k

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Metodika pre lektora

Vzdelávanie pre zamestnancov verejnej správy v kategórii používateľov „IT manažér“, „informatik“, „zamestnanec v kybernetickej bezpečnosti“

verzia 1.0

Košice, marec 2025

Úvodné poznámky

Krátka anotácia vzdelávania

Vzdelávací program pre zamestnancov verejnej správy v kategórií používateľov „IT manažér“, „informatik“, „zamestnanec v kybernetickej bezpečnosti“ sa zameriava na kľúčové oblasti kybernetickej a informačnej bezpečnosti (ďalej len „KIB“), pričom pokrýva technické, právne, ako aj procesné aspekty. Účastníkom vzdelávacieho programu poskytne prehľad o tom, čo je kybernetická a informačná bezpečnosť a ako je legislatíve upravená. Súčasne poskytne informácie o riadení KIB v súlade s legislatívou SR a technickými normami, osobitne normami rodiny ISO/OSI 27000. V rámci technickej časti vzdelávania sa jednotlivé časti (moduly) zameriavajú na návrh a implementáciu bezpečnostných opatrení v oblastiach kryptografie a počítačových sietí, kde účastníci získajú vedomosti o šifrovacích algoritmoch, digitálnych podpisoch, bezpečnostných systémoch. Súčasťou vzdelávania sú aj aktivity na predchádzanie a riešenie kybernetických bezpečnostných incidentov, vrátane forenznej analýzy digitálnych stôp. Samostatný modul je venovaný rozvoju komunikačných a prezentačných zručností potrebných pri riešení kybernetických bezpečnostných incidentov. V rámci právnej časti sa vzdelávanie venuje nielen právnej úprave KIB, ale aj rôznym aspektom práva informačných a komunikačných technológií, ktoré úzko súvisia s oblasťou KIB. Moduly sa bližšie venujú témam ako ochrana osobných údajov, duševné vlastníctvo, právna zodpovednosť v online priestore, elektronická identifikácia, elektronický podpis a kybernetická kriminalita. Jednotlivé moduly sú doplnené o praktické úlohy, kde si účastníci vzdelávacieho programu vyskúšajú jednotlivé činnosti nevyhnutné pre oblasť KIB.

Cieľová skupina

Cieľovou skupinou sú kategórie používateľov „IT manažér“, „informatik“, „zamestnanec v kybernetickej bezpečnosti“. V zmysle prílohy č. 1 vyhlášky NBÚ č. 492/2022 Z. z. ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti:

- **IT manažér** - riadiaci zamestnanec organizačných jednotiek zodpovedných za poskytovanie IT služieb, návrh, implementáciu, obstaranie, prevádzku, údržbu a posudzovanie prostriedkov IKT
- **informatik** - zamestnanec zodpovedný za poskytovanie IT služieb, návrh, implementáciu, obstaranie, prevádzku, údržbu a posudzovanie IKT,
- **zamestnanec v kybernetickej bezpečnosti** - zamestnanec špecializovaný na oblasť bezpečnosti informácií a riadenia rizík kybernetickej bezpečnosti, zodpovedný za návrh, implementáciu, obstaranie, prevádzku, údržbu a posudzovanie bezpečnostných mechanizmov a riešení.

Ciele vzdelávania

Absolventi vzdelávacieho programu budú schopní:

IT manažér:

- porozumieť významu kybernetickej bezpečnosti pre činnosť organizácie,
- poznať jednotlivé oblasti kybernetickej bezpečnosti,
- porozumieť systému riadenia bezpečnosti informácií a informačných aktív a osvojiť si ho,
- nadobudnúť schopnosť implementovať bezpečnostné opatrenia v konkrétnom prostredí,
- nadobudnúť schopnosť určiť zodpovednosti zamestnancov organizácie vo vzťahu k informačným a komunikačným technológiám,
- osvojiť si metódy vyhodnocovania efektívnosti prijatých bezpečnostných opatrení,
- vedieť definovať a kontrolovať plnenie požiadaviek kybernetickej bezpečnosti pri obstarávaní, dodávaní, správe, prevádzke, údržbe a rozvoji sietí a informačných systémov a ich komponentov,
- nadobudnúť schopnosť presadzovať politiky kybernetickej bezpečnosti v organizácii.

Informatik:

- doplniť vlastné odborné znalosti špecificky pre oblasť kybernetickej bezpečnosti,
- porozumieť podstate bezpečnostných požiadaviek na IKT a IT služby,
- porozumieť zraniteľnostiam, hrozbám a rizikám spojeným s používanými IKT a IT službami,
- nadobudnúť schopnosť navrhnúť, implementovať, udržiavať a prevádzkovať mechanizmy na naplnenie bezpečnostných požiadaviek na IKT a IT služby,
- nadobudnúť zručnosť kvalifikovane komunikovať a spolupracovať so špecialistami kybernetickej bezpečnosti, formulovať problémy, posudzovať a implementovať navrhované opatrenia.

Zamestnanec v kybernetickej bezpečnosti:

- poznať a osvojiť si právne a etické požiadavky na zaručenie bezpečnosti informačných aktív,
- rozumieť zraniteľnostiam, hrozbám a rizikám v informačnej a kybernetickej bezpečnosti,
- nadobudnúť schopnosť navrhnúť, implementovať, udržiavať a prevádzkovať bezpečnostné mechanizmy a riešenia,
- nadobudnúť schopnosť navrhovať a prezentovať bezpečnostné stratégie, bezpečnostné politiky a bezpečnostnú architektúru,
- nadobudnúť znalosti o technikách a metódach vyhodnocovania efektívnosti bezpečnostných mechanizmov a riešení a uplatňovať ich v procesoch organizácie,
- nadobudnúť zručnosť kvalifikovane komunikovať a spolupracovať s informatikmi, formulovať problémy, posudzovať a implementovať navrhované opatrenia,
- nadobudnúť schopnosť navrhovať procesy riadenia rizík v informačnej a kybernetickej bezpečnosti.

Obsah metodiky (moduly)

Číslo modulu	Názov modulu	Časová dotácia (45 min.)	Forma stretnutia
Modul č. 1	**Úvod do KIB a riadenie KIB**	**6**	**Prezenčne / Online**
Modul č. 2	**Vybrané kapitoly z kryptografie**	**8**	**Prezenčne / Online**
Modul č. 3	**Vybrané kapitoly zo sieťovej bezpečnosti**	**8**	**Prezenčne / Online**
Modul č. 4	**Reaktívne a proaktívne činnosti**	**7**	**Prezenčne / Online**
Modul č. 5	**Reaktívne činnosti – komunikácia**	**7**	**Prezenčne / Online**
Modul č. 6	**Vybrané kapitoly z práva informačných a komunikačných technológií I.**	**8**	**Online / Prezenčne**
Modul č. 7	**Vybrané kapitoly z práva informačných a komunikačných technológií II.**	**8**	**Online / Prezenčne**

Poznámky

Modul č.1 - Úvod do kybernetickej a informačnej bezpečnosti (KIB) a riadenia KIB

Obsah vzdelávacieho modulu

Obsahom modulu bude poskytnutie základných informácií o tom, ako prebieha riadenie KIB s ohľadom na právnu úpravu platnú pre územie SR ako aj technických noriem, najmä rodiny ISO/OSI 27000. Súčasťou modulu bude aj poskytnutie informácií o aktuálnych bezpečnostných hrozbách a taktikách a technikách útočníkov. V rámci praktickej časti si účastníci vyskúšajú identifikáciu aktivít, hrozieb, zraniteľností a rizík. Modul zároveň predstaví základy systému riadenia kybernetickej bezpečnosti, princípy riadenia kontinuity činností a bezpečnostné aspekty vzťahov s dodávateľmi a tretími stranami, vrátane rámcov ako Cyber kill chain a MITRE ATT&CK.

1) Úvodné poznámky o KIB
    a) Svet okolo nás
    b) Pojem informačnej a kybernetickej bezpečnosti
2) Model KIB
    a) Aktívum
    b) Bezpečnostné hrozby
    c) Bezpečnostné zraniteľnosti
    d) Útok
    e) Útočník
    f) Riziko
    g) Bezpečnostné opatrenie
3) Právna úprava KIB
    a) Európsky právny rámec
    b) Slovenský právny rámec
    c) Smernica NIS 2
    d) Zákon o KB
    e) Zákon o ITVS
4) Taktiky a techniky útočníkov
    a) Analýza skupín útočníkov
    b) Cyber kill chain
    c) MITRE ATT&CK rámec
5) Systém riadenia KIB
    a) Úvod a ISO normy
    b) Zavedenie systému riadenia
    c) Implementácia a prevádzka

6) Riadenie kontinuity činností
    a) Kontinuita činností
    b) Dôležité pojmy
    c) Riadenie kontinuity činností
7) Dodávateľské vzťahy
    a) Hrozba dodávateľských vzťahov
    b) Vzťah s tretími stranami
8) Riadenie bezpečnostných rizík
    a) Bezpečnostné riziko
    b) Proces riadenia rizík
    c) Identifikácia aktív
    d) Identifikácia hrozieb
    e) Identifikácia zraniteľností
    f) Analýza rizík
    g) Vyhodnotenie rizík

Odporúčané metódy

- *interaktívna prednáška s diskusiou – na vysvetlenie základných rámcov, legislatívy a technických štandardov,*
- *cvičenie – analýza rizík v organizácii,*
- *prípadové štúdie (case studies) – na analýzu reálnych bezpečnostných hrozieb a incidentov.*

Metodický postup

Téma	**Podtéma**	**Materiál a pomôcky**	**Metodické poznámky**	**Hod.**
Úvodné poznámky o KIB	*Svet okolo nás* *Pojem informačnej a kybernetickej bezpečnosti*	*Prezentácia*	*Prednáška* *Prednáška*	*30 min.*

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Model KIB	*Aktívum* *Bezpečnostné hrozby* *Bezpečnostné zraniteľnosti* *Útok* *Útočník* *Riziko* *Bezpečnostné opatrenie*	*Prezentácia*	*Prednáška s diskusiou*	*60 min.*
Právna úprava KIB	*Európsky právny rámec* *Slovenský právny rámec* *Smernica NIS 2* *Zákon o KB* *Zákon o ITVS*	*Prezentácia* *Portál slov-lex a eur-lex*	*Prednáška s diskusiou*	*30 min.*
Taktiky a techniky útočníkov	*Analýza skupín útočníkov* *Cyber kill chain* *MITRE ATT&CK rámec*	*Prezentácia* *Mitre Attack rámec* *CTI správa o skupine útočníkov*	*Prednáška s diskusiou* *Prednáška s diskusiou* *Workshop – analýza činnosti vybranej skupiny (podľa CTI správy o skupine útočníkov)*	*30 min.*
Systém riadenia KIB	*Úvod a ISO normy* *Zavedenie systému riadenia* *Implementácia a prevádzka*	*Prezentácia* *ISO 27000 normy*	*Prednáška s diskusiou* *Prednáška s diskusiou* *Prednáška s diskusiou*	*30 min.*

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Riadenie kontinuity činností	*Kontinuita činností* *Dôležité pojmy* *Riadenie kontinuity činností*	*Prezentácia* *Vzorová dopadová analýza*	*Prednáška s diskusiou* *Workshop - Dopadová analýza*	*30 min.*
Dodávateľské vzťahy	*Hrozba dodávateľských vzťahov* *Vzťah s tretími stranami*	*Prezentácia* *Ukážka vzorovej zmluvy s dodávateľom*	*Prednáška s diskusiou*	*30 min.*
Riadenie bezpečnostných rizík	*Bezpečnostné riziko* *Proces riadenia rizík* *Identifikácia aktív* *Identifikácia hrozieb* *Identifikácia zraniteľností* *Analýza rizík* *Vyhodnotenie rizík*	*Prezentácia* *Ukážkový materiál – analýza rizík*	*Prednáška s diskusiou* *Prednáška s diskusiou* *Workshop – identifikácia aktív* *Workshop – identifikácia hrozieb* *Workshop – identifikácia zraniteľností* *Workshop – analýza rizík* *Workshop – vyhodnotenie rizík*	*30 min.*

Podklady

- *študijný materiál – Prezentácia KCKB_A2_V2.1.1_IT_M6_01_Uvod_KIB.pptx,*
- *študijný materiál – vzorová analýza rizík,*
- *študijný materiál – vzorová dopadová štúdia,*
- *študijný materiál – CTI správa o skupine útočníkov,*
- *študijný materiál – vzorová zmluva s dodávateľom,*
- *spätná väzba od účastníkov.*

Poznámky

Modul č.2 - Vybrané kapitoly z kryptografie

Obsah vzdelávacieho modulu

Obsahom tohto modulu bude oboznámenie sa s kryptografiou používanou v súčasnosti. S účastníkmi sa prejdú základné symetrické a asymetrické šifry, vysvetlia sa jednosmerné (hešovacie) funkcie a digitálne podpisy. Účastníci si budú môcť jednotlivé šifry vyskúšať a lepšie pochopiť podstatu týchto kryptografických primitív. Predstavené budú možnosti aplikovania kryptografických mechanizmov na zabezpečenie dôvernosti, integrity a nepopierateľnosti údajov v praxi.

1) *Úvod do kryptografie a klasické šifry*
    a) Steganografia
    b) Kryptografia - konfúzia a difúzia
    c) Kryptoanalýza
    d) Kryptografické protokoly
    e) Klasické substitučné a transpozičné šifry, mechanické šifrovacie stroje
    f) Symetrické šifrovanie
    g) Asymetrické šifrovanie
    h) Postkvantová kryptografia
2) Symetrické algoritmy (tajný kľúč)
    a) Blokové šifry - Feistelova štruktúra, režimy
    b) Prúdové šifry
3) Asymetrické algoritmy (súkromný a verejný kľúč)
    a) Hešovacie funkcie
    b) Šifrovanie/dešifrovanie, podpisovanie, dohodnutie kľúča
    c) Problém diskrétneho logaritmu
    d) Faktorizácia veľkých čísel
    e) Eliptické krivky
4) Distribúcia verejných kľúčov
    a) Autentifikácia používateľov a protokoly
    b) Certifikácia

Odporúčané metódy

- *prednáška s diskusiou,*
- *cvičenie.*

Metodický postup

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Úvod do kryptografie a klasické šifry	*História a vývoj kryptografie*	*Prezentácia*	*Prednáška s diskusiou*	*30 min*
	Posuvná šifra, Fleissnerova mriežka, Vigenérova šifra	*Jupyter notebook*	*cvičenie*	*60 min*
Symetrické algoritmy	*Šifrovanie tajným kľúčom*	*Prezentácia*	*Prednáška*	*30 min*
	Šifry DES, AES, RC4 režimy ECB, CBC	*Jupyter notebook*	*cvičenie*	*60 min*
Asymetrické algoritmy	*Verejný kľúč - šifrovanie, podpisovanie, dohoda kľúča*	*Prezentácia*	*Prednáška*	*40 min*
	RSA, ElGamal, ECC, Diffie-Hellman	*Jupyter notebook*	*cvičenie*	*60 min*
Distribúcia verejných kľúčov	*Autentifikácia používateľov, certifikácia*	*Prezentácia*	*Prednáška s diskusiou*	*20 min*
	PKI, X.509, SSL/TLS	*Jupyter notebook*	*cvičenie*	*60 min*

Podklady

- *študijný materiál – Prezentácia KCKB_A2_V2.1.1_IT_M6_02_Kryptografia.pptx,*
- *interaktívne elektronické materiály - Jupyter notebook-y v jazyku Python,*
- *spätná väzba od účastníkov.*

Poznámky

Modul č. 3 - Vybrané kapitoly zo sieťovej bezpečnosti

Obsah vzdelávacieho modulu

Obsah vzdelávacieho modulu „Úvod do sieťovej bezpečnosti a konfigurácie zariadení MikroTik“ je zameraný na základné princípy bezpečnosti počítačových sietí a ich praktické uplatnenie. Účastníci sa oboznámia so základnou terminológiou, typmi sieťových útokov a bezpečnostnými požiadavkami na prepínače, smerovače a koncové zariadenia. Osobitná pozornosť je venovaná konfigurácii zariadení MikroTik – od úvodného nastavenia, cez využitie v úlohe prepínača a smerovača, až po konfiguráciu VLAN a smerovacích protokolov. Modul tiež pokrýva praktickú realizáciu útokov typu MITM pomocou MikroTik-u a možnosti ochrany pomocou Layer 2 a paketového filtrovania. V závere sa účastníci oboznámia s bezpečným nasadením VPN riešení vrátane konfigurácie jednotlivých VPN protokolov ako L2TP, IPsec či OpenVPN.

1) Úvod do sieťovej bezpečnosti
    a) Terminológia
    b) Sieťové útoky
    c) Bezpečnosť prvkov v sieti
        i) Prepínače
        ii) Smerovače
        iii) Koncové zariadenia

2) Úvod k zariadeniam MikroTik
    a) RouterOS
    b) Hardvér
    c) Konfigurácia zariadenia - základné nastavenia
    d) MikroTik ako prepínač
        i) Klasický prístup (bridge)
        ii) VLAN
    e) MikroTik ako smerovač
        i) Statické a dynamické smerovanie
3) Sieťové útoky
    a) Rozdelenie
    b) Realizácia MITM pomocou MikroTik-u
4) Filtrovanie rámcov (Layer 2)
    a) Princíp
    b) Postup konfigurácie
    c) Aplikácia Layer 2 filtrov
5) Filtrovanie paketov
    a) Princípy

b) Postup konfigurácie
c) Aplikácia paketových filtrov

6) Zabezpečenie smerovacích protokolov
   a) Verifikácia smerovačov
   b) Pasívne rozhrania
7) VPN
   a) Definícia, použitie
   b) Realizácia VPN
      i) Client – Site
      ii) Site – to - Site
   c) VPN protokoly
   d) Konfigurácia VPN protokolov
      i) PPTP
      ii) L2TP
      iii) L2TP + IPsec
      iv) OpenVPN

Odporúčané metódy

- *prednáška s diskusiou,*
- *cvičenie,*
- *samostatná práca.*

Metodický postup

Téma	**Podtéma**	**Materiál a pomôcky**	**Metodické poznámky**	**Hod.**
Úvod do sieťovej bezpečnosti	*a) Terminológia* *b) Sieťové útoky* *c) Bezpečnosť prvkov v sieti* *i) Prepínače* *ii) Smerovače* *iii) Koncové zariadenia*	*Prezentácia*	*Workshop*	*90 min.*
Úvod k zariadeniam MikroTik	a) RouterOS b) Hardvér c) Konfigurácia zariadenia - základné nastavenia d) MikroTik ako prepínač - Klasický prístup (bridge) a VLAN e) MikroTik ako smerovač i) Statické a dynamické smero	*Prezentácia*	*workshop*	*60 min.*

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Sieťové útoky	*a) Rozdelenie* *b) Realizácia MITM pomocou MikroTik-u*	*Prezentácia*	*Workshop*	*60 min.*
Filtrovanie rámcov (Layer 2)	*a) Princíp* *b) Postup konfigurácie* *c) Aplikácia Layer 2 filtrov*	*Prezentácia*	*Workshop*	*45 min.*
Filtrovanie paketov	*a) Princípy* *b) Postup konfigurácie* *c) Aplikácia paketových filtrov*	*Prezentácia*	*Workshop*	*45 min.*
Zabezpečenie smerovacích protokolov	*a) Verifikácia smerovačov* *b) Pasívne rozhrania*	*Prezentácia*	*Workshop*	*30 min.*
VPN	*a) Definícia, použitie* *b) Realizácia VPN (*Client – Site, Site – to – Site) *c) VPN protokoly* *d) Konfigurácia VPN protokolov* *(PPTP, L2TP, L2TP + IPsec, OpenVPN)*	*Prezentácia*	*Workshop*	*30 min.*

Podklady

- *študijné materiály - Prezentácia KCKB_A2_V2.1.1_IT_M3_01_Sietova_bezpecnost.pptx,*
- *spätná väzba od účastníkov.*

Poznámky

Modul č. 4 - Reaktívne a proaktívne činnosti

Obsah vzdelávacieho modulu

Obsahom modulu sú činnosti potrebné k predchádzaniu vzniku kybernetických bezpečnostných incidentov (proaktívne činnosti) a činnosti nevyhnutné k reakcii na kybernetické bezpečnostné incidenty (reaktívne činnosti). V rámci modulu Pôjde najmä o nasledujúce témy bezpečnostné zraniteľnosti a ich životný cyklus, vyhodnocovanie a zverejňovanie, identifikácia a riešenie kybernetických bezpečnostných incidentov vrátane životného cyklu, digitálna forenzná analýza vrátane identifikácie a zaisťovania digitálnych stôp. Účastníci modulu si vyskúšajú riešenie jednoduchých kybernetických bezpečnostných incidentov z technického ako aj procesného pohľadu (tabletop cvičenie). Budú si môcť odskúšať spôsob identifikácie a zaisťovania digitálnych stôp, či vykonanie live forenznej analýzy.

1) Úvod do reaktívnych a proaktívnych činností
2) Manažment bezpečnostných zraniteľností
    a) Bezpečnostné zraniteľnosti a ich životný cyklus, databázy zraniteľností
    b) Závažnosť zraniteľností
    c) Manažment zraniteľností
    d) Testovanie a vyhodnotenie zraniteľností
3) Riešenie kybernetických bezpečnostných incidentov
    a) Úvod a história
    b) Kybernetický bezpečnostný incident
    c) Taxonómia incidentov
    d) Tímy na riešenie incidentov
    e) Riešenie kybernetických bezpečnostných incidentov
4) Digitálna forenzná analýza
    a) Digitálna forenzná analýza a digitálna stopa
    b) Fázy digitálnej forenznej analýzy, princípy
    c) Zaisťovanie digitálnych stôp
    d) Triage
    e) Live forenzná analýza

Odporúčané metódy

- *prednáška s diskusiou*
- *cvičenie – identifikácia skóre zraniteľnosti, zaisťovanie a triedenie digitálnych stôp, live forenzná analýza*
- *tabletop cvičenia a role-play scenáre – pre trénovanie reakcií na kybernetické bezpečnostné incidenty*

Metodický postup

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Úvod do reaktívnych a proaktívnych činností		*Prezentácia*	*Prednáška*	*10 min.*
Manažment bezpečnostných zraniteľností	*Bezpečnostné zraniteľnosti a ich životný cyklus, databázy zraniteľností*	*Prezentácia*	*Prednáška*	*30 min.*
	Závažnosť zraniteľností	*Ukážka – výstup – nástroj na testovanie zraniteľností*	*Prednáška a praktická úloha - identifikácia skóre zraniteľnosti (CVSS)*	*30 min.*
	Manažment zraniteľností		*Prednáška*	*15 min.*
	Testovanie a vyhodnotenie zraniteľností		*Praktická úloha - testovanie zraniteľností*	*15 min.*
Riešenie kybernetických bezpečnostných incidentov	*Úvod a história*	*Prezentácia*	*Prednáška*	*15 min.*
	Kybernetický bezpečnostný incident		*Prednáška*	*15 min.*
	Taxonómia incidentov		*Prednáška a praktická úloha*	*15 min.*
	Tímy na riešenie incidentov		*Prednáška*	*15 min.*
	Riešenie kybernetických bezpečnostných incidentov		*Prednáška a praktická úloha – prvý kroky riešenia incidentu*	*60 min.*

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Digitálna forenzná analýza	*Digitálna forenzná analýza a digitálna stopa*	*Prezentácia*	*Prednáška*	*15 min.*
	Fázy digitálnej forenznej analýzy, princípy		*Prednáška*	*15 min.*
	Zaisťovanie digitálnych stôp	*KAPE FTK Imager Eric Zimmerman nástroje*	*Workshop – praktická úloha – zaistenie pomocou nástroja FTK imagera*	*30 min.*
	Triage		*Workshop – praktická úloha – triage pomocou nástroja KAPE*	*15 min.*
	Live forenzná analýza		*Workshop – praktická úloha – zaistenie digitálnych stôp pomocou nástrojov*	*45 min.*

Podklady

- *študijné materiály - Prezentácia KCKB_A2_V2.1.1_IT_M4_01_Reaktívne_proaktívne_činnosti.pptx,*
- *nástroje KAPE, FTK Imager, Eric Zimmerman nástroje,*
- *manuál pre použitie nástroja KAPE a FTK Imager, Eric Zimmermanových nástrojov,*
- *spätná väzba od účastníkov.*

Poznámky

Modul č. 5 – Komunikačné zručnosti pri reaktívnych činnostiach

Obsah vzdelávacieho modulu

Modul sa zameriava na rozvoj komunikačných a prezentačných schopností nevyhnutných pre úspešné zvládnutie kybernetického bezpečnostného incidentu. Dôraz bude kladený na asertívnu komunikáciu, efektívnu spätnú väzbu, na riešenie zameranú komunikáciu, komunikáciu pri riešení problémov v tíme a tiež na základné techniky zvládania akútneho stresu. Súčasťou budú aj témy identifikácie krízových situácií, neverbálnej komunikácie a zásad tímovej spolupráce. Účastníci sa oboznámia s najčastejšími komunikačnými bariérami, technikami ich prekonávania a špecifikami interakcie pod stresom či v kritických situáciách.

1) Kríza, základy komunikácie v krízových situáciách
    a) Identifikácia krízovej situácie a zvládanie akútneho stresu
    b) Rozpoznanie a súlad neverbálnych prejavov v komunikácii
    c) Zásady komunikácie v krízových situáciách
2) Základy asertívnej komunikácie
    a) Asertívne techniky využiteľné v krízových situáciách
    b) Spätná väzba - zásady podávania spätnej väzby
3) Komunikácia v tíme
    a) Základy tímovej spolupráce a komunikácie v tíme
    b) Komunikačné bariéry a tímovej práci

Odporúčané metódy

- *prednáška s diskusiou,*
- *interaktívne metódy,*
- *rozhovor, diskusné metódy, riadená diskusia,*
- *rolové hry, nácvik modelových situácii.*

Metodický postup

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Kríza, základy komunikácie v krízových situáciách	*Identifikácia krízovej situácie a zvládanie akútneho stresu* *Zásady komunikácie v krízových situáciách* *Rozpoznanie a súlad neverbálnych prejavov v komunikácii*	*Prezentácia*	*Prednáška, diskusia* *Nácvik techník zvládania akútneho stresu*	*120 min.*
Základy asertívnej komunikácie	*Asertívne techniky využiteľné v krízových situáciách* *Spätná väzba - zásady podávania spätnej väzby*	*Prezentácia*	*Prezentácia, diskusia, rolové hry/modelové situácie*	*90 min.*
Komunikácia v tíme	*Základy tímovej spolupráce a komunikácie v tíme* *Komunikačné bariéry a tímovej práci*	*Prezentácia*	*Prezentácia, diskusia, rolové hry/modelové situácie*	*90 min.*

Podklady

- *študijné materiály - Prezentácia KCKB_A2_V2.1.1_IT_M5_01_Komunikacne_zrucnosti.pptx,*
- *spätná väzba od účastníkov*

Poznámky

Modul č. 6 - Vybrané kapitoly z práva informačných a komunikačných technológií I.

Obsah vzdelávacieho modulu

Vzdelávací modul sa zameriava na právne aspekty informačných a komunikačných technológií (IKT), pričom ponúka úvod do základných pojmov a oblastí práva IKT. Osobitná pozornosť je venovaná dôveryhodným službám, ako sú elektronický podpis, certifikáty a digitálne právne úkony, ktoré zohrávajú kľúčovú úlohu v elektronickej komunikácii. Modul tiež objasňuje problematiku duševného vlastníctva a jeho právnej ochrany v digitálnom prostredí. Druhá časť sa venuje ochrane súkromia a osobných údajov, vrátane práv dotknutých osôb, cezhraničného prenosu údajov a bezpečnostných opatrení. Tretia tematická oblasť pokrýva elektronický obchod, jeho typy, špecifiká elektronických zmlúv a právne výzvy, ktoré z neho vyplývajú. Cieľom je poskytnúť účastníkom praktický právny rámec pre orientáciu v digitálnom svete.

1) Právo informačných a komunikačných technológií (úvod, pojem, vymedzenie IKT)
    a) Dôveryhodné služby a elektronický podpis – služby vytvárajúce dôveru, poskytovatelia dôveryhodných služieb, elektronické právne úkony, elektronický dokument a elektronický podpis, elektronická pečať, digitálny podpis, certifikát.
    b) Duševné vlastníctvo a jeho ochrana.
2) Ochrana súkromia a osobných údajov
    a) Definícia osobného údaju. Subjekty v oblasti ochrany osobných údajov - prevádzkovateľ, sprostredkovateľ, dotknutá osoba. Práva dotknutých osôb.
    b) Spracovanie osobných údajov, cezhraničný prenos údajov, bezpečnosť osobných údajov, kódexy správania, certifikácia. Uchovávanie údajov (data retention).
3) Elektronický obchod
    a) Pojem a charakteristika elektronického obchodu.
    b) Typy elektronického obchodu.
    c) Výhody a nevýhody elektronického obchodovania.
    d) Zmluvy uzatvorené prostredníctvom elektronických prostriedkov.
    e) Typy elektronických zmlúv.

Odporúčané metódy

- *prednáška s diskusiou,*
- *samostatná práca.*

Metodický postup

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Právo informačných a komunikačných technológií (úvod, pojem, vymedzenie IKT).	*Dôveryhodné služby a elektronický podpis – služby vytvárajúce dôveru, poskytovatelia dôveryhodných služieb, elektronické právne úkony, elektronický dokument a elektronický podpis, elektronická pečať, digitálny podpis, certifikát* *Duševné vlastníctvo a jeho ochrana*	*Prezentácia*	*Prednáška s diskusiou* *Prednáška s diskusiou*	*90 minút* *90 minút*
Ochrana súkromia a osobných údajov	*Definícia osobného údaju. Subjekty v oblasti ochrany osobných údajov - prevádzkovateľ, sprostredkovateľ, dotknutá osoba. Práva dotknutých osôb. Spracovanie osobných údajov, cezhraničný prenos údajov, bezpečnosť osobných údajov, kódexy správania, certifikácia. Uchovávanie údajov (data retention).*	*Prezentácia*	*Prednáška s diskusiou*	*120 minút*

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Elektronický obchod	*Pojem a charakteristika elektronického obchodu. Typy elektronického obchodu. Výhody a nevýhody elektronického obchodovania. Zmluvy uzatvorené prostredníctvom elektronických prostriedkov. Typy elektronických zmlúv.*	*Prezentácia*	*Prednáška* *Cvičenie*	*90 minút*

Podklady

- *študijné materiály - Prezentácia KCKB_A2_V2.1.1_IT_M6_01_Právo_IKT_I.pptx,*
- *spätná väzba od účastníkov.*

Poznámky

Modul č. 7 - Vybrané kapitoly z práva informačných a komunikačných technológií II.

Obsah vzdelávacieho modulu

Modul „Právne aspekty kybernetickej bezpečnosti“ poskytuje prehľad o kľúčových právnych otázkach spojených s ochranou pred kybernetickými hrozbami a reakciou na incidenty. Účastníci sa oboznámia s pojmom kybernetického bezpečnostného incidentu a úlohou CSIRT/CERT tímov pri ich riešení, vrátane procesov notifikácie a zdieľania informácií o incidentoch. Pozornosť sa venuje aj medzinárodnoprávnym otázkam, ako je určenie rozhodného práva a právomoci v prípade cezhraničných kybernetických útokov. Trestnoprávne a trestnoprocesné aspekty kybernetickej kriminality sú rozobraté z pohľadu skutkových podstát, vyšetrovania a dokazovania. Dôležitú časť tvorí analýza digitálnych stôp, ich kriminalistické spracovanie a digitálnu forenznú analýza. Záverečná časť sa zaoberá právnym rámcom obstarávania elektronických dôkazov na medzinárodnej úrovni vrátane bilaterálnych a európskych mechanizmov spolupráce.

1) Právne aspekty kybernetickej bezpečnosti
    a) Pojem kybernetického bezpečnostného incidentu.
    b) CSIRT/CERT tímy.
    c) Notifikácia a riešenie kybernetických bezpečnostných incidentov.
    d) Zdieľanie bezpečnostných incidentov.
    e) Medzinárodnoprávne aspekty kybernetickej bezpečnosti (medzinárodná právomoc, rozhodné právo).
2) Trestnoprávne aspekty kybernetickej kriminality
    a) Trestnoprávne (hmotnoprávne) aspekty kybernetickej kriminality.
    b) Trestnoprocesné aspekty kybernetickej kriminality.
3) Kriminalisticko – technické aspekty odhaľovania a objasňovania kybernetickej kriminality
    a) Digitálne stopy, charakteristické vlastnosti a špecifiká ich využívania pri odhaľovaní kybernetickej kriminality
    b) Forenzná digitálna analýza a jej význam pri objasňovaní kybernetickej kriminality
4) Medzinárodné aspekty obstarávania elektronických dôkazných prostriedkov
    a) Bilaterálne a multilaterálne zmluvy; európska právna úprava obstarávania elektronických dôkazných prostriedkov

Odporúčané metódy

- *prednáška s diskusiou,*
- *cvičenie.*

Metodický postup

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Právne aspekty kybernetickej bezpečnosti	*Pojem kybernetického bezpečnostného incidentu. CSIRT/CERT tímy. Notifikácia a riešenie kybernetických bezpečnostných incidentov. Zdieľanie bezpečnostných incidentov.* *Medzinárodnoprávne aspekty kybernetickej bezpečnosti (medzinárodná právomoc, rozhodné právo).*	*Prezentácia*	*Prednáška s diskusiou* *Prednáška s diskusiou* *Workshop - modelový prípad*	*90 minút* *60 minút*
Trestnoprávne aspekty kybernetickej kriminality	*Trestnoprávne (hmotnoprávne) aspekty kybernetickej kriminality* *Trestnoprocesné aspekty kybernetickej kriminality*	*Prezentácia*	*Prednáška s diskusiou* *Prednáška s diskusiou*	*90 minút* *60 minút*
Kriminalisticko – technické aspekty odhaľovania a objasňovania kybernetickej kriminality	*Digitálne stopy, charakteristické vlastnosti a špecifiká ich využívania pri odhaľovaní kybernetickej kriminality* *Forenzná digitálna analýza a jej význam pri objasňovaní kybernetickej kriminality*	*Prezentácia*	*Prednáška s diskusiou*	*60 minút*

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Medzinárodné aspekty obstarávania elektronických dôkazných prostriedkov	*Bilaterálne a multilaterálne zmluvy; európska právna úprava obstarávania elektronických dôkazných prostriedkov*	*Prezentácia*	*Prednáška s diskusiou*	*30 minút*

Podklady

- *študijné materiály - Prezentácia KCKB_A2_V2.1.1_IT_M7_01_Právo_IKT_II.pptx,*
- *spätná väzba od účastníkov.*

Poznámky