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

Kybernetická bezpečnost I.
Legislativa a strategie kybernetické bezpečnosti v České republice

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 (otázky a úkoly), 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

TEORETICKÁ ČÁST:

- Legislativní předpisy
- Slovníček pojmů
- Užitečné webové stránky
- Doporučená odborná literatura

PRAKTICKÁ ČÁST:

- Kontrolní otázky
- Úkoly

A. TEORETICKÁ ČÁST

Legislativní předpisy

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
- Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
- Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)

SLOVNÍK POJMŮ

Kybernetický prostor - Digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.

Bezpečnost informací - Zajištění důvěrnosti, integrity a dostupnosti informací.

Kybernetická bezpečnost - Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.

Komunikační systém - Systém, který zajišťuje přenos informací mezi koncovými účastníky. Zahrnuje koncové komunikační zařízení, přenosové prostředí, správu systému, personální obsluhu a provozní podmínky a postupy.

Informační systém - Je funkční celek zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací a dat. Zahrnuje datové a informační zdroje, nosiče, technické, programové a pracovní prostředky, technologie a postupy, související normy a pracovníky.

Kritická informační infrastruktura - Prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti.

Významný informační systém - Informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.

Správce informačního/komunikačního systému - Orgán nebo osoba, které určují účel zpracování informací a podmínky provozování informačního/komunikačního systému.

Významná síť - Síť elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře.

Kritická infrastruktura - Prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.

Prvek kritické infrastruktury - Zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií.

Subjekt kritické infrastruktury - Provozovatel prvku kritické infrastruktury.

Průřezová kritéria - Soubor hledisek pro posuzování závažnosti vlivu narušení funkce prvku kritické infrastruktury s mezními hodnotami, které zahrnují rozsah ztrát na životě, dopad na zdraví osob, mimořádně vážný ekonomický dopad nebo dopad na veřejnost v důsledku rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života.

Odvětvová kritéria - Technické nebo provozní hodnoty k určování prvku kritické infrastruktury v odvětvích energetika, vodní hospodářství, potravinářství a zemědělství, zdravotnictví, doprava, komunikační a informační systémy, finanční trh a měna, nouzové služby a veřejná správa.

Ochrana kritické infrastruktury - Opatření zaměřená na snížení rizika narušení funkce prvku kritické infrastruktury.

Riziko - Možnost, že určitá hrozba využije zranitelnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému a způsobí poškození.

Analýza rizik - Proces pochopení povahy rizika a určení úrovně rizika.

Hodnocení rizik - Proces porovnání výsledků analýzy rizika s kritérii rizika k určení, zda riziko a/nebo jeho závažnost jsou přijatelná (akceptovatelná) nebo tolerovatelná.

Hrozba - Potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace.

Analýza hrozeb - Zkoumání činností a událostí, které by mohly negativně ovlivnit kvalitu služby IT (systém zpracování a přenosu dat) i/nebo data samotná.

Zranitelnost - Slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.

Analýza zranitelnosti - Systematické zkoumání systému a provozovaných služeb vzhledem k bezpečnostním slabinám a efektivitě bezpečnostních opatření.

Hodnocení zranitelností - Proces identifikace, kvantifikace a prioritizace (nebo hodnocení) zranitelností systému.

Bezpečnostní incident - Porušení nebo bezprostřední hrozba porušení bezpečnostních politik, bezpečnostních zásad nebo standardních bezpečnostních pravidel provozu Informační a komunikační technologie

Havarijní plán - Plán pro záložní postupy, odezvu na nepředvídanou událost a obnovu po havárii.

Krizové řízení - Souhrn řídících činností orgánů krizového řízení zaměřených na analýzu a vyhodnocení bezpečnostních rizik a plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s přípravou na krizové situace a jejich řešením, nebo ochranou kritické infrastruktury.

Mimořádná událost – Událost nebo situace vzniklá v určitém prostředí v důsledku živelní pohromy, havárie, nezákonnou činností, ohrožením kritické infrastruktury, nákazami, ohrožením vnitřní bezpečnosti a ekonomiky, která je řešena obvyklým způsobem orgány a složkami bezpečnostního systému podle zvláštních právních předpisů.

Krizová situace - Mimořádná událost, narušení kritické infrastruktury nebo jiné nebezpečí, při nichž je vyhlášen stav nebezpečí, nouzový stav nebo stav ohrožení státu.

Krizové opatření - Organizační nebo technické opatření určené k řešení krizové situace a odstranění jejích následků, včetně opatření, jimiž se zasahuje do práv a povinností osob.

Stav nebezpečí – Lze jej vyhlásit v případě živelní pohromy, ekologické nebo průmyslové havárie, nehody nebo jiného nebezpečí, při němž jsou ohroženy životy, zdraví, majetek nebo životní prostředí, kde intenzita ohrožení sice nedosahuje značného rozsahu, ale není možné jej odvrátit běžnou činností správních úřadů a složek integrovaného záchranného systému.

Nouzový stav - Státní krizové opatření pro závažné živelní nebo průmyslové katastrofy. Vyhlašuje jej vláda nebo předseda vlády na základě ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky. Přitom může omezit práva osob. Nouzový stav může být vyhlášen buď pro celé území státu, nebo pro vymezené území. Bez souhlasu Poslanecké sněmovny může být vyhlášen nejvýše na 30 dnů.

Stav ohrožení státu - Mimořádný stav, který může na návrh vlády vyhlásit Parlament v případě, že je bezprostředně ohrožena svrchovanost státu, územní celistvost státu nebo jeho demokratické zásady. Tento stav zatím nebyl na území České republiky nikdy vyhlášen.

Stav kybernetického nebezpečí - Stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v IS, nebo bezpečnost a integrita služeb nebo sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací. Stav mimořádný, speciální oproti mimořádným stavům vyhlašovaným podle ústavního zákona č. 110/1998 Sb. o bezpečnosti České republiky nebo podle krizového zákona č. 240/2000 Sb. Vyhlašuje ředitel NBÚ nejdéle na 7 dnů s možností prodloužení v souhrnu na nejvýše 30 dnů. Není – li možné odvrátit nebezpečí v rámci stavu KN ředitel Úřadu požádá vládu o vyhlášení nouzového stavu.

Zájem České republiky - Zachování její ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života nebo zdraví fyzických osob.

Vládní CERT - Pracoviště provozované NBÚ jako součást Národního centra kybernetické bezpečnosti. Jde o orgán veřejné moci, který má nařizovací a sankční pravomoci. Jeho služby jsou primárně určené vybraným informačním a komunikačním systémům, které mají pro národní zájmy České republiky vitální charakter, tj. na oblast kritické informační infrastruktury a významných informačních systémů.

Národní CERT - Osoba soukromého práva bez nařizovacích nebo sankčních pravomocí. Kontaktní místo zejména pro osoby soukromého práva. K vyhodnocování a metodické podpoře subjektů, které aktivně projeví zájem o výhody kolektivní ochrany před kybernetickými bezpečnostními incidenty. K výkonu své činnosti je oprávněn na základě veřejnoprávní smlouvy uzavírané s Úřadem.

DŮLEŽITÉ POJMY A ZKRATKY

KB	Kybernetická bezpečnost
NBÚ	Národní bezpečnostní úřad
NCKB	Národní centrum kybernetické bezpečnosti
ZKB	Zákon o kybernetické bezpečnosti
VKB	Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti
KII	Kritická informační infrastruktura

VIS Významný informační systém

VVIS Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích

NSKB Národní strategie kybernetické bezpečnosti

AP Akční plán

CERT Computer Emergency Response Team

NIS Evropská směrnice o bezpečnosti sítí a informací

SCADA Supervisory Control And Data Acquisition

ICS Information control systém

ENISA Evropská agentura pro bezpečnost sítí a informací (European Network and Information Security Agency)

UŽITEČNÉ WEBOVÉ STRÁNKY

- Vládní CERT: www.govcert.cz
- Národní CERT: www.csirt.cz
- Výkladový slovník kybernetické bezpečnosti: https://www.govcert.cz/cs/informacni-servis/vykladovy-slovnik/-
- Common Criteria Portal: https://www.commoncriteriaportal.org/
- www.isaca.org
- Informace o aktivitách v oblasti kybernetické bezpečnosti: http://cybersecurity.cz/
- ENISA - https://www.enisa.europa.eu/
- Evropský program na ochranu kritické infrastruktury: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=URISERV:l33260

DOPORUČENÁ ODBORNÁ LITERATURA

- SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013, 483 s. Expert (Grada). ISBN 978-80-247-4644-9.
- ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: Akademické nakladatelství CERM, 2013, 377 s. ISBN 978-80-7204-872-4.
- DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.
- DOUCEK, Petr, Luděk NOVÁK a Vlasta SVATÁ. *Řízení bezpečnosti informací*. 1. vyd. Praha: Professional Publishing, 2008, 239 s. ISBN 9788086946887.
- *ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky*. Praha: Český normalizační institut.

B. PRAKTICKÁ ČÁST

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

KONTROLNÍ OTÁZKY

Následující sada kontrolních otázek obsahuje 10 otevřených a 15 uzavřených otázek. Ke každé uzavřené otázce Vám nabízíme možné varianty odpovědi, z nichž je vždy pouze jedna správná. Ta je součástí nabídky vždy.

1. Činnost jakých dvou dohledových pracovnišť (CERT) ZKB upravuje?
2. Co by jste zařadili mezi tři hlavní pilíře ZKB? (pílíř = skupina povinností uzožených ZKB)
3. Jmenujte tři hlavní právní předpisy regulující kybernetickou bezpečnost.
4. Co je hlavním cílem právní úpravy kybernetické bezpečnosti?
5. Kdo je obecně zodpovědný za naplnění požadavků ZKB?
6. Kde naleznete specifikace povinností a opatření, které musejí naplnit povinné osoby.
7. Kdo kontroluje naplnění požadavků zákona?
8. Jaké dva základní dokumenty (nelegislatvní) ovlivňují směřování ČR v oblasti KB?
9. Kdo je z pohledu ZKB považován za správce informačního/komunikačního systému KII/VIS?
10. Pro hodnocení naplnění kritérií pro KII/VIS je třeba uvažovat všechny tři aspekty bezpečnosti informací. Jmenujte je.

11. Kdo je gestorem kybernetické bezpečnosti v ČR?
    a. Ministerstvo vnitra
    b. Národní bezpečnostní úřad
    c. Ministerstvo průmyslu a obchodu
    d. Český telekomunikační úřad

12. Kolik druhů povinných osob nebo orgánů ZKB rozeznává?
    a. 4
    b. 3
    c. 5
    d. 6

13. Jaký subjekt může být správcem významného informačního systému?
    a. Každá organizační složka státu
    b. Pouze orgán veřejné moci
    c. Jakákoli organizace

14. Může být správcem významného informačního systému obec?
    a. Ano
    b. Ne

15. Kde naleznete průřezová a odvětvová kritéria pro určení KII?
    a. V nařízení vlády č. 432/2010 Sb.
    b. V zákoně č. 240/2010 Sb. (krizový zákon)
    c. V zákoně č. 181/2014 Sb. (zákon o kybernetické bezpečnosti)
    d. V jiném předpise

16. Které povinné osoby hlásí kontaktní údaje vládnímu CERT?
    a. Všechny povinné osoby a orgány
    b. Pouze správci VIS
    c. Pouze správci KII
    d. Pouze správci VIS a KII

17. Kdo vyhlašuje stav kybernetického nebezpečí?
    a. Vláda
    b. Ministr vnitra
    c. Ředitel NBÚ
    d. Ředitel NCKB

18. Komu jsou povinni správci KII a VIS hlásit kontaktní údaje?
    a. Vládnímu CERTu
    b. Národnímu CERTu
    c. Vojenskému CERTu
    d. Ministerstvu vnitra

19. Komu jsou povinny hlásit kontaktní údaje povinné osoby kromě správců KII a VIS?
    a. Vládnímu CERTu
    b. Národnímu CERTu
    c. Vojenskému CERTu
    d. Ministerstvu vnitra

20. Od jakého okamžiku počínají správcům KII běžet lhůty pro plnění povinností uložených ZKB (např. nahlášení kontaktních údajů)?
    a. Od účinnosti zákona
    b. Od určení
    c. Od naplnění kritérií

21. Je příkaz k vypnutí systému možné považovat za sankci dle ZKB?
    a. Ano
    b. Ne

22. Pro koho je závazné plnit Akční plán k Národní strategii kybernetické bezpečnosti ČR 2015-2020?
    a. Pouze pro NBÚ
    b. Pro všechny soukromoprávní i veřejnoprávní subjekty
    c. Pro organizace, které jsou v něm výslovně uvedeny

23. Kolik „skupin“ kritérií pro KII legislativa rozeznává?
    a. Dvě – průřezová a odvětvová
    b. Tři – průřezová, odvětvová, dopadová
    c. Čtyři – průřezová, odvětvová, dopadová, oblastní

24. Kolik kritérií z každé skupiny je třeba naplnit aby prvek splnil kritéria pro KII?
    a. Alepoň jedno z každé skupiny kritérií
    b. Stačí naplnit kritérium alepoň jedné skupiny
    c. Z jedné skupiny kritérií musí být naplněny alespoň dvě

25. Kdo posuzuje naplnění kritérií pro VIS?
    a. NBÚ
    b. Samotný správce posuzovaného informačního systému
    c. Ministerstvo vnitra

ÚKOLY

1) Vyberte informační systém ve správě vaší organizace (například spisovou službu) a zkuste jej posoudit jako VIS. (tedy posoudit, zda naplňuje kritéria stanovená vyhláškou č. 317/2014 Sb.)

2) Zkuste stručně definovat kybernetickou bezpečnost. Co vše do této oblasti podle Vás patří?

3) Jmenujte alespoň tři principy na kterých stojí ZKB

C. POZNÁMKY