IT-biztonság

Syllabus 1.0

A syllabus célja

Ez a dokumentum részletesen ismerteti az *IT-biztonság* modult és megfelelő alapokat ad az elméleti és gyakorlati vizsgához is.

© 2014 ECDL Alapítvány

Jogi nyilatkozat

A modul célja

Az IT-biztonság ECDL modul célja, hogy a vizsgázó megértse az IKT (infokommunikációs technológiai) eszközök mindennapos biztonságos használatának, a biztonságos hálózati kapcsolatok fenntartásának feltételeit; képes legyen a biztonságos és magabiztos Internet-használatra, és az adatok és információk megfelelő kezelésére.

A vizsga követelményei:

- a biztonságos információ és adat fontosságára, a fizikai biztonságra, a személyes adatok védelmére és a személyazonosság-eltulajdonításra vonatkozó kulcsfogalmak;
- a számítógép, egyéb eszközök és a hálózat megvédése rosszindulatú szoftverektől és a jogosulatlan hozzáférésektől;
- a hálózatok típusai, a kapcsolódási típusok és hálózat-specifikus kérdések, ideértve a tűzfalakat is;
- biztonságos böngészés a World Wide Weben és biztonságos kommunikáció az interneten
- az e-mailekre és azonnali üzenetküldőkre vonatkozó biztonsági kérdések
- az adatok biztonságos mentése és visszaállítása; adatok biztonságos megsemmisítése.

A jelöltnek képesnek kell lenni, hogy:

- megérteni és azonosítani a napi szintű infokommunikációs eszközhasználat alapjául szolgáló legfontosabb fogalmakat
- megfelelő technikákat és alkalmazásokat használni a biztonságos hálózati kapcsolat fenntartására
- biztonságosan és megbízhatóan használni az internetet
- megfelelően kezelni az adatokat és az információkat
- megérteni az információk és adatok védelmének fontosságára, a fizikai biztonságra, személyes adatok védelmére és eltulajdonításának megakadályozására vonatkozó kulcsfogalmakat
- megvédeni a számítógépet, eszközöket vagy hálózatot a rosszindulatú programoktól és jogosulatlan hozzáférésektől
- megérteni a hálózati típusokat, a kapcsolatok formáit és a hálózat-specifikus témákat, beleértve a tűzfalakat
- biztonságosan böngészni a World Wide Web-en és biztonságosan kommunikálni az interneten
- megérteni az e-mailekre és azonnali üzenetküldőkre vonatkozó biztonsági kérdéseket
- biztonságosan és megfelelően menteni és visszaállítani az adatokat, valamint biztonságosan megsemmisíteni az adatokat és eszközöket.

Kategória	Tudásterület	Hivatkozás	Tudáselem
1. Biztonsággal kapcsolatos fogalmak	*1.1 Az adatok fenyegetettsége*	1.1.1	Az adat és az információ közötti különbség
		1.1.2	A kiberbűnözés fogalma
		1.1.3	A hackelés, a crackelés és az etikus hackelés közötti különbségek
		1.1.4	Az adatok előre nem látható körülmények általi fenyegetettségének felismerése (tűz, áradás, háború, földrengés)
		1.1.5	Az adatok munkatársak, szolgáltatók és külső személyek általi fenyegetettségének megismerése
	1.2 Az információ értéke	1.2.1	A személyesinformáció-védelem szükségessége (személyazonosság-lopás, és a csalások megelőzése)
		1.2.2	Az üzletileg érzékeny információk védelmének fontossága (ügyfelek adatainak megszerzése, vagy a pénzügyi adatok ellopása, illetve jogosulatlan felhasználása)
		1.2.3	A jogosulatlan adat-hozzáférést megakadályázó védelmi intézkedések (titkosítás és a jelszavak)
		1.2.4	Az információbiztonság alapvető jellemzői (bizalmasság, sértetlenség és rendelkezésre állás)
		1.2.5	A főbb információ- és adatvédelmi, megőrzési, valamint a védelmi intézkedésekre vonatkozó követelmények Magyarországon
		1.2.6	Az IKT használatra vonatkozó szabályzatok és útmutatók jelentősége
	1.3 Személyi biztonság	1.3.1	A számítógépes szélhámosság (social engineering) fogalmának és jelentőségének megértése (információ-gyűjtés, csalás, számítógépes rendszerek való hozzáférés)
		1.3.2	A számítógépes szélhámosság módszerei (telefonhívások, adathalászat (phishing), kifigyelés (shoulder surfing).
		1.3.3	A személyazonosság-lopás fogalma és következményei (személyes, pénzügyi, üzleti, törvényi)
		1.3.4	A személyazonosság-lopás módszerei (információ búvárkodás (information diving), bankkártya-lemásolás (skimming), kikérdezés (pretexting).
	1.4 Fájl-biztonság	1.4.1	A makró engedélyezésének és tiltásának biztonságra gyakorolt hatásai
		1.4.2	Fájlok jelszavas védelemmel való ellátása (dokumentumok, tömörített fájlok, táblázatok)
		1.4.3	A titkosítás előnyei és korlátai
2. Rosszindulatú szoftverek	*2.1 Definíciók és funkcionalitások*	2.1.1	A rosszindulatú szoftver (malware) fogalma

		2.1.2	A rosszindulatú szoftverek különböző elrejtési módjai (trójaiak (trojans), rendszerszinten rejtőző kártékony kód (rootkit) és hátsó kapuk (back door)
	2.2 Típusok	2.2.1	A rosszindulatú fertőző szoftverek típusai (vírusok, férgek)
		2.2.2	Az adatlopások típusai, és a profit-generáló/zsaroló rosszindulatú szoftverek (reklám-szoftver (adware), kém-szoftver (spyware), zombi-hálózat szoftver (botnet), billentyűzet-leütés naplózó (keystroke-logging) és modemes tárcsázó (diallers).
	2.3 Védekezés	2.3.1	Az antivírus szoftverek működése és korlátai
		2.3.2	A kiválasztott meghajtók könyvtárak, fájlok vizsgálata és a vizsgálatok ütemezése antivírus szoftverrel
		2.3.3	A karantén fogalma és a fertőzött vagy gyanús fájlok elkülönítése
		2.3.4	A vírusirtó-szoftver frissítése és vírus-definíciós fájl letöltése; a telepítés fontossága
3. Hálózatbiztonság	*3.1 Hálózatok*	3.1.1	A hálózat fogalma és az általános hálózat-típusok (helyi hálózatok /LAN/, nagy kiterjedésű hálózatok /WAN/, illetve virtuális magánhálózatok /VPN/.
		3.1.2	A hálózati adminisztrátor szerepe a hálózaton belüli hitelesítés, feljogosítás és számonkérés kezelésében
		3.1.3	A tűzfal funkciója és korlátai
	3.2 Hálózati kapcsolatok	3.1.1	A hálózatokhoz való kapcsolódási lehetőségek (kábeles és drótnélküli kapcsolat)
		3.1.2	a hálózati kapcsolódás hatása a biztonságra (rosszindulatú szoftverek, jogosulatlan adat-hozzáférés, privátszféra fenntartása)
	3.3 Drótnélküli (wireless) biztonság	3.3.1	A jelszóhasználat fontossága a drótnélküli hálózatok védelmében
		3.3.2	A drótnélküli biztonság különböző típusai (kábeles kapcsolódással megegyező privátszféra /WEP/, WiFi védett hozzáférés /WPA/, média hozzáférés-védelem /MAC/)
		3.3.3	A nem védett drótnélküli hálózat használatának kockázatai: adataink megismerése a drót nélkül lehallgatók számára
		3.3.4	Kapcsolódás védett/nem védett drótnélküli hálózathoz
	3.4 Hozzáférés-védelem	3.4.1	A hálózati fiók célja és a felhasználói név-jelszó párral való hozzáférés szükségessége
		3.4.2	A jó jelszó-szabályozások (a jelszavak másokkal való nem- megosztása, időszakos megváltoztatása, megfelelő jelszó-hossz, megfelelő jelszó-karakterek – betűk, számok és speciális karakterek – együttes használata
		3.4.3	A hozzáférés-védelemben általánosan használt biometriai biztonsági technikák (ujjlenyomat, retina-szkenner)

4. Biztonságos web-használat	*4.1 Böngészés a weben*	4.1.1	Bizonyos online tevékenységek (vásárlás, pénzügyi tranzakciók) biztonságos web-oldalakon végzésének jelentősége
		4.1.2	A biztonságos weboldalak beazonosítása (https, zár-szimbólum)
		4.1.3	Az eltérítéses adathalászat (pharming) fogalma
		4.1.4	A digitális tanúsítvány fogalma, érvényessége
		4.1.5	Az egyszerhasználatos jelszó (one time password - OTP) fogalma
		4.1.6	Az űrlapok kitöltésekor a megfelelő engedélyezési, tiltási, automatikus kitöltési, automatikus mentési beállítások kiválasztása
		4.1.7	A süti (cookie) fogalma
		4.1.8	Megfelelő beállítások kiválasztása a sütik engedélyezéséhez és blokkolásához
		4.1.9	A személyes adatok törlése a böngészőkből (böngészési előzmények, ideiglenesen tárolt internet-fájlok, jelszavak, sütik, automatikusan kitöltött űrlap-adatok)
		4.1.10	A tartalom-ellenőrző szoftverek célja, funkciója és típusai (internet tartalmát szűrő szoftver, szülői felügyeleti szoftver)
	4.2 Közösségi hálózatok	4.2.1	A bizalmas információk közösségi oldalakon való nem felfedésének fontossága
		4.2.2	A megfelelő privátszféra beállítások alkalmazása a közösségi oldalak felhasználói fiókjaiban
		4.2.3	A közösségi oldalak használatából adódó lehetséges veszélyek (internetes zaklatás (cyber bullying), szexuális kizsákmányolás (grooming), félrevezető/veszélyes információk, hamis személyazonosságok, csalárd linkek vagy üzenetek)
5. Kommunikáció	*5.1 E-mail*	5.1.1	Az e-mailek be- és kititkosításának célja
		5.1.2	A digitális aláírás fogalma
		5.1.3	Digitális aláírás készítése és hozzáadása
		5.1.4	Csalárd és kéretlen levelek fogadásával kapcsolatos ismeretek
		5.1.5	Az adathalászat fogalmának megértése, általános jellemzői (létező cég, személy nevének felhasználása, hamis web-linkek)
		5.1.6	A makrókat vagy futtatható fájlokat tartalmazó e-mail csatolmányok megnyitásának kockázata (a számítógép rosszindulatú kódokkal való megfertőződésének veszélye)
	5.2 Azonnali üzenetküldés (IM)	5.2.1	Az azonnali üzenetküldés (Instant Messaging - IM) fogalma és jelentősége
		5.2.2	Az azonnali üzenetküldés biztonsági sebezhetősége (rosszindulatú szoftverek, hátsó kapu hozzáférés, fájl-hozzáférés)
		5.2.3	Az azonnali üzenetküldés bizalmasságát biztosító módszerek (titkosítás, fontos információk titokban tartása, fájl-megosztás korlátozása)

6. Az adatok biztonságos kezelése	*6.1 Az adatok védelme és mentése*	6.1.1	Az eszközök fizikai biztonságát biztosító módszerek (eszközök elhelyezésének és részleteinek naplózása, kábelek zárolása, fizikai hozzáférés-védelem)
		6.1.2	A mentési eljárás fontossága az adatok, pénzügyi feljegyzések, webes könyvjelzők/előzmények elvesztésének esetében
		6.1.3	A mentési eljárás tulajdonságai (ismétlődés/gyakoriság, ütemezés, tárolóhely-elhelyezkedés)
		6.1.4	Az adatok mentése
		6.1.5	A mentett adatok visszatöltése, a mentés érvényessége
	6.2 Biztonságos adat-megsemmisítés	6.2.1	A meghajtókról vagy eszközökről való végleges adattörlés jelentősége
		6.2.2	Az adatok törlése és végleges megsemmisítése közötti különbség
		6.2.3	A végleges adat-megsemmisítés általános módszerei (feldarabolás, meghajtó/média megsemmisítés, demagnetizálás, adat-megsemmisítő eszközök használata)