Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Zabezpečení IT infrastruktury orgánu veřejné moci v ČR

Pavel Charvát

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Pavel Charvát

Informatika

Název práce

Zabezpečení IT infrastruktury orgánu veřejné moci v ČR

Název anglicky

IT infrastructure security in one of the public authorities in the Czech Republic

---

Cíle práce

Hlavním cílem je analyzovat 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 náležitosti 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 rámec 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, návrh 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 a následnou analýzou zkoumané události.

Doporučený rozsah práce

60-80 stran

Klíčová slova

bezpečnost, analýza rizik, aktivum, zákon o kybernetické bezpečnosti, bezpečnostní incident

---

Doporučené zdroje informací

BS ISO/IEC 27002:2013, Information technology. Security techniques. Code of practice for information security controls, BSI, 2013, ISBN 978-0-580-91369-3

HARRIS, S., HARPER, A., EAGLE, CH., NESS, J., Gray Hat Hacking : The Ethical Hacker's Handbook 2nd, 577 str. ISBN 0-07-149568-1.

ROSS, K W. – KUROSE, J F. *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.

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). In: Sbírka zákonů. 19. 12. 2014. ISSN 1211-1244

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Sbírka zákonů. 29. 8. 2014. ISSN 1211-1244

Předběžný termín obhajoby

2016/17 LS – PEF

Vedoucí práce

Ing. Čestmír Halbich, CSc.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 18. 10. 2016

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 24. 10. 2016

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 01. 03. 2017

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Zabezpečení IT infrastruktury orgánu veřejné moci v ČR" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 27.3.2017 _____

Poděkování

Rád bych touto cestou poděkoval panu Ing. Čestmíru Halbichovi, CSc. za vedení mé diplomové práce a užitečné rady.

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 zajistit co nejvyšší shodu s požadavky tohoto zákona navržením konkrétních bezpečnostních opatření. 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

IT infrastructure security in one of the public authorities in the Czech Republic

Summary

This thesis deals with the way the securing the environment and information systems of the public authority. It is primarily based on the requirements of the Act No. 181/2014 Coll., the Cybersecurity Act. The main objective is to design specific security measures to ensure the highest possible compliance with the requirements of this Act. The theoretical part analyses the requirements of the Decree no. 316/2014 Coll., the Cybersecurity Decree, which is implementing the Cybersecurity Act and its impact on the public authority.

The practical part presents the authority's state of security measures comparative analysis results with legal requirements. These results indicates the need for elaboration of a missing documentation, setting out the organizational measures and the need for appropriate configuration of the security events collection, detection and evaluation tools. The increased level of compliance with legal requirements, after the implementation of the designed measures, is assessed in the discussion part of he thesis. The further steps necessary to achieve the full compliance are outlined there as well.

Keywords: security, risk analysis, asset, the cyber security act, security incident, monitoring, malware, SIEM, NetFlow

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

1U - 1 Rack Unit (jednotka popisu výšky zařízení určeného do racku)
ADS - Anomaly Detection System
CERT - Computer Emergency Response Team
CIDR - Classless Inter-Domain Routing
CPU - Central Processing Unit (procesorová jednotka)
CSIRT - Computer Security Incident Response Team (bezpečnostní tým pro koordinaci řešení bezpečnostních incidentů v počítačových sítích)
DNS - Domain Name Systém
DSP - Device Support Module
EPS - Events Per Second
EPS - Elektronická Požární Signalizace
EZP - Elektronická Zabezpečovací Signalizace
FMC - Flowmon Monitoring Center
FPM - Flows Per Minute
GB - Gigabyte
HA - High Availability (vysoká dostupnost)
HTTP - HyperText Transfer Protocol
ICT - Information and Communication Technologies
IDS - Intrusion Detection System
IP - Internet Protocol
IPFIX - IP Flow Information eXport
IPS - Intrusion Prevention System
IS - Informační Systém
ISIRT - Information Security Incident Response Team
ISMS - Information Security Management Systém (Systém řízení bezpečnosti informací)
ISO/IEC - International Organization for Standardization/International Electrotechnical Commission
ISP - Internet Service Provider (poskytovatel internetového připojení)
KII - Kritická Informační Infrastruktura (dle definice ZKB)
LAN - Local Area Network (místní síť)
NBÚ - Národní Bezpečnostní Úřad

NCKB - Národní Centrum Kybernetické Bezpečnosti
NDA - Non-Disclosure Agreement (Dohoda o mlčenlivosti)
NPM - Network Performance Metrics
NTP - Network Time Protokol
OS - Operační Systém
OVF - Open Virtualization Format
OVM - Orgán Veřejné Moci
PLC - Programmable Logic Controller (Programovatelný logický automat)
RAM - Random Access Memory (paměť s přímým přístupem – operační paměť)
RDP - Remote Desktop Protokol
RJ-45 - Registered Jacks -45 (označení koncovky pro síťové kabely)
RPO - Recovery Point Objective (určuje maximální stáří obnovovaných dat)
RTO - Recovery Time Objective (určuje maximální čas do obnovení chodu IS nebo obecně procesu)
SCADA - Supervisory Control And Data Acquisition (systém pro dispečerské řízení a sběr dat)
SIEM - Security Information and Event Management (nástroj pro řízení bezpečnostních informací a událostí)
SIP - Session Initiation Protocol
SLA - Service-Level Agreement (smlouva o úrovni poskytovaných služeb)
SPAN - Switched Port Analyzer
SSH - Secure Shell
SSL - Secure Sockets Layer – protokol
TB - Terabyte
TCP - Transmission Control Protocol
TLS - Transport Layer Security – protokol
TOR - The Onion Routing (anonymizační softwarový systém)
TTL - Time To Live
UDP - User Datagramm Protocol
UPS - Uninterruptible Power Supply (zdroj nepřerušovaného napájení)
VIS - Významný Informační Systém (dle definice ZKB)
VKB - Vyhláška o Kybernetické Bezpečnosti (č. 316/2014 Sb.)
VLAN - Virtual Local Area Network (virtuální LAN)
WAN - Wide Area Network (rozsáhlá síť)
ZKB - Zákon o Kybernetické Bezpečnosti (č. 181/2014 Sb.)

1 Úvod

Kybernetická bezpečnost[1] je často velmi podceňovaný aspekt, a to jak v soukromé sféře, tak především ve sféře veřejné. Bezpečnost je zanedbávána z několika hlavních důvodů. Především jde o to, že ať se na bezpečnost díváme z jakéhokoli úhlu, vždy jde o nějaké opatření, které má větší nebo menší vliv na hlavní činnost daného subjektu (ať už soukromého nebo veřejného). Zavádění bezpečnostních opatření totiž nikdy není primární činností subjektu, a to ani u společností, které se na kybernetickou bezpečnost specializují a nabízejí v této oblasti své služby zákazníkům. Zavádění bezpečnostních opatření tedy snižuje efektivitu hlavní business činnosti subjektu.

Dalším aspektem zanedbávání bezpečnosti je její cena. Ve skutečnosti neexistuje žádné bezpečnostní opatření, které by bylo zadarmo. Už jen snížení efektivity zmíněné v předchozím odstavci znamená náklad. Když si navíc uvědomíme, že budování efektivní bezpečnosti ve společnosti je proces, který je nákladný jak z materiálního, tak z organizačního pohledu, je jasné, že společnosti jen nerady alokují finance a lidský kapitál do něčeho, co snižuje efektivitu jejich hlavního oboru podnikání.

V neposlední řadě je budování bezpečnosti vysoce odborná činnost vyžadující specifické znalosti a zkušenosti. Tento fakt zajištění bezpečnosti dále prodražuje. Firmy často zkrátka nemají bezpečnostní profesionály, nemohou je na trhu práce sehnat nebo do nich nechtějí investovat. Služby v oboru kybernetické bezpečnosti jsou také jedny z těch dražších z oblasti IT služeb.

Je-li tedy bezpečnost tak drahá, složitá a komplikuje hlavní obor činnosti subjektu, proč by se jí firmy a veřejný sektor měly vůbec zabývat? Odpověď je snadná. V dnešní době se jedná v podstatě o existenční nutnost. Moderní lidská společnost je čím dál více závislá na technologiích. Moderní technologie přinesly obrovské zefektivnění spousty činností. Společnosti si samozřejmě možnost zefektivnit své procesy nenechaly ujít. Lidé zase nové technologie využívají ke své zábavě, usnadnění práce i zlepšení životního

[1] „Souhrn právních, organizačních, technických, fyzických a vzdělávacích opatření namířených na zajištění nerušeného a bezvadného fungování kybernetického prostoru.“ (5, s. 55)

standardu. Spolu s masivní elektronizací společnosti se ale začaly objevovat také nové vektory ohrožení. Odhady finančních dopadů kybernetické kriminality se podle studií pohybují v řádech stovek miliard dolarů ročně. V roce 2014 odhadl McAfee dopady kybernetické kriminality na 400 miliard dolarů, což představuje 0,8% světového HDP (1, s. 2). Agentura Forbes pak v lednu 2016 predikovala, že finanční dopady kybernetického zločinu v roce 2019 dosáhnou celosvětově hodnoty vyšší než 2 biliony dolarů (2).

Spousta společností si nutnost investovat do svého zabezpečení už začíná uvědomovat. Jejich motivace je finanční. Potřebují zabezpečit svá aktiva před dopady kybernetických hrozeb. Ale je tomu tak i ve veřejném sektoru? Pracovníci ve veřejném sektoru nespravují svá aktiva, nejsou přímo finančně zainteresovaní nebo jen velmi málo. A z pohledu konkurenceschopnosti na trhu práce s ICT a bezpečnostními odborníky jsou na tom velmi špatně. Co tedy přiměje orgány veřejné moci k tomu, aby efektivně zabezpečily své informační systémy a ICT infrastrukturu? Je to legislativa. Vláda ČR si už nějakou dobu uvědomuje rostoucí rizika hrozící z kyberprostoru i slabou ochotu veřejné správy zabezpečit svá aktiva. V roce 2011 proto přijala usnesení č. 781 o ustavení Národního bezpečnostního úřadu (NBÚ) gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Na základě tohoto usnesení vzniklo Národní centrum kybernetické bezpečnosti (NCKB), tedy centrum pro koordinaci spolupráce v oblasti předcházení i řešení kybernetických útoků a to jak na národní, tak na mezinárodní úrovni. Prvním zásadním úkolem NBÚ vyplývajícím z vládního usnesení bylo vypracování zákona o kybernetické bezpečnosti, ten byl vydán v srpnu 2014 a je účinný od 1. ledna 2015 (3, s. 1936).

Zákon o kybernetické bezpečnosti vynucuje po subjektech spravujících informační nebo komunikační systémy kritické informační infrastruktury a významné informační systémy, aby tyto svá aktiva patřičně zabezpečily. Většinou jde právě o systémy spravované veřejným sektorem, ale týká se to i vybraných důležitých soukromoprávních subjektů. Ostatně spolupráci veřejného a soukromého sektoru vidí NBÚ ve své Národní strategii jako zásadní pro správný vývoj kybernetické bezpečnosti v ČR (4, s. 8).

Ač je Zákon o kybernetické bezpečnosti novým předpisem v legislativě ČR, technicky do oblasti zabezpečení nepřináší v zásadě nic nového. V podstatě jde o převzaté principy z norem ISO/IEC 27000. Kromě organizačních opatření reprezentovaných především nutností zavést systém řízení bezpečnosti informací (známější pod anglickou zkratkou ISMS - Information Security Management System), zavádí také technická opatření. Kromě těch, které už jsou ve společnostech vesměs dobře rozšířené, tedy opatření fyzické bezpečnosti, ochrana perimetru nebo antimalwarová řešení, klade důraz také na monitorování vnitřního síťového prostředí a nástroj pro detekci a vyhodnocování kybernetických bezpečnostních událostí.

2 Cíl práce a metodika

2.1 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 náležitosti bezpečnostní politiky, návrh metodiky identifikace aktiv a řízení rizik a postup řízení bezpečnostních incidentů, včetně praktické ukázky použití nástrojů pro jejich detekci.

2.2 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, návrh 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 a následnou analýzou zkoumané události.

3 Teoretická východiska

3.1 Zákon o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti byl vydán 23. července 2014 s účinností od 1. ledna 2015. Důvody vypracování zákona popisuje NBÚ ve věcném záměru zákona. Jde především o potřebu adekvátně reagovat na výrazný nárůst používání informačních technologií, který s sebou kromě výhod nese také zvýšená rizika jejich zneužívání k nekalým činnostem a kybernetickému zločinu.

Zákon má za úkol sjednotit už existující partikulární řešení v oblasti kybernetické bezpečnosti jak ve veřejné, tak v soukromé sféře, a zajistit tak centrální institucionální zajištění kybernetické bezpečnosti prostřednictvím orgánu veřejné moci.

„*Smyslem a účelem zákona je ochrana českého kyberprostoru tak, aby bylo možno zajistit subjektům pod jurisdikcí České republiky odpovídající nástroje a standardy pro řešení kybernetické bezpečnosti jejich informačních systémů a elektronických komunikací a nerušený výkon jejich práva na informační sebeurčení.“* (5, s. 57)

Dosáhnout těchto cílů má pomocí tří pilířů, na kterých je postaven:

a) Povinnost ohlášení kontaktních údajů a povinnost hlásit kybernetické bezpečnostní události.
b) Nutnost aplikace bezpečnostních opatření pro subjekty kritické informační infrastruktury a kritické komunikační infrastruktury.
c) Systém protiopatření pro řešení kybernetické ochrany.

O sběr a vyhodnocování hlášení kybernetických bezpečnostních událostí a následné vymýšlení patřičných bezpečnostních opatření a protiopatření se starají dvě dohledová pracoviště - vládní CERT/CSIRT[2] a národní CERT/CSIRT. Pracoviště vládního CERT/CSIRT je součástí Národního centra kybernetické bezpečnosti a má v kompetenci

[2] CERT/CSIRT je expertní skupina, která řeší kybernetické bezpečnostní incidenty. Zkratky jsou z anglických názvů Computer Emergency Response Team a Computer Security Incident Response Team.

především „péči“ o veřejnoprávní subjekty. Národní CERT/CSIRT je pracoviště provozované zpravidla soukromoprávním subjektem na základě veřejnoprávní smlouvy (v současné době tuto roli zastává sdružení CZ.NIC), v jeho kompetenci jsou zase zejména soukromoprávní subjekty, akademická sféra, oblast samosprávy a neziskový sektor, pokud tyto subjekty nepodléhají přímo působnosti NBÚ.

Úkolem ZKB je ochrana práva na informační sebeurčení (tj. zejm. práva na ochranu soukromí, soukromého života, na svobodu projevu, na přístup k informacím a dalších informačních práv člověka), bezpečnosti a integrity České republiky a mezinárodních závazků České republiky.

U soukromoprávních subjektů, poskytujících služby elektronických komunikací vesměs není problém v zajištění odpovídající úrovně kybernetické bezpečnosti. Jejich motivace je totiž ekonomická, protože zajištění bezpečnosti je podmínkou fungující síťové infrastruktury. Větší problém je spíše u veřejnoprávních subjektů, které spravují informační nebo komunikační systémy pro stát kritické informační infrastruktury[3] (KII) nebo významné informační systémy[4] (VIS). Zde je často ochrana zanedbána ať už úmyslně nebo z neznalosti, či neschopnosti subjektu nastavit adekvátní bezpečnostní opatření. A právě u těchto subjektů je nutné zajistit adekvátní zabezpečení formou zákonných povinností prostřednictvím zákona o kybernetické bezpečnosti.

ZKB mimo jiné nařizuje orgánům a osobám, které spravují informační nebo komunikační systém kritické informační infrastruktury nebo významný informační systém, aby v nezbytném rozsahu zavedly a prováděly bezpečnostní opatření. Tato opatření pak dělí na opatření organizační a technická. Zákon tato opatření vyjmenovává, ale jejich obsah a rozsah stanovuje vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti (dále také VKB

[3] Kritickou infrastrukturou je *„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“* (30, s. 5602). Prvky kritické infrastruktury jsou určeny č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

[4] Významným informačním systémem je *„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“* (3, s. 1926). Významné informační systémy jsou určené vyhláškou č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.

nebo Vyhláška) (6). Dále ukládá povinnost těmto orgánům a osobám detekovat kybernetické bezpečnostní události a hlásit kybernetické bezpečnostní incidenty národnímu CERTu nebo NBÚ, podle typu subjektu. Náležitosti tohoto hlášení opět řeší VKB. Zákon dále stanovuje kdo a za jakých podmínek musí zavádět reaktivní a ochranná opatření vydaná NBÚ na základě reakce na kybernetický bezpečnostní incident nebo jeho hrozbu.

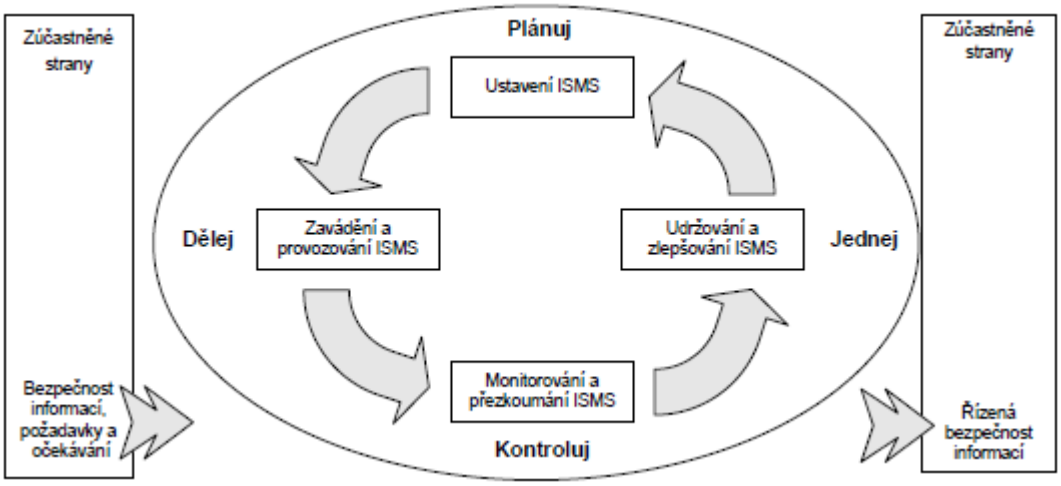
3.1.1 Organizační opatření ZKB

Zákon o kybernetické bezpečnosti vyjmenovává následující organizační bezpečnostní opatření, jejichž obsah detailněji specifikuje prováděcí předpis v podobě Vyhlášky o kybernetické bezpečnosti.

3.1.1.1 Systém řízení bezpečnosti informací

Zákon požaduje především to, aby subjekty zavedly a používaly řízení rizik, vytvořily bezpečnostní politiku a prováděly pravidelné hodnocení aktiv, rizik, bezpečnostní politiky, plánu zvládání rizik a plánu rozvoje bezpečnostního povědomí.

Subjekty spravující informační nebo komunikační systém KII pak mají systém řízení bezpečnosti informací zpřísněný především tím, že musí minimálně jedenkrát za rok provést audit kybernetické bezpečnosti. Musí také formálněji monitorovat a vyhodnocovat účinnost bezpečnostních opatření a vhodnost a účinnost bezpečnostní politiky a systému řízení bezpečnosti informací samotného. Jde zde v podstatě o převzetí známého principu Demingova cyklu (Plan, Do, Control, Act,) z ISO 27001.



Obrázek 1 - PDCA model aplikovaný na procesy ISMS (7, s. 7)

3.1.1.2 Řízení rizik

Toto opatření specifikuje požadavky pro řízení rizik, požadovaného v rámci zavedení systému řízení bezpečnosti informací (nebo také ISMS).

VKB zde říká, že subjekty mají mít pro své informační nebo komunikační systémy v režimu ZKB stanovenu metodiku pro identifikaci a hodnocení aktiv a rizik. Na základě těchto metodik pak mají identifikovat a ohodnotit důležitost aktiv[5] (pro VIS pouze primárních, pro KII také podpůrných aktiv) a identifikovat rizika[6], včetně zohlednění hrozby a zranitelnosti a posouzení možného dopadu na aktiva (pro VIS opět stačí posuzovat rizika pouze pro primární aktiva). Hodnotit musí také reaktivní a ochranná opatření vydaná NBÚ. Subjekty mají dále na základě výsledků analýzy rizik zpracovat prohlášení o aplikovatelnosti vybraných a zavedených bezpečnostních opatření a zavést plán zvládání rizik obsahujících cíle a přínosy těchto opatření spolu s určením zodpovědnosti a potřebných zdrojů.

3.1.1.3 Bezpečnostní politika

VKB specifikuje oblasti, které má pokrývat bezpečnostní politika. Počet oblastí se opět liší dle významnosti systému, které subjekt spravuje. Bezpečnostní politika pro subjekty spravující významné informační systémy má pokrývat 14 oblastí, zatímco pro systémy kritické informační infrastruktury je těchto oblastí 21. Tyto oblasti jsou vypsané v §5 Vyhlášky o kybernetické bezpečnosti. Vyhláška také subjektům dává za úkol bezpečnostní politiku pravidelně hodnotit a aktualizovat.

3.1.1.4 Organizační bezpečnost

Zajištění organizační bezpečnosti spočívá v zavedení organizace řízení bezpečnosti informací. Vrcholným orgánem je výbor pro řízení kybernetické bezpečnosti. Dále jsou

[5] Minimální rozsah hodnocení aktiv a úrovně jejich důležitosti je stanoven Přílohou č. 1 Vyhlášky o kybernetické bezpečnosti v podobě přehledných tabulek se stupnicemi hodnocení důvěrnosti, integrity a dostupnosti aktiv (6, s. 3988).

[6] Minimální rozsah hodnocení rizik je stanoven Přílohou č. 2 Vyhlášky o kybernetické bezpečnosti v podobě tabulek s hodnocením dopadů, hrozeb, zranitelností a celkového hodnocení rizika (6, s. 3990).

určeny bezpečnostní role a jsou popsány jejich práva a povinnosti vztahující se k systémům VIS a KII.

Vyhláška o kybernetické bezpečnosti stanovuje následující role:

- *manažer kybernetické bezpečnosti*
  Odpovědný za systém řízení bezpečnosti informací.

- *architekt kybernetické bezpečnosti*
  Zajišťuje návrh a implementaci bezpečnostních opatření.

- *auditor kybernetické bezpečnosti*
  Provádí audit kybernetické bezpečnosti na VIS a systémech KII.

- *garant aktiva*
  Subjektem pověřen k zajištění rozvoje, použití a bezpečnosti daného aktiva.

Manažer, architekt a auditor kybernetické bezpečnosti musí mít prokazatelnou minimálně tříletou odbornou způsobilost ve své oblasti. Role auditora musí být navíc oddělena od výkonu ostatních tří definovaných rolí. Osoby vykonávající tyto role musí být pravidelně školeny ve svých oblastech. Rozsah a přesné zaměření nejsou ve Vyhlášce specifikovány.

3.1.1.5 Stanovení bezpečnostních požadavků pro dodavatele

Toto bezpečnostní opatření subjekt zavazuje k tomu, aby zohledňoval potřeby ISMS i při jednání s dodavateli a s třetími stranami, které se nějak podílejí na rozvoji nebo fungování VIS a systémů KII. Rozsah zapojení těchto dodavatelů musí být stanoven smlouvou, jejíž součástí je ustanovení o bezpečnosti informací, často obsahující také prohlášení o mlčenlivosti[7].

[7] Prohlášení o mlčenlivosti, často označované zkratkou NDA (z anglického Non-Disclosure Agreement je dohoda dvou subjektů o omezení předávání některých informací třetím stranám. V praxi jde nejčastěji o důvěrné informace, know-how nebo obchodní tajemství apod.

V případě systému KII musí být také smluvně stanovena úroveň služeb (často se označuje SLA z anglického výrazu Service-Level Agreement). Dále musí být prováděno hodnocení rizik vždy před uzavřením smlouvy spojené s podstatnými dodávkami a také pravidelné hodnocení rizik u poskytovaných služeb.

3.1.1.6 Řízení aktiv

V rámci řízení aktiv musí být identifikována primární aktiva (pro KII také podpůrná aktiva a jejich vazby s primárními aktivy), ohodnocena jejich důležitost a musí být určeni garanti, kteří jsou za ně zodpovědní. Dále musí být stanovena pravidla ochrany a přípustné způsoby používání aktiv, včetně způsobů spolehlivého mazání nebo ničení technických nosičů.

I když se to tak nemusí na první pohled jevit, identifikace aktiv je velmi důležitou činností, na které pak závisí další kroky nutné po správné fungování ISMS. Z identifikace aktiv přímo vychází analýza rizik a ta je dále klíčová pro návrh a posuzování bezpečnostních opatření.

3.1.1.7 bezpečnost lidských zdrojů

S ohledem na bezpečnost lidských zdrojů musí být stanoven plán rozvoje bezpečnostního povědomí. Speciální pozornost musí být věnována především osobám v bezpečnostních rolích a osobám s privilegovanými účty. Kompromitace a případné následné zneužití těchto účtů totiž muže napáchat největší škodu. Osoby v bezpečnostních rolích navíc často vystupují také v rolích mentorů nebo metodických rádců ostatním zaměstnancům a definují bezpečnostní politiky a jiné řídicí dokumenty, jejich dobré vzdělání a dostatečný přehled v bezpečnostní problematice je tedy nutností.

Zásadní je též zajištění dodržování bezpečnostní politiky všemi uživateli. Musí být také zajištěno to, že uživatelé při ukončení svého smluvního vztahu vrátí svěřená aktiva.

3.1.1.8 Řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému

Toto bezpečnostní opatření spočívá v nutnosti detekovat a pravidelně vyhodnocovat kybernetické bezpečnostní události pomocí technických prostředků specifikovaných ve VKB mezi technickými opatřeními. Konkrétně jde o „Nástroj pro zaznamenávání činnosti“

systémů a jejich uživatelů, tedy o logování, ideálně pomocí nějakého log-manageru[8]. Dále jde o „Nástroj pro detekci kybernetických bezpečnostních událostí“, tedy o nějakou logiku pro rozpoznávání potenciálních bezpečnostních problémů. Takových nástrojů může být několik druhů podle toho v jaké části infrastruktury a jakým způsobem jsou použity. Toto téma bude detailněji popsáno u příslušného technického opatření níže. Posledním prostředkem, který v této souvislosti VKB zmiňuje, je „Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí“. Toto technické opatření cílí na systém typu SIEM[9]. I když samozřejmě ono „vyhodnocení“ bezpečnostní události padá v konečném důsledku spíš na obsluhu systému SIEM, než na technický prostředek samotný.

Do tohoto bezpečnostního opatření patří také provádění pravidelných záloh a prověřování jejich použitelnosti, tedy zkušební obnovování dat ze záloh.

Přísnější pravidla jsou i zde vyžadována pro systémy KII. U nich je nutné zajistit oddělení vývojového, testovacího a produkčního prostředí, řešit reaktivní opatření vydané NBÚ, i důkladně zabezpečit data při přenosu, a to jak technickými opatřeními spočívajícími v zajištění bezpečnosti a integrity příslušných komunikačních sítí, tak i organizačně, určením pravidel a postupů pro zajištění ochrany informací, jejich dokumentováním a případně také smluvním zajištěním.

3.1.1.9 Řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému

Řízení přístupů osob spočívá hlavně v zajištění toho, aby měl každý uživatel svůj jednoznačný identifikátor, a aby údaje sloužící uživatelům k autentizaci k informačním a komunikačním systémům byly adekvátně zajištěny před zneužitím neoprávněné osoby. K tomu je dle VKB nutné použít nástroje pro ověřování identity uživatelů a pro řízení jejich přístupových oprávnění. K ověřování uživatelů může docházet přímo v dané aplikaci nebo na technologickém aktivu, ke kterému se hlásí, nebo centrálně vůči službám adresářové struktury či autentizačnímu serveru. Stejně tak řízení přístupových oprávnění

[8] Log-manager je nástroj pro sběr a prohlížení provozních záznamů aplikací, zařízení nebo IS.
[9] SIEM je management bezpečnostních informací a událostí. Jde o zkratku z anglického Security Information and Event Management.

(autorizace) může probíhat na úrovni daného aktiva nebo centrálně. Výhoda v použití centralizovaného způsobu spočívá především ve snadnější a bezpečnější správě účtů. Oprávnění pro jednotlivé účty je totiž možné řídit na jednom místě pro všechna připojená aktiva. Po odchodu zaměstnance z organizace se například deaktivací jeho účtu v centrálním nástroji pro správu identit deaktivují také oprávnění a přístupy do všech aktiv. Není třeba pak procházet jednotlivá aktiva a odebírat oprávnění tam. Čím více existuje v organizaci aktiv s oddělenou správou přístupů a oprávnění, tím větší je riziko opomenutí nastavení na některém z nich.

Pro systémy KII navíc platí, že uživatelský identifikátor musí být samostatný. Nesmí se tedy používat sdílené uživatelské účty. Klade se také zvýšený důraz na omezení přidělování administrátorských oprávnění. Toto opatření cílí na princip nejnižších privilegií, kdy jsou uživatelům (ale i aplikacím nebo procesům) přidělována nejnižší možná oprávnění, která pro svou práci nebo správnou funkci potřebují. Přidělená přístupová oprávnění musí být navíc pravidelně přezkoumávána. I když zákon ani vyhláška v tomto případě nespecifikují jak často.

3.1.1.10 Akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů

Subjekt spravující systém v režimu ZKB, musí stanovit bezpečnostní požadavky na změny tohoto systému spojené s jeho akvizicí, vývojem a údržbou. Pro systémy KII navíc platí, že před jejich změnou musí subjekt provést analýzu rizik dle své stanovené metodiky, musí zajistit bezpečnost vývojového prostředí a používaných testovacích dat a musí provádět testování změn před jejich uvedením do provozu.

Pokud se v systémech zpracovávají osobní údaje podle zákona č. 101/2000 Sb., o ochraně osobních údajů, je nezbytné tato data chránit bez ohledu na to, zda jde o KII nebo nikoli. Případné porušení důvěrnosti osobních údajů neřeší ZKB (nebyl-li při tom porušen), ale právě Zákon o ochraně osobních údajů. Tento aspekt nabývá na důležitosti především proto, že v květnu 2016 vstoupilo v platnost Nařízení Evropské komise na ochranu osobních údajů (označované často svou anglickou zkratkou GDPR). Účinnosti toto nařízení nabývá dne 4.5.2018. Vzhledem k tomu, že jde o nařízení, do národních legislativ je aplikovatelné přímo, předpokládají se také změny Zákona o ochraně osobních údajů.

Tento příklad ukazuje, jak provázané mohou být jednotlivé aspekty bezpečnosti a to, že zanedbáním jednoho z nich je možné porušit i více legislativních předpisů, přičemž postihy pak hrozí od každého takto porušeného předpisu.

3.1.1.11 Zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů

Toto opatření předpokládá v první řadě zajištění oznamování kybernetických bezpečnostních událostí ze strany uživatelů. Tyto oznámené bezpečnostní události, stejně jako bezpečnostní události detekované technickými prostředky, musí být vyhodnocovány a identifikovány mezi nimi kybernetické bezpečnostní incidenty[10].

Identifikované kybernetické bezpečnostní incidenty je nutné dále klasifikovat, musí být provedena opatření, které je odvrátí nebo alespoň okamžitě zmírní jejich dopad. Ve chvíli, kdy je odstraněno bezprostřední riziko, musí být tyto incidenty nahlášeny NBÚ dle definovaného procesu, včetně podkladů pro další analýzu incidentů. Po prošetření příčin a vyřešení bezpečnostního incidentu je nutno vyhodnotit účinnost řešení a stanovit opatření, která zamezí jeho opakování..

3.1.1.12 Řízení kontinuity činností

Vyhláška stanovuje subjektům určit práva a povinnosti zainteresovaných osob a definovat cíle řízení kontinuity a strategii, kterou budou tyto cíle dosaženy. Je třeba stanovit minimální úroveň poskytovaných služeb, doby do obnovení chodu po kybernetickém bezpečnostním incidentu[11] a bod (myšleno stav v určitém čase), do kterého budou data po kybernetickém bezpečnostním incidentu obnovena.[12] Prakticky je lepší v řízení kontinuity činností počítat s jakýmkoli incidentem, nejen bezpečnostním kybernetickým, jak to stanovuje vyhláška.

---

[10] Kybernetický bezpečnostní incident je, taková kybernetická bezpečnostní událost, která způsobila narušení důvěrnosti, integrity nebo bezpečnosti některého sledovaného aktiva. Může tedy existovat mnoho bezpečnostních událostí, ze kterých je následně analýzou zjištěno jen několik málo incidentů.

[11] Doba do obnovení chodu na minimální úroveň poskytovaných služeb je často označuje jako RTO z anglického Recovery Time Objective

[12] Bod, do kterého jsou data po incidentu obnovena, se často označuje jako RPO z anglického Recovery Point Objective.

Pro systémy KII navíc platí, že je třeba na základě posouzení dopadů kybernetických bezpečnostních incidentů posoudit možná rizika pro zajištění kontinuity činností. Dále je u těchto systémů nutné stanovit, aktualizovat a pravidelně testovat plány kontinuity činností a také realizovat bezpečnostní opatření s cílem zvýšení odolnosti daného systému (včetně opatření vydaných NBÚ).

3.1.1.13 Kontrola a audit kritické informační infrastruktury a významných informačních systémů.

Subjekty spravující VIS a systémy KII musí posuzovat soulad stanovených bezpečnostních opatření s legislativou i s interními předpisy. Musí pravidelně kontrolovat zejména dodržování bezpečnostní politiky a výsledky těchto kontrol pak dále zohledňovat v plánech rozvoje bezpečnostního povědomí a zvládání rizik.

U systémů KII je navíc třeba zajistit tento audit osobou s odbornou kvalifikací - tedy auditorem kybernetické bezpečnosti. Tento auditor často bývá externí, ale může se jednat i o interní audit, ovšem nesmí ho provádět osoba, která zastává některou z ostatních tří bezpečnostních rolí definovaných vyhláškou (Manažer kybernetické bezpečnosti, Architekt kybernetické bezpečnostní nebo Garant aktiva). U systémů KII je dále potřeba provádět analýzu zranitelností pomocí automatizovaných nástrojů[13] a adekvátně reagovat na nalezené zranitelnosti.

3.1.2 Technická opatření ZKB

Zákon o kybernetické bezpečnosti vyjmenovává následující technická bezpečnostní opatření, jejichž obsah detailněji specifikuje prováděcí předpis v podobě Vyhlášky o kybernetické bezpečnosti.

3.1.2.1 Fyzická bezpečnost

Subjekty spravující VIS nebo systémy KII musí zajistit adekvátní fyzická zabezpečení vyhrazených prostor, kde jsou umístěna technická aktiva a uchovávány a zpracovávány informace.

[13] Tyto automatizované nástroje se označují jako vulnerability scannery.

Pro systémy KII jsou tato opatření opět přísnější. Vyhláška v tomto případě vyjmenovává zejména prostředky pro zabránění a detekci neoprávněného přístupu do vymezených prostor (mechanické zábranné prostředky, EZS[14], kamerové systémy a systémy pro kontrolu vstupu) a prostředky proti poruchám a živelným událostem (např. EPS[15], UPS[16] apod.). V kontextu ZKB jsou vymezenými prostorami myšleny především servrovny obsahující technická aktiva systémů v režimu kybernetického zákona a místa, kde se zpracovávají data těchto systémů, tedy často například kanceláře nebo režimová pracoviště.

3.1.2.2 Nástroj pro ochranu integrity komunikačních sítí

Toto bezpečnostní opatření spočívá v zavedení bezpečného řízení mezi vnitřní (pod správou subjektu) a vnější sítí. Typicky jde o sítě typu WAN, jde-li o vnější síť, a LAN, jedná-li se o vnitřní síť. Cílem je zabezpečit integritu komunikačních sítí. Toto opatření cílí především na standardní metody ochrany perimetru typu Firewallů, IDS/IPS systémů[17], dále na návrh architektury síťového prostředí s vytvořenou DMZ[18] a v případě systému KII na segmentaci sítí vytvořením nezávislých VLAN[19].

Firewall je nejrozšířenějším bezpečnostním prvkem pro ochranu perimetru. Existuje několik druhů firewallů z hlediska funkcionality. Nejstarší a nejjednodušší typ pracuje jako paketový filtr, kontroluje síťový provoz na 3. a 4. síťové vrstvě RM ISO/OSI[20] a podle

---

[14] ESZ je zkratkou pro Elektronickou Zabezpečovací Signalizaci a jde o systém, který je určen k detekci vstupu neoprávněnou osobou do hlídaného prostoru.

[15] EPS je zkratkou pro Elektronickou Požární Signalizaci, tedy o systém určený k včasnému hlášení a signalizaci požáru v objektu.

[16] UPS je zkratkou z anglického Uninterruptible Power Supply, jedná se tedy o zdroj nepřerušovaného napájení. Umožňuje připojeným zařízením pracovat i poté, co v objektu dojde k poruše primárního zdroje elektrické energie.

[17] IDS/IPS systémy jsou kybernetické obranné systémy, které monitorují síťový provoz a hledají podezřelé aktivity. Zatímco IDS takové aktivity pouze detekuje, IPS je dokáže i blokovat.

[18] DMZ je zkratka pro tzv. Demilitarizovanou zónu, tedy fyzickou nebo logickou oblast sítě na rozhraní mezi vnější sítí a vnitřní LAN. V této oblasti jsou většinou vystaveny webové služby společnosti, které mají být viditelné z Internetu.

[19] VLAN je zkratka pro virtuální LAN neboli virtuální lokální síť. Jde o logické členění vnitřní sítě nezávisle na fyzickém síťovém uspořádání.

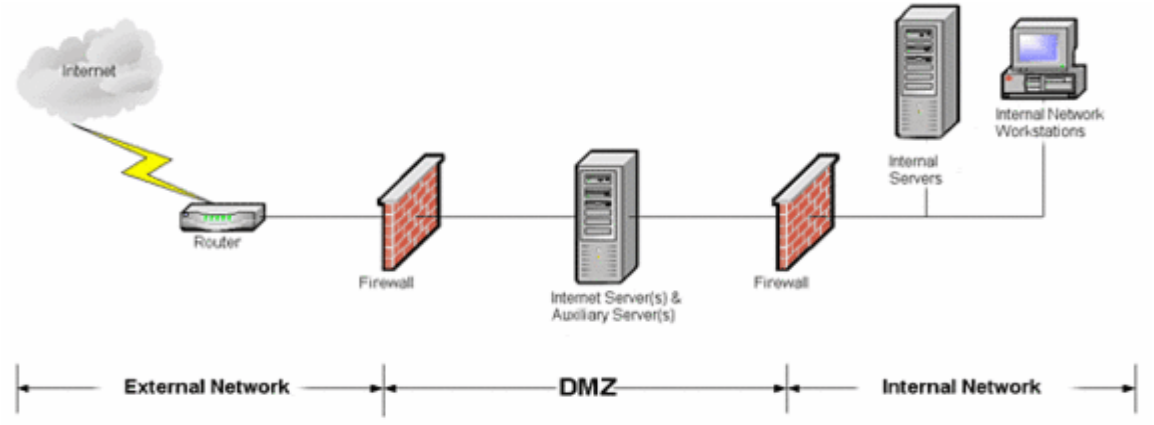
[20] RM ISO/OSI je referenční model reprezentuje příklad řešení komunikace počítačových sítí za použití sedmi vrstev, které spolu vzájemně interagují (vždy jen vzájemně sousedící vrstvy) (28). Jde o nejčastěji používaný model dekompozice síťové komunikace.

přednastavených pravidel rozhoduje o tom, zda má být daný paket propuštěn nebo zablokován. Dalším typem jsou pak stavové firewally, které pracují na stejném principu jako paketové filtry, jen si navíc uchovávají informaci o tom, že je dané spojení povolené. Jednak to šetří režii tím, že nemusí každý paket procházet rozhodovacím procesem, za druhé to umožňuje povolit komunikaci jen jedním směrem a stavový firewall rozezná odpovědi pro danou povolenou komunikaci a ty propustí, aniž by bylo potřeba povolit celou komunikaci tímto opačným směrem.

Novějším typem jsou pak aplikační firewally, které umí rozhodovat i podle aplikační (7. vrstvy RM ISO/OSI). To otevírá nové možnosti kontroly síťového provozu, protože je tímto způsobem možné zachytit i hrozby, které se šíří po běžně používaných portech služeb a protokolů, které prostě musí být firewallem propouštěny (například HTTP).

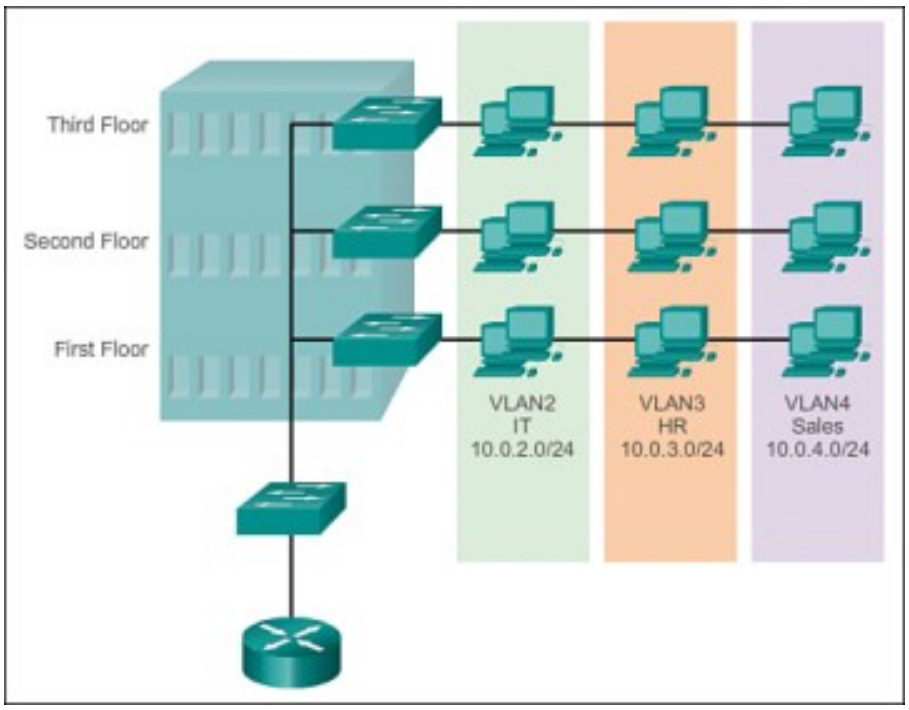
Speciálním typem jsou tzv. next-generation firewally, které kromě klasického firewallu integrují i další bezpečnostní prvky jakými jsou aplikační firewall, IPS nebo například nástroj pro hloubkovou paketovou inspekci.

Firewally od sebe typicky oddělují dvě sítě s různou mírou důvěryhodnosti. Nejčastější architektura počítá s tím, že perimetr organizace je oddělen firewallem od vnější sítě. Dále je ale většinou potřeba mít určité servery vystavené do vnější sítě, nejčastěji webservery. Ostatní servery a zbytek vnitřních zařízení tvořících interní síť je naopak potřeba co nejlépe před vnějším nebezpečným světem chránit, proto se oddělují od těch z vnějšku dostupných další vrstvou firewallů. Tato zóna mezi dvěma firewally organizace se nazývá DMZ, neboli demilitarizovaná zóna.



Obrázek 2 - Typický návrh DMZ (8)

Dalším bezpečnostním prvkem implementovaným ve vnitřních sítích jsou virtuální sítě označované jako VLAN. Jejich úkolem je dále rozdělit vnitřní síť z důvodu jednodušší správy, snížení provozních nákladů i zvýšení zabezpečení. Rozdělení vnitřní sítě do VLAN totiž umožňuje v případě změn na síti lokalizovat potřebné úpravy jen na část sítě, sníží se také množství všesměrového vysílání na síti a logicky se oddělí síťové prostředky, ke kterým je pak možné nastavit přístup jen určité skupině uživatelů nebo zařízení.



Obrázek 3 - Příklad rozdělení místní sítě do VLAN (9)

3.1.2.3 Nástroj pro ověřování identity uživatelů

U informačních a komunikačních systémů v režimu ZKB musí být zajištěno ověřováni identity přihlašovaných uživatelů. Jinými slovy, uživatelé se musí před zahájením práce v IS autentizovat. Nejčastějším způsobem autentizace je v současné době ověření na základě jména a hesla. V takovém případě Vyhláška stanovuje minimální požadavky na komplexnost hesla.

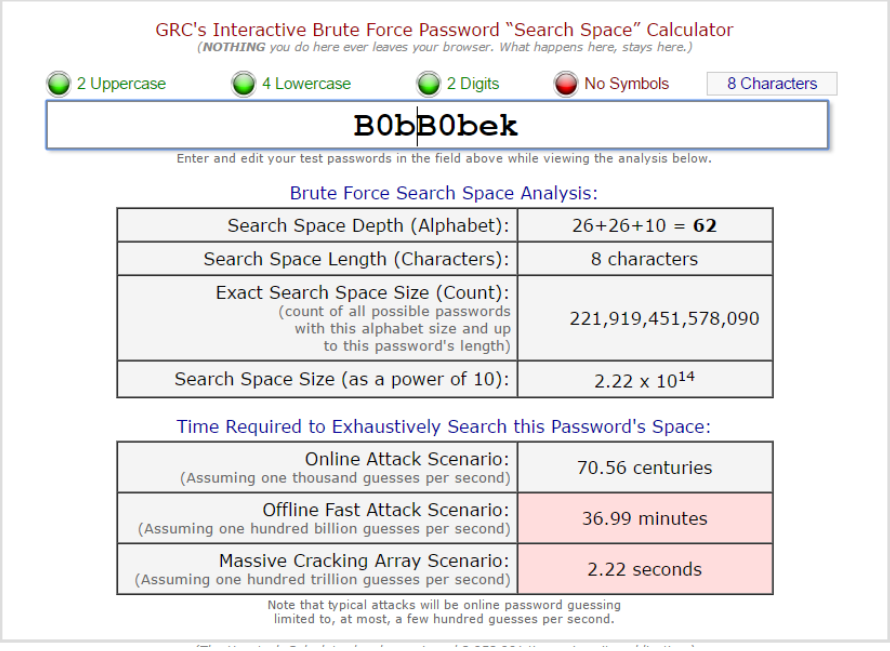
Heslo musí být alespoň 8 znaků dlouhé (u administrátorských účtů v systémech KII alespoň 15 znaků dlouhé) a musí obsahovat minimálně 3 z těchto 4 skupin znaků:

- malá písmena,
- velká písmena,

- číslice,
- speciální znaky.

Heslo navíc nesmí být starší než 100 dnů. U systémů KII navíc musí být zajištěna i podmínka neopakovatelnosti hesla, které měl uživatel už v minulosti (chybí zde však určení počtu již použitých hesel, které nesmí být použity) a minimální stáří hesla 24 hodin kvůli zamezení možnosti, aby si uživatel změnil během jednoho dne heslo tolikrát, aby vyčerpal zásobník zapamatovaných starších hesel a mohl si tak nastavit opět heslo původní.

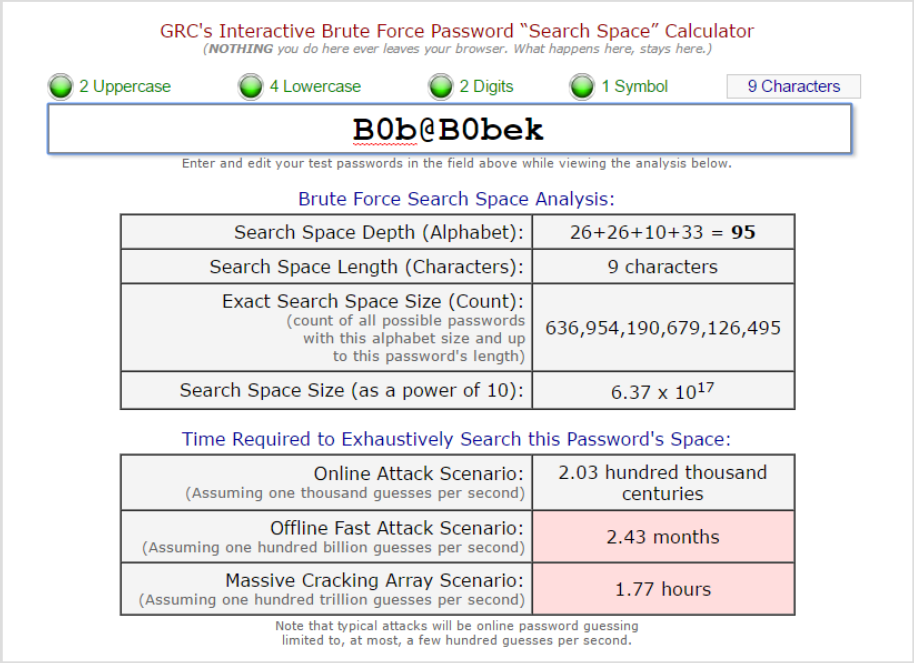
Autentizace pomocí hesla je v dnešní době čím dál kontroverznější téma a projevuje se to i v tomto paragrafu vyhlášky. Na jednu stranu je zbytečně mírná, když požaduje jen 8 znaků dlouhá hesla. Tedy standard, který byl účinný zhruba před deseti lety. V dnešní době je výpočetní výkon na takové úrovni, že osmiznakové komplexní heslo, které splňuje požadavky ZKB lze na běžně dostupných strojích hrubou silou odhalit v řádu minut nebo desítek minut.



Obrázek 4 - Parametry 8-znakého komplexního hesla 3/4 (10)

Přitom přidáním jediného znaku navíc a použitím všech 4 skupin znaků lze zvýšit počet možných kombinací o 3 řády a dobu lámání hesla na jednotky měsíců (viz obrázek č. 3) a přidáním desátého znaku pak na desítky let (viz obrázek č. 4).

Předpokladem takového útoku hrubou silou je možnost ho provádět offline. Útoky na online systém umožní hádat jen stovky až tisíce hesel za sekundu a je to možné technologicky omezit ještě více. Při takové rychlosti je dostatečně bezpečné i heslo o délce 8 znaků (z pohledu útoku hrubou silou). V případě útoků na heslo přes online systém se tedy brute force útoky nepoužívají. Místo nich se využívají spíše slovníkové útoky.



GRC's Interactive Brute Force Password "Search Space" Calculator

(*NOTHING* you do here ever leaves your browser. What happens here, stays here.)

2 Uppercase | 4 Lowercase | 2 Digits | 1 Symbol | 9 Characters

B0b@B0bek

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

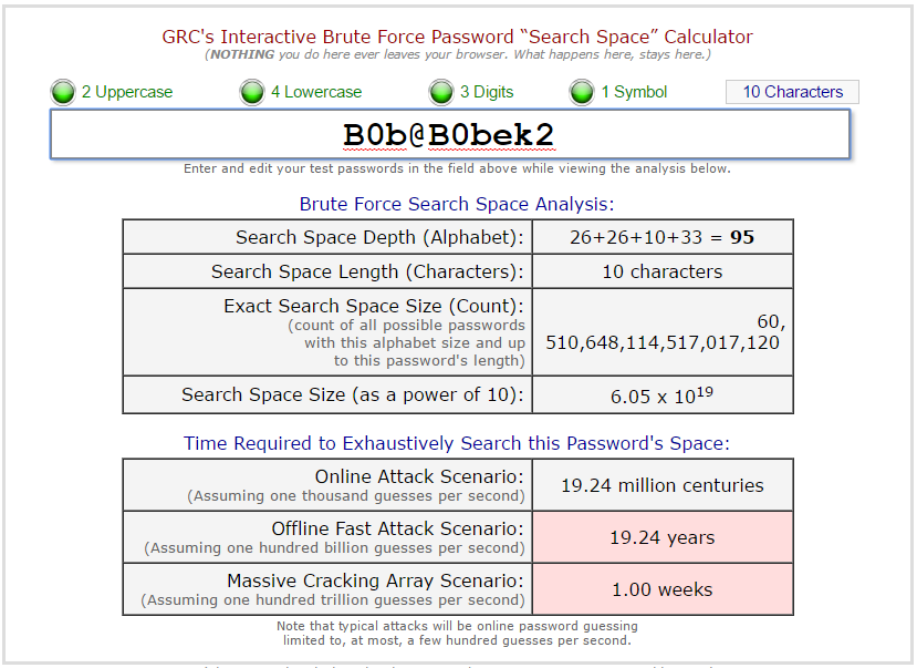
Search Space Depth (Alphabet):	26+26+10+33 = **95**
Search Space Length (Characters):	9 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	636,954,190,679,126,495
Search Space Size (as a power of 10):	6.37×10^{17}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	2.03 hundred thousand centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	2.43 months
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	1.77 hours

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

Obrázek 5 - Parametry 9-znakého komplexního hesla 4/4 (10)



GRC's Interactive Brute Force Password "Search Space" Calculator

(*NOTHING* you do here ever leaves your browser. What happens here, stays here.)

2 Uppercase | 4 Lowercase | 3 Digits | 1 Symbol | 10 Characters

B0b@B0bek2

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+10+33 = **95**
Search Space Length (Characters):	10 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	60, 510,648,114,517,017,120
Search Space Size (as a power of 10):	6.05×10^{19}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	19.24 million centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	19.24 years
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	1.00 weeks

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

Obrázek 6 - Parametry 10-znakého komplexního hesla 4/4 (10)

Na druhou stranu jsou pravidla aplikovaná Vyhláškou na hesla zbytečně přísná, když vyžadují měnit heslo 3-4 krát do roka (heslo se musí měnit alespoň jednou za 100 dnů). Toto pravidlo považuji z bezpečnostního hlediska spíše za kontraproduktivní. Nutně s sebou přináší zanesení pravidelnosti do vymýšlených uživatelských hesel. Uživatelé pak vymýšlí hesla typu „Heslo001“, po 100 dnech ho změní na „Heslo002“, a tak dále. Taková hesla sice splňují pravidla, které stanovuje Vyhláška, ale o bezpečných heslech se nedá hovořit ani náhodou.

Přitom jak ukázaly obrázky s odhadem doby potřebné k úspěšnému útoku na heslo hrubou silou, vyžadované osmiznakové heslo si nemůže dělat ambice na to, aby odolalo deklarovaných 100 dnů, pokud bude mít útočník možnost na něj útočit offline. A pokud jde o online útoky, tam i osmiznakové heslo odolá útoku hrubou silou i staletí. Měnit hesla každých 100 dnů je z bezpečnostního hlediska zbytečné. Mnohem bezpečnějším řešením by bylo požadovat desetiznakové heslo a měnit ho například jednou za 2 roky.

Výjimku v tomto ohledu mají aplikační účty, kterých se nutnost pravidelné změny hesel netýká. Což je dle mého názoru celkem rozumné rozhodnutí. Předpokladem je ovšem heslo s dostatečnou entropií.

Vyhláška také počítá s jinými typy autentizace. Povoluje jiné způsoby autentizace, pokud budou alespoň stejně bezpečné nebo bezpečnější než ty vyžadované. Toto ustanovení cílí především na metody vícefaktorové autentizace.

3.1.2.4 Nástroj pro řízení přístupových oprávnění

Toto opatření spočívá v používání nástroje, který definovaným způsobem řeší autorizaci, tedy řídí přístupy k aplikacím a datům, alespoň na úrovni odlišení práv pro čtení, zápis a změnu oprávnění. U KII navíc musí zaznamenávat použití přístupových oprávnění.

V praxi je tohoto dosaženo nikoli jedním nástrojem, ale sadou různých nástrojů na různých úrovních. Na vyšší úrovni abstrakce se může jednat o identity management nástroj, který může řídit oprávnění různých aplikací z jednoho místa, ale je třeba, aby fakticky tato oprávnění dále nastavovaly systémy na nižší úrovni. Například na úrovni operačního systému (OS) jsou těmito nástroji přímo nástroje daného OS a závisí také na

použitém typu filesystemu. Například OS Microsoft Windows u svých operačních systémů na filesystemu NTFS (u filesystemů typu FAT není možné řídit oprávnění na soubory a složky) umožňuje oprávnění nastavovat pomocí předdefinovaných tzv. „sad zvláštních oprávnění NTFS“. Vyhláškou požadovaná oprávnění obsahují tyto sady oprávnění (11):

Číst

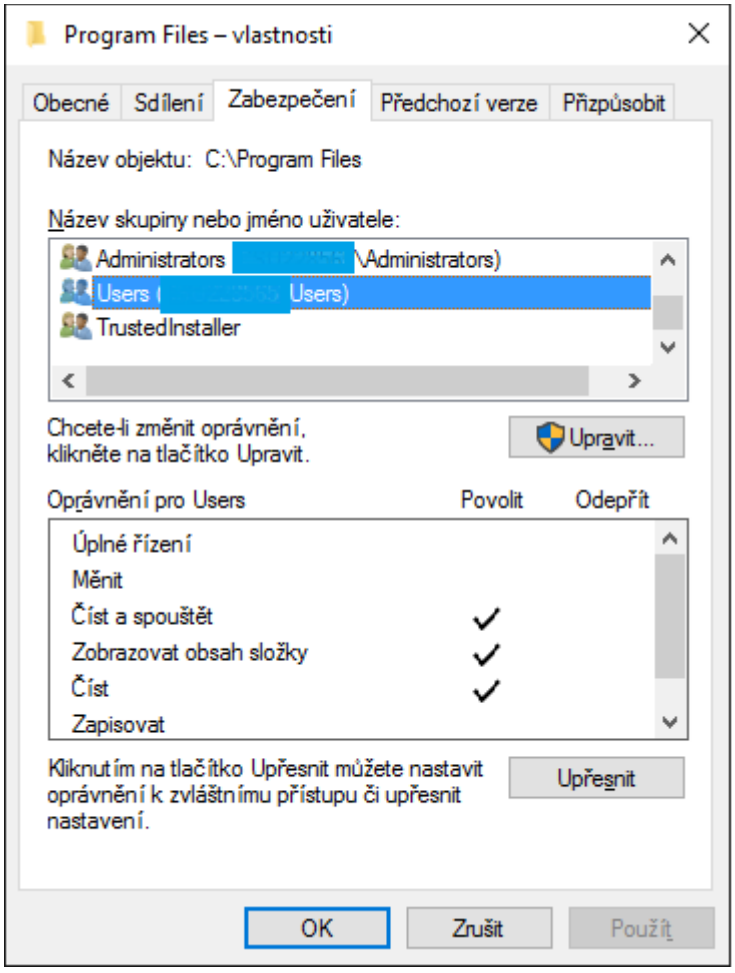
- zahrnující ve výchozím nastavení následující oprávnění
    - Zobrazovat obsah složky / Číst data
    - Číst atributy
    - Číst rozšířené atributy
    - Číst oprávnění
    - Synchronizovat

Zapisovat

- zahrnující ve výchozím nastavení následující oprávnění
    - Vytvářet soubory / Zapisovat data
    - Vytvářet složky / Připojovat data
    - Zapisovat atributy
    - Zapisovat rozšířené atributy
    - Číst oprávnění
    - Synchronizovat

Úplné řízení

- zahrnující ve výchozím nastavení kromě všech výše zmíněných ještě následující oprávnění
    - Procházet složkou / Spouštět soubory
    - Odstraňovat podsložky a soubory
    - Odstraňovat
    - **Měnit oprávnění** (tedy ono vyhláškou požadované oprávnění pro změnu oprávnění)
    - Přebírat vlastnictví



Obrázek 7 - Karta "Zabezpečení" OS Windows - zobrazuje sady přidělených oprávnění (vlastní zpracování)

Pokud je třeba nastavit oprávnění s větší granularitou než pomocí předdefinovaných sad oprávnění, je to možné pomocí rozšířených oprávnění.

Unixové/Linuxové OS, dodržují standard POSIX. V těchto OS je možné nastavit pouze oprávnění pro „Čtení“ (r), „Zápis/Vytváření souborů“ (w) a „Spuštění/Otevření“ (x) a to pro vlastníka daného objektu, pro skupinu tohoto vlastníka a pro všechny ostatní. Změna oprávnění se pak provádí příkazem chmod a provést ji může jedině vlastník daného objektu nebo správce systému (root). Majitele a skupinu pak může za standardních podmínek měnit pouze root, příkazem chown.

Další úrovní, kde je třeba řešit autorizaci, je datová vrstva. V databázích se většinou rozlišují systémová a objektová oprávnění. Nejdřív je potřeba, aby vytvořenému uživatelskému účtu byla přidělena systémová oprávnění, jako jsou například možnost přihlásit se do databáze nebo vytvářet/spravovat databázová schémata a role. Objektová

oprávnění se pak týkají především dat. V relačních, případně objektově-relačních databázích postavených nad dotazovacím jazykem SQL se oprávnění se přidělují klíčovým slovem GRANT, odebírají pak klíčovým slovem REVOKE. Ekvivalentem oprávnění pro čtení je v databázích právo SELECT, pro zápis pak UPDATE. I zde obecně platí, že modifikovat oprávnění může pouze k tomu oprávněný účet (schema), a to buď vlastník daného objektu, nebo účet s explicitně přidělenými příslušnými oprávněními.

Důležitou úrovní řízení autorizace je aplikační vrstva. Zde je situace velmi rozmanitá. V zásadě záleží na každé aplikaci, jakým způsobem (a jestli) řídí uživatelské oprávnění. Především u aplikací vytvořených na zakázku je důležité ohlídat, že bude splňovat podmínky VKB a bude řídit přístup k jednotlivým zdrojům minimálně v požadovaném rozsahu – čtení, zápis, změna oprávnění.

Řízení přístupů ale probíhá i na jiných částech informačních systémů nebo infrastruktury. Například firewally také řídí přístupy k informačním aktivům. Zde už to není na úrovni uživatelských účtů (pokud neuvažujeme operační systémy samotných zařízení), ale například na úrovni IP adres, pokud uvažujeme filtraci na 3. vrstvě referenčního modelu ISO/OSI. Zde už ale neodlišujeme oprávnění pro čtení vs. oprávnění pro zápis, nýbrž propuštění vs. nepropuštění komunikace.

3.1.2.5 Nástroj pro ochranu před škodlivým kódem

Toto opatření Vyhlášky spočívá v zavedení a provozu nástroje, který ochrání Informační systém v režimu ZKB před malware, a to jak na úrovni samotných serverů a sdílených datových úložišť, tak na úrovni síťové komunikace a na úrovni klientských stanic, které přistupují k danému IS nebo k infrastruktuře, na které tento IS běží.

Pod tímto stručným paragrafem VKB se skrývá poměrně široké portfolio nástrojů, které připadají v úvahu. U koncových stanic jde o endpoint antimalware řešení. Od řádově desítek koncových pracovních stanic je vhodné, aby antimalware řešení bylo centrálně spravované. Už dávno nejde jen o „čistokrevný“ antivirový nástroj, který pracuje jen na bázi kontroly vzorků s virovými definicemi. Tento přístup je v dnešní době velmi neefektivní a rozhodně nedostatečný. Naráží především na to, že jde o reaktivní způsob ochrany. K tomu, aby takový nástroj odhalil škodlivý kód, je nutné, aby se jednalo o známý a neupravený kód. Tedy tento kód už musel být někdy předtím objeven,

analyzován, musela být vytvořena jeho signatura, ta musela být přidána k ostatním signaturám do virových definic a tyto definice se musely dostat až na danou koncovou stanici.

Medián doby od napadení do odhalení škodlivého kódu v postižené společnosti se podle studií pohybuje kolem 150 - 200 dnů (12, s. 3), (13, s. 17), (14, s. 2). Jedná se o tzv. Advanced Persistent Threats (APT), tedy hrozby, které se vyznačují tím, že se v napadených systémech snaží co nejlépe skrývat a vyhýbat se co nejdéle odhalení. Často jsou k těmto účelům využívány 0-day zranitelnosti[21]. V takových případech nemají konvenční bezpečnostní prostředky založené na signaturách ani nejmenší šanci útok odhalit. Tyto útoky jsou odhalitelné pomocí sledování projevů, které je provázejí a jejich porovnáváním se standardním chováním systémů. K tomuto účelu slouží behaviorální nebo heuristické analýzy. Tyto analýzy mohou probíhat nad nasbíranými informacemi z prostředí IS a jeho okolí, například sledování síťového provozu na bázi NetFlow nebo korelacemi logů v nástrojích typu SIEM, případně mohou probíhat aktivním vyvoláním projevů zkoumaného škodlivého software v odstíněném virtualizovaném prostředí zvaném sandbox[22].

Jako ochrana proti škodlivému kódu mohou být chápány nástroje pro kontrolu obsahu (Content-control) nazývané také jako URL filtering nebo Secure Web Gateways. Tyto nástroje umožňují firmám blokovat přístup svých zaměstnanců na vybrané weby pomocí blacklistů. Jde spíše o proaktivní ochranu, pokud zaměstnancům nepovolíme přístup k potenciálně rizikovému obsahu, snižujeme tím riziko napadení škodlivým kódem. Často se tyto nástroje ale používají i při snaze zamezit zaměstnancům se v pracovní době věnovat nepracovním činnostem. Problém této ochrany spočívá v tom, že jde o kontrolu proti seznamu webových stránek se známým a roztříděným obsahem. Stránky, které zatím nebyly do seznamu zařazeny, tedy nebudou filtrovány.

---

[21] 0-day nebo také zero-day zranitelnosti jsou zranitelnosti SW, které nejsou obecně známé a neexistuje na ně žádná obrana.

[22] Vymezené uzavřené prostředí, které je odděleno od okolního prostředí tak, aby jej procesy, které v něm běží nemohli nijak ovlivnit. Často se využívají pro prověřování podezřelých souborů, které přišly například jako přílohy elektronické pošty nebo které se uživatel pokouší stáhnout z internetových stránek.

Dalšími nástroji pro ochranu před škodlivým kódem jsou IDS a IPS zařízení, která už byly popsány výše jako nástroje pro ochranu integrity komunikačních sítí. Tyto nástroje také závisí na existujícím seznamu pravidel.

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

Subjekty, spravující informační systémy v režimu ZKB musí zajistit to, že budou zaznamenány činnosti v těchto IS. A to minimálně v rozsahu přihlášení/odhlášení uživatelů a administrátorů, činností prováděných administrátory, činností vedoucích ke změně přístupových oprávnění, z důvodů nedostatečných oprávnění neprovedených činností, zahájení/ukončení činností technických aktiv a jejich automatická varovná nebo chybová hlášení, přístupy k logům a změny jejich nastavení a použití mechanismů identifikace a autentizace včetně změny těchto údajů.

Záznamy musí obsahovat především typ zaznamenané činnosti, přesný datum a čas výskytu (k tomu je nutné zajistit nejméně jednou za 24 hodin synchronizaci jednotného systémového času na technických aktivech IS), identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a místa a informaci o (ne)úspěšnosti dané činnosti. Musí být také zajištěno to, že takto získané údaje o činnosti budou chráněny před neoprávněným čtením a především před neoprávněnou změnou.

U systémů spadajících do KII je navíc nutné zajistit minimálně tříměsíční retenční dobu. Tedy všechny záznamy činnosti musí být uchovány nejméně 3 měsíce tak, aby je v případě potřeby bylo možné analyzovat. Ve světle faktů o dobách mezi napadením systému prostřednictvím APT a jejich odhalením je doba 3 měsíců diskutabilní. Jak už bylo psáno v předchozí kapitole, medián této doby se pohybuje spíše kolem 5 až 6 měsíců. V tomto případě tedy platí, čím delší retenční doba, tím lépe pro případné dohledávání informací při analýzách potenciálních dlouhotrvajících útoků.

3.1.2.7 Nástroj pro detekci kybernetických bezpečnostních událostí

Pod tímto opatřením, podle toho, jak jej popisuje VKB, si můžeme představit nástroj na perimetru síťového prostředí informačního systému nebo infrastruktury. Tento systém má za úkol ověřovat, kontrolovat a případně zablokovat nežádoucí komunikaci mezi vnitřní a vnější sítí. Tento popis se docela dobře hodí na systém IPS, případně na

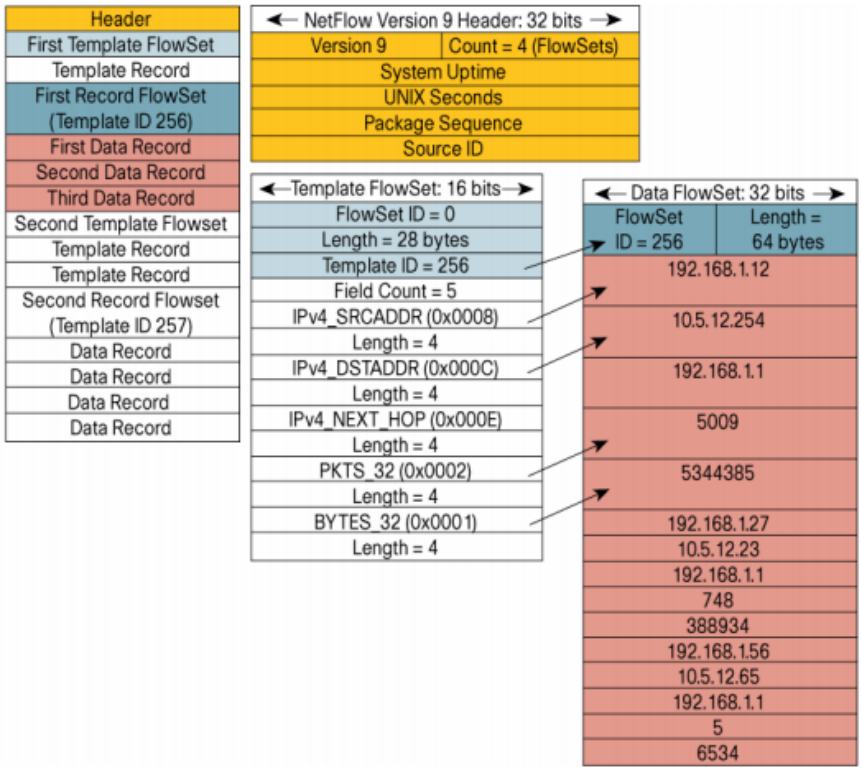
next-generation firewally a pokročilé konsolidované bezpečnostní systémy obsahující jak ochranné prvky založené na signaturách, tak moderní analytické nástroje pro odhalování 0-day hrozeb a APT.

Pro systémy KII navíc Vyhláška požaduje detekci kybernetických bezpečnostních událostí i v rámci vnitřní sítě a serverů systémů KII. K tomu se jistě nedá nic namítat. Jde o rozumná opatření, protože v dnešní době se nemůžeme spoléhat pouze na nástroje zajišťující bezpečnost perimetru. V době chytrých mobilních telefonů, Internetu věcí a bezdrátových komunikací se význam ochrany perimetru významně snižuje. Mít nadstandardně chráněný přechod mezi vnitřní a vnější sítí je nutností, není to však podmínka dostatečná k zajištění efektivní ochrany. Mnoho významných bezpečnostních událostí se děje i v rámci vnitřní sítě. Například zaměstnanec připojující se svým chytrým mobilním telefonem do interní Wi-Fi sítě představuje významné riziko. V tomto případě se totiž právě jeho mobilní telefon stává vlastně perimetrem mezi vnitřní sítí a internetem. Není asi třeba zdůrazňovat, že takový soukromý smartphone nedisponuje ani zdaleka tak sofistikovaným bezpečnostním vybavením, jako ostře hlídaný firemní perimetr. Riziko ale nemusí představovat pouze chytrá zařízení. Infikovaný přenosný disk (třeba i schválně nastražený útočníkem u vchodu do budovy[23]) připojený do počítače ve vnitřní síti představuje také velké riziko.

Podobné průniky samozřejmě prvky na perimetru nemají šanci detekovat. Zde jsou právě neocenitelnými pomocníky nástroje pro monitorování vnitřního síťového prostředí a jednotlivých prvků infrastruktury (tedy nejen serverů, jak požaduje vyhláška). Výbornou metodou monitorování síťového prostředí je tzv. NetFlow monitoring. Jde o sledování síťového provozu na bázi monitorování datových toků. Nejčastěji jde o protokol NetFlow nebo jeho novější verzi IPFIX.

[23] Jedná se o jednu ze známých metod sociálního inženýrství. Útočník nastraží na zaměstnance firmy, kterou se snaží napadnout několik návnad v podobě naoko ztracených flash disků, které obsahují malware. Lidská zvědavost pak většinou vykoná své. A zprvu náročný úkol, proniknout do sítě, která je velmi dobře chráněna na svém perimetru, se stává triviálním za pomoci zaměstnanců, kteří si neuvědomí rizikovost svého počínání. Lidský faktor bývá největší zranitelností chráněných prostředí.

Tato metoda monitoringu spočívá v exportování NetFlow toků ze síťových zařízení do kolektoru, který tyto toky následně dále zpracovává. Dříve se k exportování toků používaly především směrovače. Ostatně NetFlow protokol byl původně vyvinut právě jako doplněk směrovačů, který měl sloužit ISP[24] k účtování přeneseného objemu dat jednotlivým zákazníkům. Kvůli významnému snížení jejich směrovacího výkonu při zajišťování exportů toků a kvůli nutnosti tyto toky vzorkovat (používat pouze každý n-tý packet) se postupem času tato architektura mírně změnila.

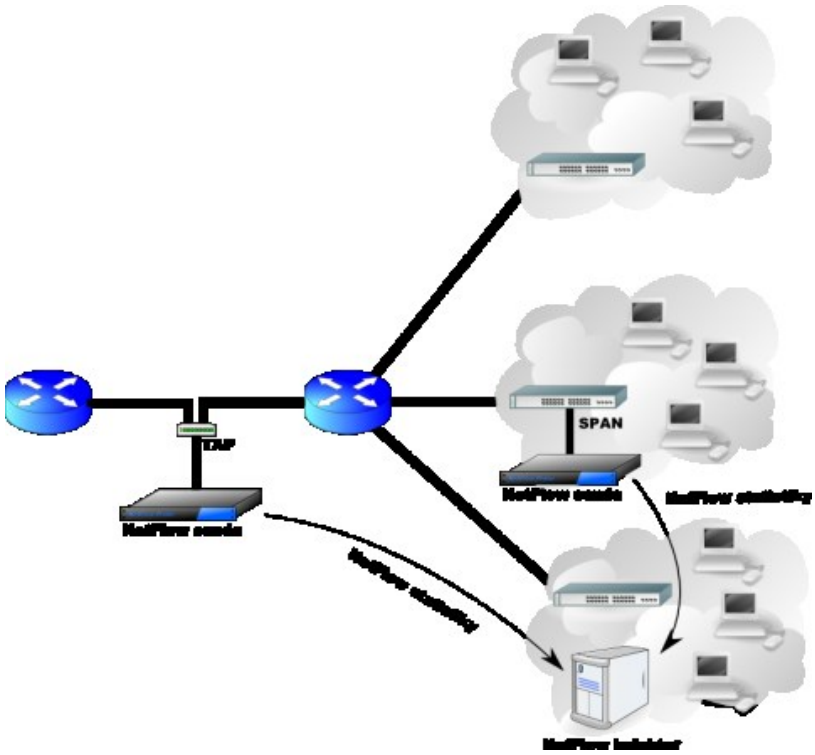


Obrázek 8 - příklad Export paketu NetFlow v9 (15, s. 13)

Dnes je nejčastějším zařízením exportující síťové toky speciálně k tomuto účelu vytvořená sonda. Sond se v síťovém prostředí většinou použije několik (dle rozsahu a dekompozice sítě) a tyto pak exportují NetFlow statistiky do kolektorů, které následně statistiky vyhodnocují, graficky prezentují a provádí nad nimi různé analýzy. Některé jsou založeny na signaturách nebo blacklistech, jiné pak na behaviorálních analýzách. Právě behaviorální analýzy neboli analýzy neobvyklého chování, jsou významným prostředkem

[24] ISP je zkratkou pro Internet Service Provider – tedy poskytovatel internetového připojení.

pro odhalení nežádoucího kódu nacházejícího se v interní síti. Tato metoda dokáže odhalit i projevy pokročilých hrozeb typu APT a 0-day hrozeb.



Obrázek 9 - příklad architektury NetFlow monitoringu s použitím NetFlow sond (Wikipedia Creative Commons Public Domain Images)

3.1.2.8 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Pod tímto opatřením se skrývá nástroj, který je známý především pod svým akronymem SIEM. Jde tedy o nástroj pro řízení bezpečnostních informací a událostí. Trochu pragmaticky vyhláška vyžaduje splnění tohoto opatření pouze po systémech KII. Jde totiž přece jen o pokročilejší a robustnější nástroj, který se většinou vyplatí nasadit u větších a komplexnějších prostředí. Spolu s tímto nástrojem je nutné zajistit také příslušné personální obsazení. SIEM bývá jedním z primárních nástrojů ISIRT[25] nebo

[25] ISIRT je Information Security Response Team, tedy tým lidí, kteří mají na starost tzv. incident handling. Jejich náplní práce je analýza bezpečnostních událostí a reakce na detekované bezpečnostní incidenty (ve smyslu kybernetické bezpečnosti)

SOC[26] týmů. Mít takový tým odborníků na kybernetické bezpečnostní události a incidenty také není levná záležitost a možná ještě větší problém než finance je takové odborníky sehnat. Proto se služby typu ISIRT nebo SOC dají také outsourcovat.

Vyhláška vyžaduje od tohoto nástroje integrovaný sběr a vyhodnocení kybernetických bezpečnostních událostí, poskytování informací o těchto událostech pro určené bezpečnostní role a nepřetržité vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů a včasné varování příslušných bezpečnostních rolí. Žádný nástroj sám o sobě není schopen vyhodnocovat to, které z nalezených bezpečnostních událostí jsou bezpečnostní incidenty. To je práce obsluhy těchto nástrojů a jde o vysoce odbornou činnost vyžadující dobrou znalost daného prostředí a kontextu nalezených událostí. Systém může „pouze“ na základě nastavených pravidel vyhodnocovat pravděpodobnost incidentu a jeho potenciální důležitost, a v případě, že důležitost dosáhne nastavené úrovně, nástroj pošle informaci obsluze.

Důležité je správně nastavit pravidla, podle kterých SIEM hodnotí bezpečnostní události a incidenty, a podle kterých posílá upozornění (alerty) na potenciální bezpečnostní incidenty stanovené závažnosti. Tato pravidla je navíc nutné pravidelně revidovat a aktualizovat, případně vymýšlet pravidla nová. Subjekty spravující KII navíc musí zajistit to, že informace z tohoto nástroje budou použity k nastavení bezpečnostních opatření na daném systému KII.

3.1.2.9 Aplikační bezpečnost

Pod tímto opatřením se skrývá potřeba zajistit bezpečnostní a penetrační testy aplikací, které jsou dostupné z vnější sítě. Pro systémy VIS požaduje Vyhláška takové testy provádět před uvedením aplikace do provozu a vždy když se změní bezpečnostní mechanismy aplikace. Zásadní změny bezpečnostních mechanismů se ale za celou dobu životnosti aplikace nemusí objevit nebo se budou objevovat například jednou za několik let. Proto je toto opatření sice vyhovující Vyhlášce, ale nemusí být vyhovující zabezpečení

[26] SOC je Security Operations Center, tedy jakési centrální oddělení, které se stará o řešení bezpečnostních záležitostí a to jak po technické, tak po organizační stránce

dané aplikace. To, že aplikace projde bez závažných nálezů penetračním testováním, rozhodně neznamená, že projde úspěšně testováním například o rok později. A to ani za předpokladu, že nebyla měněna vůbec. Bezpečnostní situace se totiž velmi dynamicky vyvíjí. Jsou objevovány nové zranitelnosti použitých technologií, mění se vektory a trendy potenciálních útoků i myšlení útočníků. Lze tedy jedině doporučit provádět bezpečnostní a penetrační testování pravidelně, s frekvencí zhruba jednoho roku. Doporučováno je také střídat osoby, které testování provádějí. Ať už se jedná o interně prováděné testy nebo testy objednané u externích subjektů. Pokud testy provádí stále stejná osoba (nebo osoby), je pravděpodobné, že zranitelnosti, které neodhalila napoprvé, neodhalí ani při opakovaném testování. Často testuje webovou aplikaci stejným procesem a stejnými nástroji. Nový pohled jiné osoby může odhalit nové zranitelnosti.

Subjekty spravující systémy KII musí navíc zajistit trvalou ochranu aplikací, informací a transakcí dostupných z vnější sítě. Tato do značné míry obecná definice cílí především na nasazení aplikačního firewallu nebo firewallu s aplikační inspekcí (také označovaného jako next-generation firewall). Na rozdíl od klasických firewallů nebo například IPS nástrojů, které mají také za úkol ochranu informací a transakcí na perimetru, jde o to, dosáhnout ochrany také na úrovni aplikační vrstvy síťové komunikace. Závadná komunikace totiž nemusí být nutně identifikovatelná na nižších vrstvách RM ISO/OSI.

3.1.2.10 Kryptografické prostředky

Subjekty spravující systémy VIS a/nebo KII musí stanovit kryptografická pravidla dle úrovně potřebné ochrany s ohledem na typ a sílu kryptografických algoritmů. Minimální požadavky na kryptografické algoritmy udává příloha č. 3 VKB.

Kryptografickými prostředky je třeba chránit především datové přenosy po komunikační síti, data na přenosných mobilních zařízeních a na vyměnitelných technických nosičích dat. Cílem je pomocí kryptografických prostředků zajistit ochranu důvěrnosti a integrity dat a to takovým způsobem, že je možné identifikovat konkrétní osobu, která s daty manipuluje.

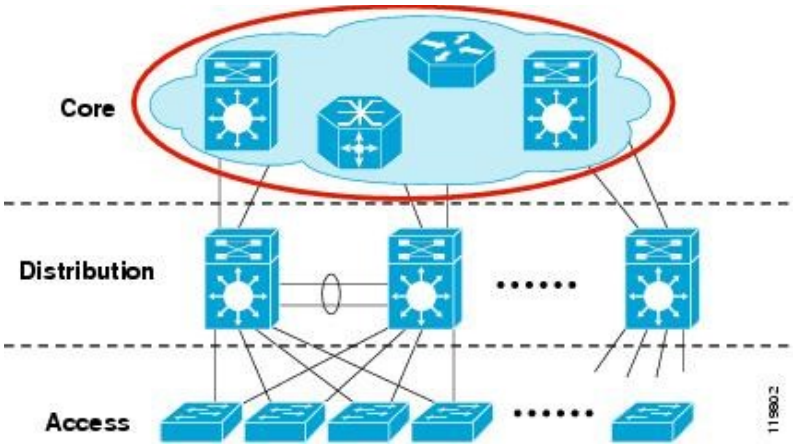
Nejčastější místa, kde se běžně využívá kryptografie, jsou šifrování dat na koncových stanicích (včetně mobilních), serverech ale také v databázích, šifrování síťové komunikace přes VPN nebo šifrovaná webová komunikace prostřednictvím protokolu

SSL/TLS nebo podepisování a šifrování pomocí certifikátů, případně autentizace pomocí certifikátů.

Pro správce KII navíc platí nutnost zavést systém správy klíčů, jejich generování, distribuci, ukládání, archivaci, změny, ničení, kontrolu a audit klíčů.

3.1.2.11 Nástroj pro zajišťování úrovně dostupnosti informací

Správce systému KII musí používat nástroj k zajištění požadované úrovně dostupnosti informací, odolnosti vůči kybernetickým bezpečnostním incidentům, které by mohly snížit dostupnost systému a musí zajistit zálohování důležitých technických aktiv systému buď využitím redundance v návrhu řešení, nebo zajištěním náhradních technických aktiv ve stanoveném čase. Redundancí v návrhu jsou myšleny HA[27] principy na úrovni síťové infrastruktury, aplikační vrstvy i datové vrstvy.



Obrázek 10 - vzor redundantního návrhu síťového připojení (16)

Zabezpečit požadovanou dostupnost je možné také zajištěním náhradních technických aktiv v požadovaném čase a to buď tím, že má subjekt potřebná technická aktiva ve svém skladu a technicky způsobilé pracovníky, nebo zajištěním rychlé servisní podpory externího subjektu s definovanou úrovní služeb, která zaručuje včasné řešení problému.

[27] HA je zkratkou z anglického High Availability. Jde tedy o metody dosažení vysoké dostupnosti daného řešení. Často jsou zajištěny zapojením zařízení do clusterů způsobem, kdy se jednotlivá zařízení vzájemně zajišťují proti výpadku.

3.1.2.12 Bezpečnost průmyslových a řídicích systémů

Tento bod se týká jen vybraných specifických subjektů spravujících systém KII, který je průmyslovým řídicím systémem (např. SCADA[28] systémy nebo PLC[29] zařízení). Omezuje fyzický i vzdálený přístup k těmto řídicím systémům, ochranu jednotlivých technických aktiv před známými zranitelnostmi a musí zajistit obnovení chodu po kybernetickém bezpečnostním incidentu.

4 Vlastní práce

Vzhledem k citlivosti některých bezpečnostních informací budu konkrétnímu OVM, o jehož bezpečnostní opatření se v této práci jedná, říkat jednoduše „Úřad“. Je to především proto, že všechna bezpečnostní dokumentace, kterou v práci popisuji, je klasifikována jako interní nebo dokonce chráněná. Vychází to například i právě z VKB, která u některých částí bezpečnostní politiky očekává střední úroveň důvěrnosti (např. politika systému řízení bezpečnosti informací, politika ochrany před škodlivým kódem nebo politika bezpečného chování uživatelů) a u některých částí dokonce vysokou úroveň důvěrnosti (např. politika klasifikace aktiv, politika řízení technických zranitelností nebo politika bezpečnosti komunikační sítě).

Vzhledem k tomu, že Úřad má více než jeden informační systém, který spadá pod ZKB, a kromě toho má také další informační systémy, které pod ZKB nespadají, je v jeho případě praktické řešit řízení bezpečnosti komplexně od nejvyšších a nejobecnějších bezpečnostních dokumentů. Opakem tohoto přístupu by bylo vytvářet pro informační systémy spadající pod ZKB jiné politiky než pro systémy, které pod ZKB nespadají. Umožnilo by to sice do jisté míry uvolnit pravidla pro systémy, které nespadají pod ZKB, bylo by však velmi nepraktické a neefektivní sledovat a rozlišovat, která aktiva patří ke které skupině vzájemně provázaných informačních systémů.

[28] SCADA systém, který monitoruje a ovládá průmyslová zařízení například ve strojní výrobě, energetice nebo distribučních sítích apod.
[29] PLC je programovatelný logický automat, který v reálném čase automatizuje procesy průmyslových strojů.

Vrcholným dokumentem řídicím kybernetickou bezpečnost Úřadu je bezpečnostní politika. Na bezpečnostní politiku pak navazují další dokumenty (směrnice, řády, metodiky a pokyny), které ji dále specifikují v jednotlivých bodech. Mezi nimi například statut a jednací řád Výboru pro řízení kybernetické bezpečnosti Úřadu, metodika analýzy rizik Úřadu nebo metodika řízení bezpečnostních incidentů v IS Úřadu.

Z technických bezpečnostních opatření se budu v této práci věnovat především těm, které jsou pro většinu OVM něčím novým, co často nemají implementováno. Jde především o NetFlow monitoring sítě jako nástroje pro detekci kybernetických událostí (3, s. 1927 - § 5, odst. 3, písm. g) a SIEM jako nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí (3, s. 1927 - § 5, odst. 3, písm. h).

V následujících kapitolách popíši jejich nasazení v provozu Úřadu, některá specifika jejich nastavení a funkce a jejich vzájemnou integraci. Nakonec oba systémy použiji v rámci šetření konkrétní bezpečnostní události.

4.1 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. Proto, abychom věděli, co vše bychom měli změnit, jsme provedli GAP analýzu neboli srovnávací analýzu stavu bezpečnosti s cílem posoudit míru souladu s jednotlivými paragrafy Vyhlášky o kybernetické bezpečnosti.

Analýza byla provedena pod záštitou externí firmy, abychom se vyhnuli subjektivnímu nadhodnocování výsledků a jakési provozní slepotě, kdy bychom se znalostí prostředí a nastavených procesů (včetně těch, které nebyly formálně dokumentovány) mohli dospět také k nadhodnoceným výsledkům. Součástí GAP analýzy bylo důsledné prověření bezpečnostní i provozní dokumentace a interview se zainteresovanými osobami – především pracovníky bezpečnostního odboru, garanty a vlastníky příslušných informačních systémů a aplikací a s odborem ICT, jakožto garantem infrastruktury.

Analýza byla zaměřena především na informační systémy Úřadu, které naplňují podmínky zařazení mezi KII nebo VIS. Posouzení bylo prováděno oproti přísnější verzi – tedy požadavkům pro informační systémy KII.

Účelem hodnocení bylo stanovit míru naplnění bezpečnostních požadavků jednotlivými systémy. Z těchto důvodů byl pro hodnocení použit zjednodušený „maturity model“, který v obecné rovině vychází z metodiky COBIT. Použitý model používá k hodnocení třístupňové stupnice hodnot naplnění požadavků Zákona o kybernetické bezpečnosti a souvisejících prováděcích předpisů.

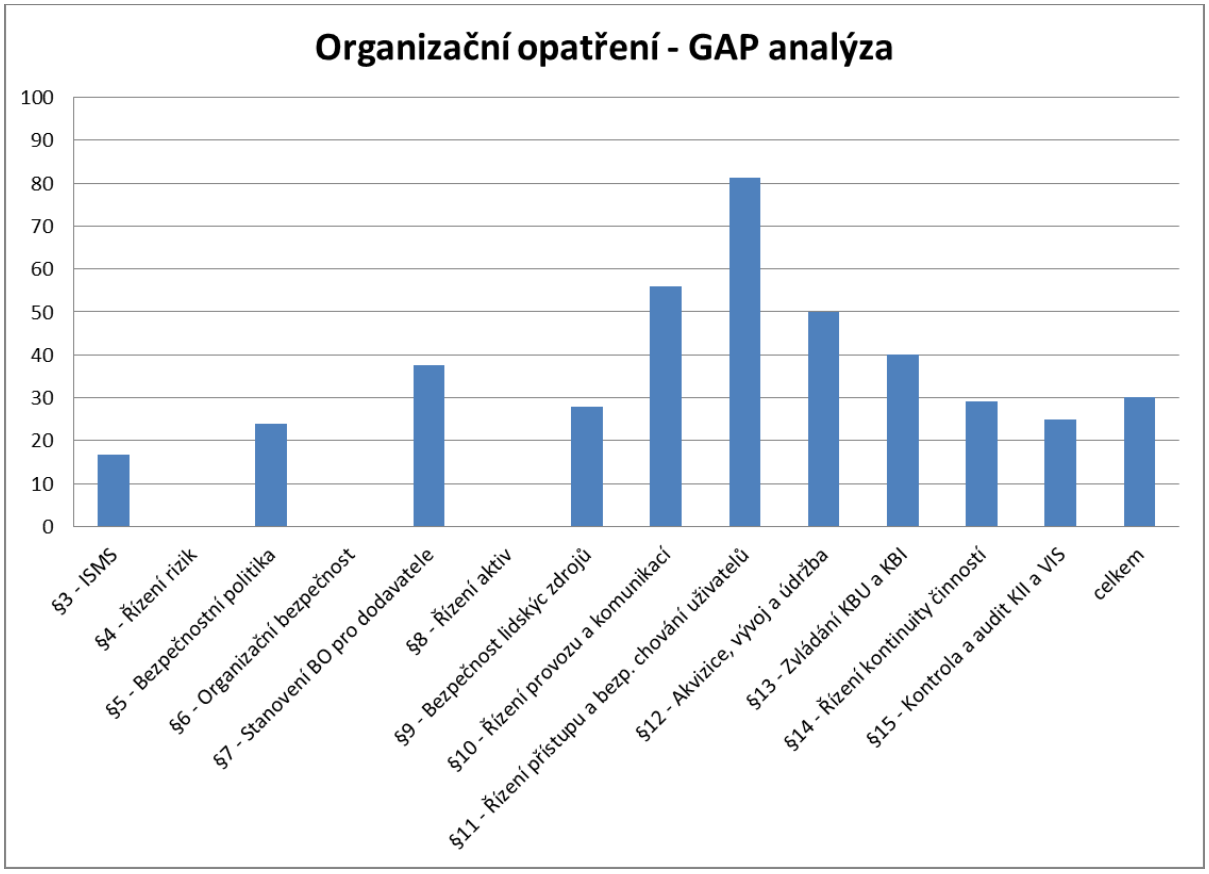
V následující tabulce jsou uvedeny definice hodnocení.

Hodnota	Stupeň vyspělosti	Charakteristika stupně
0	Neexistence	Nejsou realizována žádná opatření splňující konkrétní požadavky VKB.
1	Částečně	Jsou realizována opatření v omezeném rozsahu a nesplňují požadavky VKB. Opatření je realizováno jednou z následujících možností: • Opatření je zdokumentováno pouze částečně nebo nejednoznačně, • Opatření je prováděno, ale není zdokumentováno, • Opatření je zdokumentováno, ale není prokazatelně prováděno
2	Dostatečně	Požadavky VKB jsou realizována v požadovaném rozsahu.

Tabulka 1 - Definice hodnocení vyspělosti opatření Úřadu dle VKB (GAP analýza)

Po důkladném ohodnocení jednotlivých zákonem požadovaných bezpečnostních opatření vyplynul závěr, že Úřad dosahoval souladu především v oblasti technických opatření. Nicméně v oblasti organizačních patření významně zaostával. Výsledkem tedy bylo doporučení zaměřit se především na vylepšení organizačního zabezpečení kybernetické bezpečnosti.

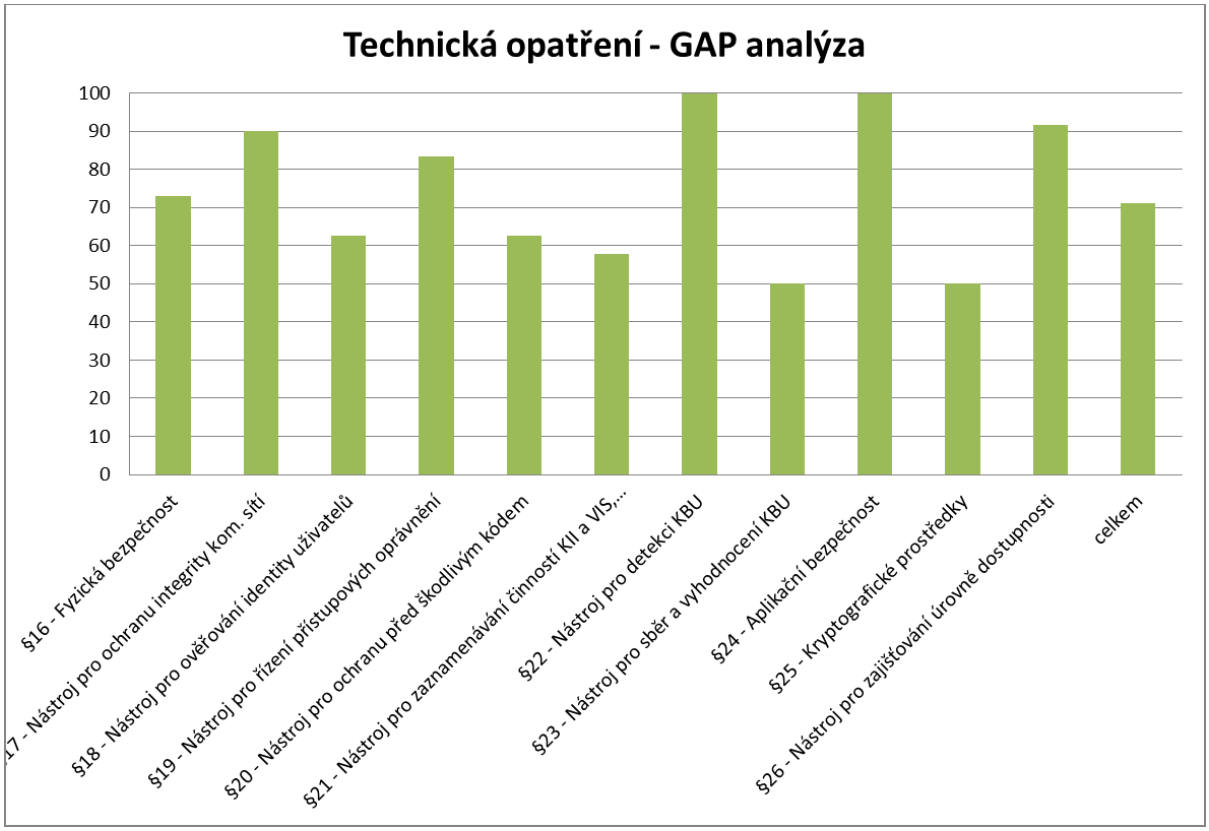
Výsledky GAP analýzy shrnují následující dva grafy. První z nich zobrazuje míru naplnění jednotlivých organizačních opatření, druhý pak míru naplnění technických opatření. Míra souladu je vyjádřena v procentech a vyplývá z hodnoceného stupně vyspělosti v jednotlivých bodech odpovídajících požadavkům kladených příslušným paragrafem vyhlášky. Maximum (tedy 100% soulad) dosáhne Úřad v případě, že všechny požadavky příslušného paragrafu vyhlášky splňuje dostatečně (tedy jsou ohodnoceny hodnotou „2“ stupně vyspělosti).



Obrázek 11 - Míra naplnění organizačních opatření - GAP analýza (vlastní zpracování)

Z grafu míry naplnění organizačních opatření vyplývá, že požadavky kladené ZKB na organizační opatření byly v době provádění GAP analýzy plněny z 30%. Nedostatky byly především v oblastech řízení aktiv a rizik a také v oblasti organizační bezpečnosti. Jediná oblast, která byla plněna vcelku uspokojivě, bylo řízení přístupů a bezpečného chování uživatelů.

Bylo jasné, že je naprosto nezbytné vypracovat novou bezpečnostní politiku, která bude zohledňovat veškeré požadavky ZKB. Současně bude třeba ustanovit pravidla řízení bezpečnosti informací a vytvořit metodiku pro řízení aktiv a řízení rizik.



Obrázek 12 - Míra naplnění technických opatření - GAP analýza (vlastní zpracování)

Pohled na výsledky souladu technických opatření je pro úřad mnohem příjemnější. Celkem splňoval Úřad technická opatření v době provádění GAP analýzy ze 70%. Přičemž nejslabší výsledky dosahoval v oblastech nasazení nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí a v oblasti kryptografických prostředků. Nicméně ani tyto dvě oblasti na tom nebyly nijak výrazně zle.

Výsledkem analýzy technických opatření vyplynula potřeba lépe nastavit SIEM a NetFlow Monitoring jakožto nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.

4.2 Bezpečnostní politika

V době, kdy jsme začali řešit tvorbu bezpečnostní politiky, která by vyhovovala parametrům stanoveným Vyhláškou o kybernetické bezpečnosti, byla původní bezpečnostní politika Úřadu stará zhruba 9 let. Její struktura a obsah zákonné parametry nesplňoval. Bylo tedy potřeba vypracovat bezpečnostní politiku novou. Rozhodl jsem se jít

cestou jednoho dokumentu, který splňuje požadavky VKB a obsahuje všechny aspekty, které Vyhláška specifikuje.

Výsledná bezpečnostní politika je tak se svými 41 stranami relativně obsáhlá. Tvoří však jednotný vrcholový bezpečnostní rámec, který vyhovuje VKB, a kterým se musí všichni pracovníci Úřadu řídit. Konkrétní implementace jednotlivých oblastí bezpečnostní politiky jsou pak specifikovány v bezpečnostních politikách jednotlivých informačních systémů Úřadu. Některé oblasti jsou specifikovány v jiných organizačních dokumentech Úřadu. Například pro, v bezpečnostní politice zavedený, výbor pro řízení kybernetické bezpečnosti, vznikl dokument určující jeho statut a jednací řád, které současně tvoří základní dokument systému řízení bezpečnosti informací.

Kapitolu „Řízení incidentů“ pak specifikuje dokument „Metodika pro řízení bezpečnostních incidentů Úřadu“. Řízení rizik, popisované v kapitole „Řízení aktiv a klasifikace informací“, je podrobněji nastaveno dokumentem „Metodika analýzy rizik Úřadu“.

Podobným způsobem jsou bezpečnostní pravidla stanovena Bezpečnostní politikou rozvedena v dalších směrnicích, které se věnují pravidlům práce s výpočetní technikou, implementaci zabezpečení databází, aplikačních serverů, klasifikaci dat, apod.

Vzhledem k citlivosti obsahu Bezpečnostní politiky Úřadu není možné celý dokument publikovat. Jako příloha A je přiložen obsah Bezpečnostní politiky, který přináší alespoň základní náhled na problematiku, kterou dokument řeší.

4.3 Systém řízení bezpečnosti informací

Základním kamenem zavedení systému řízení bezpečnosti informací bylo v Úřadu ustanovení Výboru pro řízení kybernetické bezpečnosti. Základním dokumentem je v tomto případě Statut a jednací Výboru pro řízení kybernetické bezpečnosti Úřadu.

4.3.1 Výbor pro řízení kybernetické bezpečnosti

Statut upravuje zejména složení Výboru, práva jeho členů a pravidla pro jednání.

Členy Výboru jsou:

- Garant zdrojů ISMS;
- Garant metodiky ISMS;
- Garanti aktiv IS/infrastruktury ICT;
- Architekt kybernetické bezpečnosti IS/infrastruktury ICT;
- Manažer kybernetické bezpečnosti IS/infrastruktury ICT.

Dále jsou definovány povinnosti a odpovědnosti Výboru. Výbor řídí a koordinuje všechny činnosti týkající se kybernetické bezpečnosti Úřadu a odpovídá za celkový rozvoj kybernetické bezpečnosti v organizaci. Mezi jeho povinnosti a odpovědnosti patří zejména:

- provádění dohledu nad návrhem, tvorbou, implementací a údržbou plánu rozvoje ISMS Úřadu;
- projednávání aktuálních témat v oblasti informační bezpečnosti a prezentace relevantním subjektům;
- poskytování doporučení pro řešená témata v oblasti informační bezpečnosti a doporučení vhodných činnosti pro podporu programu řízení rizik;
- posuzování řešení bezpečnostních incidentů, ověřování, zda jsou přijímána dostatečná opatření pro pokrytí rizik a bezpečnostních incidentů;
- projednávání schválení výjimek z předpisů v oblasti informační bezpečnosti, pokud není určeno jinak, případně má dohled nad tímto procesem;
- projednávání vyhodnocení stavu a účinnosti systému řízení bezpečnosti informací, které obsahuje i vyhodnocení revize hodnocení rizik, posouzení výsledků auditů kybernetické bezpečnosti a dalších kontrol a dopadů kybernetických bezpečnostních incidentů;
- návrhy ke jmenování manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti a auditora kybernetické bezpečnosti;
- návrhy ke jmenování garanty primárních aktiv, garanty IS KII a VIS.

4.3.2 Definování bezpečnostních rolí Úřadu

Nedílnou součástí systému řízení bezpečnosti informací je také Bezpečnostní politika popsaná v předchozí kapitole. Především pak úvodní kapitola, která definuje účel Bezpečnostní politiky, v němž je popsán i princip řízení bezpečnosti informací. Další

zásadní kapitolou je pak nastavení bezpečnostní organizační struktury Úřadu. Ta se skládá ze dvou úrovní – řídicí a výkonné. Dále jsou v této kapitole popsány jednotlivé bezpečnostní role a jejich a jejich odpovědností.

Bezpečnostní organizační struktura je v Úřadě určena následujícím rolemi:

Řídicí úroveň

- Výbor pro řízení kybernetické bezpečnosti;
- Bezpečnostní ředitel;
- Specialista bezpečnosti (Specialista fyzické bezpečnosti, Specialista personální bezpečnosti, Specialista organizační a administrativní bezpečnosti, Specialista ochrany důvěrných statistických údajů/osobních údajů, Specialista kybernetické/technické bezpečnosti);
- Garant infrastruktury ICT;
- Garant IS/aplikace.

Výkonná úroveň

- Pracovník bezpečnosti organizačního útvaru;
- Provozní manažer bezpečnosti infrastruktury ICT;
- Provozní manažer bezpečnosti IS/aplikace;
- Architekt kybernetické bezpečnosti;
- Auditor kybernetické bezpečnosti;
- Správce SOC (Security Operations Center);
- Provozní administrátor;
- Bezpečnostní administrátor;
- Bezpečnostní správce IS/aplikace;
- Uživatel IS/aplikace.

4.4 Metodika identifikace aktiv a řízení rizik

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. Řeší pouze rizika informací a informačních systémů. Jednotlivá rizika jsou určena kombinací hrozby, zranitelnosti, kterou tato hrozba využije, a aktiva, kterou takto uplatněná hrozba poškodí. Z této trojice také vychází odhad úrovně rizika.

Prvním krokem v analýze rizik je identifikace aktiv a ohodnocení aktiv, pro která budeme rizika řídit. Neidentifikujeme aktiva na úrovni například jednotlivých serverů, ale identifikujeme aktiva na úrovni položek mající stejný charakter nebo účel. Hodnotíme tedy tzv. typová aktiva. Tato aktiva dále dělíme do kategorií podle jejich druhu.

Primární aktiva

- Datová aktiva (data, zálohy, logy, autentizační údaje, apod.)
- Služby (obecné nebo systémové služby)

Sekundární aktiva

- SW
- HW (včetně médií)
- Lokality (provozní lokality IS, serverovny)
- Personál (zaměstnanci, dodavatelé)

Důležité je, že pro jednotlivá aktiva je zvolen jejich Garant, což je osoba odpovědná za bezpečnost tohoto aktiva, která zároveň může schvalovat jeho ohodnocení. Pro všechna identifikovaná aktiva je provedena jejich klasifikace podle klasifikačních stupňů definovaných v Bezpečnostní politice.

Všechna aktiva jsou ohodnocena podle možného dopadu při:

- narušení důvěrnosti (neoprávněné vyzrazení),
- narušení integrity (neoprávněná změna), a při
- narušení dostupnosti, kde je samostatně hodnocen dopad v případě
    - úplného zničení aktiva a
    - dočasné nedostupnosti (doba je daná SLA, v případě neexistence SLA je hranice dočasné nedostupnosti max. 1 týden);

K jednotlivým aktivům jsou dále přiřazeny hrozby z katalogu hrozeb[30] uvedeného v této metodice. Ke dvojicím ***aktivum*** x ***hrozba*** jsou přiřazeny zranitelnosti, tedy slabá místa, která mohou být využita hrozbami.

Rizika jsou určena kombinací ***aktivum*** x ***hrozba*** x ***zranitelnost***, jedná se tedy o scénáře tvořené hrozbou, zranitelností, kterou tato hrozba využije, a aktivem, kterou takto uplatněná hrozba poškodí. Hodnota dopadu na aktivum je pro každé riziko jedna hodnota a je určena jako maximum z ohodnocení těch bezpečnostních aspektů aktiva, která jsou relevantní pro dané riziko.

Výpočet rizika je proveden podle následujícího vzorce:

riziko = dopad na aktivum + hrozba + zranitelnost - 2

Výsledná úroveň rizika je hodnota na stupnici 1 až 10, kde 1 je nejméně významné riziko a 10 je nejvýznamnější riziko. Tyto číselné hodnoty úrovně rizika jsou mapovány na slovné vyjádření podle následující tabulky:

Úroveň		Popis
1 – 3	**Nízké**	Riziko je považováno za přijatelné.
4 – 6	**Střední**	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti je riziko přijatelné.
7 - 8	**Vysoké**	Riziko je dlouhodobě nepřípustné a musí být zajištěny systematické kroky k jeho odstranění.
9 - 10	**Kritické**	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

Tabulka 2 - Tabulka hodnocení úrovně rizik Úřadu (Metodika analýzy rizik)

Výsledkem hodnocení rizik je seznam rizik určený pro jejich následné ošetření. U těchto rizik je dále nutné rozhodnout, jakým způsobem s nimi bude dále naloženo, tj. určit způsob jejich zvládání.

[30] Katalog hrozeb vychází z ČSN ISO/IEC 27005:2013 a není úplně shodný se seznamem hrozeb, které definuje VKB. Přílohou vytvořené Metodiky analýzy rizik Úřadu je tedy také tabulka hrozeb definovaných VKB, která mapuje hrozby na ty, které jsou uvedeny v této metodice.

V případě výběru „modifikace rizika“ z možných variant ošetření rizik (tj. aplikace vhodných bezpečnostních opatření) jsou pro rizika vybírána opatření pro jejich zmírnění nebo pokrytí. Pro výběr opatření je používán katalog opatření, který vychází z Přílohy A normy ČSN ISO/IEC 27001:2014. K doložení úplnosti implementace všech mandatorních požadavků VKB je provedeno mapování mezi jednotlivými požadavky uvedenými ve VKB a katalogem opatření.

Výsledky řízení rizik zahrnující výsledky analýzy a zvládání rizik jsou pak dokumentovány ve Zprávě o hodnocení rizik a aktiv, Prohlášení o aplikovatelnosti a Plánu zvládání rizik.

4.5 Postup řízení bezpečnostních incidentů

Postup řízení bezpečnostních incidentů v Úřadě je stanoven Metodikou řízení bezpečnostních incidentů v informačních systémech. Tato metodika v první řadě stanovuje odpovědnost za realizaci postupů pro řízení bezpečnostních incidentů ve všech IS KII a VIS manažeru kybernetické bezpečnosti. Na zvládání bezpečnostních incidentů se pak podílí tým Information Security Incident Response Team (ISIRT) a všechny osoby, které manažer kybernetické bezpečnosti IS KII a VIS vyzve ke spolupráci.

Identifikovaným incidentům je na základě jejich závažnosti a předpokládaného dopadu na informační aktiva Úřadu přiřazena jedna z následujících kategorií:

Kategorie I – méně závažný incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo informačních aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření incidentu včetně minimalizace vzniklých škod.

Kategorie II – závažný incident, při kterém je narušena bezpečnost poskytovaných služeb nebo informačních aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření incidentu včetně minimalizace vzniklých škod.

Kategorie III – velmi závažný incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo informačních aktiv. Jeho řešení vyžaduje

neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření incidentu včetně minimalizace vzniklých i potenciálních škod.

To, zda je nahlášená bezpečnostní událost incidentem, určuje manažer kybernetické bezpečnosti. Pokud se domnívá, že není schopen adekvátně rozhodnout, vyžádá si součinnost od architekta kybernetické bezpečnosti daného IS.

Pokud vznikne podezření na existenci bezpečnostního incidentu, manažer kybernetické bezpečnosti IS KII a VIS postupuje, jako by se o incident jednalo. V takovém případě aktivuje tým ISIRT, který doplní o další ad hoc členy, vždy o vlastníka/garanta aktiva dotčeného incidentem a případně další v závislosti na charakteru incidentu (např. administrátora napadeného systému) a zahájí sběr a zaznamenávání relevantních informací k incidentu. Tým ISIRT nejprve provede předběžné vyhodnocení incidentu a pokud se incident šíří, rozhodne o okamžitých akcích k zastavení jeho šíření a informování incidentem dotčených stran. Po zastavení šíření incidentu je nezbytné zdokumentovat rozsah a dopady incidentu pro pozdější vyhodnocení a analýzu. Následně je nutné analyzovat příčinu a způsob působení incidentu a plánovat kroky k obnově zasažených procesů (obnovu podpůrných aktiv zasažených incidentem).

Po obnově a uvedení procesů zasažených incidentem do normálního provozního stavu zahájí tým ISIRT vyšetřování incidentu, jehož cílem je:

- objasnit příčiny a mechanismus vzniku incidentu,
- identifikovat bezpečnostní opatření, které selhalo a musí být zlepšeno,
- zjistit, zda došlo k zavinění konkrétní osobou a pokud ano, doplnit tvrzení důkazy,
- vyjádřit názor, zda došlo k porušení zákona a zda se doporučuje zahájení stíhání viníka,
- doporučit nápravná opatření, která mají v budoucnosti zabránit opakování incidentu a zapracovat je (případně aktualizovat stávající) do Plánu zvládání rizik.

V případě že se bezpečnostní incident týkal IS KII, nebo VIS, manažer kybernetické bezpečnosti provede klasifikaci a určení typu kybernetického bezpečnostního incidentu a zpracuje jeho hlášení pro bezpečnostního ředitele, který ho následně pošle na NBÚ.

4.6 NetFlow monitoring

Úřad pro detekci kybernetických bezpečnostních i provozních událostí na svém síťovém prostředí používá nástroj české společnosti Flowmon Networks, nazvaný Flowmon. Při nasazování tohoto systému do prostředí Úřadu bylo v první řadě důležité rozhodnout se, které síťové toky a jakým způsobem bude sledovat. Nástroj byl nasazen dle klasické architektury, tedy pomocí sond přenášejících síťové statistiky do kolektoru, kde jsou pak dále zpracovávány.

Konkrétně byla použita 4-portová sonda s označením Flowmon Probe 4000 (IFP-4000-CU). Jedná se o rackové zařízení o velikosti 1U. Každý ze čtyř monitorovacích portů sondy podporuje 10/100/1000 Mb Ethernet s maximálním výkonem až 1,48 Mp/s. (17, s. 2) Flowmon sonda je výkonná autonomní NetFlow/IPFIX sonda určená k monitorování IP toků v reálném čase a k exportu zjištěných statistik ve formátu NetFlow v5 a v9 nebo IPFIX.

Jako kolektor bylo použito virtuální zařízení s označením Flowmon Collector 1000 Virtual Appliance (IFC-1000-VA) s výkonem až 75.000 toků za sekundu. (18, s. 3)

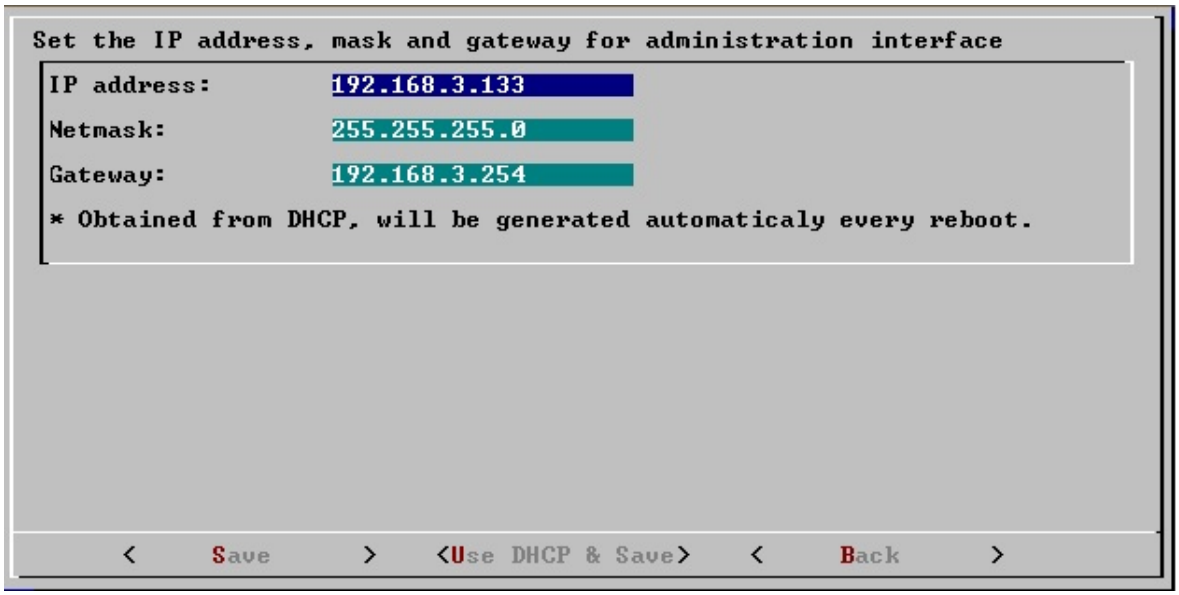
4.6.1 Konfigurace sondy

Typicky se Flowmon sonda nasazuje na centrálních aktivních prvcích sítě, jejích hraničních bodech, kritických bodech (datová úložiště, serverové farmy), místech s největšími objemy přenášených dat, či na firewallech a VPN přístupových bodech. Zapojení v Úřadu není výjimkou. Do sondy byl přiveden tok z hraničního směrovače na perimetru, směrovače v DMZ a z core přepínače v LAN Úřadu. Tím byla zajištěna viditelnost komunikace do/z internetu, v DMZ kvůli centrálním prvkům i v rámci vnitřní klientské komunikace. Pro připojení k sondě byly využity tzv. mirror porty daných směrovačů a přepínače.

4.6.1.1 Nastavení IP adresy sondy

Pro konfiguraci zařízení a práci s ním je vhodné sondu připojit přes administrativní port (RJ-45) do místní LAN. Následně je potřeba nastavit sondě IP adresu, na které bude na síti dostupná. IP adresu je možné nastavit pomocí grafického rozhraní nebo prostřednictvím konzole.

Nastavení prostřednictvím konzole vyžaduje připojení klávesnice a monitoru k zařízení. Následně je třeba se přihlásit výchozím účtem „flowmon“ a pomocí příkazu sysconfig spustit konfiguraci. IP adresu sondy nastavíme v položce „Management port“. Po vypsání stanovené IP adresy, příslušné síťové masky a výchozí brány uložíme pomocí tlačítka „Save“. Je možné nechat přidělit IP adresu i prostřednictvím DHCP serveru, v takovém případě je ale vhodné nastavit DHCP server tak, aby přiděloval sondě stále stejnou adresu.



Obrázek 13 - Nastavení IP adresy sondy flowmon pomocí aplikace sysconfig (19)

Alternativou je nastavení adresy prostřednictvím grafického rozhraní webové aplikace. V takovém případě je potřeba se připojit počítačem přímo na administrativní rozhraní pomocí UTP kabelu. Nastavit si na počítači adresu ze sítě 192.168.1.0/24 (uživatelská příručka přímo udává použít adresu 192.168.1.10). A poté spustit webovou aplikaci prohlížečem odkázaným na adresu 192.168.1.1. IP adresa zařízení se pak dá nastavit v konfiguračním centru (Configuration Center), po kliknutí na tento modul

aplikace vyžaduje autentizaci. Je potřeba se přihlásit účtem admin s heslem admin. K nastavení se dostaneme v menu Systém, v záložce „Nastavení rozhraní“.

4.6.1.2 Změna administrátorských hesel

Jedním z prvních kroků při konfiguraci zařízení by měla být změna výchozích hesel přednastavených účtů „flowmon“ a „admin“. Heslo uživatele „flowmon“ je možné změnit použitím konzolové aplikace sysconfig, heslo uživatele “admin“ pak ve webové aplikaci.

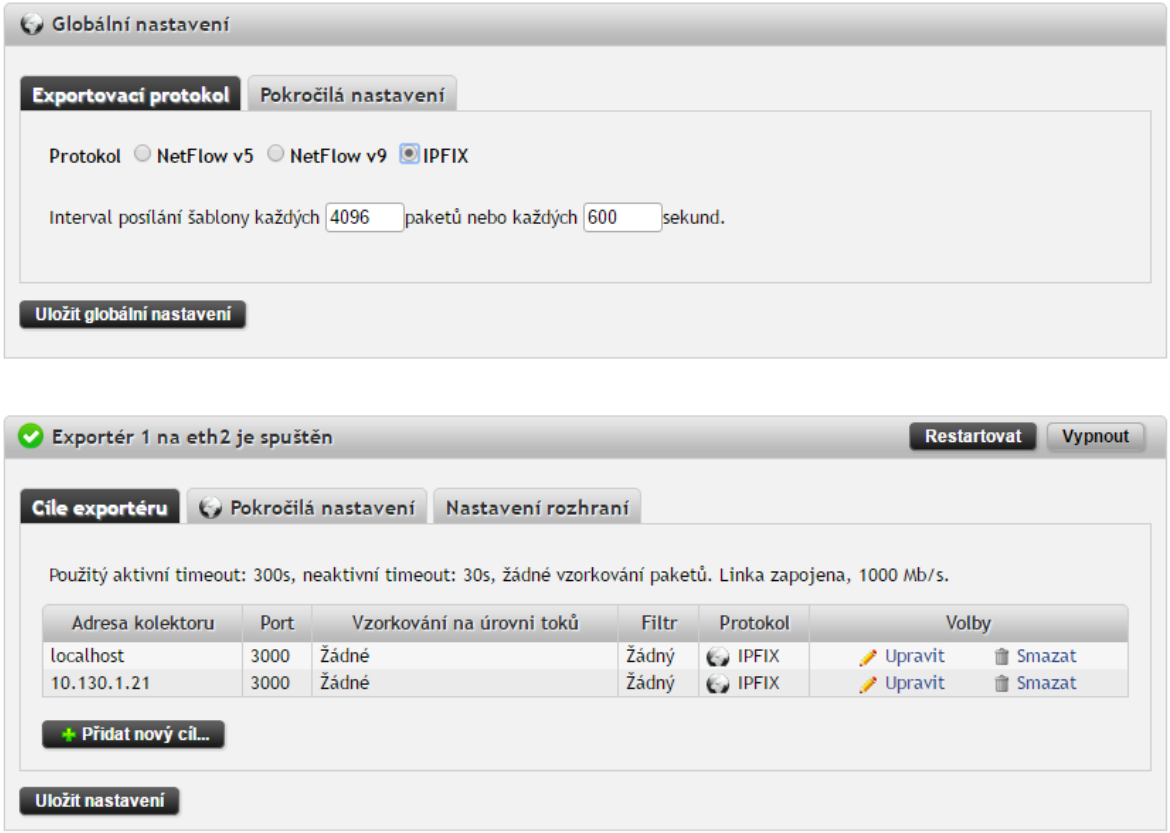
4.6.1.3 Nastavení exportérů

Nad každým monitorovacím rozhraním sondy je spuštěn jeden exportér, který zachytává všechny přicházející pakety a počítá z nich flow statistiky. Tyto statistiky jsou pak exportovány na kolektor, kde jsou zpracovány.

Toto nastavení se provede v konfiguračním centru (modul Configuration Center), menu Exportéry. U jednotlivých exportérů se nastavuje IP adresa a port kolektoru, na který chceme exporty posílat. Lze použít i vestavěný kolektor sondy zadáním adresy „localhost“ a portu 3000. Dále je možné nastavovat další parametry exportérů, a to buď jednotlivě pro každý zvlášť, nebo použitím globálních nastavení. V případě Úřadu bylo použito na všech exportérech globální nastavení.

Je možné nastavit protokol, který se pro exporty použije. V případě Úřadu byl použit protokol IPFIX, protože jak nastavovaná sonda, tak i kolektor, na který bude flow statistiky odesílat tento protokol podporují, a z rodiny NetFlow protokolů se jedná o nejnovější verzi protokolu, nabízející nejvíce možností.

NetFlow verze 9 a IPFIX jsou založeny na šablonách. Kromě samotných NetFlow dat je třeba poslat i šablonu, která definuje to, jak mají být data reprezentována. Součástí nastavení je tedy i určení frekvence zasílání této šablony. Výchozím nastavením je odesílání šablony vždy po 4096 paketech nebo po 600 sekundách (vždy to, co nastane dříve). Toto výchozí nastavení nebylo potřeba v případě Úřadu měnit.



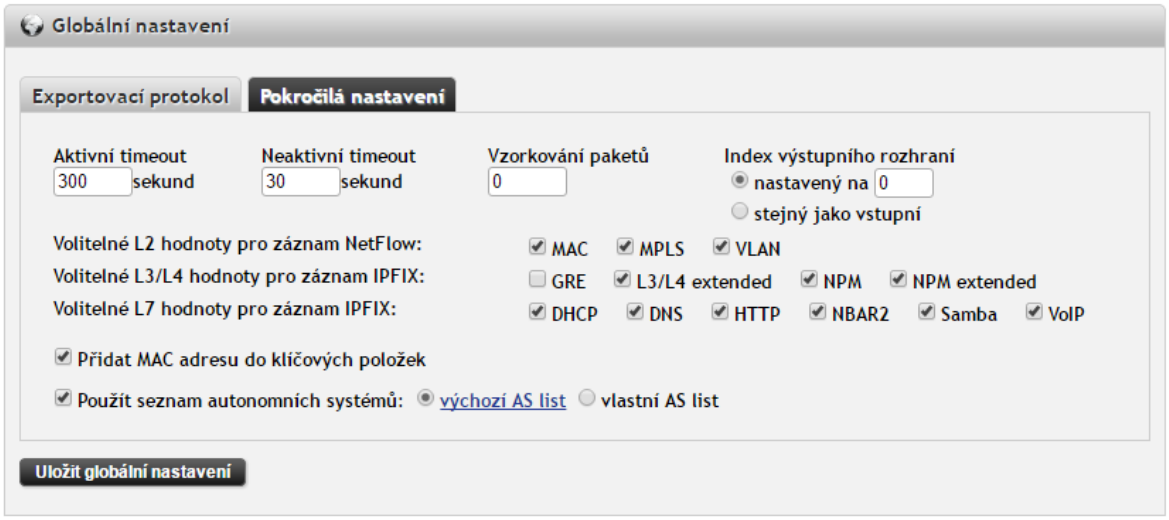
Obrázek 14 - Nastavení exportérů sondy Flowmon (vlastní zpracování)

Dále lze nastavit pokročilé možnosti. Jednou z nich je například možnost vzorkování zasílaného provozu. To je vhodné v případě, kdy potřebujeme snížit zatížení kolektoru, který nestíhá zpracovávat všechny exportované toky. K tomu v prostředí Úřadu nedochází, takže zde nebylo vzorkování nastaveno. Vzorkováním se totiž bude vyhodnocovat každý N-tý paket. To sice snižuje zátěž, ale zároveň to může zkreslit výsledky exportovaných dat.

Nastavuje se zde také tzv. aktivní a neaktivní timeout. Jde o doby, po kterých dojde k uvolnění dat o daném toku z paměti sondy a zaslání na kolektor. Výchozími hodnotami jsou 300 sekund pro aktivní timeout a 30 sekund pro neaktivní timeout. Data jsou odeslána buď po uplynutí doby neaktivního timeoutu – tedy 30 sekund po přijetí posledního paketu náležejícího k danému toku nebo pokud jde o tok, který je aktivní dlouhou dobu, po uplynutí doby aktivního timeoutu – tedy po 300 sekundách aktivity daného toku. Tyto výchozí hodnoty nebylo třeba v případě Úřadu měnit.

Volitelně lze zapnout nebo vypnout také zasílání některých atributů NetFlow/IPFIX protokolu. Z 2. síťové vrstvy (L2) jde o MAC, VLAN nebo MPLS. Pro L3 a L4 vrstvu lze

zvolit monitoring provozu v GRE tunelu, monitoring dodatečných hodnot z L3/L4 (TCP TTL, TCP SYN packet size, a TCP window size) a monitoring Network Performance metrik (NPM). Pro L7 vrstvu lze zaškrtnout volbu NBAR2, při které bude exportér provádět L7 analýzu monitorovaných paketů a zjištěné údaje exportuje s využitím polí odpovídajících standardu NBAR2. Dále lze zvolit hlubší analýzu L7 protokolů uvedených ve formuláři (DHCP, DNS, HTTP, Samba, VoIP).



Obrázek 15 - Pokročilá nastavení exportérů sondy Flowmon (vlastní zpracování)

Další nastavení, jakými jsou nastavení času a časové zóny, správa kvót, vytvoření a správa uživatelů aplikace apod. jsou stejné jako příslušná nastavení na kolektoru a budou popsána dále.

4.6.2 Konfigurace kolektoru

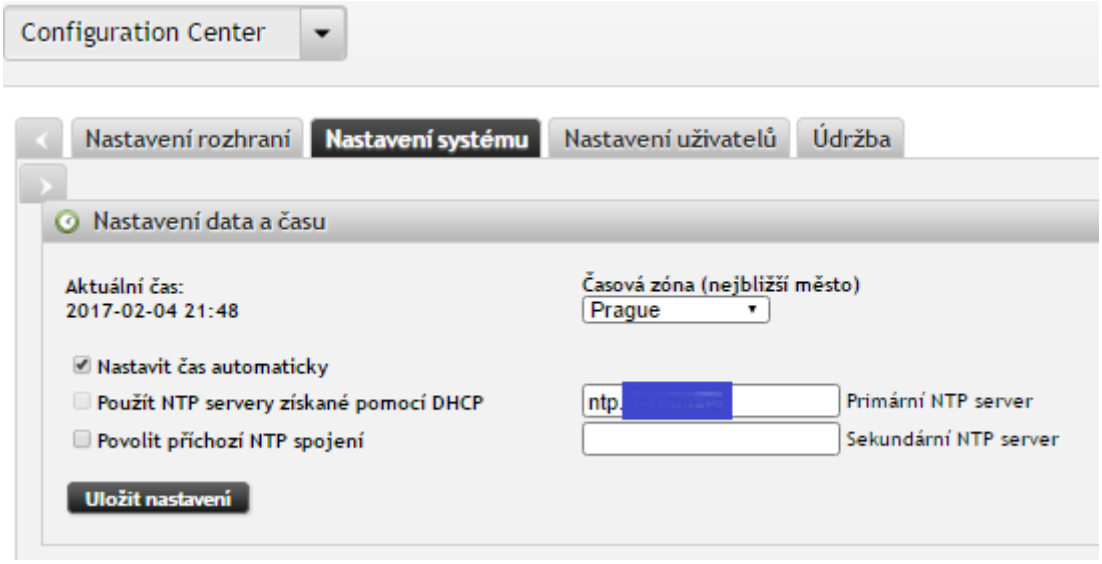
Virtuální kolektor byl nasazen do VMware prostředí Úřadu pomocí OVF šablony. Virtuální server má nastaveno 1 TB úložného prostoru pro operační systém a pro data z exportů síťového provozu, 16 GB paměti RAM a 8 jader CPU. Import do virtuálního prostředí probíhal standardním způsobem přes položku „Deploy OVF Template“ ve vSphere klientovi. Po prvním spuštění kolektoru je třeba nastavit IP adresu management portu. Provede se to přes konzoli, ke které je nutno se nejdříve autentizovat pomocí výchozího účtu flowmon. Pod tímto účtem je pak potřeba spustit pomocí příkazu sysconfig konfigurační nástroj.

V tomto nástroji pak vybereme položku Management port a v ní nastavíme zvolenou IP adresu, na které chceme mít management port dostupný. Pro tuto IP adresu je vhodné nastavit DNS záznam, abychom do nastavení kolektoru mohli přistupovat přes název a nikoli IP adresu, a také proto, že v následné konfiguraci budeme chtít nasadit interní SSL certifikát, protože komunikace s kolektorem probíhá prostřednictvím HTTPS protokolu. Zvolili jsme DNS název „flowmon-collector“. Management kolektoru je tedy v interní síti přístupný na adrese https://flowmon-collector.lan.urad.cz.

Pro první přihlášení do aplikace Flowmon kolektoru se přihlásíme pomocí výchozího účtu admin s heslem admin. Netřeba zdůrazňovat, že jedním z prvních nastavení bude změna výchozího hesla a vytvoření vlastních účtů uživatelů, kteří se budou k aplikaci Flowmon přihlašovat.

4.6.2.1 Nastavení data a času

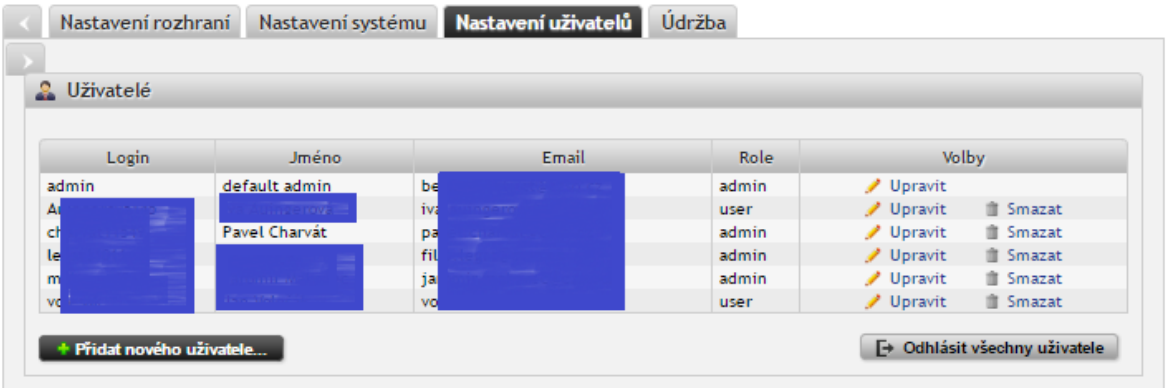
Správné nastavení času je zásadní pro správnou analýzu síťových toků, proto bylo hned na začátku provedeno nastavení času použitím interního NTP serveru. Pro správnou komunikaci NTP serveru s kolektorem je třeba, aby byl povolen síťový prostup z NTP serveru na kolektor. Protokol NTP používá UDP komunikaci na portu 123. Poté, co je tato podmínka splněna, můžeme nastavit na kolektoru adresu NTP serveru nebo serverů. Nastavena by měla být také časová zóna, v případě Úřadu „Prague“. Nastavení se provede v konfiguračním centru, menu Systém, karta Nastavení systému.



Obrázek 16 - Nastavení času a časové zóny kolektoru Flowmon (vlastní zpracování)

4.6.2.2 Změna hesla admin účtu a vytvoření uživatelských účtů

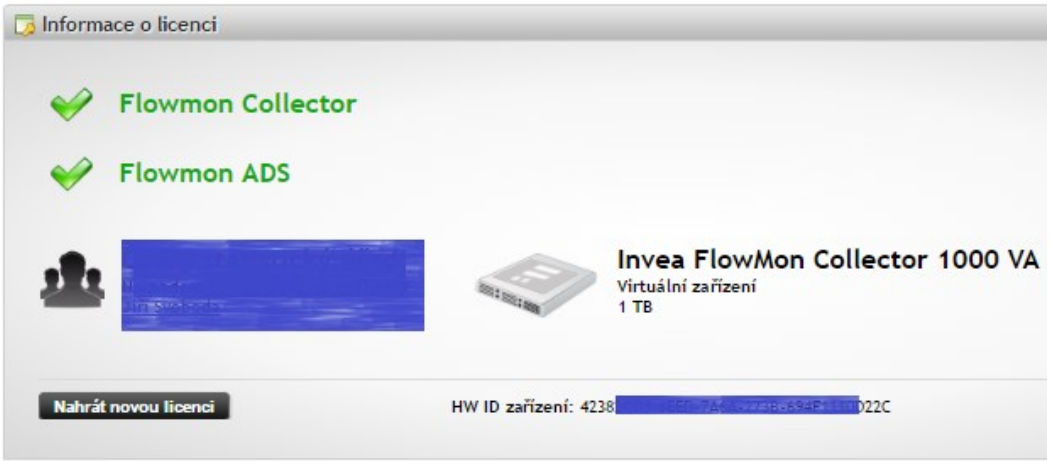
Z bezpečnostních důvodů je zásadní změnit co nejdříve výchozí heslo původního administrátorského účtu. Toto nastavení se provede v konfiguračním centru (modul Configuration Center), menu Systém, karta Nastavení uživatelů. Na tomto místě je také možné přidat další uživatele aplikace. Vzhledem k tomu, že best practice je používat účty, které jednoznačně identifikují činnost konkrétního uživatele, místo toho, aby byli všichni uživatelé „schováni“ za jednotný účet admin, byly rovnou vytvořeny účty uživatelům aplikace, včetně přiřazení příslušných oprávnění.



Obrázek 17 - Nastavení uživatelů v aplikaci Flowmon (vlastní zpracování)

4.6.2.3 Vložení licence

Aby systém správně pracoval, je třeba vložit platnou licenci. Toto nastavení se provede v konfiguračním centru, menu Licence. Prostřednictvím tlačítka „Nahrát novou licenci“ se vyvolá systémové okno, ve kterém je potřeba vybrat příslušný licenční soubor.

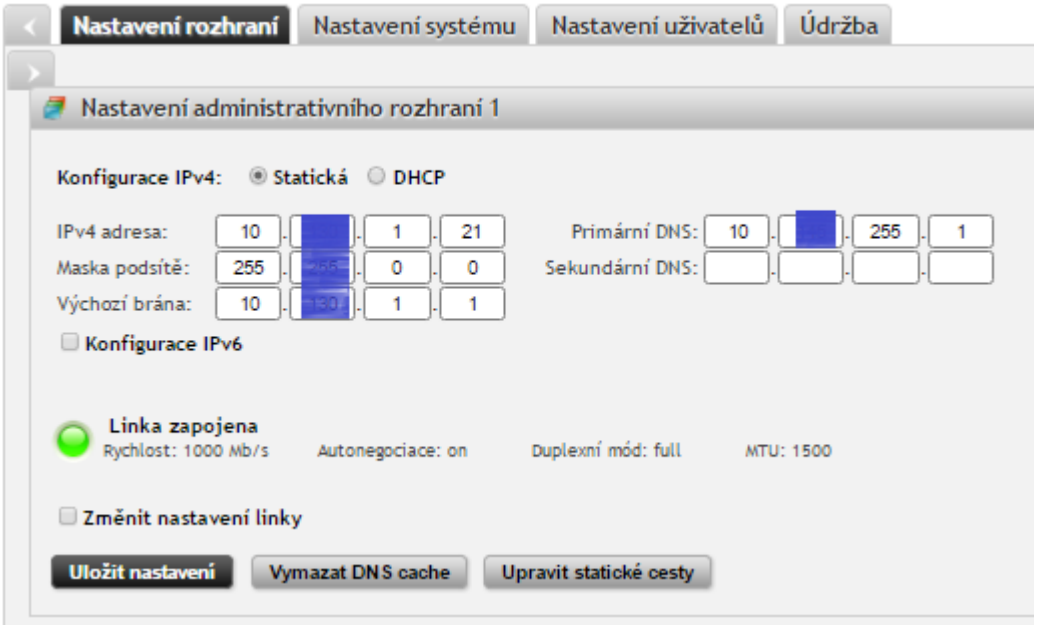


Obrázek 18 - Nastavení licence v aplikaci Flowmon (vlastní zpracování)

4.6.2.4 Nastavení IP adresy a DNS překladu

Toto nastavení se provede v konfiguračním centru (modul Configuration Center), menu Systém, karta Nastavení rozhraní. Kromě IP adresy kolektoru, je třeba nastavit také příslušnou masku sítě a výchozí bránu. Jde o alternativu nastavení IP adresy přes konzoli pomocí aplikace sysconfig. Jelikož už jsme adresu nastavili právě touto cestou, ve webové aplikaci už je přednastavená námi zvolená adresa.

Kvůli překladu IP adres na názvy je pak třeba nastavit také adresu DNS serveru, což se provádí také zde. K tomu, aby byl kolektor schopen využívat služeb DNS serveru, je nutný síťový prostup přes UDP na port 53.



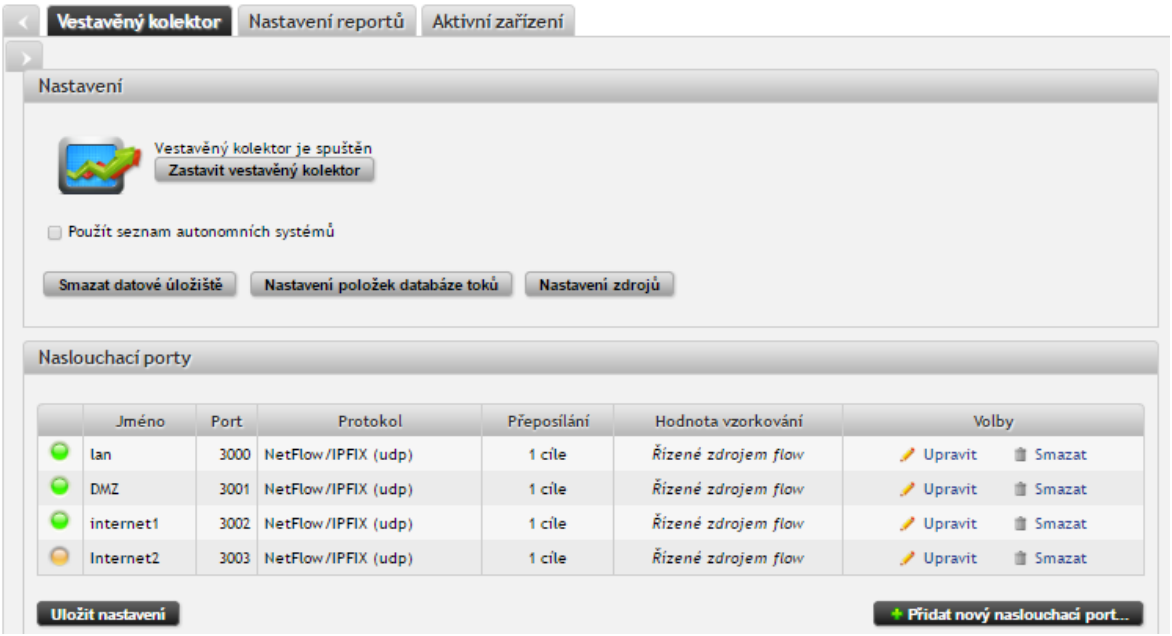
Obrázek 19 - Nastavení IP adresy kolektoru Flowmon (vlastní zpracování)

4.6.2.5 Nastavení zdrojů NetFlow

K tomu, aby kolektor měl co zpracovávat, musí být nakonfigurovány zdroje, ze kterých mu budou chodit exporty síťového provozu. Toto nastavení se provede v konfiguračním centru, menu Nastavení FMC, na kartě Vestavěný kolektor. Zde se u každého zdroje nastaví jeho název, port, který bude naslouchat pro data z tohoto zdroje, protokol exportů (NetFlow/IPFIX nebo sFlow) a síťový protokol (TCP/UDP). Případně je možné nastavit i vzorkování.

Zde se také nastavuje, jaké položky se budou ukládat do databáze toků. Tedy položky, se kterými je pak možné pracovat ve Flowmon Monitoring Centru. Položky, které zde vybereme, musí být zasílány také exportéry, aby je bylo možné uložit do databáze. Platí, že čím více položek vybereme, tím více místa je potřeba k jejich uložení. Je vhodné vybírat ty, které můžeme reálně využít. Samozřejmostí jsou HTTP fields, DHCP a DNS se hodí pro diagnostiku přidělování a překlad IP adres. Pro měření výkonových statistik síťových toků se také hodí NMP metriky. Co je možné vypnout v případě Úřadu, jsou VoIP položky, protože tuto komunikaci Úřad momentálně neprovozuje.

Předpokladem správného fungování nastavených zdrojů je opět zajištěný síťový prostup na daných portech a daném síťovém protokolu. Také je potřeba správně nakonfigurovat exportéry na sondách (viz popis nastavení sondy).



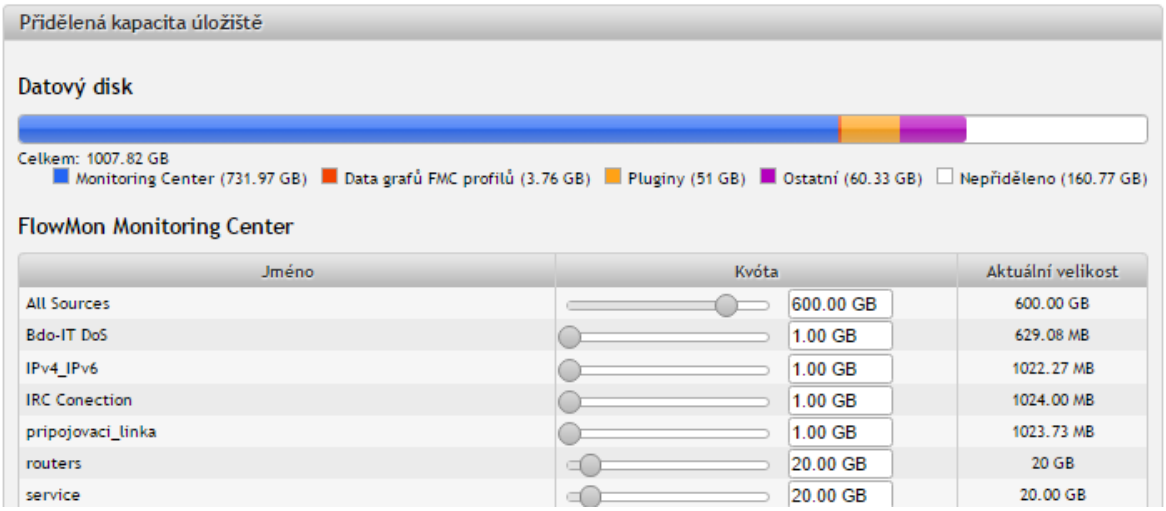
Obrázek 20 - Nastavení zdrojů NetFlow na kolektoru Flowmon (vlastní zpracování)

4.6.2.6 Nastavení kvót

Protože je na kolektoru omezené datové úložiště, zatímco síťový tok a exporty z něj jsou kontinuální, je třeba nastavit kvóty jednotlivým zdrojům, reálným profilům (budou detailněji popsány níže) a doinstalovaným pluginům. Ve chvíli, kdy zdroj (příp. profil nebo plugin) zaplní na úložišti přidělenou kvótu, začnou se mazat nejstarší data daného zdroje. Na správném nastavení kvót tedy závisí retenční doba nachytaných dat. VKB předepisuje

minimálně tříměsíční retenční dobu u IS spadajících pod ZKB. V teoretické části jsem popsal, že 3 měsíce je v praxi příliš krátká doba. Často je potřeba při řešení bezpečnostních událostí analyzovat data, která jsou starší, než 3 měsíce. Kvóty je nutno nastavovat podle priority zdroje, množství dat zdroje a velikosti dostupného úložného prostoru na kolektoru.

Toto nastavení se provede v konfiguračním centru, menu Správa kvót.



Obrázek 21 - Nastavení kvót na kolektoru Flowmon (vlastní zpracování)

4.6.2.7 Iniciace databáze kolektoru

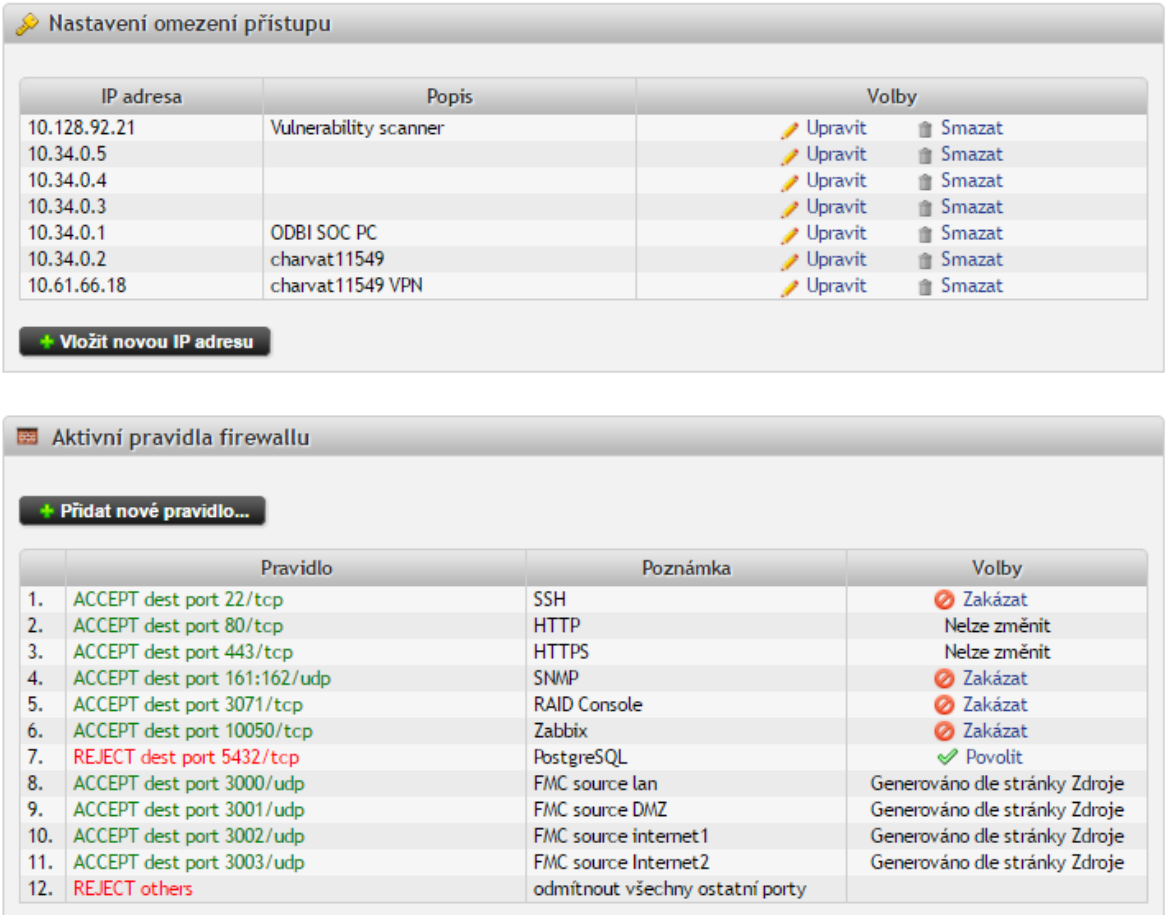
Iniciaci databáze je vhodné provést po základním nastavení. Při inicializaci dojde ke smazání všech NetFlow dat z databáze.

Toto nastavení se provede v konfiguračním centru (modul Configuration Center), menu Nastavení FMC, tlačítkem Smazat datové úložiště.

4.6.2.8 Nastavení vzdáleného přístupu

Z bezpečnostních důvodů je dobré omezit přístup k aplikaci nejen prostřednictvím přihlašovacích účtů oprávněných uživatelů, ale také pomocí IP adres, ze kterých se do aplikace mohou přihlásit. Současně je žádoucí nastavit pravidla firewallu tak, aby procházela pouze požadovaná komunikace a nežádoucí komunikace byla zablokována. K tomuto účelu slouží nastavení „Vzdálený přístup“ v konfiguračním centru. Zde jsou definovány jak IP adresy, ze kterých je povoleno se připojovat do webové aplikace kolektoru, tak pravidla firewallu filtrující příchozí komunikaci.

V případě Úřadu byly povoleny vstupy správcům aplikace kolektoru z jejich přidělených adres. Pravidla firewallu byla ponechána v podstatě na výchozích nastaveních.



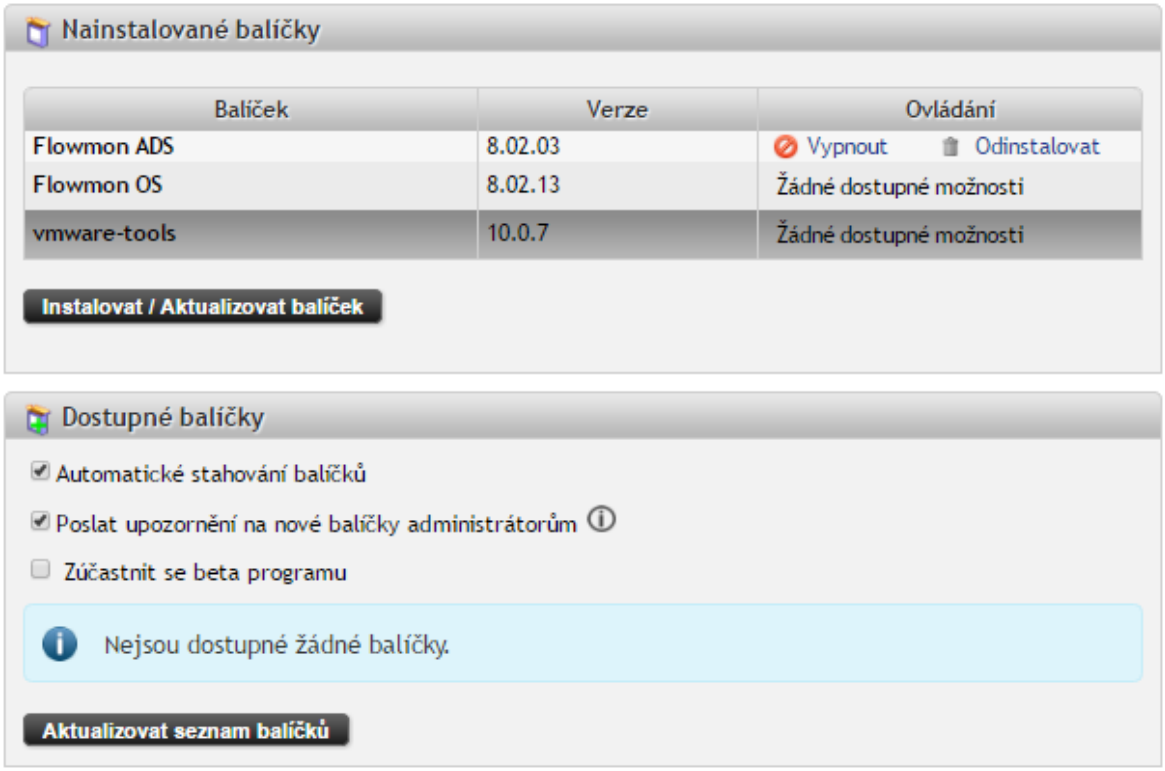
Obrázek 22 - Nastavení vzdáleného přístupu na kolektoru Flowmon (vlastní zpracování)

4.6.2.9 Instalace ADS modulu a aktualizace verzí

Flowmon Anomaly Detection System (ADS) je systém detekce anomálií a nežádoucích vzorů chování v síti založený na analýze datových toků v síti. Jeho hlavním úkolem je zvýšení bezpečnosti dané sítě. Hlavní výhodu proti běžným IDS systémům představuje orientace na celkové chování zařízení na síti, což umožňuje reagovat na dosud neznámé nebo specifické hrozby, pro které není dostupná signatura. Instalace balíčku, stejně jako instalace případných jiných pluginů (26) (27) se provádí v konfiguračním centru, menu Verze pomocí tlačítka „Instalovat / Aktualizovat balíček“.

Jak už název napovídá, kromě instalace nových pluginů slouží tato stránka i pro aktualizaci těch současných. V prostředí Úřadu byla nastavena možnost automatického

stahování aktualizací (jsou stahovány, ale nejsou automaticky instalovány), současně je nastaveno odeslání informace o nové verzi skupině administrátorů prostřednictvím informačního e-mailu. Skupinou administrátorů se rozumí všichni vytvoření uživatelé v roli admin. Je zde také možnost zúčastnit se beta programu. Úřad ale preferuje stabilní verze, proto tuto možnost nevyužívá.



Obrázek 23 - Nastavení aktualizací kolektoru Flowmon (vlastní zpracování)

4.6.3 Nastavení profilů ve Flowmon Monitoring Center

Základním modulem Flowmonu je Flowmon Monitoring Center (FMC). V tomto modulu je možné vybráním časového rozsahu a nastavením filtrů získat podrobné i agregované údaje o síťovém provozu.

Některé pohledy na síťové prostředí je potřeba sledovat opakovaně, proto se v takových případech hodí mít takový pohled předpřipravený. Někdy je zase v rámci šetření bezpečnostního incidentu potřeba opakovaně sledovat síťovou aktivitu určitého aktiva a mít tedy předpřipravený pohled na toto aktivum. Jindy je v rámci analýzy bezpečnostních událostí důležitý i pohled do minulosti. K těmto účelům slouží profily.

Profily představují specifický pohled na flow data. Jsou definovány jménem, rodičovským profilem, typem a filtry.

V případě Úřadu, který má několik krajských poboček, bylo například vhodné vytvořit si profily filtrující přehled síťových toků na jednotlivých krajích. Tyto filtry jsou vytvořeny velmi jednoduše tak, že z celkového provozu na síti Úřadu je vyfiltrován provoz, který pochází ze síťového rozsahu přiděleného aktivům v daném kraji. Profil tedy vychází z rodičovského profilu „All Sources“, který v sobě zahrnuje veškeré nachytané síťové toky. V každém krajském profilu jsou pak vytvořeny dva kanály. Jeden kanál zobrazuje upload, tedy komunikaci z kraje směrem do ústředí, a druhý kanál zobrazuje download, neboli komunikaci z ústředí, směřující na daný kraj. Oba kanály je vhodné barevně odlišit. Kód filtrů pro upload a download kanál jsou následovné:

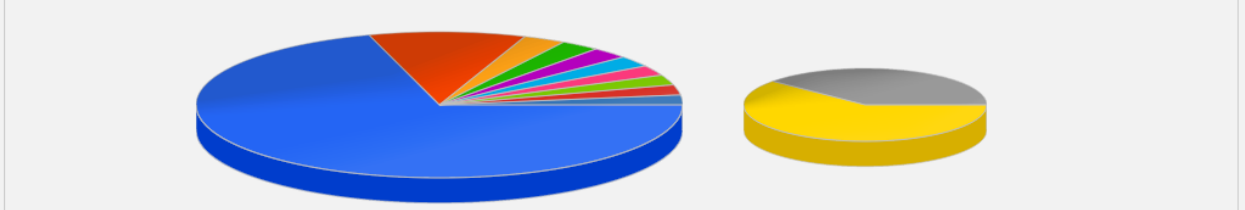
Upload: ***src net 10.10.0.0/16 or src net 10.110.0.0/16***

Download: ***dst net 10.10.0.0/16 or dst net 10.110.0.0/16***

Je zřejmé, že filtry jsou jednoduché a vzájemně analogické. Daný kraj má pro svá aktiva připojené do sítě dedikované dva síťové rozsahy. V upload filtru nás zajímá komunikace, která pochází z daného kraje. IP adresy tedy vystupují v síťovém toku jako zdrojové (src). U download filtru nás naopak zajímají síťové toky, které směřují na dedikované síťové rozsahy. Krajské IP adresy zde vystupují jako cílové (dst).

Vzhledem k tomu, že rozdělením komunikace na všechny krajské pobočky bychom zbytečně duplikovali velké množství uložených NetFlow dat, byly tyto krajské profily vytvořeny jako tzv. shadow profily. Shadow profily si ve skutečnosti neukládají vyfiltrovaná NetFlow data. Místo toho si data při každém jejich použití znovu za vybraný časový úsek vyfiltrují z rodičovského (tedy v tomto případě z celkového) provozu. Výhoda je zřejmá, tyto profily nezaplňují zbytečně úložný prostor. Nevýhodou je naopak pomalejší zpracování dat a závislost na datech rodičovského profilu. Jakmile rodičovský profil naplní přidělenou kvótu, začnou se odmazávat jeho nejstarší data. Pro shadow profil, který je na něm závislý, to znamená, že ani pro něj tato stará odmazaná data nebudou dostupná. Jelikož cílem těchto profilů je mít kdykoli aktuální pohled na síťové toky vybraného kraje, jsou tyto profily vytvořeny jako neukončené.

Tyto profily se pak hodí například k řešení provozních problémů na síti. Jedním z takových případů, ve kterých našel krajský profil uplatnění, bylo řešení problému s pomalou odezvou internetového provozu na klientských stanicích uživatelů, která často vyústila i k hlášení o nedostupnosti webu. Krajské pracoviště je připojeno prostřednictvím VPN do ústředí Úřadu. Přes proxy server v ústředí pak přistupují pracovníci na internet. Podezření na problémovou komunikaci padlo na nedostatečnou kapacitu krajské linky. Jednoduchým zobrazením profilu síťových toků daného kraje bylo toto podezření potvrzeno. Kapacita linky byla v inkriminovanou dobu opravdu kompletně vytížena. Druhým krokem bylo pátrání po příčině tohoto zatížení. K tomu stačilo jednoduše zvolit část časového rozsahu, během kterého k tomuto problému docházelo, a zanalyzovat, která zařízení v něm intenzivně komunikovala.



KrajskePobocky/Ceske Budejovice 30s
2017-01-25 13:40:00 - 2017-01-25 15:01:00
Top 10 IP adresa řazeno dle bajtů

Barva	Počáteční čas	Trvání	IP adresa	Toky	Pakety na vstupu	Bajty na vstupu	Paketů za sekundu	Bitů za sekundu	Bajtů na paket
1	2017-01-25 13:40:02	1 h, 20 m, 56.340 s	zen02 [redacted]	2.78 K (3.4%)	8.87 M (80.7%)	7.38 GB (86.1%)	1825	13050688	893
2	2017-01-25 13:40:00	1 h, 21 m, 0.088 s	swgi01 [redacted]	57.39 K (69.4%)	1.77 M (16.1%)	1.09 GB (12.8%)	364	1933147	663
3	2017-01-25 13:40:05	1 h, 19 m, 14.486 s	10.110.0.25	5.82 K (7.0%)	393.06 K (3.6%)	301.44 MB (3.4%)	82	531840	804
4	2017-01-25 13:40:02	1 h, 16 m, 46.294 s	10.110.0.62	2.07 K (2.5%)	346.7 K (3.2%)	279.61 MB (3.2%)	75	509206	845
5	2017-01-25 13:40:01	1 h, 18 m, 43.992 s	10.110.0.38	4.01 K (4.8%)	346.69 K (3.2%)	268.47 MB (3.1%)	73	476733	811
6	2017-01-25 13:40:15	1 h, 15 m, 33.113 s	10.110.0.59	3.64 K (4.4%)	336.65 K (3.1%)	261.47 MB (3.0%)	74	483858	814
7	2017-01-25 13:40:33	1 h, 19 m, 5.519 s	10.110.0.73	2.52 K (3.0%)	306.19 K (2.8%)	242.56 MB (2.8%)	64	428774	830

Obrázek 24 - Analýza vytížení krajské linky (vlastní zpracování)

Jako původce problematické komunikace byl identifikován server, který má na starost distribuci software na pracovní stanice. Ukázalo se, že na klientské stanice uživatelů se distribuovaly aplikační balíčky ze serveru v ústředí, místo toho, aby byly aplikace distribuovány ze serveru v daném kraji. Problém byl okamžitě nahlášen IT podpoře a rychle vyřešen.

Dalším příkladem vhodného použití profilů může být upozornění NBÚ, které zaslalo seznam více než 20.000 IP adres identifikovaných jako výstupní uzly systému TOR, ze kterých byla vedena nežádoucí komunikace. Úřad měl prověřit, zda z některých těchto adres šla závadná komunikace i na jeho aktiva. Agregací provozu zachyceného sondou v období ledna 2017, byl vytvořen seznam IP jedinečných adres, se kterými komunikovala zařízení Úřadu, těch bylo více než 5 milionů. Poté byly oba seznamy porovnány a bylo zjištěno, že za měsíc leden komunikovalo nějakým způsobem se zařízeními Úřadu 979 IP adres ze seznamu výstupních uzlů TOR. Proto, abych zjistil, o jakou komunikaci přesně v případě těchto identifikovaných adres šlo, vytvořil jsem ukončený profil s filtry pro příchozí i odchozí provoz z těchto IP adres. Filtry vypadaly zhruba takto:

Z TORu: ***src ip in [100.15.101.233 100.33.42.78 100.37.177.183 100.38.62.241 100.4.51.203 101.100.141.73 101.55.124.96 …]***

Do TORu: ***dst ip in [100.15.101.233 100.33.42.78 100.37.177.183 100.38.62.241 100.4.51.203 101.100.141.73 101.55.124.96 …]***

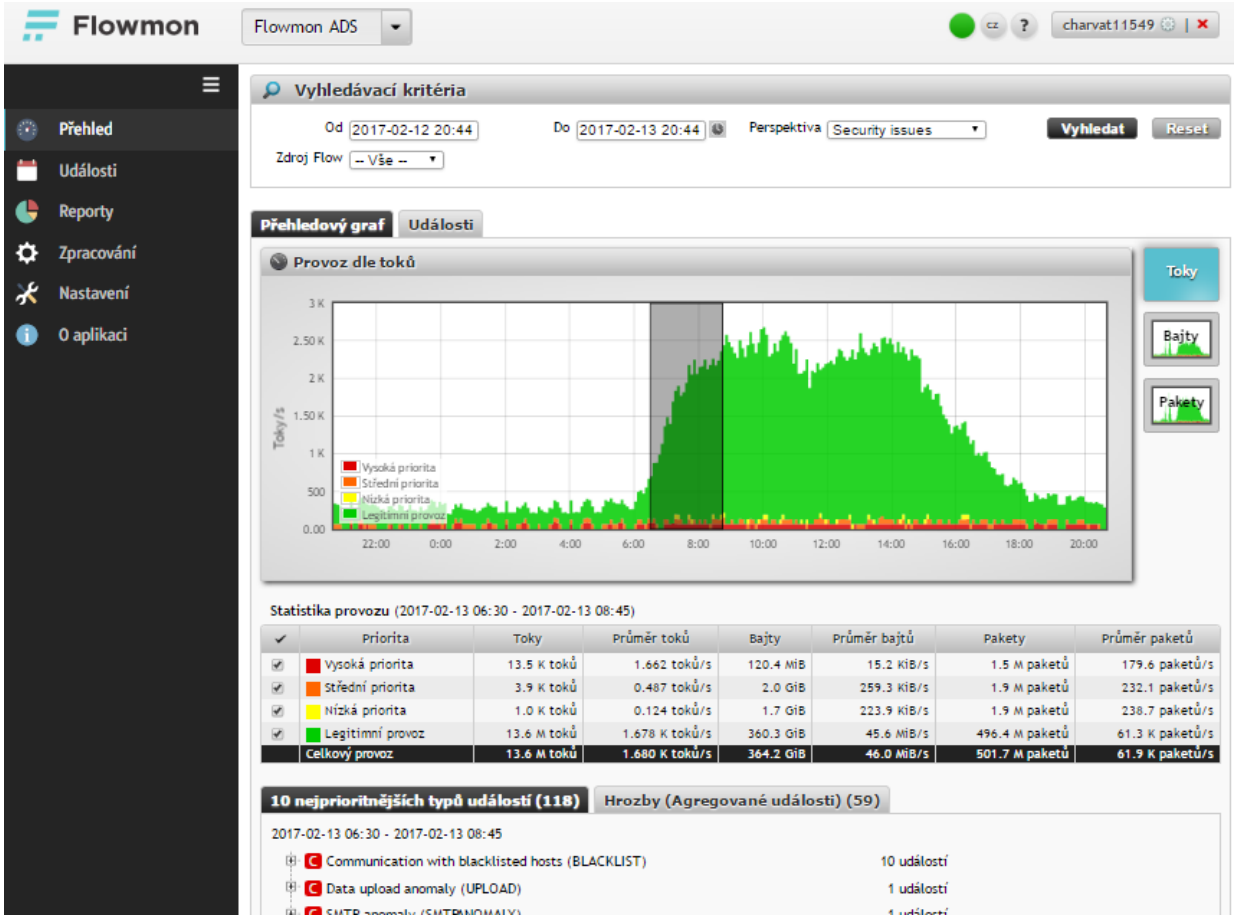
Protože takové filtry byly velmi obsáhlé i pro identifikovaných 979 IP adres a Úřad potřeboval sledovat, zda v budoucnu nebude cílem komunikace z jakékoli ze zaslaných více než 20.000 IP adres, hledali jsme elegantnější řešení. Po konzultaci s firmou Flowmon Networks jsme zjistili, že existuje ještě jedno řešení, které není obsaženo v běžné dokumentaci, ale lze použít na použití takovýchto rozsáhlých blacklistových seznamů. Seznam adres lze vést v textovém souboru uloženém na kolektoru a ve filtru je možné se na tento soubor odkázat. Konstrukce filtru je pak následující.

src ip in [@include /home/flowmon/tor_nods_filtr.txt]

Následně bylo potřeba data vyfiltrovaná v profilu analyzovat. V první řadě jsem zjišťoval, na které porty komunikace směřovala. Následně také jaká byla odezva aktiv Úřadu. Zásadní bylo především to, jestli a případně jakým způsobem, odpovídala zařízení Úřadu na SSH komunikaci a na pokusy o přihlášení pomocí RDP protokolu. V žádném z případů nebyla identifikována nežádoucí aktivita.

4.6.4 Konfigurace a práce s ADS pluginem

Flowmon Monitoring Center a nastavené profily jsou velmi cenným prostředkem pro monitorování síťových toků. Ještě cennější prostředek pro boj proti kybernetickým hrozbám je však plugin Flowmon Anomaly Detection System (ADS). Zatímco FMC se hodí především na ad hoc analýzu síťových toků nebo na profilování filtrovaných částí síťových toků, ADS prostřednictvím přednastavených korelačních pravidel umí upozornit na neočekávané odchylky síťového provozu. Anomální jevy v síti jsou často projevy působení škodlivého kódu, kybernetických útoků, nevhodného chování uživatelů nebo provozních problémů. Neocenitelným pomocníkem je především v boji proti APT a neznámému malware. K tomu, aby byly výsledky detekce ADS modulu užitečné, je potřeba ho vhodně nastavit a také dlouhodobě udržovat.



Obrázek 25 - Flowmon ADS - náhled na uživatelské rozhraní (vlastní zpracování)

Nejprve je třeba provést základní nastavení. To se provádí v menu „Nastavení“ v ADS pluginů. Nastavuje se, jak dlouho budou uložena data pro vykreslení grafů ADS.

V případě Úřadu bylo ponecháno výchozí nastavení 183 dnů, což představuje data za půl roku. V nastavení databáze nebylo potřeba žádné pokročilé nastavení ani zapínání metod pro rychlejší zpracování dat nebo použití filtrů. Provoz o velikosti toho, který je na Úřadě, není tak silný, aby bylo potřeba tyto speciální funkce zapínat. Jejich zapnutí by naopak mohlo zpracování dat zpomalit.

V nastavení aplikace v případě Úřadu také nebylo potřeba nic zásadního nastavovat. Jediné nastavení, které zde stojí za trochu pozornosti je nastavení maximálního počtu vláken, která mohou být aplikací využita. Z přidělených 8 CPU může ADS využít maximálně 6.

V nastavení konfigurace lze zvolit předdefinovanou šablonu. Vybírat lze ze 3 základních šablon – malá firma (do 500 zařízení), velká firma (více než 500 zařízení) a Internet service provider. V případě Úřadu byla zvolena šablona pro velkou firmu, následně ale musela být dokonfigurována. V nastavení konfigurace je kdykoli možné smazat všechna uživatelská data, DNS cache nebo uvést zařízení do továrního nastavení.

Dále je nutné nastavit zdroje dat. V případě Úřadu je použita jedna sonda, takže by se mohlo zdát, že vše vyřešíme nastavením jednoho zdroje dat do ADS. V zásadě by to tak mohlo být, kdyby nebylo potřeba korelovat toky kvůli tomu, že klienti LAN Úřadu přistupují na internet pomocí proxy serveru. Primární zdroj dat tedy nastavíme tak, aby používal informace o proxy, což je důležité pro funkci korelace provozu před a za proxy serverem. Protože ale jednou z metod ADS je metoda DIRINET, která zachytává zařízení přistupující přímo do Internetu, potřebuje vycházet ze zdroje dat, který není zkreslený proxy korelací. Ta totiž interpretuje komunikaci klient -> proxy -> Internet jako klient -> Internet, takže jakékoli takto interpretovaná komunikace by se tvářila jako přímé spojení do Internetu. Pro tuto metodu tedy nastavíme zdroj dat bez použití proxy.

Nastavení zdroje dat spočívá v určení jména (v případě Úřadu to bude LAN-proxy, resp. pro druhý zdroj LAN2). Dále vybereme kanály daného zdroje, které mají být sledovány. V případě Úřadu to u obou zdrojů budou všechny 3 kanály představující aktivní monitorovací porty sondy – LAN, DMZ a Internet. U obou zdrojů také nastavíme funkci deduplikace, která zajistí, že toky přijaté jedním zdrojem dat nebudou obsahovat duplicitní toky. Ponecháme aktivní také funkci kontroly času, která zajistí, že toky s časovou

známkou lišící se od systémového času kolektoru o více než půl hodiny budou zahozeny. U zdroje LAN-Proxy navíc nastavíme parametry proxy serveru – interní IP adresu a port a externí IP (ta je v případě Úřadu shodná s interní). Samplovací poměr necháme v obou případech na hodnotě 1:1 – nebudeme tedy používat vzorkování ani na jednom ze zdrojů. Nakonec přenastavíme výchozí parametry proxy korelace. V praxi se nám osvědčilo hodnotu tolerance objemu přenesených dat přenastavit z hodnoty 100 na 95 a hodnoty „Maximální rozdíl trvání požadavku“ a „Maximální rozdíl trvání odpovědi“ obě shodně na 500 (ms). Na závěr nastavení proxy korelace byl nastaven parametr proxy klienti na skupinu všech potenciálních klientů přistupujících přes proxy, tedy v případě Úřadu kompletní rozsah vnitřních IP adres s výjimkou právě adresy proxy serveru.

4.6.4.1 Konfigurace filtrů

Správné nastavení zdrojů dat síťových toků spolu s logickou topologií sítě má vliv na výsledky detekčních metod a celkovou vypovídající schopnost pluginu ADS. Základní rozlišovanou entitou v pluginu je IP adresa. Filtry představují pojmenovaná logická seskupení libovolných IP adres. Každý filtr má unikátní jméno, může být navázán na definované zdroje dat síťových toků a zahrnuje libovolný počet rozsahů IP adres. Filtry jsou dále využívány detekčními metodami pro omezení rozsahu adres relevantních pro každou detekční metodu. (20, s. 21)

Existují dva typy filtrů, atomické a relační. Atomické filtry jsou definovány přímo IP adresami nebo jejich rozsahy, s těmi si vystačíme ve většině případů. Relační filtry jsou definované jako závislosti na jiných filtrech (např. inverze, sjednocení nebo rozdíl filtrů). IP adresy do filtrů (atomických) je možno definovat několika způsoby. Buď zadáním síťové adresy a masky ve formátu CIDR, zadáním rozsahu IP adres nebo výčtem IP adres. IPv4 adresy mohou obsahovat wildcard znaky (vždy ale maximálně nahrazující jeden oktet adresy).

V první řadě je potřeba nastavit rozsah vnitřní sítě (LAN). V korporátním prostředí to často bývají, a stejně je to i v případě Úřadu, následující tři rozsahy adres:

10.0.0.0 – 10.255.255.255
192.168.0.0 – 192.168.255.255
172.16.0.0 – 172.31.255.255

Dále je vhodné nastavit adresy serverů, které pro síť zprostředkovávají některé základní služby typu SMTP, DNS, NTP nebo DHCP. Jde o to, že tyto servery mají specifické chování, které by různé detekční metody například u klientských stanic vyhodnotily jako podezřelé. Tyto filtry se pak právě v nastavení detekčních metod často nastavují mezi výjimky.

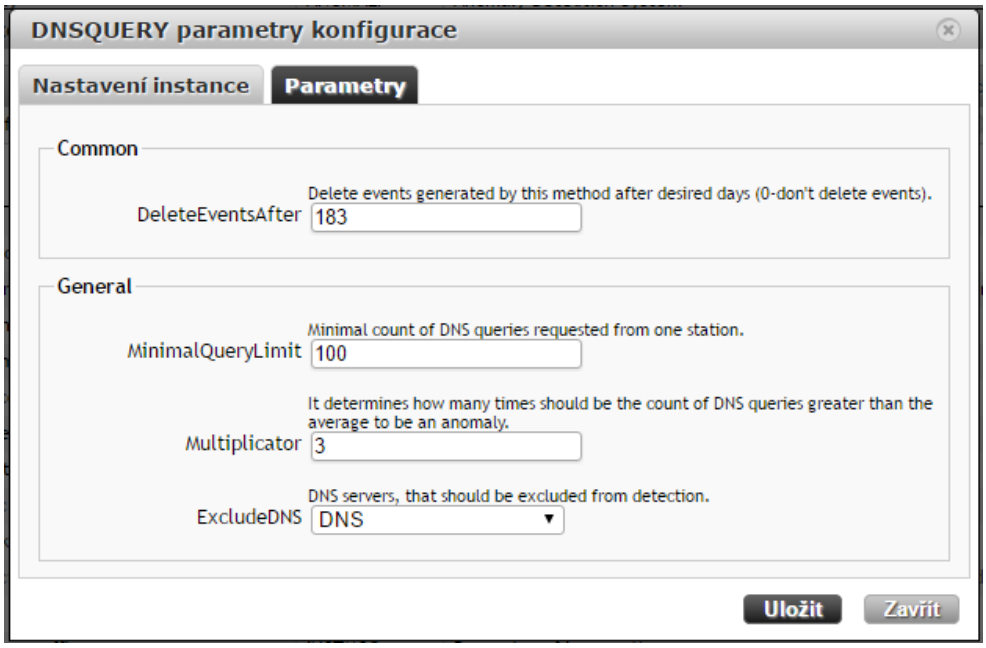
✓	Jméno	Rozsah IP adres	Poznámka
☐	DHCP	10.1.2.17	
☐	DIRINET_vyjimky	10.145.31.30 192.168.199.32 192.168.199.33 10.145.31.10 10.145.31.11	 sis-pp-dnsi01 sis-pp-dnsi02
☐	DMZ	192.168.199.0 - 192.168.199.255	
☐	DNS	10.1.2.17 10.1.1.30 10.145.255.1 10.146.255.1 10.145.31.10 10.145.31.11 192.168.199.2 10.195.1.250	abdnsdhcp abbman DNS koncova zarizeni DNS servery sis-pp-dnsi01 sis-pp-dnsi02 gatekeeper.czso.cz - pro klienty z internetu swg-man.ab.czso.cz
☐	File Servery	10.[10-21].10.1 10.[10-21].10.2	
☐	Firewall Checkpoint	10.3.1.[1-2]	Stará DMZ
☐	ICMP_vyjimky	10.32.0.1 10.128.1.15 10.128.1.61 10.128.1.20	 hp-sim - kontroluje dostupnost serverů
☐	KrajskeDNS	10.[10-21].10.5	

Obrázek 26 - ukázka nastavení filtrů v ADS (vlastní zpracování)

4.6.4.2 Konfigurace detekčních metod

Detekční metody jsou předdefinovány už ve výchozím nastavení. Je jich celkem 45 a jejich konfigurace spočívá především v tom vybrat si, které budou zapnuté a které vypnuté. Není asi potřeba zdůrazňovat, že vypnout můžeme detekční metody, které pro danou síť nemá smysl používat. Například, pokud na síti neprobíhá IP telefonie, můžeme mít vypnuté metody, které se týkají SIP protokolu, apod. Seznam a popis detekčních metod je uveden v uživatelské příručce pluginů ADS. (20, s. 36-83) K efektivnímu nastavení ADS je potřeba tyto metody znát alespoň z hlediska jejich účelu, aby bylo jasné, které jsou pro danou síť užitečné, a které by naopak jen bezdůvodně spotřebovávaly přidělené systémové prostředky nebo komplikovaly výstupy. U zapnutých detekčních metod je pak vhodné znát je až na úroveň vlastností a určení jednotlivých parametrů. Je to především kvůli případnému ladění metod.

Samotné parametry jednotlivých detekčních metod ale není příliš potřeba měnit. Alespoň ne hned při zavádění ADS. Ne, že by to nebylo možné, každá metoda má několik parametrů, které je možné nastavit, ale jejich výchozí hodnoty jsou nastaveny vcelku rozumně a je záhodno je měnit pouze ve chvíli, kdy k tomu vyvstane z provozu nějaký důvod. Některé parametry ale potřeba nastavit je. Typicky jde o nastavení filtrů s adresami serverů, které představují výjimky z běžných detekčních pravidel. Například v detekční metodě DNSQUERY je kromě základních parametrů, které definují pravidla detekce, potřeba zadat, že DNS servery má tato metoda vyloučit z detekce. Toho se docílí právě zadáním filtru, který obsahuje seznam DNS serverů v dané síti.



Obrázek 27 - Nastavení detekční metody DNSQUERY (vlastní zpracování)

V běžném provozu se relativně často vyskytne situace, která aktivuje nějaká detekční pravidla, ale po jejím prověření dospějeme k závěru, že se nejedná o bezpečnostní ani provozní incident. V takových případech (pokud nelze vhodně a bez ztráty detekčních schopností upravit příslušnou detekční metodu) je vhodné takovou událost nebo skupinu událostí označit jako tzv. false positive. Například víme-li, že nějaký server jednou za týden posílá administrátorům e-mailové reporty o provozu, jejichž množství aktivuje detekční metodu SMTPANOMALY, cílem které je detekovat potenciální zdroje spamu, můžeme nastavit výjimku, která říká, že pokud odchází e-mailové zprávy z tohoto serveru a jsou přes interní SMTP server, je to v pořádku a jedná se jen o planý poplach. Můžeme

dokonce nastavit časové omezení takového pravidla. Pokud víme, že tyto reporty se rozesílají každou neděli kolem 8. hodiny večer, můžeme takovou komunikaci označit jako false positive pouze, pokud k ní dojde v neděli 20:00 +/- 30 minut. Pokud by byla stejná detekční metoda aktivována třeba ve středu, událost by byla nahlášena jako každá jiná.

4.7 SIEM

Jako nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí, využívá Úřad SIEM od společnosti Extreme Networks. Jde o verzi SIEMu QRadar od firmy IBM. V Úřadu je nasazen prostřednictvím appliance DSIMBA7-SE s licencí pro 1000 EPS[31] a 25000 FPM[32]. Zařízení disponuje 1 management síťovým portem pro správu a 3 monitorovacími porty, kterými je možno přivést do něj síťový provoz určený pro analýzu toků. Jde tedy o podobný princip jako u řešení Flowmon popsaném výše, kdy zařízení SIEM je si samo sobě sondou (monitorovacími porty zachytává síťový provoz poslaný ze SPAN[33] portu aktivního síťového zařízení) i kolektorem (zachycený síťový provoz je zpracován na jednotlivé toky). Primární určení SIEMu není zpracovávání síťového provozu, takže NetFlow statistiky neobsahují tolik atributů jako u Flowmonu, přesto je výhodné monitorovací porty pro zpracování síťového provozu použít. Výhodou je například to, že Extreme SIEM umožňuje nastavit zachytávanou velikost payloadu jednotlivých toků. Což je například v případě dlouhých URL výhoda oproti Flowmonu, který právě URL ořízne, pokud její délka překročí 64 znaků. V případě Úřadu je v SIEMu hodnota maximum data capture nastavena na 256B, ale podporovány jsou i hodnoty přes 2kB. Čím větší hodnota, tím se samozřejmě ukládá větší množství dat a případně se tím snižuje retenční doba.

4.7.1 Nastavení síťové hierarchie

Jde o nastavení síťových rozsahů používaných v organizaci a nastavení některých zařízení v síti (např. proxy servery, rozsah VPN adres nebo rozsahy bezdrátových sítí).

[31] EPS (Events Per Second) určuje počet událostí, které zařízení může zpracovat za sekundu.
[32] FPM (Flows Per Minute) určuje počet síťových toků, které může zařízení zpracovat za minutu.
[33] SPAN (Switched Port Analyzer) metoda zrcadlení portu, představuje asi nejjednodušší způsob, jak zachytávat provoz cílového zařízení v přepínané síti. (32, s. 39)

Extreme SIEM toto nastavení využívá k pochopení síťové dekompozice, zaměření monitoringu na určitou skupinu zařízení nebo k rozlišení mezi vnitřními a vnějšími klienty.

Toto nastavení se provádí na kartě Admin v sekci Systém Configuration a nazývá se Network Hierarchy. Je vhodné sem vyplňovat adresy v souladu s nastavením filtrů ADS pluginů Flowmonu. Jde v podstatě o dvě principiálně shodná nastavení. Obě jsou zdrojem informací pro behaviorální analýzy jednotlivých produktů.

4.7.2 Nastavení automatických aktualizací

K udržení aktuálního SIEMu je vhodné nakonfigurovat automatické aktualizace. Jde o to nejen mít správně nastavenou URL aktualizačního serveru a případně adresu proxy serveru organizace, pokud jde komunikace SIEMu přes proxy. Je potřeba také rozmyslet si, které typy updatů se budou automaticky stahovat. V tomto nastavení je totiž oddělena logika pro jednotlivé druhy aktualizací. Odděleny jsou hlavní updaty (Major updates), které přináší nové funkce, menší updaty (Minor updates), jež opravují méně závažné problémy a aktualizace DSM[34], skeneru a protokolu, ty opravují problémy v DSM, problémy s parsingem a aktualizace protokolu. Hlavním rozdílem Major a Minor aktualizací s ohledem na nastavení automatizace je to, že Major aktualizace vyžadují následný restart služby. Což je hlavní důvod toho, proč jsou v případě Úřadu automatické aktualizace Major verzí zakázané. U ostatních dvou typů aktualizací je povolen „Auto Install“.

Dále se zde ještě nastavuje frekvence, s jakou budou aktualizace kontrolovány. Vybírat lze ze standardních period – denní, týdenní, měsíční. V případě Úřadu jsme nastavili kontrolu na denní bázi.

4.7.3 Nastavení a sběr logů

Extreme SIEM je z pohledu sběru dat logicky rozdělen na dvě části. Jednou z nich je sběr dat zaslaných nebo SIEMem aktivně vyčtených z logů sledovaných zařízení. Události

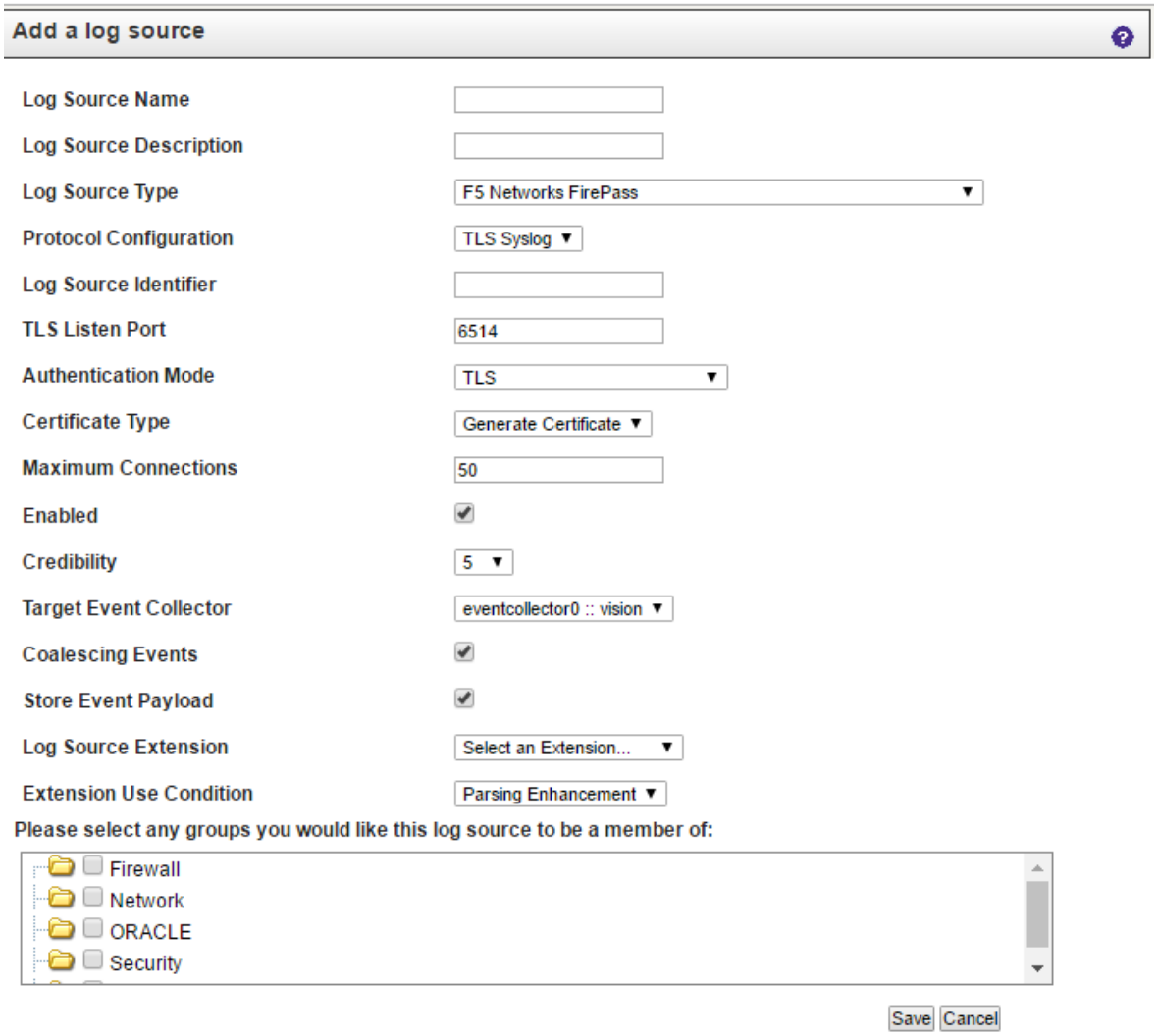
[34] DSM (Device Support Module) je přednastavený konfigurační soubor, který obsahuje parsování (rozkladu) zasílaných logů dle typu zařízení, které je do SIEMu zasílá.

zachycené tímto způsobem je možné zobrazit na kartě Log Activity. Zde se dají filtrovat podle různých atributů. Prohledávání dat z logů je sice tímto způsobem možné a často používané při různých analýzách, ale to hlavní, kvůli čemu chcete mít SIEM, je to co tu vlastně vidět přímo není. A tím je celá logika, která jednotlivé události získané z logů vyhodnocuje a vzájemně koreluje. Ve chvíli, kdy je během automatické analýzy nalezena aktivita, která splňuje některé z přednastavených pravidel, vykoná se nastavená činnost. Ta ve většině případů znamená vypsání tzv. „offense“, neboli bezpečnostní události.

Cílem administrátora SIEMu je získat relevantní data z logů relevantních aktiv. Výběr těchto aktiv i hloubky logování by měl vycházet z identifikace aktiv a následné analýzy rizik. Tyto činnosti by měly identifikovat aktiva, která chci z nějakého důvodu sledovat, a také důležitost těchto aktiv. Podle důležitosti aktiv lze nastavit významnost jednotlivých zdrojů logů a ta pak hraje roli při vyhodnocovacím mechanismu.

Zdroje logů lze do Extreme SIEMu dostat dvěma základními cestami. První z nich je nastavení zasílání logů přímo na daném aktivu směrem k SIEMu. Většinou jde o syslog protokol. Pokud jde o syslog protokol a frekvence odesílaných událostí je dostatečná (zhruba desítky za minutu), je zdroj (Log Source) na SIEMu objeven automaticky. Je mu pak přiřazen příslušný DSM kvůli správnému rozpoznání údajů obsažených v logu. Takto objevený zdroj je také automaticky pojmenován dle formátu „TypZdroje @ IPadresa“ nebo „TypZdroje @ NázevZdroje“.

Druhým způsobem, jak vytvořit v SIEMu zdroj, je ručním vytvořením v nastavení na kartě Admin, v sekci Data Sources pomocí funkce Log Sources. Zde je potřeba přidat nový zdroj, vybrat typ zařízení, ze kterého budou logy pocházet (tedy příslušné DSM), protokol, kterým budou data posílána a dle toho pak také všechny potřebné atributy. Především tedy název a identifikátor zdroje apod. Pokud nebude log zasílat aktivně jeho původce, ale je potřeba nastavit SIEM, aby si jej ze zařízení nebo nějakého zdroje vyčítal sám, je většinou nutné nastavit také autentizační údaje k zařízení, na kterém se logy nacházejí.



Obrázek 28 - Příklad nastavení Log Source na SIEMu (vlastní zpracování)

Atributem Credibility můžeme nastavit důležitost daného zdroje událostí. Výchozí hodnotou je 5. U zdrojů, které jsou pro nás z nějakého důvodu důležité, můžeme důležitost zvýšit až do maximální hodnoty 10. Méně kritickým zdrojům můžeme naopak tuto úroveň snížit. Minimem je 0. Tato hodnota pak v rámci vnitřní logiky vyhodnocování událostí přispívá k určení celkového dopadu dané identifikované bezpečnostní události, tzv. Magnitude.

Každý z vytvořených zdrojů událostí můžeme přiřadit do jedné nebo několika skupin. Tyto skupiny jsou vytvářeny administrátorem SIEMu a slouží k lepší orientaci při vyhledávání a třídění jednotlivých zdrojů.

Pokud jde o zdroj, který nemá nativní podporu v Extreme SIEMu (tedy neexistuje příslušný DSM), je nutné použít univerzální DSM nebo nějaký, který je danému zdroji podobný, a vytvořit tzv. Log Source Extension, což je XML soubor, jenž obsahuje parsovací pravidla, která dokáží správně přečíst údaje z daného zdroje. Obsah takového jednoduchého rozšíření je na obrázku níže.

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<ns2:device-extension xmlns:ns2="event_parsing/device_extension">
    <pattern id="allEventNames">(.*)</pattern>
    <pattern id="EventName-PIS">UDALOST_ID\:\s\"(\d{8})\"</pattern>
    <pattern id="EventCategory-PIS">KOD_TYPU_UDALOSTI\:\s\"(\d{1,3}?)\"</pattern>
    <pattern id="DeviceTime-PIS">CAS_UDALOSTI\:\s\"(\d{4}\-\d{1,2}\-\d{1,2}\s\d{1,2}\:\d{1,2}\"</pattern>
    <pattern id="UserName-PIS">UZIVATEL_NAZEV\:\s\"(\w+)\"</pattern>
    <pattern id="HostName-PIS">HOST_NAME\:\s\"(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\"</pattern>
  - <match-group order="1" description="Log Source Extension">
        <matcher order="1" field="EventName" pattern-id="EventName-PIS" capture-group="1" enable-substitutions="false"/>
        <matcher order="1" field="EventCategory" pattern-id="EventCategory-PIS" capture-group="1"/>
        <matcher order="1" field="DeviceTime" pattern-id="DeviceTime-PIS" capture-group="1"/>
        <matcher order="1" field="UserName" pattern-id="UserName-PIS" capture-group="1"/>
        <matcher order="1" field="HostName" pattern-id="HostName-PIS" capture-group="1"/>
        <event-match-multiple pattern-id="allEventNames" capture-group-index="1" device-event-category="unknown" send-
            identity="OverrideAndAlwaysSend"/>
    </match-group>
</ns2:device-extension>
```

Obrázek 29 - Ukázka Log Source Extention pro log z Personální IS Úřadu (vlastní zpracování)

4.7.4 Nastavení zachytávání síťových toků

Druhou částí Extreme SIEM je zpracování síťových toků. Připojení zdrojů síťových toků je možno dvěma způsoby. Prvním je přivedení síťového provozu přímo do jednoho ze 3 monitorovacích portů zařízení. A to je vlastně vše. Další nastavení pak není potřeba. Všechny 3 monitorovací porty jsou totiž přednastaveny tak, aby po připojení zdroje flow automaticky začaly zdroj přijímat a zpracovávat.

Druhým způsobem příjmu síťových toků je exportování z nějakého zařízení, které exporty flow umožňuje, na management port SIEMu. Exporty do SIEMu například může posílat sonda Flowmon (nebo i kolektor Flowmon). Stačí nakonfigurovat SIEM jako další z cílů exportérů na sondě. Pokud má SIEM pracovat s takto poslanými exporty, musí se nakonfigurovat na kartě Admin, v sekci v sekci Data Sources, nastavení Flow Sources. Toto nastavení je vcelku přímočaré. Jediné, co je potřeba nastavit, je přijímací port, formát flow (protokoly NetFlow a IPFIX, JFlow, SFLow, Packeteer FDL nebo načtením flow ze souboru) a protokol transportní síťové vrstvy - TCP nebo UDP. Pokud exportér nastavíme tak, aby posílal NetFlow/IPFIX přes UDP a pošleme data na port 2055 Extreme SIEMu, pak vlastně také není na SIEMu co nastavovat. Tato konfigurace totiž vyhovuje výchozímu nastavení.

Síťový provoz pak můžeme v Extreme SIEMu sledovat na kartě Network Activity. Podobně jako u sledování událostí platí to, že silnějším nástrojem než samotné ruční filtrování ze všech toků zpracovávaných zařízením je vnitřní logika vyhodnocující provoz na SIEMu dle přednastavených pravidel. Vyhodnocené bezpečnostní události se opět objevují na kartě Offenses. Nutno podotknout, že korelace zdrojů není omezena jen na události nebo jen na síťové toky. Koreluje se vše dohromady a jednotlivé offenses mohou být detekovány díky kombinaci událostí i flows.

V případě Úřadu je do SIEM přiveden síťový tok z Internetového provozu přímo do jednoho z monitorovacích portů. V plánu máme ještě přivedení LAN provozu (také přímo do monitorovacího portu zařízení) a toky z datacentra, které ale z důvodu velkého objemu budou exportovány na virtuální port SIEMu.

Pro lepší orientaci ve flows, i pro případné použití ve filtrech nebo v pravidlech, je možné definovat si vlastní atributy (Flow Properties). Příkladem může být „vypreparování" HTTP GET požadavku z payloadu zdrojového toku. Nejdříve je potřeba novou vlastnost nějak pojmenovat, v našem případě se hodí „HTTP GET Request". Poté je potřeba vymyslet regulární výraz, který bude vyhovovat našemu vyhledávání. Předpokládejme, že request bude mít zhruba formát „***GET /dir/file.jsp?param=123***". Regulární výraz musí tedy začínat na GET a poté bude řetězec znaků až do ukončení řádku, které v případě payloadu budou tvořit hexadecimální znaky 0d a 0a. Vyhovující regulární výraz tedy bude: „***GET (.+?)\x0d\x0a***". Do závorek uzavřeme hodnotu, která nás zajímá a SIEMu řekneme, že nás zajímá Capture group č. 1 (neboli první závorka).

Podobně si můžeme zachytit také HTTP odpověď (Response code), která nám může posloužit například k diagnostice chybových stavů webserveru nebo odhalení toho, jakým způsobem náš webserver reagoval na útočníkovy snahy o zneužití zranitelnosti pomocí různých úprav GET požadavků. Tentokrát nás bude zajímat obsah cílového paketu, tedy odpovědi našeho serveru na dotaz z Internetu. Víme, že response má formát „***HTTP/1.1 404 Not Found***" nebo třeba „***HTTP/1.1 200 OK***". A my máme zájem o výsledek, nezajímá nás tedy ona úvodní část s verzí protokolu. Vyhovující regulární výraz bude mít tuto podobu: „***HTTP\/(.+?)\s(\d+\s.+?)\x0d\x0a***". Tentokrát nás zajímá Capture group č. 2, obsah druhé závorky. Zajímavostí může být to, že stejný regulární výraz můžeme použít i

pro určení verze HTTP protokolu. Stačí jen zachytit první Capture group. Pro zjištění verze HTTP protokolu by ale postačil i kratší výraz „***HTTP\/(.+?)\s***“. Teď už zbývá jen tyto naše vytvořené vlastnosti použít ve filtrech a případně i pravidlech.

4.7.5 Ladění a vytváření pravidel

Veškerá logika vzájemných korelací událostí a toků a jejich vyhodnocování je založena pravidlech a tzv. Building blocích. SIEM jich obsahuje stovky už v továrním nastavení a spoustu z nich i rovnou zapnutých. Všechna tato pravidla vychází z nějakých obecných často se vyskytujících vlastností a jevů. A fakt, že jsou už při nasazení SIEMu zapnutá, nám ušetří spoustu práce s počátečním nastavováním. S trochou nadsázky se dá říci, že SIEM stačí nainstalovat, dostat do něj několik zdrojů událostí a už to vše běží a pracuje. V praxi je ale nezbytné pravidla upravovat podle aktuálních potřeb daného prostředí. Toto ladění je dlouhodobá práce, která nikdy nekončí. Administrátor SIEMu totiž musí být připraven reagovat na změny a nové okolnosti.

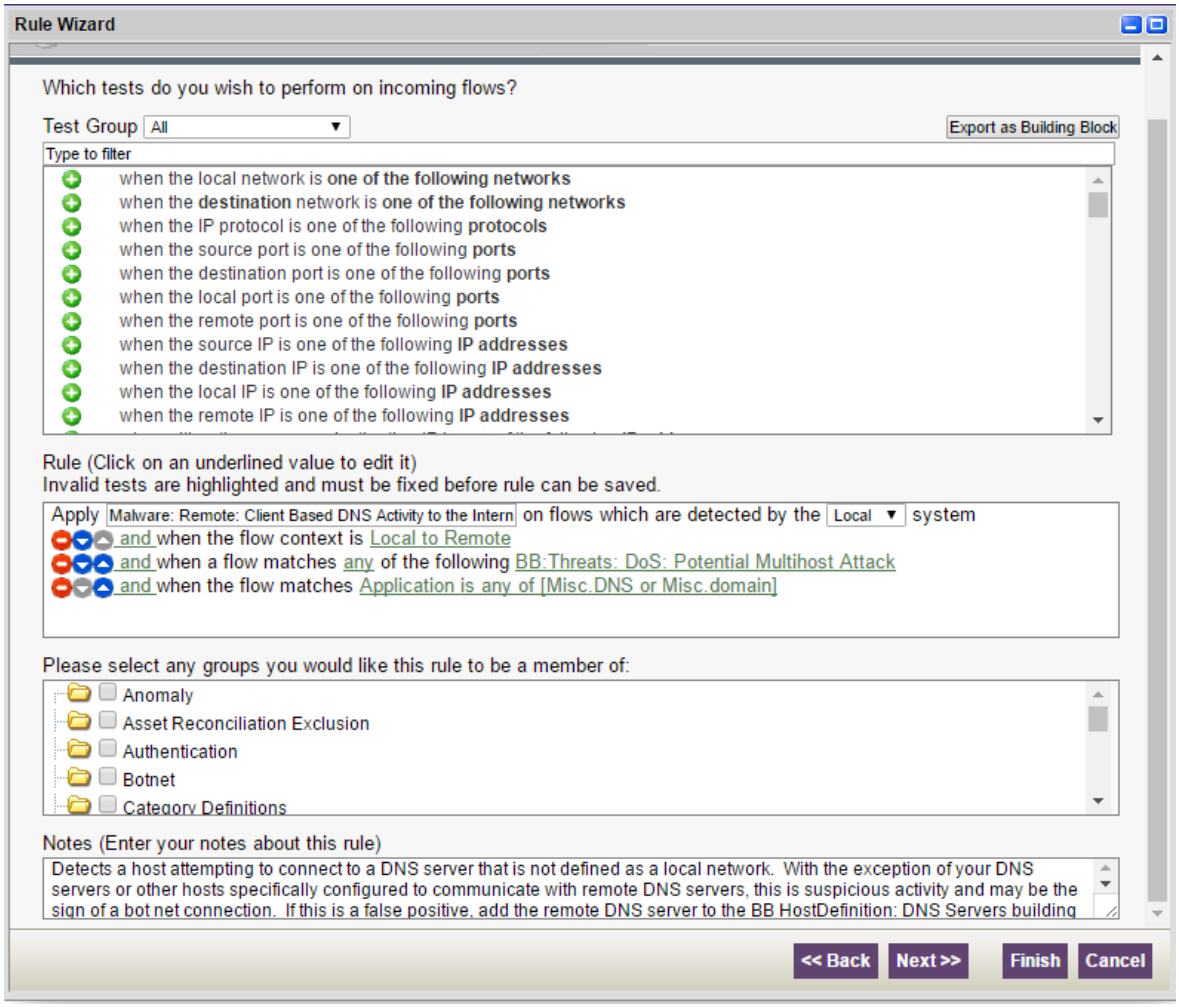
Byť při nasazení SIEMu existuje spousta pravidel, pravděpodobně se setkáte s potřebou vytvářet si i některá nová. Ladění a vytváření pravidel se provádí na kartě Offenses, v sekci Rules. Pravidla i Building bloky jsou členěny do různých skupin dle typu a určení. Tento fakt zpřehledňuje situaci a usnadňuje práci.

Při ladění pravidel existují dva základní přístupy. Prvním je reakce na zachycené offenses. Pokud se objevuje mnoho offenses stejného typu, které jsou vyhodnoceny jako false positives, je možné místo prostého označení každé offense jako false positive přehodnotit, zda by nebylo pro dané prostřední lepší upravit nějaký parametr v pravidle, které tyto offenses detekuje. U každé offense jsou pravidla, na základě kterých byla detekována a vypsána. Druhým důvodem ke změně nebo vytvoření nových pravidel je zjištění, že potřebujete detekovat něco, na co pravidla vytvořená nejsou.

Jednotlivá pravidla se skládají z předdefinovaných testů typu „***jestliže je zdrojový port jedním z následujících portů…***“ nebo „***jestliže je lokální IP adresa jedna z těchto adres…***“ případně složitější konstrukce jako například „***jestliže během tolika minut množina alespoň takového množství pravidel v následujícím pořadí a se stejným uživatelským jménem byla následována množinou nejméně tolika pravidel v jakémkoli pořadí přicházejících na tuto cílovou IP adresu…***“. Tyto testy se dají skládat pomocí

logických operátorů ***and*** a ***not and*** do složitějších konstrukcí. Tyto konstrukce pak vystupují jako ucelená pravidla. Je možné také vytvořit obecné konstrukce, které pak půjde použít do více pravidel a ty je pak možné uložit jako „stavební kameny“ (Building blocks) právě pro tvorbu dalších složitějších pravidel.

Poté co vytvoříme vyhovující pravidlo, je potřeba nastavit, co se vlastně má stát poté, co bude nějaká komunikace tímto pravidlem detekována. Zde máme několik možností - od vytvoření nové události, přes vytvoření offense, úpravu vlastností, generování syslog zprávy nebo poslání alertu na definované e-mailové adresy.



Obrázek 30 - Ukázka tvorby detekčního pravidla v SIEM (vlastní zpracování)

4.8 Ukázka detekce bezpečnostní události

Jako demonstraci použití technologií pro sběr, detekci a vyhodnocování bezpečnostních událostí jsem vybral bezpečnostní událost nahlášenou nástrojem SIEM

jako offense. Jednalo se o hlášení antimalware klienta Symantec Endpoint Protection, který je nainstalován na uživatelských stanicích. Antimalware nástroj je centrálně spravován a jeho bezpečnostní hlášení jsou zasílána na SIEM.

Offense v SIEM tedy upozorňovala na detekci a smazání malware na klientské stanici. Respektive SIEM na základě korelací spojil do dané offense hned 3 napadené stanice, díky tomu, že byly napadené v horizontu několika hodin, ve stejné lokální síti a ve všech případech se jednalo o útok typu Web Attack. V každém případě však šlo o samostatnou vzájemně nesouvisející událost (zdroj události byl vždy jiný). I když v tomto případě korelace spojila nesouvisející události, jde často o cenný zdroj, který umí upozornit na hrozbu v širším kontextu. Proto se vždy vyplatí takovou možnost prověřit. V tomto případě tedy můžeme pokračovat v řešení tří na sobě nezávislých událostí.

Další zajímavou informací, kterou nám SIEM v tomto případě říká (opět na základě korelace a statistik) je fakt, že jeden ze tří PC, na kterých se malware objevil, už byl dříve zdrojem jiných bezpečnostních událostí. To je podezřelé a dále se tedy v této ukázce budu věnovat analýze tohoto PC.

Ve všech případech se jednalo o hlášení antimalware systému. Nicméně jednotlivá hlášení od sebe byla vždy vzdálena minimálně týden, v některých případech i více než měsíc. Typ události byl vždy stejný „Fake Browser Update“ a antimalware klient vždy potenciální nákazu zablokoval. Spíše než o napadený PC se tedy jedná o uživatele, který se chová na webu neopatrně. Vzhledem k opakujícím se incidentům stejného typu se zdá, že tento uživatel navštěvuje opakovaně stejný web obsahující danou hrozbu. Tomu odpovídá kromě opakujícího se typu události také stejná struktura blokovaných URL:

URL: p39.satirisefdggg.online/22039/986/dfeyei/hplw7nf/5802
URL: 8u.mtsdbbyhraillery.online/708/1293/26k5beo/2s6
URL: w.nbtsuunsecret.club/27021/1403/6hu7/qcoxtc9/3125
URL: p.qjsoylremissly.club/8317/1354/waab1/8wnj

Vždy jde o jinou doménu, takže pravděpodobnější, než že by daný uživatel navštívil v průběhu doby cíleně všechny tyto domény, je scénář, kdy navštěvuje stále stejný web,

který ale obsahuje zdroje odkazující na nalezené problémové domény (buď schválně, nebo je napaden například nějakou malwertisingovou kampaní).

V tuto chvíli se nabízejí 2 důležité otázky, na které je třeba najít odpovědi:

1) Kterou napadenou stránku tedy tento uživatel opakovaně navštěvuje?
2) Je zablokovaný malware jediný, který se na dané stránce objevuje nebo do PC prošel i jiný malware, který ale antimalwarový klient neumí rozeznat?

Ke zodpovězení obou otázek nám může pomoci analýza síťového provozu. Zapneme si tedy aplikaci Flowmon. Vybereme nejaktuálnější incident a ve zvoleném časovém intervalu vyfiltrujeme komunikaci na IP adrese napadeného PC. Výpis síťové aktivity nepřináší příliš optimistické výsledky. Těsně předtím, než byl zablokován přístup na napadenou stránku, přistupoval PC na několik dalších podezřelých stránek, které antimalware klient nenahlásil (tedy pokud na nich byl funkční malware, nezablokoval ho).

První v řadě vypsaných URL je server ***youwatch.org***. Trocha hledání na Internetu nám prozradí, že se jedná o web pro sdílení videí. Vyzkoušením URL (samozřejmě na testovacím PC, izolovaném od zbytku sítě) zjistíme, že se daný uživatel v pracovní době díval na seriál. Okamžitě po přístupu na web vyskočí několik reklamních oken, některé z nich odkazují na URL, které jsme dříve identifikovali v síťové komunikaci uživatele, jsme tedy na správné stopě. Vzhledem k tomu, že Flowmon ukazuje ještě další síťový provoz před přístupem na youwatch.org, je pravděpodobné, že uživatel nenavštívil server youwatch.org přímo, ale prostřednictvím jiného serveru. Zde se bohužel projevil problém pro síťový monitoring, který se v dnešní době zhoršuje, a tím je neviditelnost šifrovaného SSL/TLS provozu[35]. K tomu, aby bylo vidět, kam uživatel přistupuje šifrovaně, je třeba zavést SSL inspekci. Vzhledem k tomu, že se v konečném důsledku jedná

[35] SSL/TLS protokoly (Secure Socket Layer a Transport Layer Security) jsou dnes často používány k zajištění bezpečnosti transakcí přes HTTP. Protože ale zabezpečují TCP komunikaci, lze jimi zajistit důvěrnost, integritu a ověřování obecně pro libovolnou aplikaci komunikující přes TCP, nejen HTTP. (31, s. 547)

v podstatě o „legální“ subjektem prováděný Man-in-the-middle útok, je často nasazení takové inspekce v dané organizaci kontroverzním tématem. V případě Úřadu zatím taková inspekce zavedena není, musíme si tedy poradit jiným způsobem. URL uživatelem navštívených HTTPS stránek můžeme zachytit například na proxy serveru. Případně nám nezbyde, než prohlédnout historii webového prohlížeče daného uživatele.

youwatch.org	http://youwatch.org/embed-avcvie7i1dsh-720x405.html	http-alt	7	1278
voodaith7e.com	http://voodaith7e.com/embed-avcvie7i1dsh-_-Uys1cHhTT2hQbUFzNVIw	http-alt	14	1266
190.211.254.59	http://190.211.254.59/i/03/00000/avcvie7i1dsh.jpg	http-alt	7	776
go.onclasrv.com	http://go.onclasrv.com/apu.php?zoneid=593365	http-alt	13	2731
190.211.254.59	http://190.211.254.59/xvqvdyqfqvtlvseigzv5ezw7kqoc7vytsmu4rer5j	http-alt	1123	45475
serve.popads.net	http://serve.popads.net/checkInventory.php?w=1488183661&v=3&sit	http-alt	12	2933
163.172.16.147	http://163.172.16.147/go/PropWW	http-alt	5	775
onclkds.com	http://onclkds.com/?auction_id=68763be5-832c-4d1c-a5be-4afa7432	http-alt	6	1801
		http	1	52
		http	1	52
		http-alt	24	4940
www.bet365.com	http://www.bet365.com/dl/~offer?affiliate=365_536023	http-alt	5	777
		http	2	104
		http	2	104
bidserver.clickpapa.io	http://bidserver.clickpapa.io/c.php?id=8968&campaign_id=7433&cl	http-alt	5	622
190.211.254.59	http://190.211.254.59/xvqvdyqfqvtlvseigzv5ezw7kqoc7vytsmu4rer5j	http-alt	5234	209955
youwatch.org	http://youwatch.org/dl?op=view&file_code=avcvie7i1dsh&hash=5074	http-alt	7	1555
ogranictraffic.com	http://ogranictraffic.com/go/15264/436?subid=8968	http-alt	5	561
prpops.com	http://prpops.com/p/mboi/direct/t:8968	http-alt	5	602
ogranictraffic.com	http://ogranictraffic.com/favicon.ico	http-alt	22	1718
www.predictivadnetwork.com	http://www.predictivadnetwork.com/a/display.php?r=1406629	http-alt	11	2440
tr1srtr.com	http://tr1srtr.com/rtr?id=1403&utm_campaign=1406629&clickid=148	http-alt	9	1641

Obrázek 31 - Výpis komunikace napadeného PC - Flowmon (vlastní zpracování)

Flowmon nám prozradil, že nákaza se do PC dostala při používání Firefoxu. Historie navštívených stránek je ve Firefoxu uložena v souboru places.sqlite. Jde o speciální typ databáze. K jejímu prohlížení potřebujeme nějakou aplikaci, která nám to umožní. V našem případě jsme použili DB Browser for SQLite. Vyhledáním příslušné ho časového

intervalu[36] zjistíme, že uživatel prohlížel seriál prostřednictvím stránek ***topserialy.sk***. Dopátrali jsme se tedy k věrohodné odpovědi na první otázku - Kterou napadenou stránku tedy tento uživatel opakovaně navštěvuje? Výsledkem pátrání je zablokování přístupu z interního prostředí na domény ***topserialy.sk*** a ***youwatch.org*** na proxy serveru.

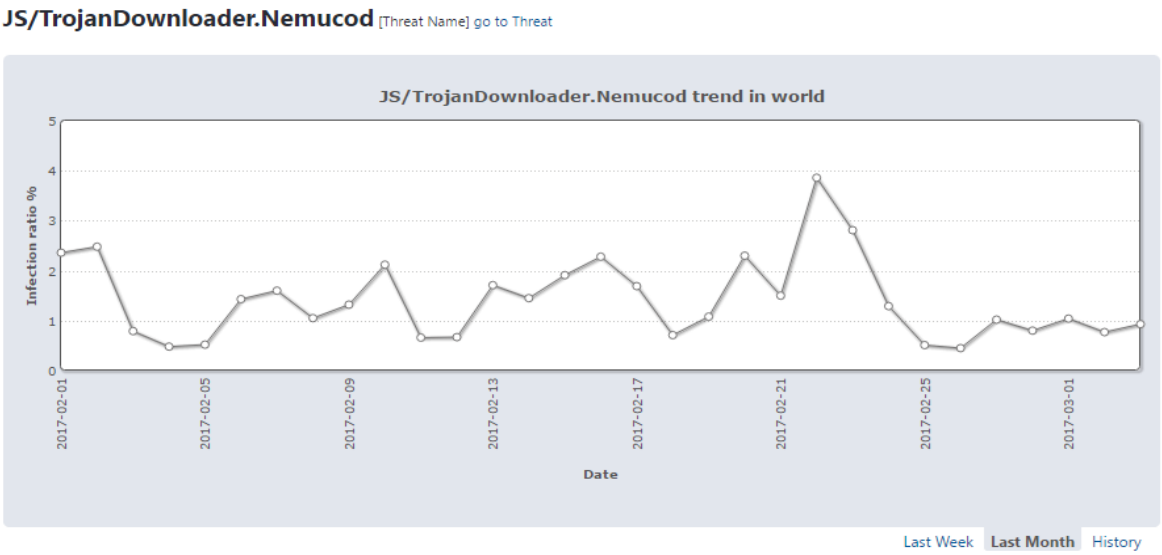
Odpověď na druhou otázku už jsme z části také odkryli. Víme jistě, že uživatel přišel do kontaktu s více podezřelými zdroji, než byl ten jeden zablokovaný antimalware klientem. Podle seznamu navštívených URL se dá vypozorovat, že některé spolu souvisí (např. podle parametru zoneid=593365, který slouží pravděpodobně profilování oběti). Vhodným začátkem prověřování navštívených URL může být jejich prověření online nástrojem VirusTotal.com, který v sobě sdružuje virové definice desítek antimalware řešení. Často se však setkáte s tím, že antimalware nástroje danou nákazu prostě neznají. Prověřovanou adresu ***http://go.onclasrv.com/apu.php?zoneid=593365*** například vyhodnotil jako závadnou pouze 1 ze 64 nástrojů.

Nicméně už samotným zobrazením PHP zkoumaného kódu je jasné, že jde o něco podezřelého. Kód je totiž obfuskovaný, aby bylo zabráněno jeho snadné analýze[37]. Zkoušet kód upravit a analyzovat ručně by bylo zdlouhavé. Nejdříve je možné využít online sandbox řešení, které umožňuje kód spustit a zanalyzovat jeho chování. Takovým nástrojem je například ***hybrid-analysis.com***. Tento nástroj zjistil několik zajímavých faktů. Především to, že se jedná o malware zařazený do skupiny JS.Nemucod.CGN. Jde o trojan downloader - tedy program, který se snaží stáhnout malware z Internetu. Rozšíření tohoto typu malware dle virusradar.com momentálně kolem 1%.

---

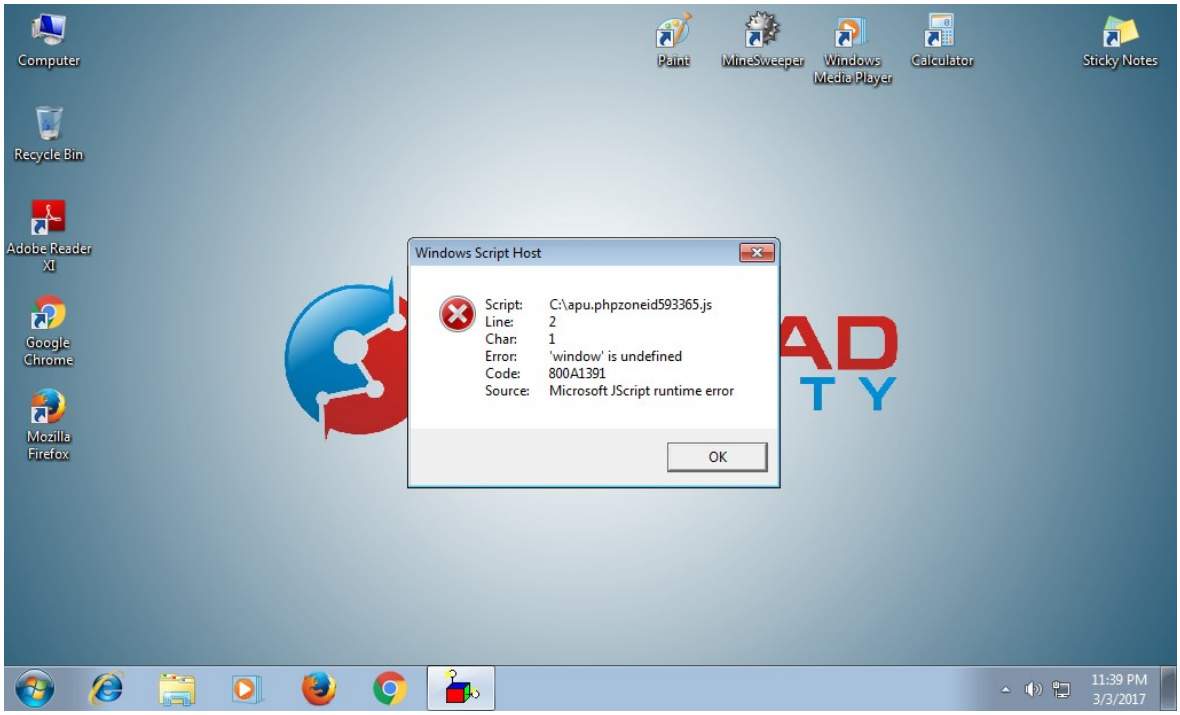
[36] Určitou překážkou v pátrání může být specifický způsob značení data a času v historii Firefoxu. Jde o mírně upravený formát Unix Epoch. Datum a čas je reprezentován velkým celým číslem. Jedná se o počet mikrosekund od referenčního data 1.1.1970 1:00. Pro přepočet na klasický formát lze použít například vlastnost Excelu odečítat data a získat tak počet dnů – po vynásobení 24 x 3600 x 1 000 000 dostaneme příslušný počet mikrosekund.

[37] Obfuskace nebo také zatemnění kódu je metoda, kterou využívá moderní malware k tomu aby skryl svůj skutečný účel a co nejvíce znepříjemnil analýzu kódu. Automatizovaná analýza obfuskovaného kódu je téměř nemožná, manuální analýza se tímto výrazně stíží. (29, s. 524)



Obrázek 32 - Graf rozšíření JS/TrojanDownloader.Nemucod (21)

PHP skript obsahuje JavaScript, který vyčítá z napadeného systému některé informace o jeho parametrech a nastavení – například název PC, Cryptographic machine GUID, nastavení důvěryhodných poskytovatelů ve Windows nebo nastavené jazykové prostředí. Evidentně jde o profilování potenciálního cíle kvůli správnému zacílení útoku. Pro analýzu PC je zajímavým faktem i to, že daný JavaScript se uloží lokálně v cestě ***C:\apu.phpzoneid593365.js***.



Obrázek 33 - Výstup nástroje Free Automated Malware Analysis Service (22)

Dalším krokem je tedy prověření, zda napadený PC obsahuje tento soubor. V našem případě naštěstí neobsahuje. To však není dostatečným důkazem toho, že PC nebyl kompromitován. Byť momentálně nejsme schopni odhalit žádný zjevný projev napadení PC, politika Úřadu velí PC přeinstalovat. Uživatel byl navíc poučen o rizicích svého jednání.

5 Výsledky a diskuse

V diplomové práci byla představena hlavní bezpečnostní opatření, která byla v Úřadě provedena během posledního roku a půl s cílem zvýšit úroveň zabezpečení proti kybernetickým hrozbám. Opatření spočívala jak v organizační sféře, tak ve sféře technické.

Správné nastavení a soulad jak organizačních, tak technických opatření, je podmínkou pro dobře fungující bezpečnost informací. Náplň a postup tvorby obou aspektů bezpečnostních opatření jsou odlišné. Každý z těchto dvou typů opatření má jiné nároky na lidské zdroje i na finance. Zatímco organizační opatření vyžadují především dobrou znalost norem, v tomto případě především ČSN ISO/IEC 27000 a Zákona č. 181/2014 Sb., o kybernetické bezpečnosti, včetně související Vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti, ale jejich tvorba nevyžaduje velké finanční investice, u technických opatření jde v první řadě právě o finance a také o vysoce specifické technické znalosti a know-how. Co je však pro oba typy opatření společné, je to, že nejde a nesmí jít pouze o jednorázovou činnost vyvinutou při jejich tvorbě a nasazení, ale o činnosti a procesy, které jsou do společnosti zavedeny a udržovány, kontrolovány a řízeny kontinuálně.

5.1 Připravenost OVM před implementací opatření

5.1.1 Organizační připravenost

Úřad samozřejmě řešil bezpečnost i předtím, než byl vytvořen a schválen Zákon o kybernetické bezpečnosti. Nikdy však formálně nefungoval a ani neměl ambice fungovat plně dle některé z norem řízení bezpečnosti. I před počátkem snahy o zajištění souladu se ZKB existovala jako vrcholný dokument stanovující bezpečnost v Úřadě bezpečnostní politika. Její rozsah i zaměření bylo velmi obecné a zacílené především na výčet legislativních předpisů a interních směrnic, které se bezpečnosti informací týkaly. Nejdůležitější pojmy a východiska tohoto legislativního rámce byly v bezpečnostní politice

opět velmi obecně zmíněny. Problém byl především v tom, že tato původní bezpečnostní politika nepokrývala všechny požadavky, které s sebou následně přinesl Zákon o kybernetické bezpečnosti. Chyběla především témata k zabezpečení mobilních zařízení, řízení vztahů s dodavateli, pravidla ochrany před škodlivým kódem nebo používání kryptografické ochrany. Dalším problémem bylo, že se tato politika pravidelně nerevidovala a neposuzovala se její účinnost. V platnost vstoupila v roce 2007 a od té doby nebyla nijak upravována. Nahrazena byla novou Bezpečnostní politikou v roce 2016, tedy po celých 9 letech.

Z hlediska organizační bezpečnosti přinesl nový zákon také požadavky na obsazení některých bezpečnostních rolí, které do té doby Úřad neměl formálně definované a obsazené. Kromě explicitně stanovených bezpečnostních rolí manažera, architekta a auditora kybernetické bezpečnosti, chyběl Úřadu také vrcholový výbor, který by se pravidelně scházel za účelem řešení bezpečnostních otázek. Roli výboru do té doby, dle původní bezpečnostní politiky, zastávala Porada vedení Úřadu. Což je ovšem orgán primárně určený k vedení „business“ cílů organizace. Jak víme, bezpečnostní opatření často hlavní provozní aktivity spíše brzdí. Řízení bezpečnosti Poradou vedení tedy představoval určitý konflikt zájmů. Přednost mělo vždy spíše řešení provozních otázek, než těch bezpečnostních.

Nedostatečným způsobem byla řešena také otázka řízení aktiv, a to už základního prvku, tedy identifikace aktiv a jejich následného hodnocení z hlediska důvěrnosti, integrity a dostupnosti a následné řízení rizik.

Důležitými otázkami při tvorbě organizačních opatření a jejich dodržováním jsou zajištění informovanosti a osvěty všech zainteresovaných osob a schopnost nějakým způsobem opatření kontrolovat a vymáhat jejich dodržování. Toto jsou vždy velmi obtížné body. V případě Úřadu byly řešeny v podstatě pouze formálně. Informovanost byla zajišťována pouze tím způsobem, že nové směrnice a řídicí dokumenty byly umístěny na společný intranet a jednotlivé odbory Úřadu zajistily podepsání svých zaměstnanců na podpisovou listinu prohlašující, že se daný zaměstnanec s dokumentem seznámil. Prakticky tím byla na zaměstnance přenesena odpovědnost za to, že bude dodržovat stanovená pravidla, nicméně nijak nebylo ověřováno, že se zaměstnanec s pravidly

opravdu seznámil a že je chápe a respektuje. Jediným „osvětovým“ obdobím si každý zaměstnanec prošel při svém přijetí, kdy byl seznámen prostřednictvím úvodního školení s některými nejvýznamnějšími pravidly, která byla v danou dobu platná. Jedinými normami, jejichž znalost se alespoň základním způsobem průběžně ověřovala, byla pravidla požární ochrany a bezpečnosti a ochrany zdraví při práci. Co se týče otázky vymáhání dodržování stanovených pravidel, vzhledem k problému s jejich neefektivní kontrolou, byla vymahatelnost prakticky nulová.

5.1.2 Technická připravenost

Co se týče technických bezpečnostních opatření, nebyl na tom před kontrolou shody se ZKB Úřad vůbec špatně. Tedy minimálně z hlediska vlastnictví a nasazení potřebných technologií. Z technických požadavků Zákona o kybernetické bezpečnosti měl Úřad ve více či méně pokročilém stádiu zavedeny téměř všechny potřebné technologie. Co byl a stále je zásadní problém v tomto ohledu, je akutní nedostatek technických pracovníků s potřebnou kvalifikací, kteří by tyto technologie udržovali ve správném chodu a dokázali na nich a pomocí nich kontrolovat aktuální bezpečnostní stav z pohledu kybernetických hrozeb a zranitelností. Snahou Úřadu je a i v minulosti bylo získat technické know-how i pracovní kapacitu také formou outsourcingu.

5.2 Stav OVM po implementaci opatření

V rámci provedených opatření jsem se zaměřil především na organizační bezpečnostní opatření. Z provedené GAP analýzy, které měla posoudit míru souladu Úřadu s požadavky Zákona o kybernetické bezpečnosti, jasně vyplynuly nedostatky právě v této oblasti.

Úřadu chybělo jakékoli formální vymezení systému řízení bezpečnosti informací. Současně měl bezpečnostní politiku, která nevyhovovala podmínkám kladeným ZKB a naprosto chyběla obecná metodika pro řízení rizik.

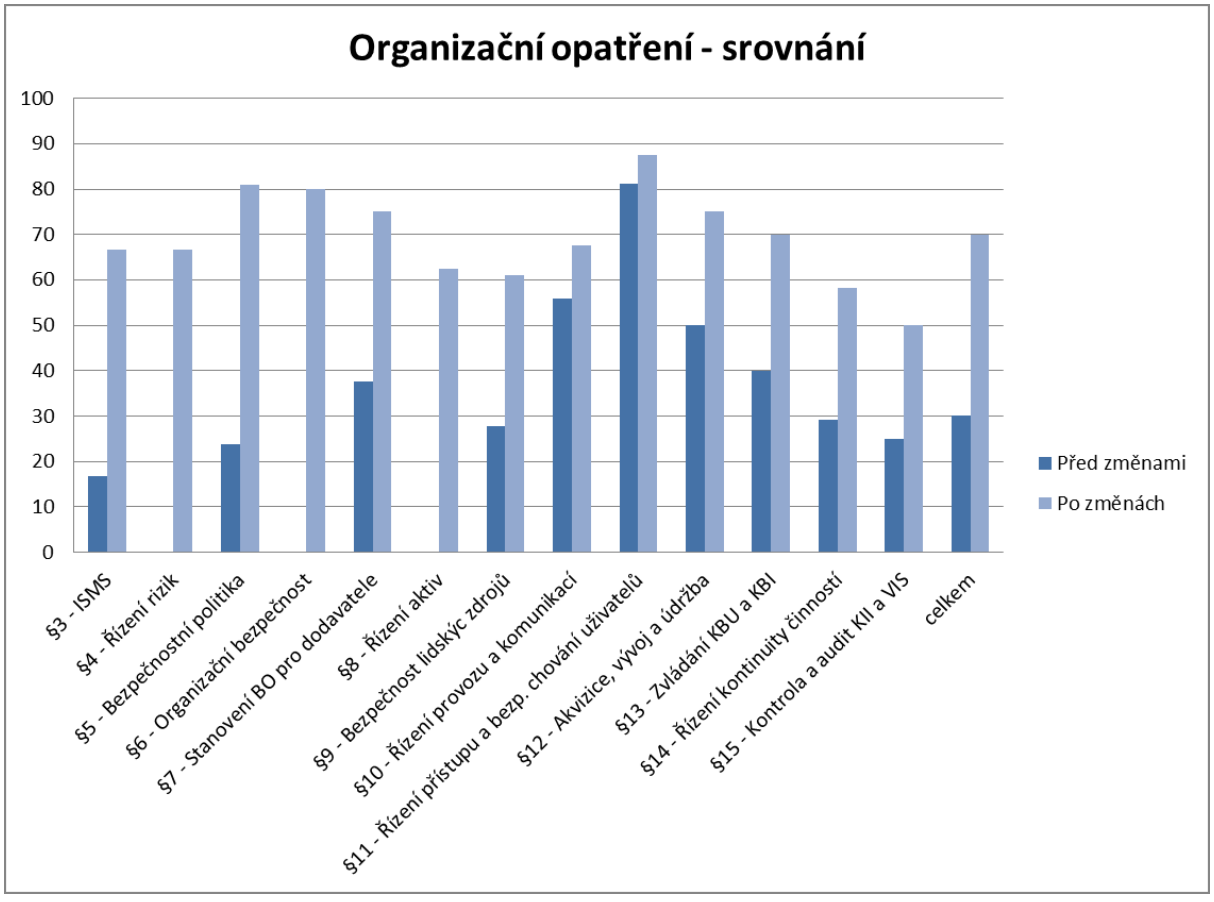
Vypracováním těchto dokumentů se skóre naplnění souladu se Zákonem o kybernetické bezpečnosti značně vylepšilo. Dá se předpokládat, že se v horizontu jednoho roku ještě dále vylepší. Formálním ustanovením příslušných dokumentů byl totiž učiněn pouze první, byť podstatný, krok. Dalším krokem bude důsledné vymáhání nově

stanovených procesů a vžití těchto procesů do běžného pracovního běhu zaměstnanců Úřadu.

Oblast technických opatření byla už v době provádění srovnávací analýzy na dobré úrovni. Přesto i opatřením v této oblasti byla věnována pozornost. Stanovením jasného postupu řízení bezpečnostních incidentů i vyladěním nástrojů pro sběr a vyhodnocení kybernetických bezpečnostních událostí bylo zlepšeno skóre Úřadu i zde.

5.3 Zhodnocení přínosů opatření

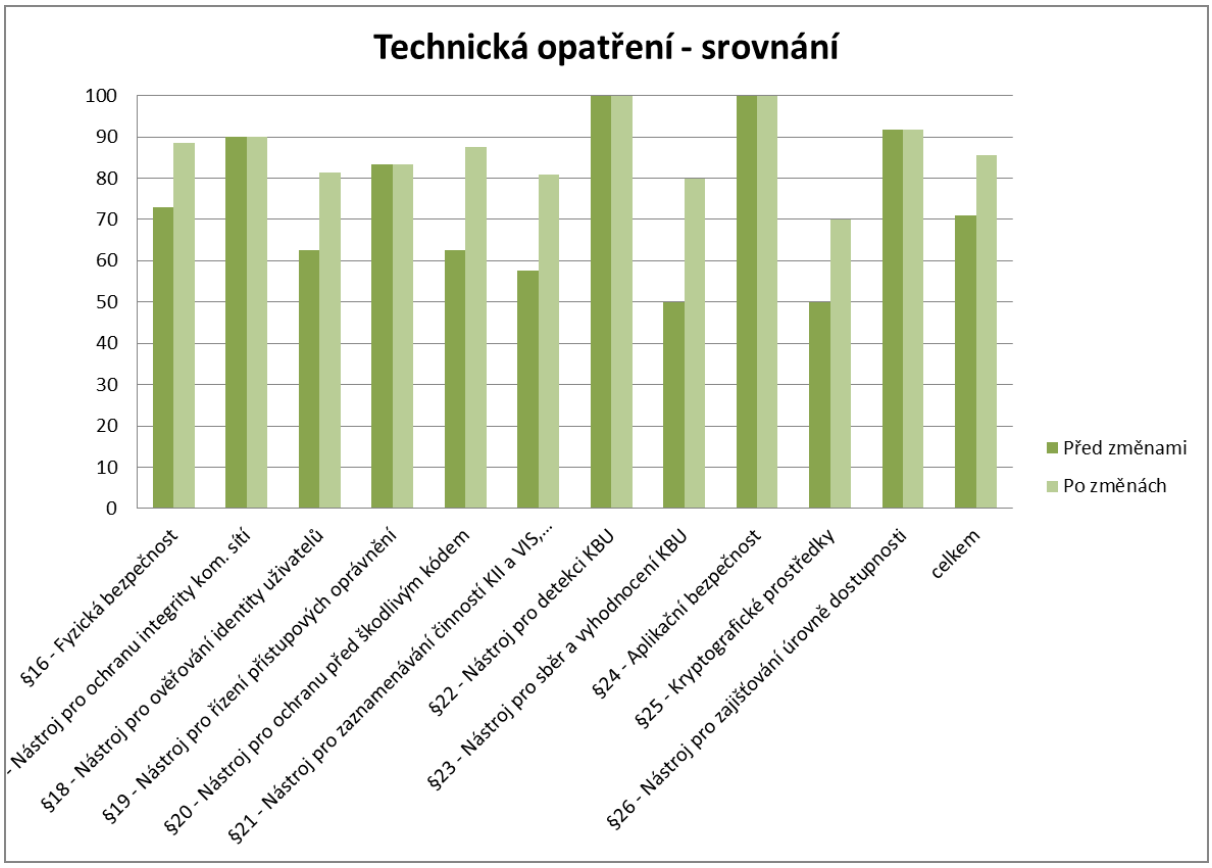
Přínosy, které přinesla provedená opatření, shrnují následující dva grafy. Jde o porovnání dosažené shody se Zákonem o kybernetické bezpečnosti v oblastech organizačních i technických opatření.



Obrázek 34 - 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.



Obrázek 35 - Srovnání hodnocení dosažení shody se ZKB - technická opatření (vlastní zpracování)

Z grafu srovnání hodnocení shody technických opatření vyplývá, že už tak dobré výsledky byly provedenými opatřeními mírně zlepšeny. Celkové hodnocení shody s požadavky ZKB se vyšplhaly ze 70 na 85 %. Důraz byl kladem především na zlepšení opatření, která měla v provedené srovnávací analýze nejnižší skóre.

K udržení dosažené míry shody bude však důležité to, jak se Úřad dokáže v budoucnu vypořádat s akutním nedostatkem kvalifikovaných odborníků právě v oblasti analýzy kybernetických bezpečnostních událostí a správy těchto bezpečnostních technologií. Obecně zde platí, že technologie Úřad má, základní zavedení do provozu a výchozí konfigurace proběhla, ale samotná práce s technologiemi a zpracování a analýza výstupů z těchto technologií vyžaduje tým expertů, které Úřad nemá. Chybí jejich

dostatečný počet i patřičná odbornost. S tím, jak jsou postavena kritéria Služebního zákona v oblasti ohodnocení úředníků, není reálné, že Úřad sežene takto kvalifikované pracovníky. Jedinou reálnou šancí Úřadu je hledat pracovní sílu mezi čerstvými absolventy bez praxe v oblasti kybernetické bezpečnosti a vychovat si je dle aktuální potřeby. Toto řešení je však velmi neefektivní, protože samotné vyškolení alespoň na základní přijatelnou úroveň trvá řádově roky a po jejím dosažení inklinují tito pracovníci k odchodu do soukromé sféry, kde dostávají i dvojnásobné finanční ohodnocení. Druhou možností je zajištění dostatečné úrovně odbornosti prostřednictvím outsourcingu příslušných služeb. Tato možnost je drahá a do jisté míry snižuje předchozí rozhodnutí Úřadu investovat do nasazení vlastních bezpečnostních technologií.

5.4 Ekonomická stránka implementace opatření

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.

Z hlediska investic byl pro Úřad výhodou fakt, že už před návrhem technických opatření disponoval potřebnými technologiemi a nemusel tedy vynakládat milionové investice do drahého vybavení. Nad rámec plánovaných investic investoval především do zajištění servisní podpory a dílčích konfiguračních a poradenských činností nástroje SIEM, prodloužení servisní podpory nástroje Flowmon, servisní podpory a rozvojových prací do nástroje pro identity management a licencí nástroje pro správu hesel. Do nákladů technických opatření patří také výdaje za zajištění aplikační bezpečnosti v podobě provádění bezpečnostních a penetračních testů.

Jednorázové náklady - technická opatření	**Cena**
Konfigurační a poradenské služby SIEM	48 000 Kč
Licence nástroje pro správu hesel	250 000 Kč
Konfigurační činnosti na SIEM (interně 28 MD)	72 800 Kč
Konfigurační činnosti na Flowmon (interně 25 MD)	65 000 Kč
Konfigurační činnosti správa hesel (interně 4 MD)	10 400 Kč
Celkem	**298 000 Kč**

Tabulka 3 - Jednorázové náklady na technická opatření

Pravidelné roční náklady - technická opatření	Cena/rok
Servisní podpora SIEM	295 000 Kč
Servisní podpora Flowmon	315 000 Kč
Bezpečnostní a penetrační testy aplikací	490 000 Kč
Celkem	**1 100 000 Kč**

Tabulka 4 - Pravidelné roční náklady na technická opatření

Některé z nákladů byly vynaloženy jednorázově pro dosažení konkrétního dílčího cíle, jiné jsou pravidelnými ročními náklady. Kromě nákladů uvedených v tabulce je třeba počítat ještě s nákladem lidského kapitálu pro správu bezpečnostních nástrojů a analýzu bezpečnostních událostí v odhadované výši 500 MD ročně. Což je při ceně 2600,- Kč na 1 MD zaměstnance Úřadu roční náklad ve výši 1 300 000,- Kč.

V oblasti organizačních opaření Úřad více využil interní práce zaměstnanců. Externě financoval jen úvodní srovnávací analýzu a audity ISMS na jednotlivých informačních systémech.

Organizační opatření	Cena
Úvodní GAP analýza	250 000 Kč
Audity ISMS	320 000 Kč
Tvorba dokumentací (interně 120 MD)	312 000 Kč
Provádění auditu (interně 40 MD)	104 000 Kč
Celkem	**882 000 Kč**

Tabulka 5 - Náklady na organizační opatření

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) na správu používaných bezpečnostních technologií a provádění analýz zachycených bezpečnostních událostí. Další zhruba půl pracovního úvazku vynakládá Úřad na personální zajištění organizačního zabezpečení ISMS.[38] Personální zabezpečení kybernetické bezpečnosti je v současné době v případě Úřadu ne zcela dostatečné. Úřad se potýká s nedostatkem osob kvalifikovaných v oblasti kybernetické bezpečnosti i v oblasti ICT. Pokud se toto nepodaří

[38] Do přehledu nákladů vynaložených na popisovaná bezpečnostní patření nebyly započítány náklady (a pracovní úvazky) potřebné na zajištění běžného provozu, které by byly vynaloženy i v případě, že by se tato opatření nerealizovala.

v dohledné době výrazně zlepšit, bude muset více investovat do outsourcingu některých služeb.

6 Závěr

Hlavním cílem práce bylo dosáhnout takových bezpečnostních opatření, které jsou ve shodě s požadavky Zákona o kybernetické bezpečnosti. K tomuto cíli vedlo vypracování chybějící nebo nedostatečně zpracované interní dokumentace Úřadu. Především bezpečnostní politiky a dokumentů definujících systém řízení bezpečnosti informací. Z technických opatření pak bylo třeba zaměřit se na správnou konfiguraci nástrojů pro detekci, sběr a vyhodnocování kybernetických bezpečnostních událostí.

Prostřednictvím navržených organizačních i technických bezpečnostních opatření bylo dosaženo podstatného přiblížení ke shodě se Zákonem o kybernetické bezpečnosti. Došlo výraznému zlepšení především v oblasti organizačních opatření, kde z původní míry souladu v hodnotě cca 30 % bylo dosaženo zvýšení až k 70 %. V oblasti technických opatření pak došlo ke zlepšení z původních 70 % na zhruba 85 %. Pro úplný soulad se ZKB je třeba ještě vylepšit některá z opatření a především také zajistit jejich dlouhodobé udržování.

Díky tomuto vylepšení celkových bezpečnostních opatření prošel Úřad úspěšně metodickým auditem NBÚ zaměřeným na posouzení stavu jednoho z jeho informačních systémů s požadavky ZKB.

Zdokonalením technických opatření týkajících se nástrojů pro detekci, sběr a vyhodnocení kybernetických událostí bylo dosaženo relevantnějšího řešení kybernetických bezpečnostních událostí a incidentů. Tím se také zlepšila možnost kontroly zabezpečení aktiv Úřadu.

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.

7 Seznam použitých zdrojů

1. **McAfee**. *Net Losses: Estimating the Global Cost of Cybercrime Economic - impact of cybercrime II*. McAfee. [Online] 2014. [Cit.: 24. listopad 2016.] (PDF). Dostupné z WWW: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

2. **MORGAN, Steve**. *Cyber Crime Costs Projected To Reach $2 Trillion by 2019*. Forbes. [Online] Forbes, 17. leden 2016. [Cit.: 24. listopad 2016.] Dostupné z WWW: http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#238139003bb0.

3. **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

4. **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.

5. **ČR NBÚ**. *Věcný záměr zákona o kybernetické bezpečnosti*. Národní centrum kybernetické bezpečnosti. [Online] 30. květen 2012. [Cit.: 21. září 2016.] (PDF). Dostupné z WWW: https://www.govcert.cz/download/legislativa/container-nodeid-926/vecny-zamer-final-vlada.pdf.

6. **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

7. **ČSN** ISO/IEC 27001:2005 *Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2006. Třídící znak 36 9790.

8. **RÓZANSKI, Krzysztof**. *Secure Architecture for an SQL / Web Server*. WindowSecurity.com. [Online] 10. prosinec 2003. [Cit.: 24. listopad 2016.] Dostupné z WWW: http://www.windowsecurity.com/articles-tutorials/web_server_security/Secure_Architecture_SQL_Web_Server.html.

9. **Cisco Networking Academy**. *Cisco Networking Academy's Introduction to VLANs*. CiscoPress.com. [Online] Cisco Press, 7. duben 2014. [Cit.: 24. listopad 2016.] Dostupné z WWW: http://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=4.

10. **GIBSON, Steve**. *How Big is Your Haystack?* Gibson Research Corporation. [Online] 28. březen 2012. [Cit.: 13. říjen 2016.] Dostupné z WWW https://www.grc.com/haystack.htm.

11. **Microsoft Corporation**. *Oprávnění souborů a složek*. TechNet. [Online] Microsoft Corporation. [Cit.: 27. říjen 2016.] Dostupné z WWW: https://technet.microsoft.com/cs-cz/library/cc732880(v=ws.11).aspx.

12. **Mandiant**. M-TRENDS 2015: *A view from the frontlines*. FireEye. [Online] 24. únor 2015. [Cit.: 6. listopad 2016.] Dostupné z WWW: https://www.fireeye.com/offers/2015-security-trends-mtrends-view-from-the-frontlines-taboola.html.

13. **Ponemon Institute LLC**. *The State of Malware Detection & Prevention*. Ponemon.org. [Online] březen 2016. [Cit.: 6. listopad 2016.] Dostupné z WWW: http://www.ponemon.org/blog/new-ponemon-study-on-malware-detection-prevention-released.

14. **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.

15. **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

16. **Cisco Systems**, **Inc**. *Campus Network for High Availability Design Guide*. Cisco.com. [Online] Cisco Systems, Inc., 21. květen 2008. [Cit.: 17. listopad 2016.] Dostupné z WWW: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html.

17. **Flowmon Networks**. *Seznam modelů Flowmon sond*. Flowmon. [Online] 12. říjen 2016. [Cit.: 30. leden 2017.] (PDF). Dostupné z WWW: https://www.flowmon.com/getattachment/da606f00-747a-461c-b3a9-150837967c5e/Flowmon-Probe-Spec.aspx.

18. **Flowmon Networks**. *Seznam modelů Flowmon kolektorů*. Flowmon. [Online] 1. červenec 2016. [Cit.: 30. leden 2017.] (PDF). Dostupné z WWW: https://www.flowmon.com/getattachment/df711231-b60b-4567-b303-8db6125483e4/Flowmon-Collector-Spec.aspx.

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

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

21. **ESET, spol. s r.o**. *ESET Virus Radar*. [Online] ESET, spol. s r.o., 8. březen 2017. [Cit.: 8. březen 2017.] Dostupné z WWW: http://virusradar.com/en/JS_TrojanDownloader.Nemucod/chart/month.

22. **Payload Security**. *Free Automated Malware Analysis Service*. hybrid-analysis.com. [Online] Payload Security, 3. březen 2017. [Cit.: 3. březen 2017.] Dostupné z WWW: https://www.hybrid-analysis.com/sample/7396b32bafae312079c866f9a975f5ae9ccf22a55f65d80a72743b3f95f68910?environmentId=100.

23. **CLAISE, B.** *Cisco Systems NetFlow Services Export Version 9*. The Internet Engineering Task Force. [Online] říjen 2004. [Cit.: 20. únor 2016.] Dostupné z WWW: https://tools.ietf.org/html/rfc3954.

24. **CLAISE, B., TRAMMELL, B. a AITKEN, P**. *Specification of the IP Flow Information Export (IPFIX) Protocol*. Internet Engineering Task Force. [Online] září 2013. [Cit.: 20. únor 2016.] Dostupné z WWW: https://tools.ietf.org/html/rfc7011.

25. **GONG, Yiming**. *Detecting Worms and Abnormal Activities with NetFlow, Part 2*. Symantec Connect. [Online] Symantec Corporation, 7. leden 2015. [Cit.: 22. únor 2016.] Dostupné z WWW: http://www.symantec.com/connect/articles/detecting-worms-and-abnormal-activities-netflow-part-2.

26. **Flowmon Networks**. *Pakety nelžou. Kompletní záznam datové komunikace pro forenzní analýzu sítě*. Flowmon. [Online] 2015. [Cit.: 4. duben 2016.] Dostupné z WWW: https://www.flowmon.com/cs/products/flowmon/traffic-recorder.

27. **Flowmon Networks**. *Flowmon DDoS defender: vyspělá ochrana před volumetrickými útoky*. Flowmon. [Online] Flowmon Networks, 2015. [Cit.: 4. duben 2016.] Dostupné z WWW: https://www.flowmon.com/cs/products/flowmon/ddos-defender.

28. **PETERKA, Jiří**. *Archiv článků a přednášek Jiřího Peterky*. eArchiv.cz. [Online] 1992. [Cit.: 16. listopad 2016.] Dostupné z WWW: http://www.earchiv.cz/a92/a213c110.php3.

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

30. **ČESKO**. Zákon č. 430/2010 Sb. ze dne 30. prosince 2010, kterým se mění zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). In: *Sbírka zákonů České republiky*. 2010, částka 149, s. 5602-5616. ISSN 1211-1244. (PDF) Dostupné také z: http://ftp.aspi.cz/opispdf/2010/149-2010.pdf

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

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

8 Přílohy

Příloha A – Obsah Bezpečnostní politiky Úřadu