Reg. č. projektu: CZ 1.04/ 4.1.00/A3.00004

Kybernetická bezpečnost III.
Technická opatření

Pracovní sešit

Materiál vznikl v rámci řešení projektu **„Vzdělávání v oblasti základních registrů a dalších kmenových projektů eGovernmentu“,** registrační číslo projektu: CZ 1.04/ 4.1.00/A3.00004, který je financován z prostředků Evropského sociálního fondu ČR, Operačního programu Lidské zdroje a zaměstnanost.

Zpracovatel – Institut pro veřejnou správu Praha
Realizátor – Ministerstvo vnitra

Praha, červenec 2015

OBSAH PRACOVNÍHO SEŠITU

TENTO PRACOVNÍ SEŠIT:

- slouží pro opakování a procvičování učiva probraného v teoretické části kurzu
- aktivizuje účastníky kurzu, usiluje o jejich participaci při plnění cílů výuky
- obsahuje zadání zpětnovazebních aktivit (testy, případové studie), které účastníci kurzu řeší ve skupinách nebo individuálně
- přináší doplňující informace k výkladu (např. odkazy na užitečné webové stránky k tématu, různé přehledy, studijní texty a podobně)
- může absolventy kurzu inspirovat k aktivitám nejen v rámci prezenční výuky, ale také při následném domácím samostudiu
- má dvě části (teoretickou a praktickou) členěné na kapitoly

TEORETICKÁ ČÁST:

- legislativní předpisy
- slovníček pojmů
- užitečné webové stránky
- doporučená odborná literatura

PRAKTICKÁ ČÁST:

- kontrolní otázky
- úkoly
- test

A. TEORETICKÁ ČÁST

Legislativní předpisy

předpis č. 316/2014 Sb., Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)

HLAVA II

TECHNICKÁ OPATŘENÍ

§ 16

Fyzická bezpečnost

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona v rámci fyzické bezpečnosti

a) přijme nezbytná opatření k zamezení neoprávněnému vstupu do vymezených prostor, kde jsou zpracovávány informace a umístěna technická aktiva informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému,

b) přijme nezbytná opatření k zamezení poškození a zásahům do vymezených prostor, kde jsou uchovány informace a umístěna technická aktiva informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, a

c) předchází poškození, krádeži nebo zneužití aktiv nebo přerušení poskytování služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále uplatňuje prostředky fyzické bezpečnosti

a) pro zajištění ochrany na úrovni objektů a

b) pro zajištění ochrany v rámci objektů zajištěním zvýšené bezpečnosti vymezených prostor, ve kterých jsou umístěna technická aktiva informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury.

(3) Prostředky fyzické bezpečnosti jsou zejména

a) mechanické zábranné prostředky,

b) zařízení elektrické zabezpečovací signalizace,

c) prostředky omezující působení požárů,

d) prostředky omezující působení projevů živelních událostí,

e) systémy pro kontrolu vstupu,

f) kamerové systémy,

g) zařízení pro zajištění ochrany před selháním dodávky elektrického napájení a

h) zařízení pro zajištění optimálních provozních podmínek.

§ 17

Nástroj pro ochranu integrity komunikačních sítí

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona pro ochranu integrity rozhraní vnější komunikační sítě, která není pod správou orgánu nebo osoby, a vnitřní komunikační sítě, která je pod správou orgánu nebo osoby, zavede

a) řízení bezpečného přístupu mezi vnější a vnitřní sítí,

b) segmentaci zejména použitím demilitarizovaných zón jako speciálního typu sítě používaného ke zvýšení bezpečnosti aplikací dostupných z vnější sítě a k zamezení přímé komunikace vnitřní sítě s vnější sítí,

c) kryptografické prostředky (§ 25) pro vzdálený přístup, vzdálenou správu nebo pro přístup pomocí bezdrátových technologií a

d) opatření pro odstranění nebo blokování přenášených dat, které neodpovídají požadavkům na ochranu integrity komunikační sítě.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále využívá nástroje pro ochranu integrity vnitřní komunikační sítě, které zajistí její segmentaci.

§ 18

Nástroj pro ověřování identity uživatelů

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona používá nástroje pro ověření identity uživatelů a administrátorů informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému.

(2) Nástroj pro ověřování identity uživatelů a administrátorů zajišťuje ověření identity uživatelů a administrátorů před zahájením jejich aktivit v informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury a významném informačním systému.

(3) Nástroj pro ověřování identity uživatelů, který používá autentizaci pouze heslem, zajišťuje

a) minimální délku hesla osm znaků,

b) minimální složitost hesla tak, že heslo bude obsahovat alespoň 3 z následujících čtyř požadavků

1. nejméně jedno velké písmeno,

2. nejméně jedno malé písmeno,

3. nejméně jednu číslici, nebo

4. nejméně jeden speciální znak odlišný od požadavků uvedených v bodech 1 až 3,

c) maximální dobu pro povinnou výměnu hesla nepřesahující sto dnů; tento požadavek není vyžadován pro samostatné identifikátory aplikací.

(4) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále

a) používá nástroj pro ověření identity, který

1. zamezí opětovnému používání dříve používaných hesel a neumožní více změn hesla jednoho uživatele během stanoveného období, které musí být nejméně 24 hodin, a

2. provádí opětovné ověření identity po určené době nečinnosti a

b) využívá nástroj pro ověřování identity administrátorů. V případě, že tento nástroj využívá autentizaci heslem, zajistí prosazení minimální délky hesla patnáct znaků při dodržení požadavků podle odstavce 3 písm. b) a c).

(5) Nástroj pro ověřování identity uživatelů může být zajištěn i jinými způsoby, než jaké jsou stanoveny v odstavcích 3 až 5, pokud orgán a osoba uvedená v § 3 písm. c) až e) zákona zabezpečí, že používá opatření zajišťující stejnou nebo vyšší úroveň odolnosti hesla.

§ 19

Nástroj pro řízení přístupových oprávnění

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona používá nástroj pro řízení přístupových oprávnění, kterým zajistí řízení oprávnění

a) pro přístup k jednotlivým aplikacím a datům a

b) pro čtení dat, pro zápis dat a pro změnu oprávnění.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále používá nástroj pro řízení přístupových oprávnění, který zaznamenává použití přístupových oprávnění v souladu s bezpečnostními potřebami a výsledky hodnocení rizik.

§ 20

Nástroj pro ochranu před škodlivým kódem

Orgán a osoba uvedená v § 3 písm. c) až e) zákona pro řízení rizik spojených s působením škodlivého kódu používá nástroj pro ochranu informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému před škodlivým kódem, který zajistí ověření a stálou kontrolu

a) komunikace mezi vnitřní sítí a vnější sítí,

b) serverů a sdílených datových úložišť a

c) pracovních stanic,

přičemž provádí pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem, jeho definic a signatur.

§ 21

Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona používá nástroj pro zaznamenávání činností informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému, který zajistí

a) sběr informací o provozních a bezpečnostních činnostech, zejména typ činnosti, datum a čas, identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a místa činnosti a úspěšnost nebo neúspěšnost činnosti a

b) ochranu získaných informací před neoprávněným čtením nebo změnou.

(2) Orgán a osoba uvedená v § 3 písm. c) až e) zákona dále pomocí nástroje pro zaznamenávání činnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému zaznamenává

a) přihlášení a odhlášení uživatelů a administrátorů,

b) činnosti provedené administrátory,

c) činnosti vedoucí ke změně přístupových oprávnění,

d) neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů,

e) zahájení a ukončení činností technických aktiv informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému,

f) automatická varovná nebo chybová hlášení technických aktiv,

g) přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností a

h) použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.

(3) Orgán a osoba uvedená v § 3 písm. c) a d) zákona záznamy činností zaznamenané podle odstavce 2 uchovává nejméně po dobu 3 měsíců.

(4) Orgán a osoba uvedená v § 3 písm. c) až e) zákona zajišťuje nejméně jednou za 24 hodin synchronizaci jednotného systémového času technických aktiv patřících do informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.

§ 22

Nástroj pro detekci kybernetických bezpečnostních událostí

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona používá nástroj pro detekci kybernetických bezpečnostních událostí, který vychází ze stanovených bezpečnostních potřeb a výsledků hodnocení rizik a který zajistí ověření, kontrolu a případně zablokování komunikace mezi vnitřní komunikační sítí a vnější sítí.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále používá nástroj pro detekci kybernetických bezpečnostních událostí, které zajistí ověření, kontrolu a případně zablokování komunikace

a) v rámci vnitřní komunikační sítě a

b) serverů patřících do informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.

§ 23

Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

(1) Orgán a osoba uvedená v § 3 písm. c) a d) zákona používá nástroj pro sběr a průběžné vyhodnocení kybernetických bezpečnostních událostí, který v souladu s bezpečnostními potřebami a výsledky hodnocení rizik zajistí

a) integrovaný sběr a vyhodnocení kybernetických bezpečnostních událostí z informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury,

b) poskytování informací pro určené bezpečnostní role o detekovaných kybernetických bezpečnostních událostech v informačním systému kritické informační infrastruktury nebo komunikačním systému kritické informační infrastruktury a

c) nepřetržité vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování určených bezpečnostních rolí.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále zajistí

a) pravidelnou aktualizaci nastavení pravidel pro vyhodnocování kybernetických bezpečnostních událostí a včasné varování, aby byly omezovány případy nesprávného vyhodnocení událostí nebo případy falešných varování, a

b) využívání informací, které jsou připraveny nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí, pro optimální nastavení bezpečnostních opatření informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.

§ 24

Aplikační bezpečnost

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona provádí bezpečnostní testy zranitelnosti aplikací, které jsou přístupné z vnější sítě, a to před jejich uvedením do provozu a po každé zásadní změně bezpečnostních mechanismů.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále v rámci aplikační bezpečnosti zajistí trvalou ochranu

a) aplikací a informací dostupných z vnější sítě před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou a

b) transakcí před jejich nedokončením, nesprávným směrováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním.

§ 25

Kryptografické prostředky

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona

a) pro používání kryptografické ochrany stanoví

1. úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu a

2. pravidla kryptografické ochrany informací při přenosu po komunikačních sítích nebo při uložení na mobilní zařízení nebo vyměnitelné technické nosiče dat a

b) v souladu s bezpečnostními potřebami a výsledky hodnocení rizik používá kryptografické prostředky, které zajistí ochranu důvěrnosti a integrity předávaných nebo ukládaných dat a průkaznou identifikaci osoby za provedené činnosti.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona dále

a) stanoví pro používání kryptografických prostředků systém správy klíčů, který zajistí generování, distribuci, ukládání, archivaci, změny, ničení, kontrolu a audit klíčů, a

b) používá odolné kryptografické algoritmy a kryptografické klíče; v případě nesouladu s minimálními požadavky na kryptografické algoritmy uvedenými v příloze č. 3 k této vyhlášce řídí rizika spojená s tímto nesouladem.

§ 26

Nástroj pro zajišťování úrovně dostupnosti

(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona v souladu s bezpečnostními potřebami a výsledky hodnocení rizik používá nástroj pro zajišťování úrovně dostupnosti informací.

(2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona používá nástroj pro zajišťování úrovně dostupnosti informací, který zajistí

a) dostupnost informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury pro splnění cílů řízení kontinuity činností,

b) odolnost informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury vůči kybernetickým bezpečnostním incidentům, které by mohly snížit dostupnost, a

c) zálohování důležitých technických aktiv informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury

1. využitím redundance v návrhu řešení a

2. zajištěním náhradních technických aktiv v určeném čase.

SLOVNÍK POJMŮ

EZS: Elektronický Zabezpečovací Systém

EPS: Elektronický Protipožární Systém

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

CSIRT : Computer Security Incident Response team

CERT: Computer Emergency Response team

UŽITEČNÉ WEBOVÉ STRÁNKY

Internet může být zdrojem užitečných informací, a to také pro výkon státní správy. Proto přinášíme **několik dobrých tipů, co a kde lze na internetu najít (ve vztahu k obsahu kurzu):**

Doporučené stránky o kyberbezpečnosti

- https://www.govcert.cz/cs/ Národní centrum kybernetické bezpečnosti (NCKB)
- http://csirt.cz Stránky národního CSIRT týmu
- http://www.security-portal.cz/
- http://thehackernews.com/
- http://www.securityfocus.com/

- http://krebsonsecurity.com/
- https://isc.sans.edu/

DOPORUČENÁ ODBORNÁ LITERATURA

- ***Kevin Mitnik: Umění klamu***
- ***Kybernetická kriminalita - Smejkal Vladimír***
- ***Kol. autorů: ČESKÝ SLOVNÍK POJMŮ KYBERNETICKÉ BEZPEČNOSTI***
- ***Mischa Glenny: Temný trh***

B. PRAKTICKÁ ČÁST

Praktická část pracovního sešitu slouží k procvičení a ověření získaných znalostí a dovedností.

KONTROLNÍ OTÁZKY

Tyto otázky slouží k zamyšlení nad danou problematikou a k otevřené diskuzi s lektorem, během které si můžete ověřit klíčové aspekty pro zajištění kybernetické bezpečnosti Vaší organizace.

1. Definujte pojem fyzická bezpečnost.
2. Jakým bývá realizován nástroj pro zajištění integrity informační sítě?
3. Co je obsahem vyhlášky č. 316/2014 Sb.?
4. Jakým způsobem se zajišťuje aplikační bezpečnost?
5. Jakým způsobem se zajišťuje dostupnost informačních aktiv?
6. Jakými technickými zařízeními je zajišťována integrita komunikačních sítí?
7. Může být nástroj pro ověřování identity zajištěn i jiným způsobem než uvedeným v § 18, odst. 1-4 vyhlášky č. 316/2014 Sb.? Pokud ano, pak za jakých podmínek?
8. Musí být nástroj pro ochranu před škodlivým kódem (podle § 20 vyhlášky č. 316/2014 Sb.) zajišťovat i kontrolu komunikace serverů a vzdálených úložišť?
9. Je podle vyhlášky č. 316/2014 Sb. nutno každodenně aktualizovat bezpečnostní nástroje a jejich definiční soubory?
10. Zajistí instalace bezpečnostních aktualizací operačního systému a aplikací též aktualizaci kryptografických nástrojů?

ÚKOLY

Úkol č. 1

Navrhněte schéma možného technického řešení nástroje pro zajišťování úrovně dostupnosti informací tak, aby byly splněny požadavky § 26 vyhlášky 316/2014 Sb. Předpokládejme informační systém sestávající z jedné aplikace, jedné databáze a jednoho webového uživatelského rozhraní přístupného z internetu.

Úkol č. 2

Vytvořte administrátorské heslo vyhovující požadavkům § 18 vyhlášky 316/2014 Sb. (nepoužívejte žádné ze svých skutečných hesel!) a ověřte kvalitu tohoto hesla pomoci příkazu

echo "password" | cracklib-check

Úkol č. 3

Nainstalujte na svém školicím počítači antivirový program ClamAV a aktualizujte jej o nejnovější virové signatury.

#apt-get update

#apt-get install clamav clam-tk

#freshclam

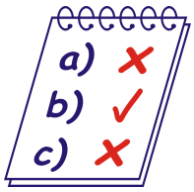
Následně proveďte download testovacího souboru "EICAR"

#wget https://secure.eicar.org/eicar.com.txt

a otestujte funkčnost antivirového softwaru ClamAV

#clamscan -i -r eicar.com.txt

TEST



Následující test obsahuje uzavřené otázky. Ke každé testové otázce Vám nabízíme čtyři varianty odpovědi, z nichž je vždy pouze jedna správná. Ta je součástí nabídky vždy. K žádné otázce v tomto testu nejsou přiřazeny dvě nebo dokonce tři správné odpovědi.

1) **Fyzická bezpečnost informačních aktiv NENÍ zajištěna**
   a. oplocením
   b. kamerovým systémem
   c. uzamčením dveří
   d. firewallem

2) **Nástrojem na ochranu před škodlivým softwarem NENÍ**
   a. antivirus
   b. antimalware
   c. Microsoft Outlook
   d. Antispyware

3) **Požadovaná složitost přístupových hesel je ověřována**
   a. Bezpečnostním manažerem
   b. Přímým nadřízeným
   c. Nástrojem pro ověřování identity uživatelů
   d. Útvarem síťové bezpečnosti

4) **Pravidelné aktualizace operačního systému, aplikačního softwaru, a nástroje proti škodlivému softwaru nechrání proti**
   a. známým virům
   b. chybám aplikačního softwaru
   c. lidskému selhání
   d. morálnímu zastarání aplikačního softwaru

5) **Elektronický zabezpečovací systém (EZS) je součástí:**
   a. nástroje pro ochranu před škodlivým kódem
   b. nástroje pro zajišťování dostupnosti informační infrastruktury
   c. fyzické bezpečnosti
   d. nástroje pro řízení přístupových oprávnění

6) **K vynucené změně přístupového hesla musí dojít vždy nejpozději po uplynutí:**
   a. 50 dnů
   b. 75 dnů
   c. 90 dnů
   d. 100 dnů

7) **Požadavky vyplývající § 18 vyhlášky o kybernetické bezpečnosti ohledně nástroje pro ověřování identity uživatelů lze zajistit:**
   a. Výhradně pomocí nástroje Microsoft Active Directory
   b. Výhradně pomocí nástroje OpenLDAP
   c. Jak prostřednictvím nástroje Microsoft Active Directory, tak OpenLDAP
   d. Prostřednictvím elektronických občanských průkazů vydávaných dle zákona č. 328/1999 Sb., o občanských průkazech

8) **Pravidla pro používání kryptografických prostředků určuje:**
   a. Národní centrum kybernetické bezpečnosti (NCKB)
   b. Orgán a osoba uvedená v § 3 písm. c) až e) zákona
   c. Ministerstvo vnitra
   d. zvláštní vyhláška

9) **Minimální požadavky, které musí splnit kryptografické algoritmy, jsou definovány:**
   a. Nařízením vlády
   b. Technickou normou vydanou Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví
   c. Přílohou č. 3 Vyhlášky č.316/2014 Sb.
   d. Matematickým ústavem akademie věd

10) **Nejmenší přípustná frekvence synchronizace systémového času technických aktiv patřících do informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému je:**
   a. 1 hodina
   b. 6 hodin
   c. 24 hodin
   d. 30 dnů

C. POZNÁMKY