Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Teze diplomové práce

Zabezpečení IT infrastruktury orgánu veřejné moci v ČR

Pavel Charvát

Zabezpečení IT infrastruktury orgánu veřejné moci v ČR

Souhrn

Diplomová práce se zabývá způsobem zabezpečení prostředí a informačních systémů orgánu veřejné moci. Vychází především z požadavků, které stanovuje Zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Hlavním cílem je navržením konkrétních bezpečnostních opatření zajistit co nejvyšší shodu s požadavky tohoto zákona. V teoretické části práce jsou analyzovány požadavky Vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti, která je prováděcím předpisem Zákona o kybernetické bezpečnosti, a jejich dopady na orgán veřejné moci.

Praktická část práce představuje výsledky srovnávací analýzy stavu bezpečnostních opatření orgánu veřejné moci se zákonnými požadavky. Z těchto výsledků pak vyplývá nutnost vypracování chybějící dokumentace stanovující organizační opatření a potřeba vhodné konfigurace nástrojů pro sběr, detekci a vyhodnocení bezpečnostních událostí. V části diskuse je pak posouzeno zvýšení míry souladu se zákonnými požadavky po implementaci navržených opatření a jsou v ní také nastíněny další kroky nutné k dosažení kompletního souladu.

Klíčová slova: bezpečnost, analýza rizik, aktivum, zákon o kybernetické bezpečnosti, bezpečnostní incident, monitoring, malware, SIEM, NetFlow

Cíl práce

Hlavním cílem je zanalyzovat dopady zákona o kybernetické bezpečnosti (ZKB) na konkrétní orgán veřejné moci (OVM) v ČR. Stanovit výchozí stav připravenosti tohoto OVM na podmínky kladené ZKB a následně navrhnout konkrétní opatření potřebná pro zajištění shody se ZKB.

Dílčími cíli jsou obecná charakteristika systému řízení bezpečnosti informací, popis náležitostí bezpečnostní politiky, návrh metodiky identifikace aktiv a řízení rizik a postup řízení bezpečnostních incidentů, včetně praktické ukázky použití nástrojů pro jejich detekci.

Metodika

Výchozím bodem metodiky je prostudování legislativního rámce kybernetické bezpečnosti v ČR a posouzení kompatibility výchozího stavu OVM s tímto rámcem. Následuje návrh potřebných organizačních i technických změn a popis náležitostí bezpečnostní politiky. Z návrhu vyplyne také obecná charakteristika požadované úrovně systému řízení bezpečnosti informací, vytvoření metodiky pro identifikaci aktiv a řízení rizik a postup řízení bezpečnostních incidentů. Řízení bezpečnostních incidentů bude podpořeno praktickou ukázkou detekce bezpečnostních událostí prostřednictvím nástrojů určených

pro detekci, sběr a vyhodnocení kybernetických bezpečnostních událostí s následnou analýzou zkoumané události.

GAP analýza

Ve chvíli, kdy vstoupil v platnost Zákon o kybernetické bezpečnosti, bylo jasné, že Úřad není plně v souladu podmínkami, které na něj zákon kladl. Aby bylo jasné, které aspekty nesplňuje, byla provedena srovnávací analýza stavu bezpečnosti s cílem posoudit míru souladu s jednotlivými paragrafy Vyhlášky o kybernetické bezpečnosti. Z analýzy vyplynul závěr, že Úřad dosahoval souladu především v oblasti technických opatření (shoda 70%). Nicméně v oblasti organizačních patření významně zaostával (shoda 30%). Výsledkem tedy bylo doporučení zaměřit se především na vylepšení organizačního zabezpečení kybernetické bezpečnosti.

Organizační opatření

Základním opatřením bylo kompletní přepracování bezpečnostní politiky Úřadu tak, aby splňovala požadavky kladené ZKB. Dále bylo nutné formálně zavést proces řízení bezpečnosti informací. To spočívalo především ve stanovení potřebné bezpečnostní organizační struktury. Byly definovány jednotlivé bezpečnostní role a stanoveny jejich práva a povinnosti. Základním kamenem zavedení systému řízení bezpečnosti informací bylo v Úřadu ustanovení Výboru pro řízení kybernetické bezpečnosti.

Základem v podstatě každého rozhodování v organizaci, která má systém řízení bezpečnosti informací, je řízení rizik. K tomu, aby tento proces probíhal v Úřadu jednotně, slouží především nově vytvořená Metodika analýzy rizik Úřadu. Tato metodika vychází z principů uvedených v ČSN ISO/IEC 27005:2013, přičemž zohledňuje stupnice a katalogy uvedené ve vyhlášce č. 316/2014 Sb. o kybernetické bezpečnosti.

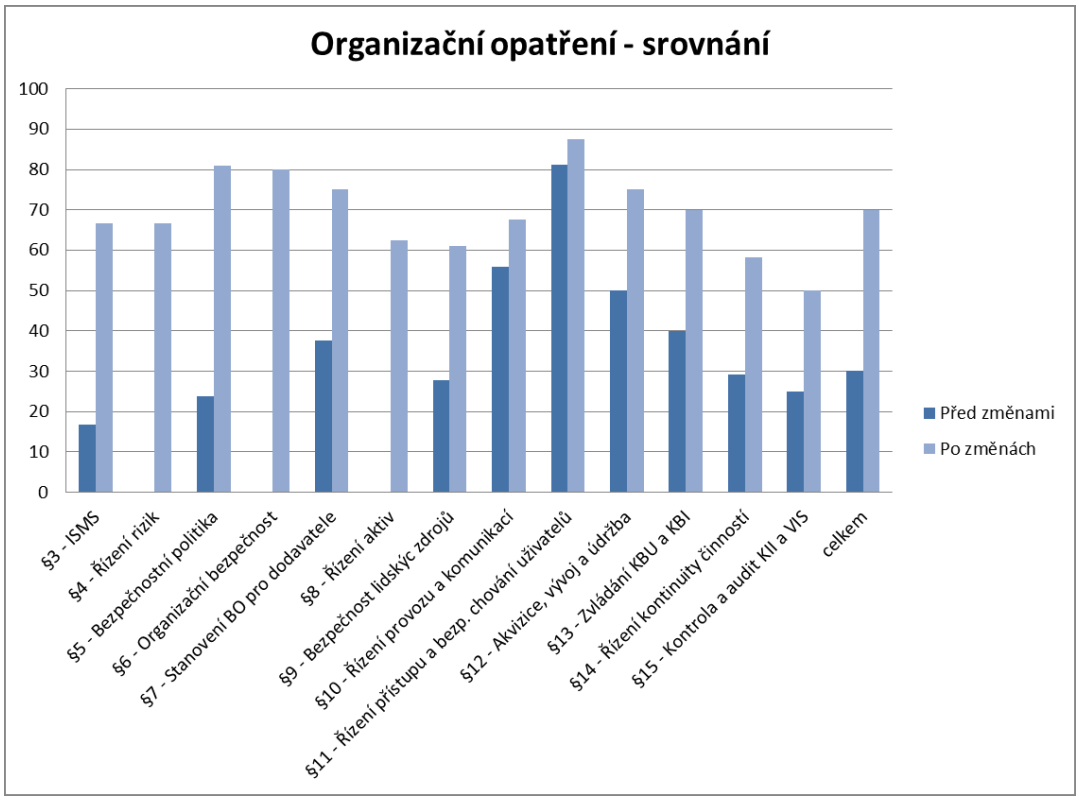
Posledním organizačním opatřením řešeným touto prací je oblast řízení bezpečnostních incidentů. K zajištění této oblasti byla zpracována Metodika řízení bezpečnostních incidentů v informačních systémech.

Technická opatření

Oblast technických opatření byla už v době provádění srovnávací analýzy na dobré úrovni. Přesto i opatřením v této oblasti byla věnována pozornost. Výsledkem analýzy technických opatření vyplynula potřeba lépe nastavit SIEM a NetFlow Monitoring jakožto nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí (KBU). Práce také obsahuje ukázku využití těchto systémů při šetření konkrétní bezpečnostní události.

Zhodnocení přínosů opatření

Přínosy, které přinesla provedená opatření, shrnuje především následující graf. Jde o porovnání dosažené shody se Zákonem o kybernetické bezpečnosti v oblastech organizačních opatření před a po jejich implemetaci.



Obrázek 1 - Srovnání hodnocení dosažení shody se ZKB - organizační opatření (vlastní zpracování)

Z grafu srovnání hodnocení shody organizačních opatření vyplývá, že dopracovaná dokumentace zvýšila celkovou míru plnění požadavků Zákona o kybernetické bezpečnosti ze 30 na 70 %. To představuje zásadní zlepšení, které ve své podstatě znamená rozdíl mezi úspěšným a neúspěšným průchodem auditem. Tento fakt byl potvrzen úspěšným provedením metodického auditu NBÚ na jeden z informačních systémů Úřadu spadajícího pod ZKB. Audit nalezl jen několik dílčích nesouladů.

Ekonomická stránka implementace

K dosažení výše popsaného zlepšení souladu se Zákonem o kybernetické bezpečnosti ze 30 na 70 % u organizačních opatření a ze 70 na 85 % u technických opatření bylo potřeba jak finančních investic, tak práce zaměstnanců Úřadu.

Celkové náklady na bezpečnostní opatření navržená touto prací tedy činily 2 280 000,- Kč. S tím, že 1 100 000,- Kč jsou pravidelné roční náklady na servis použitých technologií. Dále je třeba připočíst zhruba 2 plné pracovní úvazky (cca 500 MD/ročně) na správu používaných bezpečnostních technologií a provádění analýz zachycených bezpečnostních událostí. Další zhruba půl pracovního úvazku vynakládá Úřad na personální zajištění organizačního zabezpečení ISMS.

Závěr

Prostřednictvím navržených organizačních i technických bezpečnostních opatření bylo dosaženo podstatného přiblížení ke shodě se Zákonem o kybernetické bezpečnosti a relevantnějšího řešení kybernetických bezpečnostních událostí a incidentů. Pro úplný soulad se ZKB je třeba ještě vylepšit některá z opatření a především také zajistit jejich dlouhodobé udržování. Zásadním předpokladem je pro Úřad také zajištění a udržení dostatečného počtu kvalifikovaných osob.

Prosazování nových bezpečnostních opatření s sebou přineslo také zvýšení osvěty a zájmu o kybernetickou bezpečnost ze strany managementu i běžných pracovníků Úřadu, což je naprosto zásadní posun v zajišťování bezpečnosti jakéhokoli subjektu.

Seznam vybraných použitých zdrojů

ČESKO. Zákon č. 181/2014 Sb. ze dne 29. srpna 2014, o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky*. 2014, částka 75, s. 1926-1936. ISSN 1211-1244. (PDF) Dostupné také z: http://ftp.aspi.cz/opispdf/2014/075-2014.pdf

ČR NBÚ. *Národní strategie kybernetické bezpečnosti ČR na období let 2015 až 2020*. Národní centrum kybernetické bezpečnosti. [Online] 16. únor 2015. [Cit.: 18. září 2016.] (PDF). Dostupné z WWW: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf.

ČESKO. Vyhláška č. 316/2014 Sb. ze dne 19. prosince 2014, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky*. 2014, částka 127, s. 3972-4006. ISSN 1211-1244. (PDF) Dostupné také z: http://ftp.aspi.cz/opispdf/2014/127-2014.pdf

Microsoft Corporation. *Microsoft Advanced Threat Analytics*. Microsoft.com. [Online] 2016. [Cit.: 6. listopad 2016.] (PDF). Dostupné z WWW: http://download.microsoft.com/download/C/F/6/CF62335F-C46B-4D84-B0C9-363A89B0C5E6/Microsoft_advanced_threat_analytics_datasheet.pdf.

Cisco Systems Inc. *Cisco IOS NetFlow Version 9 Flow-Record Format*. Cisco. 2011. [Cit.: 20. únor 2016.] (PDF). Dostupné z WWW: http://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9.pdf. Třídicí znak: C11-395693-01

Flowmon Networks. *Flowmon 8.02.00 - Uživatelská příručka*. (PDF). 19. srpen 2016. [Cit.: 2. únor 2017.]

Flowmon Networks. *Flowmon ADS Business 8.02.00 - Uživatelská příručka*. (PDF). Brno. Flowmon Networks, 2015. prosinec 2016.

HARRIS, Shon. *Gray hat hacking: the ethical hacker's handbook*. 2nd ed. New York: McGraw-Hill, c2008. ISBN 0-07-149568-1.

KUROSE, James F. a ROSS, **Keith W.** *Počítačové sítě*. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.

SANDERS, Chris. *Analýza sítí a řešení problémů v programu Wireshark*. 1. vyd. Brno: Computer Press, 2012. ISBN 978-80-251-3718-5.