LINUX SERVICES

Doporučení pro zařízení pro detekci a obranu proti zneužití systému (IDS/IPS/Honeypot)

Z hlediska zákona o kybernetické bezpečnosti

Ing. Jiří Richter
Ing. Michal Vymazal

Srpen 2015

Úvod

Tato nabídka je relevantní k bezpečnostní dokumentaci a bezpečnostním opatřením subjektů (právnické osoby, fyzické osoby) na něž se vztahuje zákon 181/2014 Sb. (Zákon o kybernetické bezpečnosti).

V textu jsou vždy uvedeny názvy jednotlivých dokumentů technického projektu, jednotlivá doporučení a odkazy na jednotlivé dokumenty (EU, NIST), dle kterých jsme nabídku zpracovávali.

Obsah

Zařízení pro detekci hrozeb a jejich prevenci (IDS/IPS)

Jedná se o zařízení, které je součástí technických opatření dle Hlavy II, §22 a §23 Vyhlášky 316/2014 Sb. (Vyhláška k zákonu o kybernetické bezpečnosti, Nástroj pro detekci kybernetických bezpečnostních událostí a Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí).

Vlastní specifikaci zařízení (požadavky na funkčnost) jsme stanovili dle metodik a dokumentace národních bezpečnostních autorit členských zemí EU (konkrétně BSI) a dále dle dokumentů a metodik NIST.

Vlastní zařízení může podle potřeb pracovat v několika režimech:

1. **Režim IDS/IPS**. V tomto režimu zařízení vyhodnocuje hrozby v reálném čase (IDS) a provádí potřebná opatření k odvrácení útoku (IPS). Je zde tedy užito i jisté míry interakce se síťovým provozem.

2. **Honeypot**, tedy systém, který má útočníky přilákat na produkční zařízení, které nemá jiné uživatele než administrátory monitorující a zaznamenávající jejich činnost.

3. **Klamný cíl**. Ten se chová podobně jako Honeypot, ale je nasazován v případě ohrožení produkčního stroje jako alternativní cíl, na kterém útočník nemůže napáchat nenahraditelné škody.

Požadované vlastnosti zařízení

- soulad funkčnosti zařízení s metodikami a doporučeními národních bezpečnostních autorit členských zemí EU
- více síťových rozhraní, jedno je public, ostatní jsou dostupná pouze z interní sítě (private)
- zařízení se nachází v zabezpečeném perimetru, přístup pouze pro povolané osoby (konkrétně se jedná zejména o přístup ke konzoli)
- admin přístup na zařízení pouze pomocí věrohodné šifrované služby (SSH server apod.)
- veškerý kód a veškeré procesy jsou pod kontrolou provozovatele
- může být provozován na samostatném HW nebo na virtuálu. Obojí má své výhody a nevýhody.
- v případě, že zařízení představuje "klamný cíl", pak se jedná o plnohodnotný cíl
- všechny procesy jsou logovány ve formátu syslog, logy jsou uchovávány lokálně a dále (1:1) zasílány na syslog logserveru, který je v "bezpečné zóně".
- celé zařízení je možné obnovit z image nebo ze záložního archivu (výchozí konfigurace + dílčí konfigurace).
- kompletní dokumentace všech nainstalovaných a provozovaných služeb.
- logy (týkající se činnosti zařízení) vyhodnocuje jak vlastní zařízení, tak logserver v "bezpečné zóně".
- několik typových zapojení (průchozí, jako sonda, paralelní sonda, klamný cíl)
- možnost povolování a zakazování dílčích IP adres nebo celých rozsahů na public síťovém rozhraní
- žádná osobní ani citlivá data na zařízení
- škálovatelnost
- interoperabilita – systém dokáže vyhodnocovat jevy na síti pro všechny zadané systémy

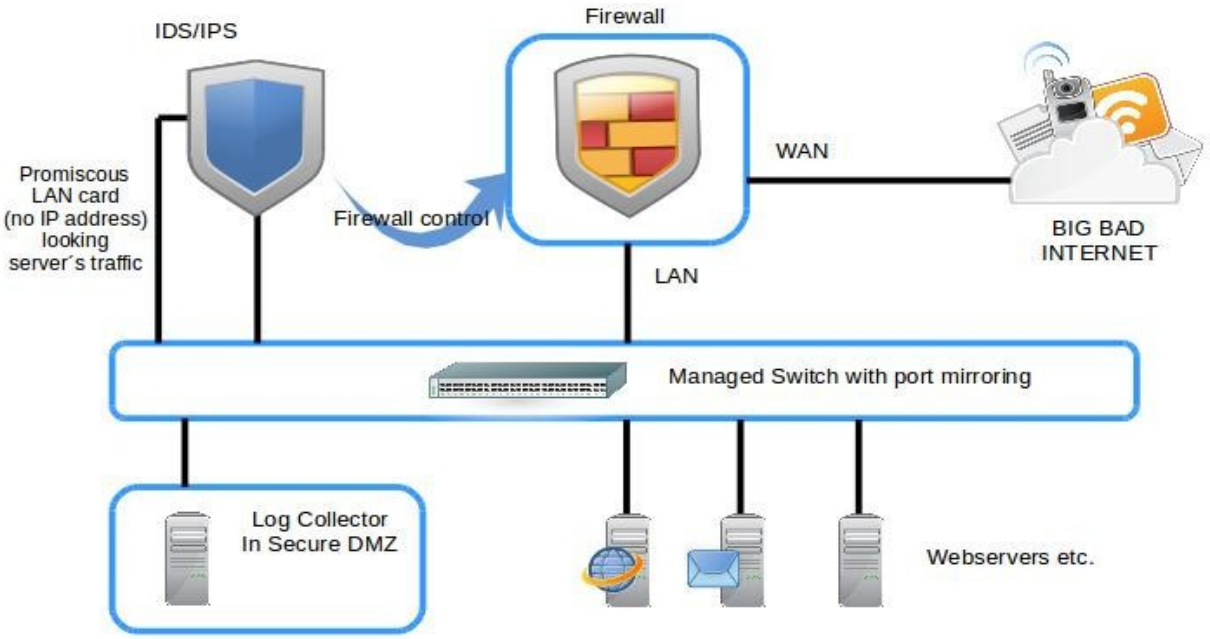
IDS/IPS

IDS/IPS (Intrusion Detection System /Intrusion Prevention System) je systém detekce a prevence síťových útoků. Může být použit pro ochranu konkrétního počítače či nasazen na internetové bráně a chránit tak celou lokální síť, která je přes tuto bránu připojena k Internetu. Analyzuje veškerou síťovou komunikaci, v níž rozpoznává a blokuje známé typy útoků (například port scanning, DoS aj.) a rovněž analyzuje určité podezřelé aktivity, čímž může zabránit i dosud neznámým typům útoků.

Intrusion Detection System (systém pro odhalení průniku) je obranný systém, který monitoruje síťový provoz a snaží se odhalit podezřelé aktivity.

Intrusion Prevention Systems (systémy pro prevenci průniku) jsou zařízení přímo podporující zabezpečení kybernetického prostoru. Hlavní funkcí je identifikace škodlivé činnosti, zaznamenávání informací o jejím průběhu, její nahlašování (např. odesláním logů na log collector), případně blokování. Hlavní rozdíl oproti IDS systémům je ten, že IPS je zařazen přímo do síťové cesty. Může provádět vyvolání poplachu, filtrování škodlivých paketů, násilné resetování spojení či blokování provozu z podezřelé IP adresy. Všechny tyto úkony často provádí ve spolupráci s firewallem. Také umí defragmentovat proudy paketů, předcházet problémům s řazením TCP paketů a čistit nežádoucí přenos včetně nastavení síťové vrstvy.

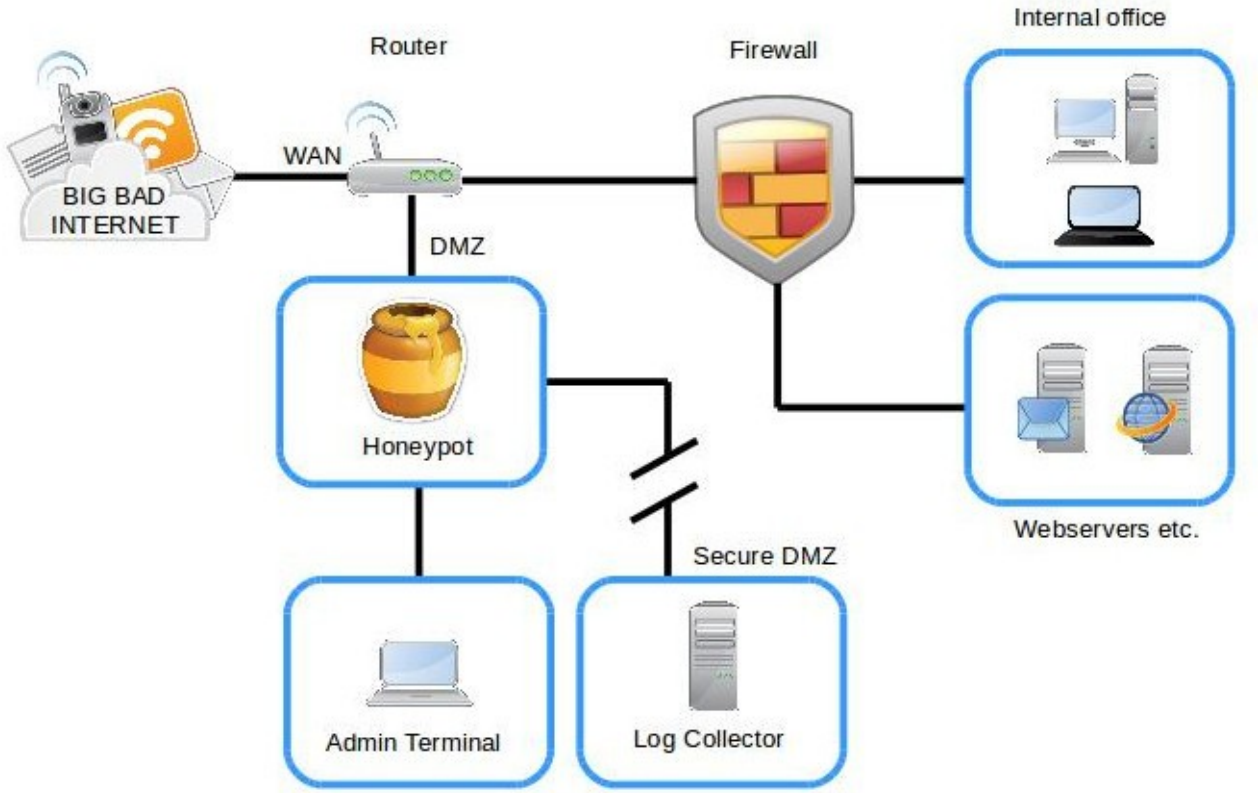
Celé toto zařízení je samozřejmě možné postavit na bázi open source. Zde konkrétně se jedná o programové vybavení zvané SNORT (www.snort.org), které využívají i národní bezpečnostní autority EU (např. BSI – německá národní bezpečnostní autorita, odkaz zde a zde). SNORT má dvě licenční strategie, GNU General Public License (GPL) a Non-Commercial Use License for the Proprietary Snort® Rules.



Honeypot

Honeypot (nebo-li „hrnec medu“) je informační systém, jehož účelem je přitahovat potenciální útočníky a zaznamenat jejich činnost.
Honeypoty jsou užívány zejména pro včasné detekování malwaru a následnou analýzu jeho chování. Malwary stále mění svoji strategii útoku a různými způsoby se skrývají a vyhýbají nalezení. Z těchto důvodů je nutno malware nějak nalákat a poté analyzovat jeho chování – takto získané informace se mohou použít pro aktualizování antivirových systémů. Problém je, že nelze jednoduše zjistit aktivitu malwaru v reálném systému, který byl napaden. Nicméně honeypoty zneklidňují případné útočníky, protože ti si nejsou nikdy jisti, jestli při průniku do systému nebudou odhaleni.

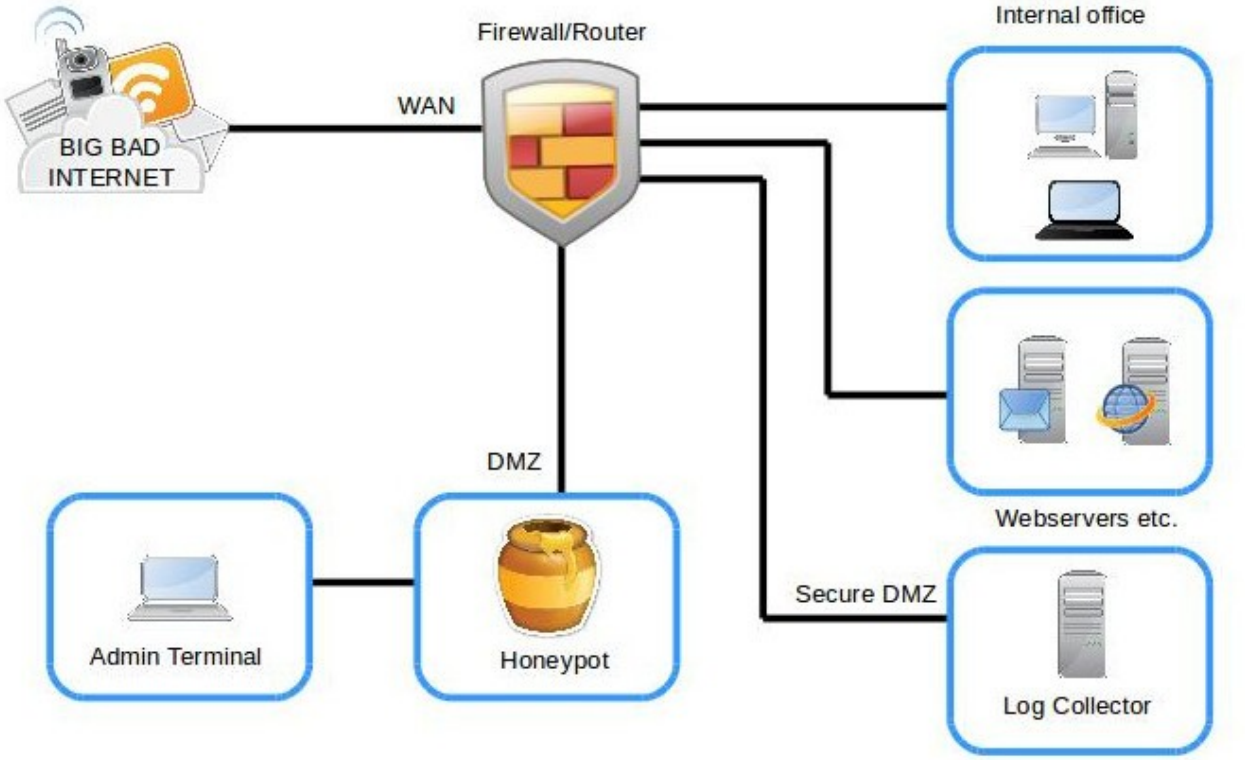
Honeypoty detekují činnost neoprávněných zdrojů přicházejících do systému. Tato detekce je po odhalení útočníka plně automatická. Automaticky se sbírají data o činnosti potenciálního útočníka. Detekce buď vyloučí, že se jednalo o útočníka, nebo to jen potvrdí. Je to rychlejší, než kdyby se sbírala data z funkčního napadeného systému. Honeypoty se někdy sdružují do sítě, tzv. **honeynetu**. V těchto sítích jsou sdílena data o malwarech a jejich trendech. Nejčastěji jsou to způsoby šíření, užité algoritmy v malwaru, atd.



Honeypot jako klamný cíl

Honeypoty (honeynety) jsou také užívány jako klamné cíle v případě napadení produkčního systému. Jejich nasazení má za cíl útočníka nasměrovat do prostředí, ve kterém je jeho činnost do detailu pozorovatelná. Obránce tak má možnost zjistit například míru jeho dovedností nebo zda má konkrétní specifické znalosti, které by jinak než od pracovníka zevnitř nezískal.

Přesměrování útočníka na honeypot nejčastěji provádí administrátor úpravou směrovacích tabulek na základě vyhodnocení alertů z Log Collectoru. Lze však využít i automatického přesměrování na základě předem očekávaného typu útoku pomocí pravidel a skriptů na firewallu (SNORT, Fail2ban).



Operační systém

Jako operační systém je vhodná jedna z osvědčených linuxových distribucí, které jsou převážně šířeny pod nekomerční licencí GNU GPL 2.0, popřípadě LGPL 2.1.

Doporučené distribuce jsou např. UBUNTU Server LTS a Debian.

http://www.ubuntu.com/server

http://www.debian.org/

Instalované síťové služby

Na zařízení jsou instalovány tyto výchozí síťové služby

- SSH server (open_ssh server)
- NFS server
- SMTP server
- syslog server
- mysql server
- Apache server (www server vč.PHP, redakčních systémů a věrohodných webů s falešnými údaji v backoffice)
- LDAP server
- DNS server
- DHCP server
- TFTP server

Poznámka:

„Falešná data“ pro výše uvedené síťové služby nejsou součástí dodávky. Součástí dodávky je pouze výchozí konfigurace jednotlivých démonů a dále založení uživatelských účtů nezbytných pro administrátorský přístup k danému zařízení (open_ssh_server).

Softwarové nástroje

Na zařízení jsou instalovány tyto výchozí nástroje pro detekci hrozeb

- SNORT – open source síťový IDS a IPS systém

Hardwarové prostředí

Instalace na samostatný fyzický stroj je preferovaná varianta, protože má stoprocentní přístup k fyzickým prostředkům zařízení, zejména jde o síťová rozhraní.

Bude mít k dispozici minimálně 3 síťová rozhraní

- public rozhraní na straně útočníka
- interní rozhraní pro správu a dohled
- interní rozhraní pro sběr událostí (možnost sledování provozu v celé síti)

Požadavky HW prostředků pro plně funkční honeypot jsou

- 8 jader CPU
- 32GB RAM
- 250GB diskového prostoru v RAID1

Vzhledem k tomu, že se jedná o důležité zařízení z hlediska ZKB, musí mít vysokou spolehlivost a ze všech variant diskových prostorů se RAID1 jeví jako nejspolehlivější.
Dalším předpokladem spolehlivosti je zajištění redundantního napájení.

Varianta instalace na virtuální stroj

Zařízení bude nainstalováno na virtualizační vrstvě s technologií KVM. Bude mít k dispozici minimálně 3 síťová rozhraní

- public rozhraní na straně útočníka
- interní rozhraní pro správu a dohled
- interní rozhraní pro sběr událostí

Požadavky HW prostředků pro plně funkční honeypot jsou

- 8 jader CPU
- 32GB RAM
- 200GB diskového prostoru

Ukládání a vyhodnocování logů

Vlastní logy budou ve formátu syslog (RFC 5424) ukládány jednak lokálně (na vlastní filesystém zařízení – např. /var/log/) jednak (v poměru 1:1) odesílány na syslog centrálního log serveru. Centrální logserver je umístěn v zabezpečené zóně. Pro lokální vyhodnocování logů bude využit nástroj logcheck. V případě potřeby (např. interakce útočníka) je možné spustit adaptivní firewall fail2ban.

Logcheck

http://logcheck.org/

Poměrně výkonný analyzátor logů šířený pod GNU GPL licencí. Analyzuje logy a podle předem nastavených pravidel je zařazuje a posílá např. mailem nebo prostřednictvím SMS předem určeným bezpečnostním rolím. Spouštěn je prostřednictvím CRON. Pravidla pro analýzu logů je samozřejmě možné upravovat, je možné spouštět logcheck s různými konfiguračními soubory (a analyzovat tak pokaždé jinou množinu logů).

Adaptivní firewall – fail2ban

Jedná se o velmi účinný adaptivní firewall, který je součástí prakticky každé linuxové distribuce.

https://en.wikipedia.org/wiki/Fail2ban
http://www.fail2ban.org/wiki/index.php/Main_Page

V systému (na serveru) běží démon fail2ban (napsáno v jazyce Python), který registruje změny v předem určených souborech log systému. Pokud nalezne v daném logu předem danou kombinaci textu (např. Invalid user, spoof syn - těch "varovných výrazů“ je celá řada - fali2ban je má předem dané v samostatnych konfiguračních souborech), pak fail2ban vydá pokyn k určité činnosti. Máme na výběr z těchto kroků:

- Pokyn firewallu (integrovaném v jádru linuxu) a firewall IP adresu "útočníka" dočasně zablokuje.
- Pouze mailové hlášení, nedojde k zablokování IP adresy útočníka
- Spuštění jiného skriptu

Výše uvedené kroky je samozřejmě možné kombinovat. Filtry pro fail2ban je

možné samozřejmě upravovat, doplnit vlastními filtry apod.

Mail hlášení adminovi obsahuje:

- IP adresu utočníka
- Úplný popis IP rozsahu (CIDR) včetně identifikace providera
- Výpis z logu, kde se vyskytuje IP adresa útočníka

Ukázka hlášení administrátorovi:

Hi,
The IP 109.230.94.54 has just been banned by Fail2Ban after
6 attempts against ssh.
Here are more information about 109.230.94.54:
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf
% Note: this output has been filtered.
% To receive output for a database update, use the "-B" flag.
% Information related to '109.230.94.0 - 109.230.94.255'
inetnum: 109.230.94.0 - 109.230.94.255
netname: KFZO
descr: Kish Free Zone Organization
country: IR
admin-c: AV5398-RIPE
tech-c: AV5398-RIPE
status: ASSIGNED PA
mnt-by: mnt-boom
source: RIPE # Filtered
person: Afshin Vafaei
address: Kish Free Zone Organization-Kish Island
phone: +987644422048
nic-hdl: AV5398-RIPE
source: RIPE # Filtered
% Information related to '109.230.80.0/20AS50591'
route: 109.230.80.0/20

descr: Boomerang-Route2
origin: AS50591
mnt-by: MNT-BOOM
mnt-lower: MNT-BOOM
mnt-routes: MNT-BOOM
source: RIPE # Filtered
% This query was served by the RIPE Database Query Service version 1.67.4 (WHOIS1)
Lines containing IP:109.230.94.54 in /var/log/auth.log
Aug 7 19:16:36 server sshd[27434]: refused connect from 109.230.94.54 (109.230.94.54)
Aug 7 19:16:36 server sshd[27435]: refused connect from 109.230.94.54 (109.230.94.54)
Aug 7 19:16:36 server sshd[27436]: refused connect from 109.230.94.54 (109.230.94.54)
Aug 7 19:16:36 server sshd[27437]: refused connect from 109.230.94.54 (109.230.94.54)
Aug 8 23:08:56 server sshd[3386]: refused connect from 109.230.94.54 (109.230.94.54)
Aug 8 23:08:56 server sshd[3390]: refused connect from 109.230.94.54 (109.230.94.54)
Aug 8 23:08:56 server sshd[3388]: refused connect from 109.230.94.54 (109.230.94.54)
Aug 8 23:08:56 server sshd[3391]: refused connect from 109.230.94.54 (109.230.94.54)
Aug 8 23:08:56 server sshd[3387]: refused connect from 109.230.94.54 (109.230.94.54)
Aug 8 23:08:56 server sshd[3389]: refused connect from 109.230.94.54 (109.230.94.54)

Regards,
Fail2Ban

SW licence

Naprostá většina použitého softwaru včetně OS je šířena pod licencí GNU GPL.

GNU General Public License, **GNU GPL** (česky „všeobecná veřejná licence GNU“) je licence pro svobodný software, původně napsaná Richardem Stallmanem pro projekt GNU. GPL je nejpopulárnějším a dobře známým příkladem silně copyleftové licence, která vyžaduje, aby byla odvozená díla dostupná pod toutéž licencí. V rámci této filosofie je řečeno, že poskytuje uživatelům počítačového programu práva svobodného softwaru a používá copyleft k zajištění, aby byly tyto svobody ochráněny, i když je dílo změněno nebo k něčemu přidáno. Toto je rozdíl oproti permisivním licencím svobodného softwaru, jejímž typickým případem jsou BSD licence.

Školení, dokumentace, údržba, životní cyklus

Školení proběhne v místě dle zadavatele, viz poptávka. Školení zaměstnanci jsou před započetím školení povinni se podrobně seznámit s dokumentací systému. Znalost síťových protokolů a standardních open-source systémů použitých v systému (apache,...) se u zaměstnanců předpokládá apriori. Školitel není povinen v rámci zadání školit zaměstnance o funkci standardních protokolů (telnet, tcp...), standardních sítových systémů a procesů, standardní znalosti konfigurace ethernet sítí. Takové nadstandardní školení je samozřejmě možné zajistit, je to však potřeba učinit předem.

Dokumentace se skládá z popisu řešení, instalační příručky, provozního manuálu, popisu výstupů (logů, událostí), dle bodu Specifikace dokumentace poptávky.

Údržbu systému může provádět na přání zadavatele dodavatel, který pak přebírá zodpovědnost za jeho provoz, pokud mu k tomu dodavatel poskytne nezbytné prostředky. Vzhledem k tomu, že se jedná o řešení na bázi open-source, může údržbu provádět sám zadavatel dle dokumentace, pak je zcela zodpovědný za jeho funkci.

Údržba spočívá v kontrole běhu systému, pravidelných updatech sw komponent, pravidelných updatech bezpečnostních pravidel, a přizpůsobení

systému aktuálním normám.

Životní cyklus spočívá hlavně v pravidelných updatech sw komponent systému, a bezpečnostních pravidel. Ze zadání vyplývá, že systém bude využíván provozovatelem v režimu 24/7 a bezpečnostní pravidla si bude nastavovat a spravovat provozovatel sám. Potom se bude řídit provozním manuálem a doporučeními dodavatele. S ohledem na životní cyklus použitých open-source komponent se předpokládá maximální doporučený interval pro update sw komponent o délce 6ti měsíců. V případě, že se vyskytnou 0-day zranitelnosti jednotlivých komponent, je logická neprodlená reakce.

Platná legislativa, metodiky národních bezpečnostních autorit EU

Níže je uveden rozpis dokumentů, ze kterých jsme vycházeli. Jedná se zejména o platnou legislativu a metodiky národních bezpečnostních autorit členských zemí EU. Dále jsme využili metodiky a dokumenty NIST.

Legislativa

Gestorem oblasti kybernetické bezpečnosti je v ČR **Národní bezpečnostní úřad** (známý též pod zkratkou NBÚ). Stalo se tak usnesením vlády ze dne 19. října 2011 č. 781 o ustanovení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. NBÚ následně vypracoval **Návrh zákona o kybernetické bezpečnosti**, jež vláda schválila. NBÚ dále vypracoval návrh vyhlášky o kybernetické bezpečnosti a vydal prohlášení k vývoji legislativy v oblasti kybernetické bezpečnosti.

Zákon o kybernetické bezpečnosti byl podepsán prezidentem Milošem Zemanem dne 13.8.2014. Zákon nabyl platnosti dnem vyhlášení ve Sbírce zákonů, účinný je od 1. ledna 2015.

Prováděcí právní předpisy k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) jsou následující:

- NAŘÍZENÍ VLÁDY č. 315/2014 Sb. ze dne 8. prosince 2014, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
- VYHLÁŠKA ze dne 15. prosince 2014 č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
- VYHLÁŠKA ze dne 15. prosince 2014 č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích

Viz.
http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/provadeci-pravni-predpisy-k-zakonu-c-1812014-sb-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu/

V této souvislosti je dobré připomenout, že i Trestní zákoník zná trestné činy související s neoprávněnými přístupy do informačních systémů, konkrétně **§ 230** nazvaný "Neoprávněný přístup k počítačovému systému a nosiči informací".

Nový občanský zákoník pak pamatuje na škodu způsobenou informací nebo radou (§ 2950 NOZ).

Metodika / Národní autority

Dle prohlášení ředitele NCKB (Národní centrum kybernetické bezpečnosti, odbor NBÚ), NCKB do vlastního zákona zapracuje odkazy na související normy a metodiky (např. ISO 27032). Dále bude respektovat metodiky relevantní (např. metodiky národních autorit členských zemí EU, NIST atp.)

Implementační scénáře

Tato otázka zatím není řešena ani legislativně, ani metodicky. Předpokládáme, že zde se situace začne rychle měnit a implementační scénáře budou jednak veřejně dostupné, jednak budou navazovat na metodiku. K dnešnímu dni můžeme odkázat na vzorové implementační scénáře volně dostupné na stránkách německé národní autority (BSI).

Bezpečnostní dokumentace

Vzhledem k faktu, že licence ISO dokumentů neumožňuje jejich „volnou“ distribuci a dále vzhledem k faktu, že ISO dokumenty nezahrnují tzv. „best practice“, rozhodli jsme se (v souladu s Č.j.: 1649/2013-NBÚ/41) využít pro jednotlivá doporučení metodik a dokumentů národních bezpečnostních autorit EU (BSI – Německá národní bezpečnostní autorita, *Bundesamt für Sicherheit in der Informationstechnik*) a NIST (National Institute of Standards and Technology, USA).

Níže uvedené dokumenty a procesy jsou v souladu s Přílohou č.4 Vyhlášky k ZKB (Vyhláška o kybernetické bezpečnosti).
http://www.govcert.cz/cs/legislativa/legislativa/

Primárními a podpůrnými aktivy jsou v tomto případě jednotlivé moduly daného zařízení. Vlastní topologie, zabezpečení a funkčnost zařízení jsou popsány výše v textu.

Výchozí dokumenty EU / NIST

Pro potřeby tohoto dokumentu jsme vycházeli z těchto metodik a dokumentů národních bezpečnostních autorit EU:

BSI

BSI-Standards

https://www.bsi.bund.de/EN/Publications/BSIStandards/standards.html

BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen

https://www.bsi.bund.de/DE/Publikationen/Studien/IDS02/gr1_htm.html;jsessionid=D1BF2F9757410A6592CAED0ACFC69206.2_cid368

BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen

https://www.bsi.bund.de/DE/Publikationen/Studien/IDS02/lf_phase3_htm.html;jsessionid=D1BF2F9757410A6592CAED0ACFC69206.2_cid368

BSI Leitfaden IT-Forensik Version 1.0.1

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/Leitfaden_IT-Forensik_pdf.html;jsessionid=D1BF2F9757410A6592CAED0ACFC69206.2_cid368

IDS Leitfaden v10

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/IDS/Leitfadenv10_pdf.html

BSI - Studie Penetrationstests

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest_pdf.html

ICS-Security-Kompendium

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.html

BSI - Study A Penetration Testing Model

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.html

NBU

Národní strategie kybernetické bezpečnosti České republiky na období let 2015 – 2020

http://www.govcert.cz/cs/informacni-servis/strategie-a-akcni-plan/

Výkladový slovník kybernetické bezpečnosti

http://www.govcert.cz/cs/informacni-servis/vykladovy-slovnik/

NIST

Publication Citation: *Guide to Intrusion Detection and Prevention Systems (IDPS)*

http://www.nist.gov/manuscript-publication-search.cfm?pub_id=50951

NIST Special Publication on Intrusion Detection Systems

http://www.21cfrpart11.com/files/library/reg_guid_docs/nist_intrusiondetectionsys.pdf

Free IDS/IPS for small businesses

http://nist.org/news.php?extend.70.6

Slovníček pojmů

Zkratka	Vysvětlení zkratky
BSI	*Bundesamt für Sicherheit in der Informationstechnik* Německá národní bezpečnostní autorita (obdoba českého NBÚ). www.bsi.bund.de
ISO	International Organization for Standardization Označení mezinárodní normy http://www.iso.org/iso/home.html
NBÚ	Národní bezpečnostní úřad www.nbu.cz
NIST	National Institute of Standards and Technology, USA http://www.nist.gov/