksen ja henkilöllisyyden todentamisen. Menetelmiä ja työkaluja ovat kulunvalvontalistat, avaimet (fyysiset ja digitaaliset), monivaiheinen tunnistautuminen (MFA) sekä käyttäjä- ja ryhmäoikeuksien hallinta (read/write/execute).
7. **Seuranta:** turvallisuusuhkien jatkuva seuranta ja analysointi poikkeamien havaitsemiseksi ja niihin reagoimiseksi. Toimenpiteisiin kuuluvat valvonta, lokit, tapahtumien hallinta, verkkoliikenteen analysointi ja tapahtumien vastausryhmät.
8. **Salaus:** tietojen suojaaminen koodaamalla ne niin, että vain ne, joilla on oikea salauksenpurkuavain, voivat purkaa ne. Tällä tavoin varmistetaan tietojen luottamuksellisuus ja eheys sekä siirron aikana että levossa.
9. **Resilienssi:** kyberpoikkeamiin valmistautuminen, niihin reagoiminen ja niistä toipuminen. Työkaluja ovat katastrofipalautuksen ja liiketoiminnan jatkuvuuden suunnittelu, näiden suunnitelmien tehokkuuden testaaminen, tietojen varmuuskopiointi, varmuuskopiointijärjestelmät ja vaihtoehtoiset strategiat.



10. Toimintapolitiikat: ohjeiden ja menettelyjen laatiminen tietovarojen hallintaa ja suojaamista varten. Käytännöt sisältävät turvallisuuden ja omaisuuden hyväksyttävän käytön sekä häiriötilanteisiin reagoitisuunnitelmat. Tavoitteena on auttaa varmistamaan, että kaikki ymmärtävät kyberturvallisuusroolinsa.

Joitakin kyberturvallisuuskonsepteja ovat:

- **IDS/IPS** = yleensä ohjelmistopohjainen ratkaisu tunkeilijoiden tai kyberhyökkääjien havaitsemiseen
- **Tietovarannot** = tietokannat, tallenteet ja dokumentaatio, joita yritys tai organisaatio käyttää päätöksenteossaan
- **läpäisytestaus** = menetelmä tietokonejärjestelmien testaamiseksi etsimällä ja hyödyntämällä niiden haavoittuvuuksia
- **VPN** = suojattu ja salattu yhteys käyttäjän laitteen ja verkon tai kahden verkon välillä

Harjoitus: Yhdistä kyberturvallisuustoimenpiteet näkökohtiin.

Suunnitelmat	Fyysinen, pääsynhallinta
Updates	Verkko
Avaimet	Päätepiste, sovellus
Salaus	Pilvi, Seuranta
Valvonta	Resilienssi, toimintapolitiikat
IDS/IPS	Salaus, päätepiste, pilvi
	3,6,2,5,1,4

Pohdintatehtävä 1: Miten kyberturvallisuus näkyy työssäsi?

Reflektiotehtävä 2: Miten voit valvoa yPäätepisteen, sovellustyömme (työpaikka, työnantaja, työyhteisö) kyberturvallisuutta?

Seuraava vaihe

[Siirry henkilökohtaisiin tietoihin](#)



**Euroopan unionin
osarahoittama**



**Kokkola
Karleby**

centria
University of Applied Sciences

kpedu