ECDL Foundation

ECDL / ICDL Modul 12 – Bezpečnosť pri využívaní IKT

Sylabus, verzia 1.0

ECDL / ICDL Module 12 - IT Security

Syllabus Version 1.0

Syllabus Version 1.0

PREHLÁSENIE (zrieknutie sa zodpovednosti)

Hoci príprave tejto publikácie bola v ECDL Foundation venovaná najvyššia pozornosť, ECDL Foundation nedáva ako vydavateľ žiadnu záruku na úplnosť informácií v tomto materiáli a ECDL Foundation nemá povinnosť ani zodpovednosť v spojení s akýmikoľvek chybami, omylmi, nepresnosťami, stratou alebo škodou, ktorá by kedykoľvek vznikla na základe informácií alebo inštrukcií obsiahnutých v tomto materiáli. ECDL Foundation si vyhradzuje právo vykonávať zmeny podľa vlastného uváženia a bez predchádzajúceho upozornenia.

Oficiálna verzia tohto materiálu je verzia zverejnená na webovej stránke ECDL Foundation: www.ecdl.org

ECDL Modul 12 – Bezpečnosť pri využívaní IKT

Tento dokument uvádza *v plnom znení* sylabus pre Modul 12 - *Bezpečnosť pri využívaní IKT. Sylabus podrobne popisuje* znalosti a zručnosti, ktoré by uchádzač o certifikát z tejto oblasti mal mať. Sylabus je zároveň aj východiskom pre zostavenie teoretických a praktických testov na overenie znalostí a zručností z tejto oblasti.

Ciele modulu

Modul 12

Bezpečnosť pri využívaní IKT, vyžaduje od uchádzača pochopenie základných pojmov, ktoré podporujú bezpečné používanie IKT v každodennom živote a využívanie zodpovedajúcich techník a aplikácií na udržiavanie bezpečného pripojenia do počítačovej siete, spoľahlivé a bezpečné využívanie internetu a zodpovedajúce spracovanie údajov a informácií. Úspešný uchádzač bude vybavený schopnosťou bezpečne pracovať s IKT a zvládať bežné bezpečnostné situácie, s ktorými bude konfrontovaný pri pouzívaní IKT.

Uchádzač bude schopný:

- rozumieť základným pojmom, ktoré sa týkajú dôležitosti zabezpečenia údajov a informácií, ich fyzickej bezpečnosti, ako aj hrozieb krádeže súkromia a identity,
- chrániť počítač, prislúchajúce zariadenia a počítačovú sieť pred škodlivým softvérom a neautorizovaným prístupom,
- rozoznávať typy počítačových sietí a typy pripojení k nim a rozumieť špecializovaným otázkam z oblasti počítačových sietí vrátane pojmu firewall,
- pohybovať sa po webe a bezpečne komunikovať na Internete,
- rozumieť bezpečnostným otázkam z oblasti elektronickej komunikácie vrátane elektronickej pošty (e-mailu) a komunikácie v sieti v reálnom čase (Instant Messaging),
- správne a spoľahlivo zálohovať a obnovovať údaje, bezpečne spravovať údaje a príslušné zariadenia.

KATEGÓRIA	OBLASŤ VEDOMOSTÍ	REF.	VYŽADOVANÁ ZNALOSŤ
12.1 Pojmy z oblasti informačnej bezpečnosti	*12.1.1 Ohrozenie údajov*	12.1.1.1	Rozlišovať medzi údajom a informáciou.
		12.1.1.2	Rozumieť pojmu kyberzločin (cybercrime).
		12.1.1.3	Rozumieť rozdielom medzi pojmami hacking, cracking a etický hacking.
		12.1.1.4	Rozlišovať ohrozenie údajov z vyššej moci, ako sú: požiar, potopa, vojna, zemetrasenie.
		12.1.1.5	Rozlišovať ohrozenie údajov zo strany zamestnancov, poskytovateľov služieb ako aj zvonka pôsobiacich jednotlivcov.
	12.1.2 Hodnota informácie	12.1.2.1	Rozumieť dôvodom na ochranu osobných údajov, ako sú: predchádzanie krádeži identity, získanie údajov podvodom.
		12.1.2.2	Rozumieť dôvodom na ochranu obchodne citlivých informácií, ako sú: predchádzanie krádeži alebo zneužitiu detailov o klientovi, ochrana finačných informácií.
		12.1.2.3	Poznať opatrenia na zamedzenie neoprávnenému prístupu k údajom, ako sú: šifrovanie alebo používanie hesiel.

KATEGÓRIA	OBLASŤ VEDOMOSTÍ	REF.	VYŽADOVANÁ ZNALOSŤ
		12.1.2.4	Rozumieť základným charakteristikám informačnej bezpečnosti, ako sú: dôvernosť, integrita (celistvosť), dostupnosť.
		12.1.2.5	Poznať hlavné požiadavky na ochranu, uchovávanie a riadenie prístupu k údajom a osobným informáciám v Slovenskej republike.
		12.1.2.6	Rozumieť významu vytvárania a dodržiavania bezpečnostných zásad a politík, ktoré sa týkajú využívania informačných a komunikačných technológií.
	12.1.3 Osobná bezpečnosť	12.1.3.1	Rozumieť pojmu sociálne inžinierstvo a jeho následkom, ako sú: zhromažďovanie informácií, podvodné konanie, neoprávnený prístup k počítačovým systémom.
		12.1.3.2	Poznať metódy sociálneho inžinierstva, ako sú: telefonáty vrátane napodobenín automatických telefonických hlások, podvodné získavanie prístupových údajov (phishing), odpozorovanie displeja (shoulder surfing).
		12.1.3.3	Chápať pojem krádež identity a jeho osobné, finančné obchodné a právne dôsledky.
		12.1.3.4	Rozlišovať metódy krádeže identity, ako sú: information diving[1], skimming[2], pretexting[3].
	12.1.4 Bezpečnosť súborov	12.1.4.1	Rozumieť bezpečnostným dôsledkom spojeným s povolením / zakázaním makier.
		12.1.4.2	Nastavenie hesla pre súbory, ako sú: dokumenty, komprimované súbory, výpočtové tabuľky (spreadsheets)
		12.1.4.3	Chápať výhody a obmedzenia pri šifrovaní súborov.
12.2 Škodlivý softvér (malware)	*12.2.1 Definície a funkcie*	12.2.1.1	Rozumieť pojmu škodlivý softvér (malware).
		12.2.1.2	Rozlišovať rôzne spôsoby skrývania sa škodlivého softvéru, ako sú: trójske kone, maskujúce sa aplikácie (rootkit), zadné dvierka (back door).
	12.2.2 Typy	12.2.2.1	Poznať rôzne typy nákazlivého škodlivého softvéru, ako sú: vírusy alebo červy, a rozumieť ich pôsobeniu.
		12.2.2.2	Rozlišovať formy odcudzenia údajov, typy škodlivého softvéru zameraného na dosiahnutie zisku / predražovanie a chápať na akom princípe fungujú škodcovia ako: adware[4], spyware[5], keylogger[6] (keystroke logging), botnet[7], dialler[8].
	12.2.3 Ochrana	12.2.3.1	Rozumieť princípom fungovania antivírusového softvéru a

[1] neoprávnené obnovovanie vymazaných dôverných informácií
[2] používanie technických prostriedkov na krádež údajov z identifikačných prvkov, napr. z platobných kariet
[3] využívanie naoko dôveryhodných scenárov za účelom získavania citlivých informácií
[4] škodlivý reklamný softvér
[5] "špehovací" softvér na zisťovanie a odosielanie citlivých údajov v počítači bez vedomia používateľa
[6] softvér na odchytávanie stlačených kláves
[7] škodlivý softvér, ktorý vybrané počítače (pripojené k internetu) v pozadí podriadi tretej osobe a vytvorí z nich svoju sieť
[8] Softvér, ktorý uskutočňuje drahé telefonické hovory na účet používateľa bez jeho vedomia

KATEGÓRIA	OBLASŤ VEDOMOSTÍ	REF.	VYŽADOVANÁ ZNALOSŤ
			poznať jeho obmedzenia.
		12.2.3.2	Vedieť pomocou antivírusového softvéru skontrolovať (skenovať) konkrétnu pamäťovú jednotku, priečinok alebo súbory. Vedieť naplánovať uskutočnenie kontroly (skenovania) s využitím antivírusového programu.
		12.2.3.3	Rozumieť pojmu karanténa a chápať účinok umiestnenia infikovaných alebo podozrivých súborov do karantény.
		12.2.3.4	Rozumieť významu a chápať dôležitosť sťahovania a inštalácie aktualizácií antivírusového programu a jeho vírusovej databázy.
12.3 Bezpečnosť počítačových sietí	*12.3.1 Počítačové siete*	12.3.1.1	Rozumieť pojmu počítačová sieť a rozlišovať jednotlivé typy počítačových sietí, ako sú: lokálne siete (LAN), rozľahlé siete (WAN), virtuálne privátne siete (VPN).
		12.3.1.2	Chápať úlohu správcu počítačovej siete v procese autentifikácii[9], autorizácii[10] a správe používateľských účtov v rámci siete.
		12.3.1.3	Rozumieť pojmu firewall, chápať jeho funkciu a poznať jeho obmedzenia.
	12.3.2 Pripájanie sa k sieti	12.3.2.1	Rozlišovať spôsoby pripojenia sa k sieti, ako sú: káblové alebo bezdrôtové pripojenie.
		12.3.2.2	Chápať aký vplyv na bezpečnosť môže mať pripojenie sa do siete, napríklad na šírenie škodlivého softvéru, na neoprávnený prístup k údajom, na narušenie súkromia.
	12.3.3 Bezpečnosť bezdrôtovej siete	12.3.3.1	. Chápať dôležitosť používania hesla pri ochrane prístupu k bezdrôtovej sieti.
		12.3.3.2	Rozlišovať jednotlivé typy zabezpečenia bezdrôtovej siete, ako sú: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Media Access Control (MAC).
		12.3.3.3	Uvedomovať si, že používanie nezabezpečenej počítačovej siete môže umožniť „sliedičom“ prístup k vašim údajom.
		12.3.3.4	Vedieť sa pripojiť k zabezpečenej / nezabezpečenej bezdrôtovej sieti.
	12.3.4 Riadenie prístupu k sieti	12.3.4.1	Poznať účel používateľského účtu v počítačovej sieti a chápať význam používateľského mena a hesla na prístup k používateľskému účtu.
		12.3.4.2	Poznať zásady pre výber / politiku hesiel, ako sú: nezdieľanie hesla, pravidelná zmena hesla, primeraná dĺžka hesla, vhodná štruktúra hesla s využitím kombinácie písmen, číslic a špeciálnych znakov.
		12.3.4.3	Poznať bežné techniky riadenia prístupu k sieti na základe biometrických údajov, ako sú: odtlačky prstov alebo obraz (sken)dúhovky oka.

[9] overovanie identity používateľov

[10] poskytovanie oprávnení

KATEGÓRIA	OBLASŤ VEDOMOSTÍ	REF.	VYŽADOVANÁ ZNALOSŤ
12.4 Bezpečná práca s webom	*12.4.1 Prezeranie webových stránok*	12.4.1.1	Uvedomovať si, že niektoré činnosti na webe (online nákupy, finančné transakcie) by sa mali uskutočňovať iba na zabezpečených webových stránkach.
		12.4.1.2	Rozpoznať zabezpečenú webovú stránku, napríklad na základe označenia jej protokolu ako https alebo zobrazenia symbolu zámku.
		12.4.1.3	Byť si vedomý, čo znamená a spôsobuje presmerovanie na podvrhnuté webové stránky (pharming).
		12.4.1.4	Rozumieť pojmu digitálny certifikát, vedieť overovať digitálny certifikát.
		12.4.1.5	Rozumieť pojmu jednorazové heslo.
		12.4.1.6	Dokázať zvoliť vhodné nastavenia pre umožnenie / zakázanie automatického dokončovania a automatického ukladania pri vypĺňaní formulárov.
		12.4.1.7	Rozumieť pojmu cookie.
		12.4.1.8	Dokázať zvoliť vhodné nastavenia na povolenie alebo blokovanie cookies.
		12.4.1.9	Dokázať odstrániť z webového prehliadača súkromné údaje, ako sú: história prehliadania, pamäť dočasných súborov (cache), heslá, cookies, údaje automatického dokončovania.
		12.4.1.10	Chápať účel, funkciu a poznať druhy softvéru na kontrolu obsahu webových stránok, ako sú: softvér na filtrovanie internetového obsahu, softvér na účely rodičovskej kontroly.
	12.4.2 Sociálne siete	12.4.2.1	Chápať dôležitosť neuvádzania dôverných informácií na stránkach sociálnych sietí.
		12.4.2.2	Uvedomovať si význam vhodného nastavenia úrovne súkromia účtu na sociálnej sieti.
		12.4.2.3	Poznať potenciálne nebezpečenstvá spojené s používaním sociálnych sietí, ako napríklad: internetové šikanovanie, predstieranie cudzej identity voči neplnoletým (grooming), zavádzajúce alebo nebezpečné informácie, falošná totožnosť, podvodné odkazy alebo správy.
12.5 Komunikácia	*12.5.1 Elektronická pošta (E-mail)*	12.5.1.1	Rozumieť účelu šifrovania / dešifrovania pri používaní elektronickej pošty.
		12.5.1.2	Rozumieť pojmu digitálny podpis.
		12.5.1.3	Vedieť vytvoriť digitálny podpis a pridať ho k správe / dokumentu v elektronickej pošte.
		12.5.1.4	Uvedomovať si možnosť obdržania podvodnej a nevyžiadanej správy elektronickej pošty.
		12.5.1.5	Rozumieť pojmu phishing. Poznať charakteristické znaky phishingu, ako sú: zneužívanie oficiálnych názvov firiem, používanie falošných odkazov na webové stránky.

KATEGÓRIA	OBLASŤ VEDOMOSTÍ	REF.	VYŽADOVANÁ ZNALOSŤ
		12.5.1.6	Uvedomovať si nebezpečenstvo nákazy počítača škodlivým softvérom pri otvorení prílohy elektronickej pošty, ktorá obsahuje makro alebo spustiteľný súbor.
	12.5.2 Komunikácia v sieti v reálnom čase (Instant Messaging, IM)	12.5.2.1	Rozumieť pojmu komunikácie v sieti v reálnom čase (instant messaging, IM) a jej používaniu.
		12.5.2.2	Rozumieť bezpečnostným hrozbám pri komunikácii v sieti v reálnom čase, ako je: škodlivý softvér, prístup prostredníctvom "zadných dvierok", neoprávnený prístup k súborom.
		12.5.2.3	Rozlišovať spôsoby zabezpečenia dôverných informácií pri komunikácii v sieti v reálnom čase, ako sú: šifrovanie, nezverejňovanie dôležitých informácií, obmedzenie zdieľania súborov.
12.6 Bezpečná správa údajov	*12.6.1 Bezpečnosť a zálohovanie*	12.6.1.1	Poznať spôsoby zabezpečenia fyzickej bezpečnosti zariadení obsahujúcich údaje, napríklad: ich vhodné umiestnenie, používanie káblových zámkov, kontrola prístupu.
		12.6.1.2	Chápať dôležitosť existencie záložných postupov v prípade straty údajov, finančných záznamov, záložiek webových stránok a histórie pohybu po webových stránkach.
		12.6.1.3	Poznať zásady správneho zálohovania, ako sú: pravidelnosť a frekvencia zálohovania, plán zálohovania, umiestnenie dátového úložiska.
		12.6.1.4	Vedieť zálohovať údaje.
		12.6.1.5	Vedieť obnoviť údaje zo zálohy a overiť ich.
	12.6.2 Bezpečná likvidácia	12.6.2.1	Rozumieť dôvodom, kvôli ktorým je potrebné trvalé odstránenie údajov z pamäťových médií a zariadení.
		12.6.2.2	Odlišovať vymazanie údajov od ich trvalého odstránenia.
		12.6.2.3	Poznať metódy na trvalú likvidáciu údajov, napríklad: skartácia, fyzická likvidácia zariadení a médií, demagnetizácia (degaussing), používanie softvérových prostriedkov na likvidáciu údajov.