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

Kybernetická bezpečnost II.
Management kybernetické bezpečnosti

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:

- Oblasti k prostudování
- Slovníček pojmů k ZKB
- Seznam zkratek
- Užitečné webové stránky
- Doporučená odborná literatura

PRAKTICKÁ ČÁST:

- Úkoly
- Kontrolní otázky

A. TEORETICKÁ ČÁST

Oblasti k prostudování

Níže naleznete přehled klíčových oblastí, které je nutné nastudovat z doporučené literatury a z webových stránek.

- Zákon o kybernetické bezpečnosti v ČR
- Prováděcí právní předpisy k zákonu o kybernetické bezpečnosti
- Řízení rizik, informační aktiva, identifikace a hodnocení aktiv
- Systém řízení bezpečnosti informací (ISMS)
- ITIL v3
- COBIT
- Procesní řízení
- Bezpečnostní role podle ZKB
- Bezpečnostní opatření
- Bezpečnostní politika
- DRP (ISO 22 301)
- Bezpečnostní dokumentace
- Audit kybernetické bezpečnosti
- ITAF

SLOVNÍK POJMŮ

Pojem	Vymezení pojmu
Orgán a osoba	Orgán a osoba, které je uložena povinnost v oblasti kybernetické bezpečnosti podle § 3, písmene c) až e) zákona č. 181/2014 Sb. (zákon o kybernetické bezpečnosti).
Systém řízení bezpečnosti informací (ISMS)	Část systému řízení orgánu a osoby, založená na přístupu k rizikům informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, která stanoví způsob ustavení, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací.
Aktivum	Primární a podpůrné aktivum.
Primární aktivum	Informace nebo služba, kterou zpracovává nebo poskytuje informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém.
Podpůrné aktivum	Technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.
Technické aktivum	Technické vybavení, komunikační prostředky a programové vybavení informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému a objekty, ve kterých jsou tyto systémy umístěny.
Riziko	Možnost, že určitá hrozba využije zranitelnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému a způsobí poškození aktiva.
Hodnocení rizik	Proces, při němž je určována významnost rizik a jejich přijatelná úroveň.
Řízení rizik	Činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik.
Hrozba	Potencionální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, jejímž výsledkem může být poškození aktiva.
Zranitelnost	Slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.

Přijatelné riziko	Riziko zbývající po uplatnění bezpečnostních opatření, jehož úroveň odpovídá kritériím pro přijatelnost rizik.
Bezpečnostní politika	Soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv orgánem a osobou.
Garant aktiva	Fyzická osoba pověřená orgánem a osobou k zajištění rozvoje, použití a bezpečnosti aktiva.
Uživatel	Fyzická nebo právnická osoba anebo orgán veřejné moci, která využívá primární aktiva.
Administrátor	Fyzická osoba pověřená garantem aktiva odpovědná za správu, provoz, použití, údržbu a bezpečnost technického aktiva.
Manažer kybernetické bezpečnosti	Osoba odpovědná za systém řízení bezpečnosti informací, která je pro tuto činnost řádně vyškolena a prokáže odbornou způsobilost praxí s řízením bezpečnosti informací po dobu nejméně tří let.
Architekt kybernetické bezpečnosti	Osoba odpovědná za návrh a implementaci bezpečnostních opatření, která je pro tuto činnost řádně vyškolena a prokáže odbornou způsobilost praxí s navrhováním bezpečnostní architektury po dobu nejméně tří let.
Auditor kybernetické bezpečnosti	Osoba odpovědná za provádění auditu kybernetické bezpečnosti, která je pro tuto činnost řádně vyškolena a prokáže odbornou způsobilost praxí s prováděním auditů kybernetické bezpečnosti po dobu nejméně tří let. Auditor kybernetické bezpečnosti vykonává svoji roli nestranně a výkon jeho role je oddělen od výkonu rolí manažera, architekta a výboru kybernetické bezpečnosti.
Výbor pro řízení kybernetické bezpečnosti	Organizovaná skupina tvořená osobami, které jsou pověřeny celkovým řízením a rozvojem informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, anebo se významně podílejí na řízení a koordinaci činností spojených s kybernetickou bezpečností těchto systémů.
Prostředky fyzické bezpečnosti	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.
Nástroj pro ověřování identity uživatelů a administrátorů	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.

SEZNAM ZKRATEK

Pozn.: seznam zkratek obsahuje pouze nejčastěji užívané zkratky v rámci tohoto kurzu. V případě zájmu, doporučujeme stáhnout si z webu www.govcert.cz „Výkladový slovník kybernetické bezpečnosti - třetí vydání“.

ISMS	Information Security Management System
ZKB	Zákon o kybernetické bezpečnosti
VKB	Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti
KII	Kritická informační infrastruktura
VIS	Významný informační systém
SIEM	Security Information and Event Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
MDM	Mobile Device Management
BYOD	Bring your own Device
BYOS	Bring your own Software
IoT	Internet of Things
SDN	Software Defined Networks
APT	Advance Presistent Threat

UŽITEČNÉ WEBOVÉ STRÁNKY

- Vládní CERT - www.govcert.cz
- Národní CERT - www.csirt.cz
- Common Criteria Portal - https://www.commoncriteriaportal.org/
- Organizace ISACA - www.isaca.org
- CyberSecurity.cz - http://cybersecurity.cz/
- Open Sourced Vulnerability Database - http://osvdb.org/
- ENISA - https://www.enisa.europa.eu/
- CCDCOE - https://ccdcoe.org/

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.
- WONG, Wei Ning Zechariah a Jianping SHI. *Business continuity management system: a complete framework for implementing ISO 22301*. xvi, 279 pages.
- DOUCEK, Petr, Miloš MARYŠKA a Lea NEDOMOVÁ. *Informační management v informační společnosti*. 1. vyd. Praha: Professional Publishing, 2013, 264 s. ISBN 978-80-7431-097-3.
- SVATÁ, Vlasta. *Audit informačního systému*. 2. vyd. Praha: Professional Publishing, 2012, 219 s. ISBN 978-80-7431-106-2.

B. PRAKTICKÁ ČÁST

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

KONTROLNÍ OTÁZKY

1. Jaký je rozdíl mezi událostí a incidentem?
2. Na jaké úrovni řízení, by měla být řízena bezpečnost?
3. Co znamená PDCA? (popsat vč. jednotlivých fází)
4. Jaké znáte metodiky, knihovny a normy zabývající se ICT bezpečností?
5. Co byste zařadili do organizačních a co do technických opatření?
6. Jaký je rozdíl mezi primárním, podpůrným a technickým aktivem?
7. Jaké bezpečnostní role definuje ZKB?
8. Jaké znáte metody analýzy rizik?
9. Jak jsou rozdělena aktiva podle VKB?
10. Jaký je hlavní rozdíl v přístupu ISMS a ZKB k ochraně informací?
11. Co je to kyberprostor?
12. Jaké znáte typy kybernetických útoků?
13. Řekněte příklad bezpečnostní události a bezpečnostního incidentu.
14. Co v projektovém managementu znamená pojem SMART?
15. Jaký je zásadní rozdíl mezi efektivností a efektivitou?
16. Co definuje rozsah ISMS?
17. Popište roli výboru pro řízení kybernetické bezpečnosti.
18. Popište role auditora, architekta a manažera KB.
19. Popište roli garanta aktiva.
20. Jaké znáte způsoby výpočtu rizika?
21. Co je to registr rizik?
22. Jakým způsobem identifikujete hrozby, zranitelnosti a rizika?
23. Co je to SLA a jakou roli hraje v oblasti kybernetické bezpečnosti?
24. Jaké výhody a nevýhody vidíte u CLOUDových řešení?
25. Jaké typy CLOUDových služeb znáte?

ÚKOLY

1) Jakým způsobem byste zajistili ve Vaší organizaci bezpečnost lidských zdrojů?

2) Jakým způsobem byste se rozhodli, zda pořídit nový systém a provozovat jej interně, nebo zda jej outsourcovat?
   a) Jaké další souvislosti byste společně s tímto rozhodnutím řešili?

3) Pokuste se navrhnout, několika body, strukturu školení pro své zaměstnance, zaměřené na ICT bezpečnost.

4) Sestavte jednoduchou úvahu na téma interní zaměstnanec vs. externí odborník.

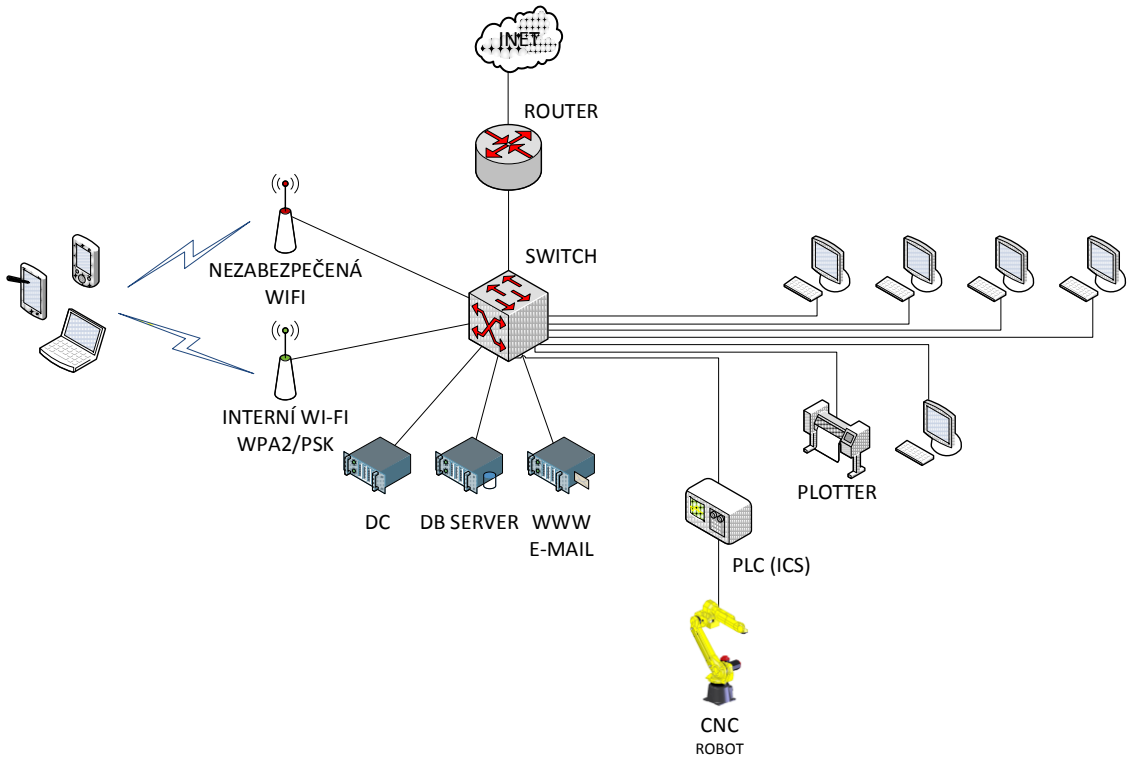
5) Pokuste se sestavit jednoduchý DRP plán pro případ:
   a) Ztráty dat
   b) Kybernetický útok, zaměřený na webovou aplikaci

6) Pokuste se stručně definovat „desatero kybernetické bezpečnosti“ k interpretaci zaměstnancům

7) Jak myslíte, že by bylo možné předejít kybernetickému útoku ze strany interních zaměstnanců?

8) Pokuste se navrhnout bezpečnou architekturu z těchto prvků (jejich funkce si upřesněte a odůvodněte; jednotlivé prvky můžete použít více krát) – firewall, switch, databázový server, aplikační server, domain controller, webový server, e-mailový server, router, wifi router, síťová tiskárna, PC, notebook, tablet, ovládání klimatizace, IP kamera.

9) Zamyslete se nad zobrazenou architekturou a pokuste se navrhnout ji správně.



Pozn.: Schema představuje architekturu infrastruktury malého výrobního podniku s poměrně jednoduchou síťovou architekturou. Kromě serverů pro provoz DC, webu a e-mailových služeb společnost vlastní i DB server, který hostuje databázi ERP systému. Na stejné infrastruktuře je připojena i veřejná WiFi síť pro zákazníky prodejny a obráběcí CNC robot.

C. POZNÁMKY