

TENTTI 25.3.2019

KYBERTURVALLISUUS I: PERUSTEET, TIE-30151

Marko Helenius

Tentissä ei saa käyttää oheismateriaalia eikä laskinta. Vastaa selkeästi.

Huomaa, että viimeinen viides tehtävä on toisella sivulla.

(6 pistettä/tehtävä)

Tehtävä 1

Mikä on? (lyhyt määrittely riittää)

- a) Digitaalinen allekirjoitus
- b) Ransomware
- c) Tietoturvapoliittikka
- d) WPA2
- e) DES
- f) SHA-256

Tehtävä 2

Olet laatimassa yrityksen henkilöstölle salasanojen luomiseen ja käyttöön liittyvää ohjeistusta. Yrityksen sisäisten järjestelmien salasanat (3 eri järjestelmää) on muistettava ulkoa, jolloin niitä ei saa tallentaa salasananhallintaohjelmaan, mutta yrityksen ulkoisia salasanvoja varten käytössä on salasananhallintaohjelma.

Millaisia ohjeita annat ja miten perustelet ne?

Tehtävä 3

Piirrä kuva, josta selviää mahdollisimman hyvin, miten VPN toimii. Ota mukaan kuvaan tietoliikennepakettien rakenne. Selvennä kuvaa tarvittaessa tekstillä.

Tehtävä 4

Piirrä mahdollisimman täsmällinen kuva Diffie-Hellman -avaintenvaihdosta. Selvennä kuvaa tarvittaessa tekstillä.

Tehtävä 5

Oikeusministeriön oppaassa ”Miten valmistautua EU:n tietosuoja-asetukseen?” on luvussa 7 oheiset kohdat. Mitä nämä tarkoittavat ja mitä ne merkitsevät toisaalta rekisteristä vastuullisen ja toisaalta rekisteröidyn kannalta?

7.1 Oikeus saada läpinäkyvää informaatiota henkilötietojen käsittelystä

7.2 Rekisteröidyn oikeus saada pääsy tietoihin

7.3 Oikeus tietojen oikaisemiseen ja oikeus tulla unohdetuksi

7.4 Oikeus käsittelyn rajoittamiseen ja rekisterinpitäjän velvollisuus ilmoittaa rajoituksesta

7.5 Oikeus siirtää tiedot järjestelmästä toiseen

7.6 Vastustamisoikeus

7.7 Automatisoidut yksittäispäätökset ja profilointi