ECDL Foundation

ECDL Tietoturva - IT Security 2.0

Vastuuvapauslauseke

Vaikka ECDL Foundation on huolellisesti valmistanut tämän julkaisun, ECDL Foundation ei anna takeita tässä esitetyn tiedon täydellisyydestä. ECDL Foundation ei myöskään ole vastuussa mistään tappioista tai vahingoista, jotka saattavat aiheutua tässä julkaisussa esitetyistä ohjeista tai neuvoista. ECDL:n tutkintovaatimusten asiakirjoihin voidaan tehdä muutoksia ECDL Foundationin valinnan mukaan.

ECDL Tietoturva - IT Security

Tässä esitellään tutkintovaatimukset tietoturvamoduulille, joka määrittelee tarvittavat tiedot ja taidot näyttökokeen suorittamiseen.

Moduulin tavoitteet

Moduulin suorittamisen jälkeen kokelas osaa:

- Ymmärtää tietoturvan tärkeyden ja tunnistaa yleisimmät tietoturvan ja tiedonhallinnan periaatteet.
- Tunnistaa henkilökohtaisen suojauksen uhat (identiteettivarkaus, mahdolliset haittaohjelmat ja jopa pilvipalveluiden käyttämisen uhat)
- Osaa käyttää salasanoja ja salausta suojatakseen tiedostoja ja data.
- Ymmärtää haittaohjelmien uhan ja osaa suojata tietokoneen, laitteen tai verkon haittaohjelmilta
- Tunnistaa yleisimmät verkko- ja langaton verkkotyypit ja osaa hallita henkilökohtaisia palomuureja ja hotspotteja.
- Suojata tietokoneen tai laitteen luvattomalta yhteydenotolta ja hallita salasanoja turvallisesti
- Käyttää sopivia selainasetuksia ja ymmärtää miten verkossa surffataan turvallisesti
- Ymmärtää kommunikaatioon liittyvät tietoturvariskit, joita voi kohdata käyttäessään sähköpostia, sosiaalisia verkostoja, VoIP:ia, pikaviestintää ja mobiililaitteita
- Varmuuskopioida ja palauttaa tietoja paikalliseen / pilvitallennustilaan sekä poistaa tietoa ja hävittää laitteita turvallisesti

1 Turvallisuus konseptit	*1.1 Datan uhat*	1.1.1	Datan ja tiedon erottaminen.
		1.1.2	Termin verkkorikollisuus ymmärtäminen.
		1.1.3	Ymmärtää termien hakkerointi, krakkerointi ja eettinen hakkerointi eroavaisuudet.
		1.1.4	Ymmärtää erilaiset pakottavat uhat kuten: tulipalot, sodat, tulvat ja maanjäristykset.
		1.1.5	Tunnistaa erilaiset pilvipalvelussa dataan kohdistuvat uhat kuten: datan hallinnoiminen sekä datan yksityisyyden mahdollinen menettäminen.
	1.2 Tiedon arvo	1.2.1	Ymmärtää syyt henkilötietojen turvaamiseen esim. Identiteettivarkauden estäminen sekä erilaiset huijauksien välttäminen.
		1.2.2	Ymmärtää syyt suojata kaupalliseen käyttöön tarkoitettua hienovaraista tietoa estääkseen mm. Varkauksia, asiakastietojen väärinkäyttämistä sekä suojatakseen taloustietoja.

		1.2.3	Tunnistaa tavat joilla voidaan estää sallimattomat pääsyt verkkoon tai tietoihin esim. salasanoilla sekä enkryptauksella.
		1.2.4	Ymmärtää tietoturvan peruskäsitteitä kuten: luottamuksellisuus, eheys ja saatavuus.
		1.2.5	Tunnistaa tietojen/yksityisyyden suojausta ja säilyttämistä sekä hallintaa oman maan lakien ja käytäntöjen mukaisesti.
		1.2.6	Ymmärtää IT-käytäntöjen, strategioiden sekä ohjeistuksien merkityksen organisaatiossa.
	1.3 Henkilökohtainen turva	1.3.1	Ymmärtää termin sosiaalinen manipulointi ja sen seuraukset esim. Huijaukset, yksityisyyden tai tietojen menettäminen yms.
		1.3.2	Tunnistaa sosiaalisen manipuloinnin keinot kuten: puhelut, tietokalastelun (phishing, pharming), ja olantakaasurffauksen (shoulder surffing)
		1.3.3	Ymmärtää termin identiteettivarkaus ja sen seuraukset henkilölle ja yritykselle sekä lain mukaan että rahallisesti.
		1.3.4	Tunnistaa identiteettivarkauden keinot kuten: tietokalastelu, skimmaus, toisena ihmisenä esittäytyminen.
	1.4 Tiedostojen turvallisuus	1.4.1	Ymmärtää makrojen turva-asetuksien kytkemisen päälle/pois
		1.4.2	Tietää kuinka käyttää salasanaa esim. Dokumenttien, pakattujen tiedostojen sekä laskutaulukkojen salaukseen.
		1.4.3	Osaa salata (enkryptata) tiedoston, kansion ja aseman.
		1.4.4	Ymmärtää salauksen hyödyt ja rajoitteet.
2 Haittaohjelmat	*2.1 Määritelmät ja tyypit*	2.1.1	Ymmärtää termin haittaohjelma. Tunnistaa erilaisia tapoja, jolla haittaohjelmat piilotetaan kuten: Troijalaiset, rootkitit ja takaovet.
		2.1.2	Tunnistaa tarttuvat haittaohjelmat ja miten ne toimivat, kuten: virukset, madot.
		2.1.3	Tunnistaa tietovarkauden, haittaohjelmat joilla tehdään rahaa ja ymmärtää kuinka ne toimii, esimerkkitekniikkoina adware, spyware, botnet sekä painallusten nauhoitus.

	2.2 Suojaaminen	2.2.1	Ymmärtää miten virustorjuntaohjelmisto toimii ja mitkä ovat sen rajoitukset.
		2.2.2	Ymmärtää kuinka virustentorjuntaohjelmisto tulee asentaa tietokoneille ja laitteille.
		2.2.4	Osaa skannata määrätyt asemat, kansiot ja tiedostot virustorjuntaohjelmistolla. Ajastaa virustorjuntaohjelmiston skannauksia.
		2.2.5	Ymmärtää vanhentuneiden ja ei-tuettujen ohjelmistojen riskit kuten: kasvaneet haittaohjelmien uhat ja yhteensopimattomuudet
	2.3 Selvittäminen ja poistaminen	2.3.1	Ymmärtää termin karanteeni ja karanteenin toiminnan sekä kuinka sitä käytetään tartunnan saaneisiin/ saastuneisiin tiedostoihin.
		2.3.2	Osaa käyttää karanteenia ja poistaa tartunnan saaneet/epäilyttävät tiedostot.
		2.3.3	Ymmärtää kuinka haittaohjelmien hyökkäykset voidaan tunnistaa ja selvittää käyttäen verkkoresursseja kuten: käyttöjärjestelmien web-sivuja, virustentorjuntaa, web-selaimien ohjelmistotoimittajia, asiaankuuluvien viranomaisten web-sivuja.
3 Verkon suojaus	*3.1 Verkot ja yhteydet*	3.1.1	Tunnistaa sanan verkko ja tietoverkko sekä tunnistaa yleiset verkkotyypit kuten: LAN (Local Area Network), WAN (Wide Area Network), sekä VPN (Virtual private Network).
		3.1.2	Ymmärtää verkkoon yhdistämisessä piilevät riskit kuten: haittaohjelmat, tietojen luvattoman käytön, yksityisyyden ylläpitäminen.
		3.1.3	Ymmärtää verkon ylläpitäjän roolin tunnistuksen hallinnassa, valtuutuksissa, tilien hallinnassa, asiaankuuluvien tietoturvapäivitysten asentamisen, verkkoliikenteen tarkkailussa ja verkosta löytyneiden haittaohjelmien käsittelemisessä.
		3.1.4	Ymmärtää palomuurin toiminnan ja rajoitukset työympäristössä.
		3.1.5	Osaa kytkeä henkilökohtaisen palomuurin päälle/pois käytöstä, sekä osaa sallia ja estää sovelluksen/palvelun omassa henkilökohtaisessa palomuurissa.
	3.3 Langaton tietoturva	3.2.1	Tunnistaa langattoman verkon erityyppiset salaukset kuten: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Media Access Control (MAC)

		3.2.2	Tietää että suojaamattoman verkon käyttäminen voi johtaa tietojen haluamattomaan vakoiluun tai tarkkailuun.
		3.2.3	Ymmärtää termin henkilökohtainen kuuluvuusalue (HotSpot)
4 Käyttöoikeuksien valvonta	*4.1 Keinot*	4.1.1	Osaa kytkeä sekä ottaa pois päältä oman henkilökohtaisen HotSpotin. Osaa myös turvallisesti kytkeä sekä irroittaa kannettavia laitteita.
		4.1.2	Tunnistaa tavat joilla voidaan suojautua datan haluamattomilta käyttäjiä vastaan keinoilla kuten: käyttäjätunnusten, salasanojen, PIN-koodien, salausta (enkryptausta), sekä monivaiheista tunnistusta käyttämällä
		4.1.3	Ymmärtää termin kertakäyttöinen salasana sekä ymmärtää missä sitä tavanomaisimmin käytetään
		4.1.4	Ymmärtää kuinka ja miksi verkkotunnuksia käytetään.
		4.1.5	Ymmärtää verkkotunnusten käytön ja kuinka tunnukset tulisi suojata nimellä ja salasanalla. Ymmärtää myös miksi kaikilta tunnuksilta tulisi kirjautua ulos tai ne tulisi lukita kun eivät ole käytössä. Tunnistaa yleiset biometriset turvallisuustoimenpiteet joita käytetään kulunvalvontaan kuten: sormenjäljet sekä verkkokalvoskannaus.
	3.4 Salasanojen hallinta	4.2.1	Tunnistaa hyvien salasanojen luomiseen liittyvät käytännöt: kuten: ettei jaa omaa salasanaansa, salasanan vaihtaminen aika ajoin, salasanan riittävä pituus ja että se sisältää erilaisia merkkejä kuten kirjaimia, numeroita sekä erikoismerkkejä.
		4.2.2	Ymmärtää salasanojen hallintaan käytettävien ohjelmien toimivuuden sekä rajoitukset
5 Turvallinen Internetin käyttäminen	*4.1 Internetin käyttö*	4.1.1	Osaa suhtautua kriittisesti mahdollisesti vaarallisiin online-aktiviteetteihin kuten: verkko-ostoksiin sekä rahansiirtoon Internetissä ja tietää että niitä tulee käyttää vain suojatuilla sivuilla.
		4.1.2	Tunnistaa turvallisen web-sivun joissa on esimerkiksi: https: -alkuinen domain tai lukko symboli.
		4.1.3	Osaa varoa laajempaa tietokalastelua

			(pharming).
		4.1.4	Ymmärtää termin digitaalinen sertifikaatti ja sen käytön.
		4.1.5	Ymmärtää termin kertakäyttöinen salasana/pääsykoodi.
		4.1.6	Osaa valita oikeat asetukset salliakseen/estääkseen lomakkeiden automaattisen täytön sekä automaattisen tallennuksen.
		4.1.7	Ymmärtää termin eväste.
		4.1.8	Osaa valita oikeat asetukset salliakseen tai estääkseen evästeet.
		4.1.9	Osaa poistaa henkilökohtaiset tiedot selaimesta kuten: selaushistorian, tilapäiset tiedostot, salasanat, evästeet, sekä automaattiset täytöt.
		4.1.10	Ymmärtää erilaisten sisällönhallinta ohjelmien tarkoituksen ja käyttämisen kuten: Internetin suodatin ja esto-ohjelmat sekä digitaalisen lapsilukon käytön.
	4.2 Sosiaalinen media	4.2.1	Ymmärtää henkilökohtaisten tietojen sekä yksityisyyden tärkeyden ajatellen sosiaalista mediaa.
		4.2.2	Osaa katsoa ja valita oikeat yksityisyysasetukset sosiaalisen median eri sivustoilla.
		4.2.3	Ymmärtää sosiaalisen median käytön potentiaaliset vaarat ja haitat sekä osaa varoa niitä esimerkiksi: nettikiusaamisen, erilaista houkuttelua, väärää/haitallista tietoa, vääriä identiteettejä, haitallisia linkkejä tai viestejä.
5 Viestintä	*5.1 Sähköposti*	5.1.1	Ymmärtää sähköpostien salaamisen (enkryptaus) sekä purkamisen (dekryptaus) tarkoituksen.
		5.1.2	Ymmärtää termin digitaalinen allekirjoitus.
		5.1.3	Osaa tehdä ja lisätä digitaalisen allekirjoituksen.
		5.1.4	Osaa varoa sähköpostiin tulevaa pyytämätöntä ja petollista sähköpostia.
		5.1.5	Ymmärtää termin tietokalastus (phishing) ja tunnistaa tietokalastuksen piirteitä esim. Toisena yrityksenä tai ihmisenä esiintyminen tai huijaussivustot.
		5.1.6	Osaa varoa tartuttamasta tietokonetta haitallisilla ohjelmilla sekä käyttää

			suhtautua kriittisesti avatessa sähköpostin liitteitä jotka sisältävät makroja tai ajettavia exe-tiedostoja.
	5.2 Pikaviestintä	5.2.1	Ymmärtää termin pikaviestintä sekä sen käyttötarkoituksen.
		5.2.2	Ymmärtää pikaviestimien haavoittuvaisuudet kuten: haittaohjelmat, takaovet, sekä pikaviestimien mahdollisen yhteyden tiedostoihin ja tietoihisi.
		5.2.3	Tunnistaa tavat joilla voidaan varmistaa luottamuksellisuus pikaviestinnässä esimerkkinä: enkryptaus, pikaviestien sisällön harkitseminen, sekä kriittisyys tiedostojen jaossa.
6 Turvallinen tiedonhallinta	*6.1 Tietojen turvaaminen ja varmuuskopiointi*	6.1.1	Tunnistaa tavat joilla voidaan varmistaa laitteiden fyysinen turvallisuus esimerkkinä: laitteiden fyysinen sijainti, kaapelilukkojen käyttö, sekä kulunvalvonta.
		6.1.2	Tunnistaa varmuuskopioinnin tärkeyden siltä varalta että erilaista dataa tai tietoja häviää tai tuhoutuu.
		6.1.3	Tunnistaa erilaisia varmuuskopiointiin liittyviä asioita kuten: säännöllisyys, aikataulutus, säilytyspaikka.
		6.1.4	Tietojen varmuuskopiointi.
		6.1.5	Tietojen palauttaminen ja palautetun tiedon vahvistaminen.
	6.2 Turvallinen tietojen tuhoaminen	6.2.1	Ymmärtää syyt datan pysyvän poistamisen asemilta ja laitteista.
		6.2.2	Ymmärtää datan pysyvän tuhoamisen ja poistamisen eron.
		6.2.3	Tunnistaa yleiset menetelmän datan pysyvään tuhoamiseen kuten: silppuaminen, kovalevyn demagnetoinnin, aseman formatoinnin ja tietää datan tuhoamis-työkalujen käytöstä.