Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informatiky

Analýza a návrh nasazení SIEM v prostředí středního podniku

Bakalářská práce

Autor: Jan Nedbal
Studijní obor: Informační management

Vedoucí práce: Mgr. Josef Horálek, Ph. D.

Odborný konzultant: Ing. Lukáš Vízner
AG COM a.s.

Hradec Králové duben 2016

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 21.4.2016 Jan Nedbal

Poděkování:

Děkuji vedoucímu bakalářské práce Mgr. Josefu Horálkovi, Ph.D. a odbornému konzultantovi Ing. Lukáši Víznerovi za cenné rady a metodické vedení práce, které mi byly poskytnuty v průběhu zpracování této práce.

Anotace

Hrozba úniku citlivých informací je všudypřítomná a v případě kybernetického světa to platí dvojnásob. Samotný monitoring těchto hrozeb může být bez patřičných nástrojů pro firmu velmi obtížně realizovatelný. Komplexnost a rozsáhlost problému si některé organizace do nedávna odmítaly připouštět, což mohlo vést ke ztrátě informací nebo zisku. Z toho důvodu je vlastnictví takové technologie kritické pro prevenci, monitoring i zamezení reálnému útoku. Technologií zabývající se touto problematikou je Security Information and Event Management (SIEM). Tato bakalářská práce bude mít jako hlavní cíl stanovené nastínění principů a možností, které je možné implementovat v rámci středního podniku. První kapitola práce bude věnována definování bezpečnostních norem relevantních pro kontext bezpečnosti informací. Další část je věnována zákonu o kybernetickém bezpečnosti. Třetí kapitola má za úkol přinést komplexní náhled na technologii SIEM, její principy a logickou syntax. Kapitola čtvrtá představuje konkrétní řešení SIEM od společnosti IBM – Security QRadar SIEM. V kapitole páté jsou obsaženy konkrétní implementace tohoto SIEM řešení. Šestá kapitola se věnuje shrnutí poznatků práce. Závěrečná část práce je věnována doporučení a celkovým závěrům.

Annotation

Title: Security information and event management analysis and implementation for the medium business

The threat of information misuse is a problem, which bothers everyone. In case of cyber world is even worse. The monitoring of those possible security threats without so needed features could be a real issue for every organization involved. Complexity and vastness of the problem was something, that most of the organizations were used to deny. Those bad decisions could cause damage in information loss or even profit.
From the above mentioned reasons is ownership of technology, which can prevent, monitor or even stop the real cyber-attack from happening, crucial for the organization security. The technology handling those issues is called Security Information and Event management (SIEM).

This bachelor thesis will have as its main purpose defining the essential possibilities and principles, which could be implemented in the medium business infrastructure.
First chapter explains security standards, which are relevant for the context of security information. Second chapter is about so called “Law of cyber security,” which has come into force in 2015. Third chapter describes an overview about SIEM technology and its logical syntax and principles. Fourth chapter introduces specific SIEM technology from the IBM Corporation – Security QRadar SIEM. In the fifth chapter is described specific implementation of the above-mentioned QRadar solution. Sixth chapter is summing up all the relevant findings found in this thesis. The final part of the thesis is dedicated to recommendation and overall conclusions.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Problematika bezpečnosti informačních systému a informací obecně je kritickým faktorem managementu většiny organizací. V dnešní době totiž útočníci úmyslně cílí na informační zdroje organizací, které jsou často bráněny velmi špatně. Cena těchto dat a informací v nich obsažených, může být v mnohých případech nevyčíslitelná. Naštěstí si tuto skutečnost začínají uvědomovat jak organizace soukromé, tak i ty spadající pod veřejnou správu, tj. státní instituce a vlády. Protože jsou techniky útočníků čím dál víc propracovanější, je užití technologie, umožňující prevenci, detekci a monitoring těchto kybernetických hrozeb, nutností. Takovýto globální pohled nad celou infrastrukturou organizace nabízí právě Security Information and Event Management (SIEM).

V rámci svého působení ve firmě AG COM a.s., jako externista pro bezpečnostní řešení a Big Data, mi byla nabídnuta možnost zpracovat práci věnující se této problematice. V souvislosti s tímto tématem byl vydán Zákon o kybernetické bezpečnosti, díky kterému vznikla stovkám firem ve veřejné správě povinnost implementovat řadu bezpečnostních prvků, z nichž několik splňuje právě technologie SIEM.
Z výše uvedených důvodů bylo rozhodnuto, že se práce bude zabývat otázkou návrhu a implementace SIEM řešení pro středně velkou firmu. Z demonstrativních účelů je ukázán kontrast mezi potřebnou implementací pro malou organizaci a pro střední organizaci.

Z již definovaných důvodů se bakalářská práce věnuje návrhu a realizaci SIEM řešení v prostředí středního podniku. Návrh i realizace probíhá jak v teoretické, tak praktické rovině. Stěžejním bodem je analyzování potřebných přístupů nebo alternativních možností v kontextu SIEM z hledisek technologických, logicky-relačních a legislativních.

Bakalářská práce je rozdělena do sedmi kapitol, zahrnujíce úvod i závěr.
Úvodní část pojednává o významu SIEM principů, jeho rozvrstvení a cílech práce jako takové. První kapitola představuje bezpečnostní standardy relevantní v kontextu SIEM technologie. Druhá kapitola pojednává o zákonu o kybernetické bezpečnosti, který vešel

v platnost v lednu 2015. Třetí kapitola je stěžejní kapitolou pro definování všeobecných principů a logických vazeb v SIEM technologii. Kapitola čtvrtá řeší konkrétní implementaci této technologie – IBM Security QRadar SIEM. V rámci páté kapitoly jsou demonstrovány konkrétní implementace technologie IBM Security QRadar SIEM na dvou organizacích. V šesté kapitole jsou shrnuty poznatky z celé závěrečné práce. Poslední a závěrečná kapitola je věnována připomínkám a doporučením, které plynou z celé práce.

2 ISO Standardy

2.1 Definování základní terminologie – ISO, IEC, Standard

Nejprve je třeba definovat dílčí pojmy související s tvorbou a unifikací standardů, které budou v této části práce stěžejní.

- **ISO**- mezinárodní organizace pro standardizaci (*International Organization for Standardization*), zabývající se tvorbou norem napříč rozličnou škálou odvětví. ISO je nezávislá organizace mající členy ve 162 zemích s 3368 certifikačními centry (bodies), verifikovanými firmami, díky nímž je ISO schopné shromáždit experty napříč kontinenty a vytvářet standardy, doporučené postupy, které pomáhají lidem v řešení komplexní problematiky. Vznik ISO je datován do roku 1946, kdy byl poprvé vysloven předpoklad pro unifikování standardů souvisejících s industrializací. (About ISO, 2016).

- **IEC**- mezinárodní elektrotechnická komise (*International Electrotechnical Commission*), je organizace připravující a publikující mezinárodní standardy, které se týkají všech elektronických a elektricky přidružených technologií. Tato komise úzce spolupracuje s ISO a také s ITU (*International Telecommunication Union*), čímž je zajištěno, aby nově vzniklé standardy byly relevantní i v kontextu k ostatním, již vytvořeným standardům, a doplňovaly se navzájem. (About IEC, 2016)

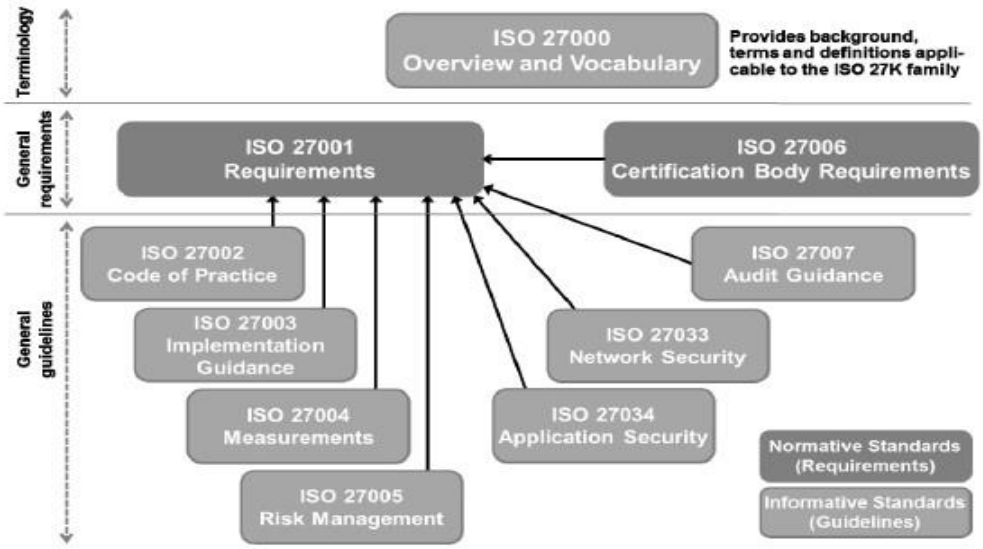
- **ISO Standard**- ISO norma je dokument, který zprostředkovává požadavky, specifikace, návody nebo charakteristiky, esenciální pro správné zvládnutí dané problematiky. Při dodržení těchto norem je zaručeno, že s produkty, procesy, materiálem a službami bude nakládáno právě správně a co nejefektivněji v kontextu daného problému. Hlavní výhodou využití ISO normy spočívá v jeho důvěryhodnosti. Pokud se organizace rozhodne ke koupi konkrétního standardu, je jí zaručeno, že postupy a služby, které standard poskytuje, jsou bezpečné,

spolehlivé a kvalitní. Během svého působení vydalo ISO již více než 19000 mezinárodních standardů. (ISO Standards, 2016)

2.2 Normy obeznamující s dílčí terminologií

Standard ISO/IEC 27000 – Overview and vocabulary
Skupina norem „ ISO/IEC 27k family," je nejdůležitějším souhrnem standardů, které souvisejí s řešením informační bezpečnosti. Nahrazují dříve užívaný standard ISO 17799 a BS 7799.

Norma ISO/IEC 27000, od mezinárodní organizace pro normalizaci, a její dodatky se detailně zabývají informačními technologiemi, bezpečnostní technikou a s nimi spojenými systémy řízení bezpečnosti informací. Tyto normy napomáhají firmám ke splnění legislativních požadavků, poskytují přehled systémů vhodných pro toto řešení, a zároveň definují termíny užívající se v řadě norem. Mezinárodní norma ISO/IEC 27000 je využitelná pro všechny druhy firem a organizací, ať už se jedná o komerční či nekomerční sektor. Díky tomu dochází ke zlepšení informačního managementu, který je stěžejním problémem v otázce informační bezpečnosti.
(ISO/IEC 2014, s. 12)



Obrázek 1 - ISO 27k family, převzato a upraveno (Disterer, 2013, s. 100)

Nejdůležitější částí informačních technologií je informace a to, jak s ní dotyčný naloží. Správnou manipulaci s informačním tokem nám definuje již zmíněná norma ISO/IEC 27000.

Všechny informace, které jsou zpracovávány společností, mohou dříve nebo později znamenat hrozbu útoku či chyby, které je třeba zamezit pokud možno už v zárodku. Zde přichází na řadu ISO 27001 a ISMS.

2.3 Normy upravující všeobecné požadavky

Standard ISO/IEC 27001 – Requirements

Tento standard představuje a specifikuje všeobecné požadavky pro zavedení, implementaci, provoz, monitorování a také další zlepšování již existujícího systému. V rámci ISO/IEC 27001 je představen nový, velmi důležitý pojem – ISMS (*Information Security Management System*).

Následuje dělení samotného ISMS, pomocí kterého je doporučováno v rámci ISO/IEC 27001 postupovat.

ISMS obsahuje nejdůležitější rysy, na nichž se shodli přední experti v daném oboru, k danému datu a dané verzi. (Jirásko, 2015)

Nyní je nutné definovat jednotlivé významy normy ISMS :

- Definují požadavky potřebné pro ISMS a pro ty, kteří certifikují tyto systémy.
- Přinášejí přímou podporu, nebo cílené vedení za účelem vytvoření, implementace, vylepšení nebo údržby ISMS.
- Adresuje sektorově-specifické vedení pro ISMS.
- Adresuje posuzování shody pro ISMS.

(ISO/IEC 27000:2014, s. VI)

Toto rozdělení však neprozrazuje, proč je ISMS tak důležité. Riziko spojené s nechtěným i chtěným šířením firemních informací musí být adekvátně řešeno. Aby bylo dosáhnuto informační bezpečnosti, musí být brány v potaz hrozby fyzické, spojené se selháním lidského faktoru, nebo technologické využívající všechny různé druhy informací, které firma používá. Jakožto preventivní opatření proti těmto ztrátám je přijmutí ISMS logickým krokem. Implementace těchto systémů se děje v souladu s potřebami a možnostmi společnosti, mírou zabezpečení a také velikostí společnosti. Finální podoba ISMS se pak odvíjí od vize, kterou si firma předem vytvoří. Ta se odráží od toho, co od systému požaduje firma a ti, kteří s ní spolupracují a jsou autorizováni do systému nahlížet. *(ISO/IEC* 27000*:2014, s. 14)*

Standard ISO 27001 - Requirements," čítající 42 stránek, předepisuje, jakých požadavků musí ISMS dosáhnout, aby bylo možné jej certifikovat Činnosti, týkající se procesů přidružených pro fungování bezpečnostního řešení, představují hlavní myšlenky tohoto standardu, která jsou odvozeny od standardu staršího.
Tento standard říká, že bezpečnost nelze pouze zavést, ale je třeba ji dále rozvíjet, sledovat a zlepšovat tak, aby bylo riziko hrozby stále minimalizováno. A právě toto ISMS nejen umožňuje, ale je to přímo vyžadováno. (Šuták,2015)

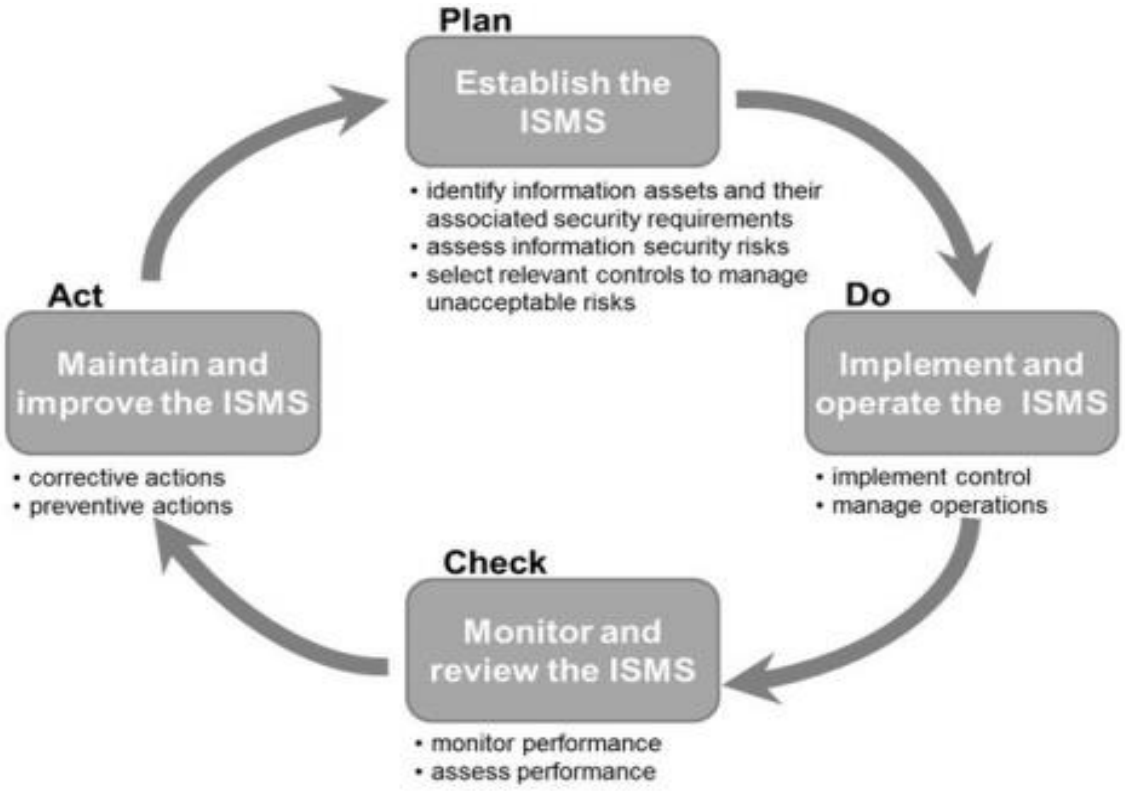
Rámcově je tento standard kompatibilní pro různě velkou společnost ze všech sektorů. Konkrétní parametry pro získání certifikátu nejsou formulovány normou, ale vyplývají spíše z implementace a vývoje specificky nastavené pro danou společnost. Certifikační požadavky pro ISO 27001 jsou objasněny smluvními podmínkami a koncepty, které jsou doplněny o implementační návod v ISO 27002.

Následuje vysvětlení samotného procesu certifikace pro normu ISO 27001.
K ověření věrohodnosti implementovaného ISMS, musí společnost projít certifikační procedurou navrženou autorizovanou certifikační organizací (Registered Certification Bodies – RCB). Mezinárodní organizace pro standardy publikovala seznam těchto verifikovaných firem, na které se může jiná organizace v případě zájmu o získání

certifikace obrátit. RCB pak blíže prozkoumá, zda je možné certifikaci udělit. V první části budou společnosti prohlédnuty všechny dokumenty související s bezpečnostní politikou, popisem procesů, které jsou po souhlasu RCB poslány certifikační instituci. Kontrolování dokumentů slouží zároveň jako příprava pro hlavní audit, na kterém zástupci dané organizace představí detailní průzkum. Po zdárném prozkoumání všech náležitostí je certifikační organizací vygenerováno hlášení, kde jsou vysvětleny a konzultovány výsledky šetření. V reportu jsou zmíněna potřebná vylepšení systému, která je nutné splnit pro obdržení certifikace. Pokud je report označen jakožto pozitivní, bude organizaci udělen oficiální certifikát pro atestaci ISMS s požadavky pro ISO 27001.

Následná implementace může vyžadovat různě dlouhý časový interval, ať už v řádu několika měsíců či několika let, v závislosti na rozsahu bezpečnostního řešení a kvantitě nedostačujících faktorů potřebných ke zlepšení. Certifikace má platnost tři roky, po tomto čase může být aplikována re-certifikace, která je časově i finančně výhodnější, než byla certifikace počáteční. V rámci certifikace jsou povinné také další audity, aby byla zaručena stálá ekvivalence s regulemi nutnými pro udržení certifikace. Tyto audity provádí RCB a první z nich musí být proveden dříve než rok od obdržení certifikace. Pokud budou zjištěny nedostatky nebo odklon od vyznačených podmínek, je společnost suspendována z certifikačních listin nebo jim tato certifikace může být odebrána úplně. (ISO/IEC 27000:2014, s. 16-19)

Přiložené schéma demonstruje proces implementace standardu.



Obrázek 2 - PDCA cyklus v ISO 27001, převzato (Disterer, 2013, s. 95)

Z výchozího schématu PCDA (plan , do, check, act), sloužícího pro neustálé zdokonalování procesu, lze detailněji nahlédnout do procesu implementace jako takového. Proces samotného plánování se zakládá na uvědomění si všech aspektů, které je třeba ochránit nebo na ně brát zřetel. Pomocí analyzování hrozeb je definován následný potenciální potřebný rozsah bezpečnostního řešení. Pro něj jsou v pozdější části vytvořeny vhodné procedury a měření, minimalizující tyto hrozby. Zmíněné procedury a měření jsou pak implementovány do bezpečnostního systému během implementační a provozní části procesu. Po spuštění monitorování systému budou pomocí vytvořených procedur generovány reporty, které poslouží pro vyvozování důsledků a zlepšení pro další vývoj ISMS.

Aby byla zajištěna neustálá ochrana ISMS, je nutné tyto procesy provádět opakovaně, aby mohl systém adekvátním způsobem pracovat a mohl minimalizovat hrozby.

Po úspěšné implementaci a monitoringu ISMS může být **očekáváno následující zlepšení**:

- Dosažení většího ubezpečení a vědomí, že informační bloky jsou adekvátně chráněny před hrozbami již od samého začátku.
- Udržení strukturovaného a celistvého rámce pro identifikaci a zhodnocování informačních bezpečnostních rizik. Následné aplikování adekvátních procedur, kontrol a měření pro zvýšení efektivity.
- Neustále zlepšující se kontrolní prostředí.
- Efektivní dodržení legislativních požadavků a omezení.

(ISO/IEC 27000:2014, s. 14-16)

V definování pojmu ISMS je ukryt pojem - informační bezpečnost, který je v kontextu ISMS velmi důležitý.

Informační bezpečnost tak, jak je definována od autorů posledního aktualizovaného spisu věnujicímu se ISO 27k, zní: „*The term information security is generally based on information being considered as an asset which has a value requiring appropriate protection, for example, against the loss of availability, confidentiality and integrity. Enabling accurate and complete information to be available in a timely manner to those with an authorized need is a catalyst for business efficiency.“ (ISO/IEC 27000:2014, s. 12)*

Z citace vyplývá, že tento pojem je založen na informaci, která je pokládána za cokoliv cenného, co si zasluhuje adekvátní ochranu. Touto ochranou se rozumí cokoliv, co zabrání ztrátě na straně dostupnosti, důvěrnosti nebo integrity. Umožnění včasného přístupu jen těm, kteří disponují správným oprávněním, má za následek velkou výhodu při zvyšování efektivity podniku.

Informační bezpečnosti lze dosáhnout pomocí implementace souhrnných aplikačních pravidel a nástrojů, které jsou vybrány pomocí zvolených kritérií a jsou spravovány pomocí ISMS. Tyto pravidla zahrnují politiku, procesy, procedury, organizační strukturu a také software a hardware. Systém je pak spravován nástroji, které také podléhají rozhodovacímu procesu (specifikace, implementace, monitoring). *(IOS/IEC 27000:2014, s. 13)*
Toto vše je potřebné pro zajištění dostačující informační bezpečnosti.

Za upozornění stojí jednotlivé nástroje ISMS, které byly zmíněny v předchozí definici:

- **Identity Manager**
- **Access Manager**
- **Accessibility monitoring**
- **Security Information and Event Management**
- **Endpoint management**

Z těchto nástrojů bude později v případové studii využit systém užívající SIEM (Security Information and Event Management), pomocí kterého bude definována implementace SIEM řešení v prostředí středního podniku.
Po zdárném definování norem ISO 27000 a 27001 je nutné zmínit další normy z ISO 27k family, které prohlubují potřebné požadavky pro správnou implementaci bezpečnostního řešení.

Standard ISO/IEC 27006 – Certification Body Requirements

Tento standard definuje požadavky a specifikuje doporučení pro orgány provádějící audit a participující v procesu certifikace systému řízení bezpečnosti informací (ISMS). Její primární využití je podpora samotného procesu akreditace certifikačních orgánů (Bodies), které pak udělují certifikování pro ISMS. Standard také kromě definování samotných postupů předepisuje kompetentnost školitelů. Ve standardu je mimo jiné zmíněno, jakým způsobem by měly být osoby, mající zájem provozovat certifikaci ISMS,

školeny, co by mělo být náplní jejich školení a jaké jsou požadavky pro udělení pravomoci certifikační autority (certification body). Norma doplňuje požadavky obsažené v ČSN ISO/IEC 17021 a ČSN ISO/IEC 27001.

Tato norma a požadavky obsažené ve standardu mohou sloužit v procesu akreditace a lze se na něj odkazovat jakožto relevantní dokument v procesu přezkušování, interního hodnocení nebo jiných auditních procesech. (ISO/IEC 27006:2015, 2015)

2.4 Doporučující standardy, všeobecné postupy

Standard ISO/IEC 27002 Information technology, Security techniques -Code of practice for information security controls je mezinárodně známý standard pro správné praktikování informační bezpečnosti. Jeho vznik se datuje do poloviny devadesátých let (dříve znám jako BS 7799). Tak jako všechny normy 27k i tento je zaměřen na informační bezpečnost. Je nutno zmínit, že ISO/IEC 27002 není certifikačním standardem v pravém slova smyslu, v tomto případě je totiž uživatelům ponechána určitá volnost výběru bezpečnostních kontrol nebo mohou adoptovat alternativní kompletní soubor týkající se kontroly informační bezpečnosti, pokud tak chtějí učinit. V praxi je však obvyklá skutečnost, kdy většina organizací, které si osvojí ISO/IEC 27001 si osvojí také ISO/IEC 27002.

Nejprve bude zmíněna jeho návaznost na normu ISO 27001.

Zatímco ISO 27001 pojednává o nezbytných požadavcích pro správnou implementaci Information Security Management Systems (ISMS) a přesně definuje kroky nezbytné pro splnění požadavků, ISO 27002 je v tomto směru více benevolentní a povoluje uživatelům jisté alternace, jelikož se jedná spíše o jakýsi „guideline.“ Z toho pramení i následující vztah s ISO 27001, který používá Code of Practise pro indikaci vhodných kontrol pro informační bezpečnost v rámci ISMS.

Norma ISO/IEC 27002 k roku 2013 byla strukturována a formátována následujícím způsobem*: „ISO/IEC 27002 is a code of practice - a generic, advisory document, not a formal specification such as ISO/IEC 27001. It recommends information security controls addressing information security control objectives arising from risks to the confidentiality, integrity and availability of information. Organizations that adopt ISO/IEC 27002 must assess their own information security risks, clarify their control*

objectives and apply suitable controls (or indeed other forms of risk treatment) using the standard for guidance." (ISO/IEC 27002, 2013)

V citaci, jak již bylo jednou zmíněno, je rozebírán rozdíl mezi normami ISO/IEC 27001 a ISO/IEC 27002. Jedná se tedy o dokument podpůrného charakteru obsahující doporučení, nikoliv nařízení, jak je tomu u předchozí normy.

Norma je logicky strukturována a seskupována pomocí souvisejících bezpečnostních kontrol. Avšak některé kontroly zasahují do více skupin, aby však bylo zabráněno duplicitním údajům, jsou trvale přiřazeny k jedné skupině a pro zbývající skupiny je na ně odkazováno. Norma ISO/IEC 27002 se opírá o tzv. CIA trojici (confidentiality, integrity, availability of information). (ISO/IEC 27002, 2015)

Tyto zmíněné principy budou dále definovány.

Důvěrnost (Confidentiality)

Důvěrnost v tomto triu reprezentuje fakt, kdy jsou informace v systému vytvářeny takovým způsobem, aby nemohlo dojít k jejich zcizení nebo nahlížení do nich někým bez patřičného autorizovaného přístupu. Proces zcizení se může týkat také procesů nebo entit, nikoliv pouze uživatele jako takového

Celistvost (Integrity)

Integrita dat v kontextu informační bezpečnosti znamená, udržování a upravování dat takovým způsobem, aby byly stále přesné, aktuální a kompletní po celou dobu jejich životního cyklu. Tento případ lze považovat jakožto zvláštní případ konsistence, pokud by měla být integrita informační bezpečnosti srovnávána s integritou určenou pro databázové systémy (ACID).

Dostupnost informací (Availability of information)

Dostupnost informací je rizikovým faktorem při jakémkoliv řešení problému. Z toho důvodu je stěžejní, aby informace byly dostupné v moment, kdy jsou potřeba. V praxi to znamená bezchybné propojení všech částí podílejících se na procesování či ukládání informací (dat). Výpočetní systémy, starající se o uložení a procesování, bezpečnostní

kontroly chránící citlivá data před zneužitím a komunikační kanály zprostředkovávající přístup – vše musí být funkční a fungovat jako jeden celek. Systému s vysokou dostupností se snaží především o schopnost dostupnosti dat 24/7 , přičemž berou v potaz veškeré vnější i vnitřní faktory, které by mohlo systém vyřadit z provozu. Kromě výpadků proudu, selhání hardwaru nebo vylepšení softwaru musí brát na zřetel také DoS útoky, umět je rozpoznat a bránit se jim. (Disterer, 2013, s. 97-98)

Standard ISO/IEC 27003 – Information security management system and implementation guidance

Norma ISO 27003 napomáhá v implementaci standardu ISO 27001, respektive ISMS. Tento standard se úzce odkazuje na standardy ISO/IEC 27000 a ISO/IEC 27001.

Popisuje proces implementace ISMS od samotného počátku až po samotné plány implementace se zaměřením na management. Tento standard v zásadě nenabízí návod pouze pro implementaci, nabízí také možná vylepšení v oblasti managementu, monitoringu a vylepšení samotného ISMS po již úspěšném zavedení.

V normě je zahrnuta příprava a plánování aktivit primárních pro zdárné splnění implementace, během které jsou brány v potaz tyto klíčové aspekty:

- Schválení a finální autorizace pro pokračování v implementaci;
- Vymezení a definování omezení v pravidlech ICT a fyzických uložišť;
- Posouzení a zvážení rizik z hlediska informační bezpečnosti, plánování adekvátních vylepšení k zamezení těchto hrozeb a nezbytné definování požadavků pro informační bezpečnost;
- Plánování implementačního procesu.

Standard ISO/IEC 27004 Measurement

Tento standard je pro organizace poskytnutím doporučení pro vývoj a používání metrik, prezentaci efektivity systémů řízení bezpečnosti informací (ISMS). Zahrnuje řídící principy obsažené v ISO/IEC 27001 a opatření v ISO/IEC 27002.(ISO/IEC 27004, 2009)

Implementování v rámci těchto řešení je užito procesech zahrnující rozvoj metrik, analyzování dat a proces jejich následného vyhodnocení.(ISO/IEC 27004,2014)

Standard ISO/IEC 27005 Information Security Risk management

Standard ISO/IEC 27005 představuje návod pro správné užití risk managementu v rámci informační bezpečnosti. Dále pak podporuje všeobecné koncepty zmíněné v normě ISO/IEC 27001. Standard je vytvořen takovým způsobem, aby dopomáhal při implementaci systému z hlediska rizikového managementu.

Norma nespecifikuje, nedoporučuje a dokonce vůbec neuvádí žádnou konkrétní metodu užití rizikového managementu.

Naproti tomu je zde zmíněn pokračující proces skládající se ze strukturovaných bloků aktivit, z nichž některé opakují svůj proces, pouze se mění kontext (iterace).

Činnosti řízení rizik, zmíněné ve standardu:

- **Stanovení kontextu** – vymezení rozsahu a hranic, stanovení struktury.
- **Hodnocení rizik** – definování hrozeb, rozdělení dle kvalitativních a kvantitativních kritérií.
- **Zvládání rizik** – výběr adekvátních protiopatření.
- **Akceptace rizik** – evidování rozhodnutí týkajících se odpovědnosti za vzniklá rizika.
- **Seznámení s riziky** – sdílení informací o rizicích.
- **Monitoring a přezkoumávání rizik** – zkoumání rizik a jejich faktorů, sledování rizik.

(ISO 27005,2011)

Standard ISO/IEC 27007 – Guidelines for Information security management auditing

Norma ISO/IEC 27007 obsahuje doporučení a specifikace pro provádění auditů funkčních ISMS, definované v normě ISO/IEC 27001. Obsahově čerpá především ze *Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu (ISO/IEC 19011:2002)*.

Mimo auditování obsahuje specifický návod pro ISMS. Kromě zmíněného standardu ISO/IEC 19011 se opírá také o ISO/IEC 27006, týkající se akreditačních standardů pro certifikační autority.

Norma má za úkol definovat, zda organizace užívající ISMS, má systém, který podléhá všem nezbytným sounáležitostem a požadavkům definovaných v ISO/IEC 27001.(ISO/IEC27007:2011, 2011)

Standard ISO/IEC 27033 – Security technique

Tento standard navádí, jak implementovat zabezpečení, respektive opatření proti hrozbám při komunikaci mezi sítěmi užívající zabezpečené brány (Firewall, Intrusion Protection System). Ve svých šesti částech, které vycházely od roku 2006, až po nynější datum standard postupně pokrývá všechny aspekty a jejich potřebné pokrytí v rámci sítě / sítí.

Norma je odvozena od normy ISO/IEC 18028

Přehled dodatků standardu ISO/IEC 27033:

1. **ISO/IEC 27033-1:**
   Network security overview and concepts – revize normy ISO/IEC 18028, aktualizováno v roce 2015;
2. **ISO/IEC 27033-2:**
   Guidelines for the design and implementation of network security – Definování bezpečnostní architektury sítí, aktualizováno v roce 2012;
3. **ISO/IEC 27033-3:**
   Reference networking scenarios – threats, design, techniques and controll issues – definování rizik, technik pro návrh adekvátního řešení problémů spojených se spravováním sítí.
   Dodatek byl vytvořen v roce 2010.
4. **ISO/IEC 27033-4**
   Securing communications between networks using security gateways – definuje návod pro zabezpečení komunikace mezi sítěmi pomocí síťových bran, firewallů, IPS, za předpokladu zachování firemní politiky, zahrnující identifikování a analýzu hrozeb síťové bezpečnosti, určení potřebných protiopatření a jejich následná implementace, provoz či monitoring.
   Tento dodatek byl aktualizován v roce 2014.
5. **ISO/IEC 27033-5**
   Securing communications between networks using Virtual Private Networks (VPN) – obsahuje návod pro výběr, implementování a následný monitoring esenciálních technických opatření ve snaze zabezpečit síťovou bezpečnost pomocí užívání připojení přes virtuální privátní sítě.

Tento standard vyšel v roce 2013.

6. **ISO/IEC 27033-6**
   Securing wireless IP network access (DRAFT) – norma by měla udávat konkrétní rizika, adekvátní metody návrhu a opatření proti prolomení bezpečnosti u bezdrátových a rádiových sítí.

   Tento dodatek by měl vyjít do konce roku 2015 nebo na začátku roku 2016. (ISO/IEC 27033-1- ISO/IEC 27033-6, 2015)

Standard ISO/IEC 27034 – Application Security

Standard ISO/IEC 27034 s názvem aplikační bezpečnost (bezpečnost aplikací) je norma, jež se zabývá poskytnutím návodu a doporučení pro správné vytvoření, implementaci a užívání aplikačního softwaru. Norma ISO/IEC 27034 má celkem osm dalších dodatků, nicméně vydán byl zatím jen první dodatek týkající se konceptů a přehledu v tématice bezpečnosti aplikačního software.(ISO/IEC 27034,2011)

Přehled dodatků normy ISO/IEC 27034

1. ISO/IEC 27034-1:2011 Application security overview and concepts;
2. ISO/IEC 27034-2 *Organization Normative Framework;*
3. ISO/IEC 27034-3 *Application Security Management Process;*
4. ISO/IEC 27034-4 *Application security validation;*
5. ISO/IEC 27034-5 *Protocols and application serucity control data structure;*
6. ISO/IEC 27034-6 *Security guidance for specific applications;*
7. ISO/IEC 27034-7 *Application security control attributee predictability;*
8. ISO/IEC 27034-8 *Protocols and application security controls data structure – XML schemas.*

Standard ISO/IEC 27044 – Guidelines for security Information and event management (SIEM)

Standard ISO/IEC 27044 pojednávající primárně o doporučených postupech týkajících se návrhu, implementace a užívání nebo managementu SIEM.

Tento standard byl však v průběhu psaní této závěrečné práce smazán.(ISO/IEC 27044,2015)

Důvodem bylo nalezení nedostačujícího objemu relevantních dat a informací o dané problematice, i když se na tomto procesu podílelo větší množství skupin.

V druhé řadě zde byla šance překrytí nebo rozporu se zněním standardu ISO/IEC 27044 s jinými standardy z 27k family. Z těchto důvodů bylo nakonec zvoleno odstranění normy týkající se řešení SIEM.

3 Zákon o kybernetické bezpečnosti

V lednu 2015 nabyl v platnosti zcela nový zákon týkající se kybernetické bezpečnosti, a jelikož úzce souvisí se zaměřením této závěrečné práce, bude zde zmíněn jakožto jeden z relevantních důvodů pro pořízení SIEM řešení.

Zákon o kybernetické bezpečnosti je regulací v oblasti zajištění bezpečnosti informačních technologií.
Nabízí návod a předepisuje požadavky pro správné zavedení zabezpečení pomocí opření se o obecně platné principy ICT a mezinárodní standardy.
Samotná implementace metodických pokynů zákona by měla probíhat ve shodě s řízením organizace takovým způsobem, aby nedošlo k narušení jejich primárních cílů.
Zákon o kybernetické bezpečnosti je „postaven“ na dvou zásadách a třech pilířích.
Zásady se zabývají především minimalizací zásahů do práv soukromoprávních subjektů a druhá zásada předepisuje individuální odpovědnost za bezpečnost vlastního informačního systému.
Pilíři se pak rozumí standardizace bezpečnostních opatření, hlášení kybernetických bezpečnostních incidentů a následné protiopatření proti těmto incidentům.
(Krčmář, 2013)

Povinné zavedení principů tohoto zákona je dané pro tzv. kritickou informační infrastrukturu.
Kritická informační infrastruktura je definována jako: “ *prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti.“* (Wolters Kluwer ČR, 2014)

Zajímat o tento zákon by se měl každý, na něhož se vztahuje zákon č.240/2000 Sb. (Krizový zákon), správci informačního systému jakéhokoliv odvětví veřejné správy – zákon č.317/2014 Sb. a poskytovatelé – zákon č.127/2005 Sb. (Zákon o elektronických komunikacích).

Zároveň je také přesně definováno, jakým organizacím vzniká povinnost v rámci plnění dílčích požadavků (péče o regulované systémy ICT v souladu se zákonem).
Tato specifikace se nachází v zákoně č. 315/2014 Sb. a vyhlášce 317/2014 Sb.
Zmíněná vyhláška obsahuje kritéria pro implementaci systému podle souladu se zákonem o kybernetické bezpečnosti.
Proces zavádění bezpečnostních opatření by měl zabránit rostoucímu riziku zcizení citlivých údajů a informací někým bez patřičných pravomocí. Bezpečnostní opatření je definováno jako *„souhrn úkolů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru.“* (Wolters Kluwer ČR, 2014)

3.1 Důvod vytvoření zákona o kybernetické bezpečnosti

Hlavním důvodem vzniku samotného zákona byla snaha o vytvoření celistvého legislativního dokumentu, který se bude opírat o relevantní zdroje či normy, za účelem nabídnutí adekvátního bezpečnostního řešení pro organizace tak, aby zůstala zachována vnitřní politika organizace a zároveň byla naplněna veškerá kritéria stanovená v zákoně. Před vydáním zákona byla ochrana kybernetického prostoru vykonávána osobami soukromého práva bez jakékoliv regulace, koordinace nebo dohledu, což mělo za následek nedostatečnou bezpečnost tohoto prostoru.

Především pak je nutné poukázat na DDoS (*Distributed Denial of Service*) útoky vedené proti bankovním a finančním institucím ve veřejné správě v březnu roku 2014. Kdyby již v tomto časovém období existovala jednotná regulace a kontrola pro tyto systémy, útoku jako takovému by bylo možné zamezit nebo jej výrazně redukovat. Tato premisa pramení z faktu, že ačkoliv měly zmíněné instituce informace o typu útoku i jeho následcích, nebyly schopné interpretovat relevantní závěry, které by pak mohly odeslat institucím, kterým tento útok hrozil také, ale napadeny ještě nebyly. Tím, že každý systém byl spravován odlišným způsobem, nelze společný postup definovat jinak, než vytvořením zákona.(Mališ, 2015)

3.2 Hlavní funkce zákona o kybernetické bezpečnosti

Jak již bylo zmíněno v úvodní části, týkající se zákona o kybernetické bezpečnosti, zákon je neoficiálně složen ze dvou zásad a tří pilířů.

- Zásada o minimalizaci zásahu do práv soukromoprávních subjektů
- Zásada o individuální zodpovědnosti za chod vlastního bezpečnostního systému
- Standardizace bezpečnostních opatření
- Hlášení kybernetických bezpečnostních incidentů
- Reakce na bezpečnostní incidenty

Zákon o kybernetické bezpečnosti je oficiálně rozdělen podle druhů opatření, která vymezuje.
Bezpečnostní opatření jsou rozdělena na opatření týkající se organizace a opatření týkající se technickým parametrů. (Wolters Kluwer ČR, 2014)

Úplný výčet obou skupin opatření bude možné shlédnout v kopii zákona přiložené k závěrečné práci. Pro účely práce není nutné zmiňovat všechny, a proto následuje výčet opatření kontextově relevantních pro tuto práci.

- Organizační opatření
    - Systém řízení bezpečnosti informací
    - Řízení rizik
    - Bezpečnostní politika
    - Stanovení bezpečnostních požadavků pro dodavatele
    - Řízení aktiv
    - Zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů
- Technická opatření
    - Nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů
        - Nástroj pro detekci kybernetických bezpečnostních událostí

- Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
- Bezpečnost průmyslových a řídicích systémů

Výše vybraná opatření úzce souvisí s implementací a užíváním SIEM řešení.
V další části bude definován dopad zákona na rozvoj užití SIEM řešení.

3.3 Dopad zákona o kybernetické bezpečnosti na SIEM

Díky nově zavedenému zákonu o kybernetické bezpečnosti, kladoucímu důraz především na sběr relevantních informací o bezpečnostních incidentech z nestejnorodého prostředí, dochází k rozšíření působnosti v rámci užití SIEM řešení.
Tím, že je nyní pro organizace, definované v zákoně, nutné splnit veškeré dílčí požadavky, musí se poohlížet po komplexnějším řešení.
Před regulací jim pro splnění bezpečnostních aspektů stačilo takřka implementování normy ISO 27001, to už však nyní neplatí.
SIEM řešení je dostačující pro splnění hned několika bodů zmíněných jak v technické, tak v organizační bezpečnostní struktuře zákona.
Zákon tedy nasazení řešení pro správu bezpečnostních událostí a informací předepisuje všem organizacím státní a veřejné správy, ale také i některým soukromým organizacím.
Po implementaci SIEM řešení však může vzniknout další problém.
Implementace konkrétního řešení totiž není nijak obtížná, naproti tomu samotné nastavení systému „proti“ firemnímu serveru je pro mnohé organizace oříškem.
Z důvodu předchozí absence znalostí z oblasti bezpečnosti informací a také správou těchto dat hrozí, že ačkoliv bude mít firma ze zákona nařízené pořízení takového řešení, neznamená to, že je schopna tuto technologii adekvátně využívat. SIEM řešení, které není správně nastaveno tak, aby načítalo takřka v reálném čase aktuální informace a správným způsobem je vyhodnocovalo, nebude schopno včas zamezit možnému bezpečnostnímu incidentu.

4 Security Information and event management (SIEM)

4.1 Definování dílčích pojmů souvisejících se SIEM

SIEM se svým vznikem řadí k relativně novým technologiím. Bezpečnostní management událostí a informací vznikl jako odpověď rostoucímu riziku hrozeb v rámci kybernetického prostředí.

Je známo, že nyní již neexistuje takřka žádné stejnorodé prostředí a komplexnost rozličných technologií může být při nejmenším ochromující.

Snaha porozumět všem druhům nových událostí, které tyto technologie produkují, a jak to může ovlivnit chování daného prostředí (systému). (Miller, Harris, Harper, VanDyke a Blask, 2011, s. XXI)

Zmíněná technologie SIEM vznikla ze dvou, již vytvořených a známých technologií SIM a SEM, spojení těchto dvou dříve užívaných částí v jeden celek (SIEM) pak bylo zejména z důvodu rostoucích nároků na komplexnost nebo větší variaci funkcí u jedné či druhé části. Zákazníci se dožadovali funkcí, které nabízel SEM u SIM a naopak. Dalším logickým krokem bylo spojení těchto dvou částí.

Po stručném představení SIEM je nutné definovat pojmy, které s tímto bezpečnostním řešením úzce souvisí.

- **Security**
- **Information**
- **Event**
- **Management**

Bezpečnost, definována jako „stav, kdy je daný předmět zabezpečen či osvobozen od nebezpečí," (Whitman a Mattord,2012, s. 3) je esenciálním prvkem SIEM, což není nijak zarážejícím faktem.

Potřeba bezpečnosti, myšleno v kontextu informační bezpečnosti, byla hlavním hnacím motorem při vzniku SIM a SEM, ze které byl vyvinut SIEM. V návaznosti na stále se zvětšující možnost úniku citlivých dat, vstupu neoprávněných osob do oblastí, kde je to

nežádoucí, nebo nedostatečné monitorování aktivit na internetu a neadekvátní reakce na bezpečnostní hrozby zákonitě vedlo k postupnému růstu důležitosti bezpečnostního aspektu systému v informačním sektoru.

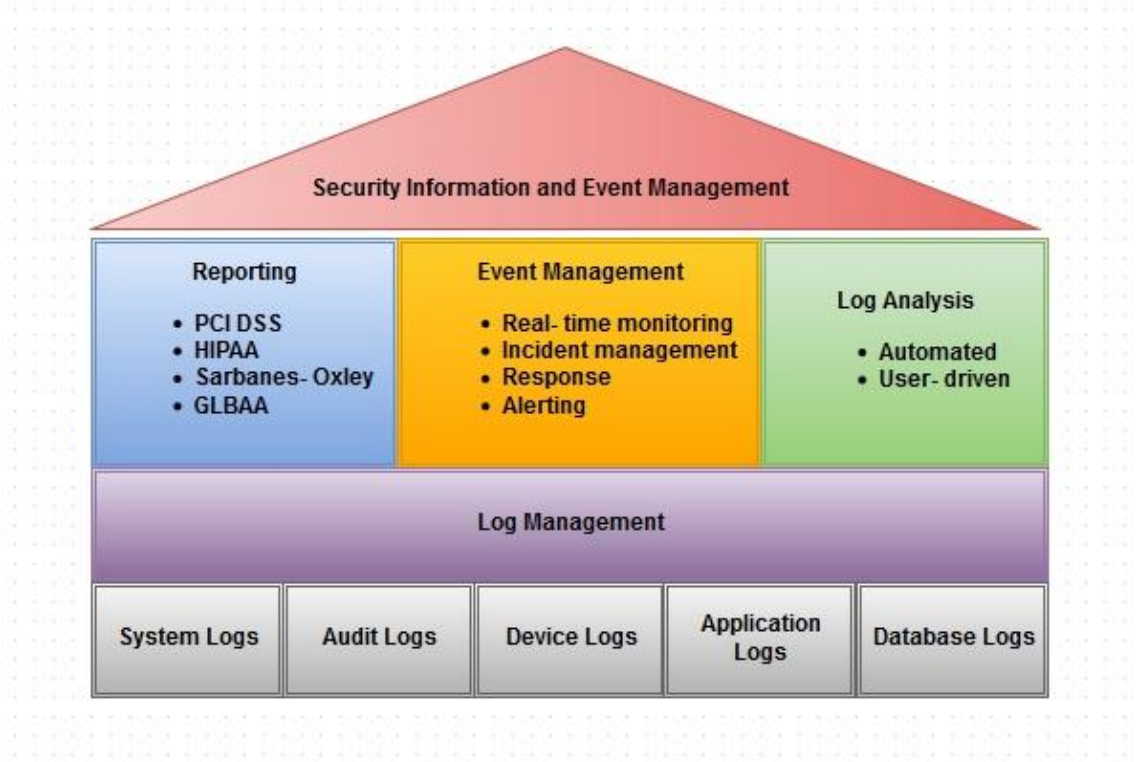
Informace je základním kamenem jakékoliv akce, reakce, procesu, který je spojen s rozhodnutím, ať již každodenním triviálním, nebo těch komplexnějších.
„Je to zpráva snižující naší (příjemcovu) míru neznalosti o tomto jevu."
(Gála, Pour a Šedivá, 2009, s. 23)
Informace tu je přítomna od pradávna, přičemž jediné, co se v čase mění, je její kvalita, způsob zachycení a rostoucí význam vlastnictví informací.
V dnešní době je obchod s informacemi stejně důležitý, ne-li důležitější, než samotný obchod se statky, kterých se týká. Množství informací, které je o dané věci shromážděno, přímo definuje, jak s ní bude naloženo a mnohdy výrazně ovlivní celkovou cenu za vlastnictví této věci. Toto tvrzení inklinuje k poznatku, že informace dosáhne plné hodnoty, pokud je dále použita.
(Vízner, 2014, s. 19)

Událost je vnímána jako *„proces, který probíhá, proběhl nebo teprve proběhne."*
Přičemž definice čerpá ze slova event (věc, která se děje). Z toho lze vyvodit, že událost v informační sféře je proces, který probíhá v daném informačním systému.

Management je posledním z výše zmíněných pojmů.
Je definován jako „proces tvorby a udržování prostředí, ve kterém jednotlivci pracují společně ve skupinách a efektivně uskutečňují vytyčené cíle." (Weihrich a Koontze, 1993, s. 16). Proces managementu je užíván už od dob starověku, kdy primárně sloužil během velkých konfliktů. Tehdy umění managementu společně s logistikou mnohdy znamenalo rozdíl mezí porážkou a vítězstvím. Užití pojmu managementu tak, jak je znám dnes, však přišlo mnohem později- v 19. století v souvislosti v průmyslovou revolucí.
Slovo management v doslovném překladu z angličtiny znamená řízení, což dle mého názoru, nejlépe vystihuje podstatu procesů funkcí, které jsou k tomuto pojmu

přidruženy. Plánování, vedení, kontrola, personalistika či organizace, tyto hlavní funkce skrývající se pod pojmem management úzce souvisí s chodem celé organizace, jež je na správném fungování těchto procesů závislá. Rovněž je nutné podotknout, že tyto principy je možné užít také v procesu managementu bezpečnostních informací.
Než bude možné přejít ke konkrétnímu typu produktu využívajícího principů SIEM, je nutné tyto principy a dílčí procesy definovat.

- Log management
- Log analysis
- Reporting (IT regulatory compliance)
- Event management
    - Event correlation
    - Active response
    - Endpoint security



Obrázek 3 - Přehled procesů v SIEM, převzato a upraveno (Miller, 2011)

Log management je definován jako přijímání esenciálních informací ze zdrojů logů (*log source)* do databáze, za účelem vytvoření bezpečnostního obrazu. Logy jsou rozuměny důležité systémové či aplikační událost, které se v daném systému udály za daný časový interval. Tyto události jsou zaslány do centralizované databáze, která je udržována konkrétní aplikací SIEM řešení. Zde je třeba přijaté logy rozdělit podle parserů, což je část programu, která má na starosti syntaktickou analýzu textu. Syntaktická analýza je proces, kdy je text zpracován v přirozeném či uměle vytvořeném jazyce pomocí gramatický pravidel, které jsou definovány v rámci daného jazyka. Parser tento text normalizuje tak, aby byl jejich výstup relevantní pro pozdější analýzu. Tyto procesy jsou nutné zejména z důvodu vysoké variace druhů událostí, které do SIEM z log source přicházejí. Jak je ilustrováno v přiloženém obrázku, do SIEM jsou posílány především logy systémové, auditní, aplikační, databázové a logy ze zařízení. Díky neexistenci jednotně uznávaného standardu formátu logovací zprávy napříč spektrum výrobců, je nutné se vypořádat s rozdílnými syntaxemi těchto zpráv. Je úkolem správce konkrétního SIEM řešení navrhnout nebo optimalizovat parser takovým způsobem, aby události byly zpracovávány efektivně a informace z nich získané byly skutečně ty, které jsou pro konečnou analýzu požadovány. Log management v SIEM funguje takřka na principu „real-time“ analýzy, což z něj činí velmi mocný nástroj při zjišťování stavu bezpečnosti a celkového zdraví informačního systému, na který je implementován. Čím větší je množství a podrobnost událostí posílaných do SIEM, tím je pohled na tyto aspekty relevantnější a celistvější. (Miller, 2011, s. XXXIV)

Log analysis je pojem, který je přidružený k managementu logů, je však nutné tyto dva pojmy rozlišit. Management logů pojednává o tom, jak se události do SIEM dostanou, jak jsou zpracovány, rozděleny a uschovány. Samotné analyzování logů je hlavní proces, který z SIEM činí tak mocný nástroj při boji s nástrahami dnešního kybernetického světa. Po úspěšném uložení logů z důležitých a kritických systémů je možné vytvoření filtrů a pravidel, která budou *auditovat data*, tzn. hledat odchylku od normálu. Tyto filtry a pravidla si může vytvořit každá organizace sama, avšak je zde také možnost si zakoupit

již přednastavenou sadu těchto pravidel, která jsou nastavena takovým způsobem, aby uspokojila nároky na různé druhy zákonů a norem, ve kterých se daná organizace pohybuje.
Za předpokladu, že jsou dané logy dostatečně podrobné a chodí v co nejmenších možných časových intervalech, probíhá analýza informačního systému na bázi již zmíněné analýzy v reálném čase. Princip zpracování dat v takřka stejném čase, kdy bezpečnostní incident vyvstane, je natolik důležitou vlastností, že díky těmto schopnostem se bude užití SIEM brzy implementovat nejen ve sféře definované kybernetickým zákonem.

Podle předpovědi agentury Gartner, v návaznosti na dřívější hackerské útoky, bude v roce 2018 o 40% více firem, které budou přecházet na tzv. proaktivní bezpečnost.
V zásadě se nejedná o nic jiného než o změny přístupu s vypořádáváním se s bezpečnostními hrozbami. Namísto čekání na hrozbu, její následnou detekci a blokaci, se budou firmy snažit pomocí analýzy detekovat bezpečnostní incident ještě v zárodku a adekvátně reagovat na hrozbu v co nejkratším čase. Za těchto zmíněných podmínek je nejlepší volbou zpracovávání a analýza dat v reálném čase se silným korelačním strojem, který včas zanalyzuje a porovná data dříve, než stihne pomyslná bomba, v podobě kybernetického útoku, vybouchnout. (Rivera, 2015)

Reporting (IT Regulatory Compliance) vycházející z centralizované infrastruktury přináší přehledné a tolik požadované informace, pomocí nichž lze snáze předpokládat kritická ale i běžná rozhodnutí související s identifikací bezpečnostních hrozeb. Užití SIEM řešení do určité míry garantuje validaci kroků firmy v souladu s právními předpisy, což může být nápomocno při zvýšení konkurenceschopnosti podniku. Právní aspekty byly zmíněny v kapitole věnující se zákonu o kybernetické bezpečnosti.
SIEM řešení také disponuje plně podporovaným reporting systémem, který obsahuje mnoho, již přednastavených, reportů, které lze nadefinovat dle libosti uživatele. Reporty se užívají jako jistá forma sebekontroly, zda byla splněna všechna nutná legislativní kritéria.

Event management je souhrn veškerých procesů, který souvisí s manipulací dat z přijatých událostí, jejich analýzou v reálném čase ze získaných logů a získáním relevantních informací pro sledování hrozeb, případně vytvoření adekvátní odezvy na bezpečnostní incident**.** Souhrnný pojem managementu událostí lze rozčlenit na několik dalších součástí, které existují především v kontextu managementu událostí, z toho důvodu budou definovány jako jeho podmnožiny.

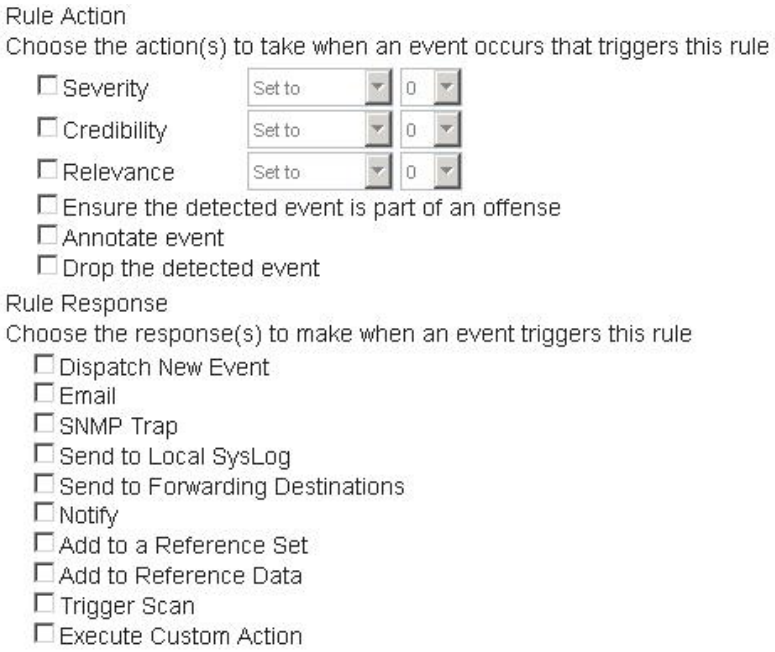
- **Event Correlation**
- **Active response**
- **Offense creation**
- **Endpoint security**

Pojem managementu událostí úzce souvisí s jejich ***korelací***, což je dílčí funkce SIEM, která je s určitou nadsázkou označována jako druh umělé inteligence. **Event correlation** je přidanou hodnotou, která přináší vyšší druh inteligence do konceptu SIEM. Uživatel učí systém zvažovat obrovskou variaci podmínek a veličin ještě předtím, než je spuštěn varovný signál. SIEM bere v rámci korelace v potaz všechny variace situací, které by mohly, ale také nemusely nastat a značně napomáhá při dalším rozhodování. Pokud by tuto funkci měl zastávat člověk, bylo by to nadmíru vysilující, a především by to odvádělo pozornost od jiných věcí, takže by bezpečnost IT organizace mohla být v ohrožení. (Brandelová, 2011)

Active response vychází z korelace událostí. Poté, co jsou události, rsp. data z událostí zanalyzována, má uživatel dvě možnosti. První možností je, aby se o tyto procesy v rámci informační infrastruktury staral správce. Hlídat vznik a řešit bezpečnostní incidenty však může vzít správci hodně cenného času. Z toho důvodu je tu druhá možnost a tou je právě SIEM, který se v rámci nakonfigurovaných automatických akcí vypořádá s bezpečnostním incidentem sám. V tomto případě ale může při špatné konfiguraci dojít k nežádoucímu průběhu vypořádání se s hrozbou, což může mít za následek ohrožení důležitých služeb a aplikací ve společnosti. Za předpokladu, že jsou bezpečnostní pravidla a ostatní procesy korektivního charakteru nastaveny správně, může

automatizace těchto procesů vést k odlehčení práce pro správce IT infrastruktury. (Miller, 2011, s. 66)

Poté, co nastala konkrétní událost (**Offense**), je nutné definovat adekvátní response na daný bezpečnostní incident, tedy akci, která bude reagovat na vzniklý problém. Bezpečnostní incident spouští související akce, jejímž úkolem je podle definovaných parametrů a podmínek v pravidle zlikvidovat potencionální hrozbu. Adekvátní reakcí na vzniklou hrozbu může být několik druhů.



Obrázek 4 - Druhy response na bezpečnostní incident, vlastní zpracování

Standardní odezvou je změna hodnot u atributů závažnosti, relevance a důvěryhodnosti. Další druhy odezvy pak záleží na konkrétním typu bezpečnostního incidentu. Velmi často je užívána emailová notifikace administrátorovi a vytvoření nové události o tomto incidentu nebo iniciace skenovacího procesu.

Endpoint security je důležitým pojmem v kontextu celé společnosti. Koncová zařízení jsou nejrizikovějšími, nejčastěji z důvodu selhání lidského faktoru. Zaměstnanci svou absencí pozornosti nebo dokonce úmyslně způsobí trhliny v IS a vytvoří problém, který

bude nutné řešit. Z toho důvodu je nutností kontrolovat také koncová zařízení. SIEM dokáže v rámci přidělených práv kontrolovat stav firewallu, zda je verze antivirového programu „up to date," definovat, kdy jsou uzly nakaženy spywarem nebo dokonce, v rámci „Active response modu," seřídit ACL (*Access control list*) na špatně nastaveném osobním firewallu. (Miller, 2011, s. 67)

Kolekce dat a událostí

Pro úplné porozumění je nutné definovat ještě dva stěžejní pojmy související s nejdůležitějšími funkcemi SIEM – kolekcí dat a událostí. V tomto kontextu se objevují níže uvedené zkratky a pojmy:

- **EPS**
- **FPM**
- **Denní nebo hodinový objem zpracovaných dat**
- **Počet připojených zdrojů událostí**

EPS (Events per second) je počet procesovaných události za sekundu, kde je možné, si jednu událost představit jako řádek v auditním logu. Tato hodnota je důležitou výkonnostní veličinou, na kterou musí být brán zřetel při každém návrhu SIEM systému. Objem událostí zasílaných do SIEM systému z koncových zařízení se liší v závislosti na nastaveném logovacím stupni, ale i na typu zařízení EPS licence je aplikována a procesována v reálném čase, dvakrát za sekundu, na příchozí nenormalizovaný tok událostí. Každou půl vteřinu systém načte alokovaný počet událostí, přičemž veškeré nadlimitní události jsou uloženy do zásobníku (Throttled) a čekají ve frontě na další kolo periody.

FPM (Flows per minute) je definováno jako počet procesovaných toků síťového provozu. Zatímco EPS je definováno jako hodnota za sekundu, hodnota datového toku je uváděna v minutách. Důvodem je životnost toků, které mohou přetrvat několik vteřin či minut. Záznamy toků síťového provozu jsou vytvářeny kolekčními nástroji SIEM systému (flow sondy). Ty jsou dále zasílány ke zpracování do samotného systému. Tak

jako v předchozím případě, dochází i zde při překročení licence k notifikaci o „overflow.“ Přebytečný datový tok je uložen do zásobníku, čekajíc na další zpracování prováděné dvakrát za vteřinu. (EPS and FPM Limits,2015)

Denní nebo hodinový objem zpracovaných dat je definováno jako interval četnosti, který udává, jak často budou přijatá data procesována. Defaultně si lze vybrat mezi zpracováním po hodině nebo za 24 hodin. Volba správného intervalu je kritická pro správnou preventivní funkci SIEM systému a rovněž je nutné tuto volby správně determinovat v závislosti na objemových a výkonnostních faktorů celého SIEM řešení.

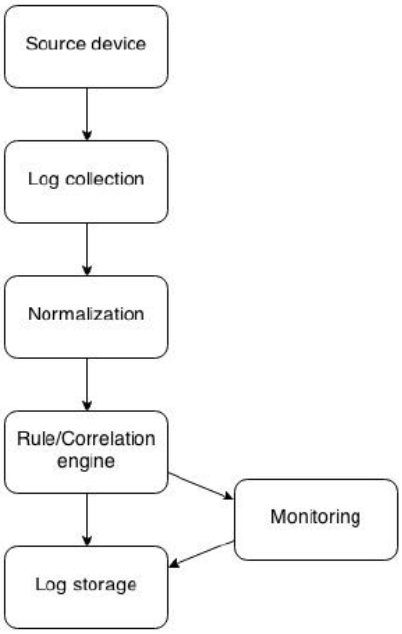
Počet připojených zdrojů událostí tento atribut udává, kolik je na SIEM systém připojeno zařízení, které do SIEM systému zasílají svá data. Velikost počtu zařízení takto připojených velmi ovlivňuje výkonnostní nároky celého řešení.
Do zdrojů událostí může být zařazena velká škála zařízení. Data jsou sbírána z Windows a Linux serverů, firewallů, aplikací, databází, antivirů, routerů nebo switchů.

4.2 Architektura SIEM

Technologii SIEM lze přirovnat k velmi komplexnímu stroji, tento stroj je rozdělen na části, které pracují do určité míry nezávisle na sobě, nicméně jejich kooperace musí být naprosto bezchybná. V opačném případě bude jakákoliv chyba v synergii vést k nefunkčnosti stroje, respektive povede k pádu celého systému.

Variace v rámci SIEM architektury jsou závislé na druhu systému, na který jsou nastaveny. Každá implementace však musí obsahovat níže zmíněné prvky, jinak celé řešení nebude fungovat.

- **Source device (*zdroj dat*)**
- **Log Collection(*shromažďování dat z logů*)**
- **Parsing / Normalization of the logs (*Normalizace logů*)**
- **The rule engine (*Engine pravidel a korelační engine*)**
- **Log storage (*Uložiště dat z logů*)**
- **Event monitoring and retrieval (*Monitoring událostí*)**



Obrázek 5 - Kooperace dílčích částí SIEM, převzato a upraveno (Miller, 2011)

Source device- je částí, která by se dala považovat za elementární. Relevance výstupu ze SIEM, tj. analýza a auditování, je podmíněna relevancí dat samotných. Pokud budou užity události, které jsou klamné či zkreslené, výstup bude totožného charakteru. Objem dat, která jsou každodenně generována, je enormní a data jsou zasílána z různých druhů zařízení. Zdrojem dat může být takřka cokoliv, co obsahuje relevantní data, tudíž je smysluplné z nich získávat logy.

Mezi hlavní zdroje dat patří:

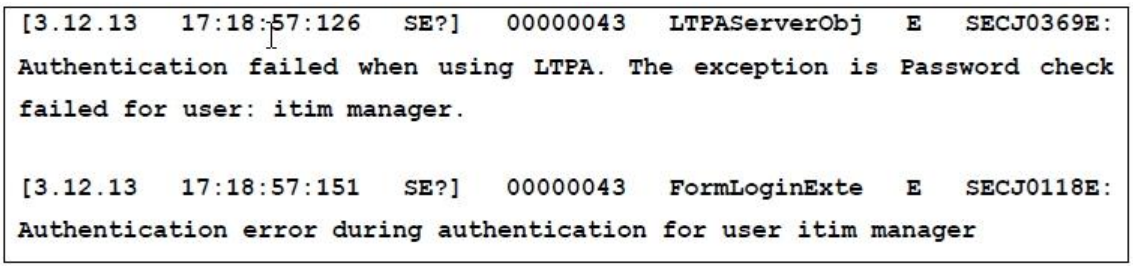
- Operating systems
- Appliances
- Applications
- Routers
- Switchers
- Firewalls

Pokud je vzat v potaz objem, v jakém logy přicházejí, je v prvé řadě důležité definovat pouze takové, které budou informativním přínosem pro organizaci. Pokud se budou zasílat na SIEM všechny typy událostí, ze všech druhů potencionálních zdrojů, může se stát, že dojde k přehlcení informacemi rozdílné kvality a ty události, jež by byly bývaly sloužily jakožto podklad pro šetření potencionálního bezpečnostního incidentu, jednoduše zaniknou v záplavě nerelevantních dat.

Dalším logickým postupem je pak determinace důležitosti faktorů, jako je frekvence, s jakou budou logy do SIEM načítány zda je skutečně třeba zpracovávání logů v reálném čase nebo postačí opakovat proces ve specifickou část dne nebo jaká bude potřebná kapacita uložiště pro logy, pokud budou generovány v daném množství.*(Miller, 2011, s. 80)*

```
1252: *Dec 03 19:13:37.011: %SEC_LOGIN-4-LOGIN_FAILED: Login failed
[user: root] [Source: 10.10.10.2] [localport: 23] [Reason: Login
Authentication Failed - BadPassword] at 19:13:36 CST Thu Dec 03 2013
```

Obrázek 6- Log záznam CISCO routeru, převzato (Vízner, 2014)



Obrázek 7- Log záznam kritické aplikace IBM ISIM 6.0, převzato (Vízner, 2014)

Na přiložených obrázcích je demonstrována rozdílnost logů, které jsou zasílány do SIEM systému.

Log collection proces sběru logových souborů je krokem, pomocí kterého budou tyto soubory přesunuty ze zdrojových zařízení do uložišť SIEM systému. Samotný sběr je procesem, jehož varianta se liší podle konkrétního druhu SIEM systému, který organizace užívá. Lze však tvrdit, že existují dvě základní možnosti, jak dostat data do SIEM systému. Níže popsané metody kolekce jsou diametrálně rozdílné, nicméně jednu věc mají společnou- obě úspěšně dostanou data ze zdrojového zařízení do SIEM systému.

- **Push metoda kolekce logů**
- **Pull metoda kolekce logů**

Tyto dvě metody lze nejsnáze diferenciovat pomocí toho, z jakého konce je tok dat iniciován. Při push metodě kolekce je iniciace na straně zdrojového zařízení, přičemž SIEM systém na procesu nijak aktivně neparticipuje. Naproti tomu při pull metodě kolekce je proces iniciován SIEM systémem, který se připojí na zdrojové zařízení a odsud si logové soubory aktivně přenáší do SIEM.

Push metoda má hlavní benefit v tom, jak lze lehce nastavit konfiguraci na SIEM.
Pomocí nastavení jednoznačného identifikátoru v koncovém zařízení, který odkazuje na SIEM systém, je zaručeno snadné vytvoření toku dat do SIEM systému. Nejčastěji se touto metodou sbírají tzv. syslogy. Ty jsou zasílány přes protokol UDP nebo TCP, pokud je třeba odeslat řetězec větší než 1024B.

U push kolekce logů, jak již bylo řečeno, je nespornou výhodou jednoduchost připojení, avšak tato metoda skýtá i svá negativa. Za předpokladu, že je užit protokol UDP pro zasílání syslogu do SIEM systému, může dojít k falsifikaci informací, která jsou zasílána, pokud je hacker natolik vynalézavý, aby zfalšoval packety a zaplavil SIEM falešnými daty, bude relativně těžké ho odhalit, pokud nemá organizace přehled o tom, z jakých zdrojových zařízení je čerpáno. Ať už se jedná o špatně nastavený systém nebo o uživatele, chystajícího se zneužít trhliny v systému. Protože SIEM přímo nepřistupuje do zdrojového zařízení, nelze nijak ověřit, zda jsou data pravá. Z toho důvodu je velmi důležité rozumět tomu, jaká zařízení zasílají do SIEM svá data.

Pull metoda je na rozdíl od push metody zajištěna aktivní iniciací od SIEM systému, který se připojí na konkrétní zdrojové zařízení a odtud si začne transferovat logy do systému. Největší nevýhodou této konkrétní metody je fakt, že logové soubory nemusí do SIEM systému přicházet v reálném čase, neboť je třeba samotná iniciace systémem SIEM, který dosáhne požadovaného umístění a teprve pak začne přemisťovat logy ze zdroje. Pull metodu lze proto využívat v časových intervalech, které jsou z pravidla nastavitelné uživatelem, ať už se jedná o opakování každých pár minut nebo pár hodin.

Po definování obou zmíněných metod následuje zamyšlení nad možnostmi implementace těchto kolekčních metod.

Zvolení konkrétní metody pak závisí na konkrétní implementaci SIEM systému.
V případě užívání produktů některých větších organizací, je možné užití předvytvořených autentizačních metod a logické struktury, která byla vytvořena organizací.
Tato možnost, bohužel neexistuje pro každou implementaci SIEM systému.
Mnohem častějším scénářem je skutečnost, že je aplikovaná upravená verze systému SIEM, sedící právě a pouze na konkrétní systém organizace. V tomto případě má organizace dvě možnosti. První možností je transformace logů do takové podoby, aby si byl s nimi schopen SIEM poradit sám, respektive aby jim rozuměl. Druhou možností je vytvoření tzv. „custom log collection.“ Vytvoření sběru logů na míru je časově náročný proces, pod který spadá kromě vytvoření zmiňované kolekce také vznik parseru, který

bude fungovat jako „rozdělovač“ logů podle kategorií. Při správném vytvoření kolekce i parseru jsou logy vytaženy ze svého přirozeného prostředí přímo do SIEM systému. Skutečnost, že nyní má organizace přehled nad všemi sběrovými i dělícími procesy, může být pozitivem i negativem zároveň. Díky možnosti vtahovat do systému i nepodporované formáty značně roste funkcionalita celého systému. To však pouze za předpokladu, že má organizace povědomí o správném provádění procesu formátování a parseru tak, aby byly správné atributy dosazeny do správných polí a SIEM jim mohl rozumět.

Myšlenka, že bude organizace čerpat z jediného zdroje logů, je utopická. Jak již bylo zmíněno, do SIEM systému jsou nahrávána data z nespočtu zdrojových zařízení. Z tohoto důvodu je nutné užití kombinace několika metod vtáhnutí dat do SIEM systému, v závislosti na typu zdrojového zařízení. (Miller, 2011, s. 81)

Parsing and normalization of the logs jsou důležitými prvky každého SIEM systému. Za předpokladu, že organizace zdárně vyřešila konfiguraci kolekce logů, vyvstává další problém. Logy do SIEM systému chodí ve svém přirozeném formátu, respektive tak, jak jsou odeslány ze zdrojového zařízení. V tomto okamžiku je za potřebí užití normalizačních a parserových procesů, díky kterým začne SIEM systém skutečně rozumět tomu, co mu logy říkají. Doposud fungoval jakožto repository pro přicházející logy. Níže přiložená tabulka znázorňuje normalizovaná data z logů, která byla uvedena i v podkapitole věnující se zdrojovým zařízením. (Miller, 2011, s. 84)

Čas	Datum	Zdrojová IP adresa	Cílová IP adresa	Událost	ID zařízení
17:18:57 SEC	12.2.2016	127.0.0.1	127.0.0.1	Login Failed	ISIM
19:13:37 SEC	12.2.2016	10.10.10.2	192.168.1.1	Login Failed	Cisco Catalyst 6500

Tabulka 1- Normalizovaná log data, převzato a upraveno (Vízner, 2014, s. 16)

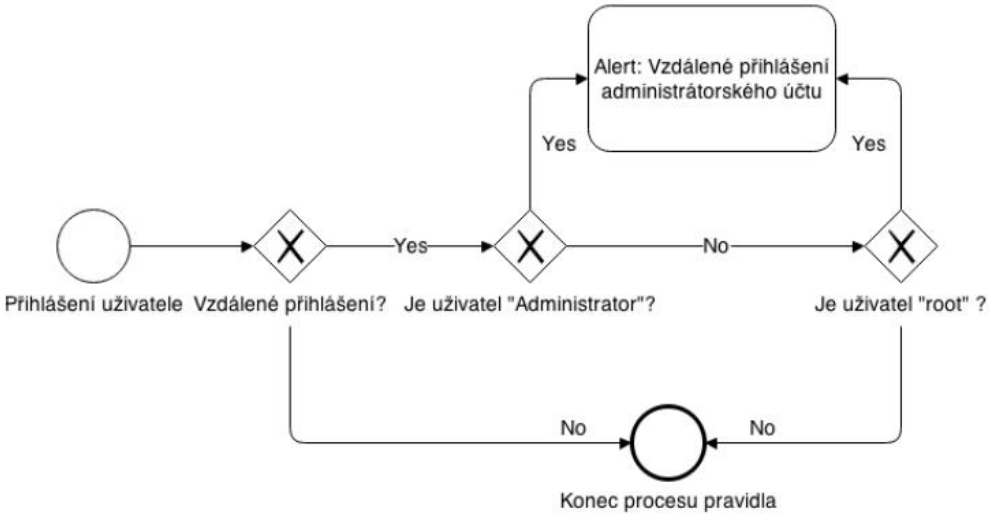
The rule engine and correlation engine každý ze zmíněných strojů hraje v prostředí SIEM systému rozdílnou roli. Důvodem, proč jsou sjednoceny pod jednou skupinou je jejich úzká závislost a synergie v prostředí SIEM systému.

Samotný průběh procesu bude určujícím faktorem při definování jednotlivých engine. Než je možné užití korelace k porovnání podezřelých událostí, musí být nejdříve spuštěno pravidlo, které na danou událost upozorní.

Nyní budou následovat definice pro rule engine a correlation engine.

- **Rule engine**
- **Correlation engine**

Rule engine slouží k vytváření pravidel, díky kterým je systém upozorněn na podezřelé události, které přicházejí do systému, při splnění kritérií nastavených v konkrétním pravidle. Pravidla jsou definována jako podmínky, které jsou nejčastěji ve formátu „what-if," přičemž konkrétní typ formátu se liší s každým druhem SIEM systému, stejně jako postupy normalizační nebo parseru. Výstupním atributem je pak hodnota typu boolean. Dalším logickým krokem se pak jeví spojení několika pravidel, respektive podmínek, do jednoho komplexního. Příkladem užití komplexního pravidla je vyhodnocení autentizačního procesu v rozdílných operačních systémech (Windows a Linux), kde se v podmínce liší název účtu, jakým uživatel přístup iniciuje.



Obrázek 8- Logická posloupnost komplexního pravidla pro autentizaci, převzato (Vízner, 2014)

Výstupem celého pravidla pak je právo vzdáleného přístupu do systému, avšak pouze pokud je uživatel administrátorem nebo root v případě Linuxu. Pokud splní obě zmíněné podmínky, bude pravidlo spuštěno, což zapříčiní druh notifikace, který není v diagramu specifikován.

Correlation engine je svou funkcí nenahraditelný v procesu rozpoznávání hrozeb. Porovnává normalizovaná data ze zdrojových zařízení a snaží se najít událost, která má potenciál pro vznik bezpečnostního incidentu. Přidává do systému SIEM určitou dávku umělé inteligence, neboť je schopen vzít v potaz obrovskou škálu informací a proměnných, které samotné nevytváří domněnku, že se jedná o hrozbu, ovšem v širším kontextu, kdy je zahrnuto několik dalších skutečností, již může dojít k rozpoznání hrozby, která nebyla při zkoumání méně proměnných na první pohled patrná. Další nespornou výhodou korelačního engine je schopnost rozpoznání tzv. false positive, což je schopnost, kterou mnohé systémy na podporu prevence průniku bez zabudované vnitřní logiky, postrádají. Příkladem demonstrujícím korelaci několika pravidel jsou kupříkladu opakující se pokusy o přihlášení se do systému, většinou pod administrátorským jménem, kdy několik prvních neúspěšných pokusů je následováno úspěšným přihlášením do systému. To, co při zkoumání jednotlivých událostí zvlášť, vypadalo pouze jako omylem špatně zadané heslo, může při filtraci podle IP adresy,

username nebo času při korelaci více událostí za daný časový interval směřovat k úspěšnému odhalení proniknutí neoprávněného uživatele za užití brute-force.

Time	Event number	Source IP	Destination IP	Event
10:10:01	1035	192.168.1.200	10.10.10.25	Failed login to server
10:10:02	1036	192.168.1.90	10.10.10.21	Sucessful login to server
10:10:03	1037	192.168.1.200	10.10.10.25	Failed login to server
10:10:04	1038	192.168.1.90	10.10.10.21	Failed login to server
10:10:05	1039	192.168.1.90	10.10.10.21	Sucessful login to server
10:10:06	1040	192.168.1.90	10.10.10.21	Sucessful login to server
10:10:07	1041	192.168.1.200	10.10.10.25	Failed login to server
10:10:08	1042	192.168.1.90	10.10.10.21	Failed login to server
10:10:09	1043	192.168.1.90	10.10.10.21	Failed login to server
10:10:10	1044	192.168.1.200	10.10.10.25	Sucessful login to server

Tabulka 2– Možný brute-force útok, převzato a upraveno (Miller, 2011, s. 88)

U tohoto konkrétního případu platí pravidlo, že pokud jsou zde od stejného zdroje za menší časový interval tři neúspěšné pokusy a vzápětí jeden úspěšný, mělo by se vytvořit varování na „Possible brute-force Login.“

If [(failed logins >=3)] and then (Successful Login) from the same source within 20 seconds = Possible Brute Force Attack

Log storage je potřebnou součástí SIEM systému, protože je nutné velké objemy dat, které do systému přicházejí, někde skladovat, aby bylo možné s nimi později pracovat. Úložiště dat však neslouží pouze pro ukládání přijatých událostí, ale také jako celkové úložiště systému. SIEM si ukládá dílčí systémové operace, transakční operace, aj. V kontextu SIEM je ale nejdůležitější uchování již právě zmíněných událostí a dat ze zdrojových zařízení. Ukládání těchto dat a informací je klíčové při provádění analýz nebo auditování.
SIEM systém ukládá svá data do tří, běžně užívaných, druhů.

- **Database** (databáze)
- **Flat text file** (textový soubor)
- **Binary file** (binární soubor)

Skladování dat v **databázi** je způsob, jakým ukládá data většina SIEM systémů. Standardně jsou užívány platformy Oracle, MySQL, Microsoft SQL.
Mezi hlavní výhody užití databáze patří především snadná interakce a vytažení dat z databáze, protože samotná volání jsou součástí databázového systému. Otázka výkonu a rychlosti odezvy při požadavku na data je pak především ovlivněna hardwarovým a systémovým vybavením, které společnost vlastní. Pokud je databázový systém optimalizován a správně implementován tak, aby kooperoval se SIEM systémem, neměly by takřka žádné problémy nastat. Problémy by však mohly nastat, pokud organizace užívá databázové aplikace, která není optimalizovaná pro firemní prostředí a společnost se rozhodla si databázi spravovat sama.

Flat text file je standardní textový soubor, který se používá především z důvodu jeho přehlednosti a snadné čitelnosti (human-readable form) obsažených informací.
Protože lze data pročítat bez jakéhokoliv dekódování, je snadné z těchto souborů vytvářet analýzy pomocí vyhledávacích funkcí textových editorů.
V každém z těchto souborů je nutné užití tzv. delimiteru. Delimiter je znak, oddělující jednotlivé výstupy. Pro tuto funkci se užívá čárka, středník nebo jiné znaky. Užití oddělovače je klíčové pro správný parsing a čtení. Textové soubory se neužívají zdaleka

tak často jako databázové aplikace. Hlavní nevýhodou je jejich absence funkčnosti u většího prostředí a ani výkon, respektive čtení a zápis, není v tomto případě nijak oslnivý. Bezpečnostní aspekt je také špatný.

Binary file formát se užívá při ukládání dat v binární podobě. Samotný proces zápisu čtení je znám jen konkrétní aplikaci SIEM. Tento soubor je na rozdíl od textového souboru pro člověka nečitelný. Tento aspekt sice zvyšuje bezpečnost, ale ani tato metoda není vhodná pro rozsáhlejší řešení.

SIEM systém umí průběžně generovat při ukládání dat kontrolní součty (tzv. digitální podpisy), které umožní pozdější kontrolu, aby bylo jisté, že nedošlo k dodatečné manipulaci s úložištěm logů.

Monitoring je finální částí SIEM architektury a poslední částí, která bude v tomto kontextu zmíněna. Tato část dává smysl úschově dat. Nyní, když jsou data uložena v úložišti, je možné s nimi dále pracovat.

Webové či aplikační rozhraní SIEM umožní, aby bylo možné provádět prohlížení, analyzování, různé druhy členění dat, vytváření pravidel nebo cokoliv jiného, co bylo zmíněno v rámci hlavní SIEM architektury. (Miller, 2011, s. 86 - 92)

4.3 Výběr produktu pro implementaci v prostředí střední firmy

Po definování principů SIEM je nutné zvolit adekvátní produkt s touto technologií při zvážení primárních aspektů firmy – politika, rozpočet, velikost firmy, velikost informační infrastruktury, technologické možnosti.

Než však bude možné přejít ke konkrétnímu výběru vhodného produktu, je nutné nejdříve definovat, co je to malá či střední firma, často souhrnně nazývána zkratkou SMB (*Small and medium Business*)

Na velikost podniku, respektive na hranici dělící malý podnik od středního lze nahlížet z několika úhlů. Klíčovými atributy pro rozeznání můžou být například počet zaměstnanců, roční obrat nebo roční bilanční suma. Absolutní čísla těchto veličin se pak mění v závislosti na legislativě konkrétního geografického celku. Pro srovnání lze uvést, že aby byl podnik definován jako *středně velký*, je nutné, aby měl méně jak 250 zaměstnanců, ale zároveň více než 50 zaměstnanců v rámci Evropské unie. Pro Spojené státy americké je tato hranice posunuta na 500 zaměstnanců namísto 250.
Pro demonstrativní účely bude prezentována příloha s konkrétními čísly pro malou i střední firmu. Níže prezentovaná čísla jsou relevantní pro území Evropské unie.

Category	Number of employees	Annual turnover (million €)		Annual balance sheet total (million €)
Small	10 < x < 50	2 < x < 10	or	2 < x < 10
Medium	50 < x < 250	10 < x < 50	or	10 < x < 43

Obrázek 9- Definování SMB, vlastní zpracování

Z přiloženého obrázku je patrné, že pro splnění podmínek pro jednotlivé kategorie je nutné, aby měla organizace potřebný počet zaměstnanců (*number of employees*), může si však vybrat, zda bude plnit limit ročního obratu (*annual turnover*) nebo roční bilanční sumy (*annual balance sheet total)*. Nemusí tedy plnit oba zmíněné limity a jeden z nich překročit bez toho, aby riskovala ztrátu statutu SMB. (Průša, Ošťádal a Topolánek, 2006)

Po zvážení všech zmíněných esenciálních faktorů, se jako optimální řešení jeví volba produktu IBM Security QRadar SIEM.

V potaz byl vzat i fakt, že po zveřejnění Gartner's magic quadrant pro odvětví SIEM byl produkt IBM opět zvolen (pro rok 2015) jako nejlepší ze všech SIEM řešení na trhu. (Burnham, 2015)

4.4 IBM Security QRadar SIEM

IBM Security QRadar je plně komerční řešení systému SIEM, v současné době je distribuce pod firmou IBM. IBM koupila tento produkt od společnosti Q1 Labs. IBM ho integrovala do svého portfolia, což ještě zvětšilo funkčnost, již i tak velmi propracovaného SIEM řešení. IBM Security QRadar SIEM běží na operačním systému společnosti Red Hat Enterprise Linux 6,7. Užívá se 64 bitová verze systému a aktuální verze, v době zpracování této práce, nese označení IBM Security QRadar 7.2.6.

Protože se jedná o plně komerční řešení, je samozřejmostí vysoká škálovatelnost řešení tak, aby bylo možné je použít pro různě veliké organizace. O všeobecné architektuře SIEM již byla napsána kapitola, z toho důvodu bude pro definování architektury QRadaru užit ryze praktický přístup – kooperace fyzických zařízení užívající logické komponenty.

Architektura IBM Security QRadar má několik desítek možných variací, v závislosti na druhu komponentu, jeho výkonu, ale především schopností bezproblémově kooperovat se zbytkem. Seznamy pro M3 a M4 server racky budou sdíleny níže.

Při splnění podmínek daných organizací, tj. především finanční možnosti, politiky organizace nebo konkrétních požadavků týkající se implementace, je vybráno a později distribuováno řešení, které odpovídá těmto požadavkům. V rámci distribuování je na výběr několik možností pořízení QRadaru.
Prvním je distribuování na konkrétní infrastrukturu pomocí nástrojů modelově sestavených pro dané řešení, což je sice náročnější na instalaci a konfiguraci, nicméně tato možnost zaručuje škálovatelnost, což u druhé možnosti nelze. Druhou možností je zakoupení All-in-one řešení.
Poslední možností je zakoupení licencí na vlastní hardware nebo využití virtuálních zařízení.

Dále je nutné definovat rozdíl mezi těmi logickými prvky, které jsou nutné pro chod SIEM systému, a pro ty, které jsou volitelné. Pomocí seznamu jsou demonstrovány prvky esenciální pro chod SIEM architektury a nadstavbové prvky, které významně dopomáhají zrychlení nebo zvýšení funkčnosti konkrétních procesů v SIEM.

- Nezbytné logické prvky
    - Event Processor
    - Event Collector
    - Flow Processor
    - Flow Collector
    - QRadar Console
- Volitelně přidávatelné logické prvky
    - Incident Forensis
    - Packet Rupture
    - Vulnerability Manager
    - Risk Manager
    - Anomaly Detection
    - Data Node

V rámci poslední vydané verze QRadar 7.2.6 existují dva typy Lenovo rack serverů, na které je nasazován QRadar. Jsou to řady M3 a M4. Jsou od sebe odlišeny především výkonem, architekturou apod. M4 je v tomto ohledu lepší, neboť se jedná o novější rack server. Do těchto serverů jsou pak umístěny tzv. appliance, což jsou hotové a funkční hardwarové prvky, obsahující rovněž přidružený software, který se liší v závislosti na druhu appliance.
V rámci poslední vydané verze QRadar 7.2.6 jsou dostupné tyto appliance:

- M3 appliance overview[1]

- M4 appliance overview[2]

Číselné značení výše uvedených appliance je odvozeno následujícím způsobem. První dvě čísla jsou označením licence (31xx) a druhá dvě čísla jsou označením typu fyzického serveru (xx28).

Pro účely této práce budou definovány appliance disponující nejvyšším možným výkonem, bude se tedy jednat o appliance užívané pro rack server M4.

Pro případ užití středního podniku bude definováno konkrétní distribuované řešení.

- **QFlow 1310** nabízí vysokou kapacitu a škálovatelnost. Provádí monitoring až 7. ISO/OSI vrstvy a sbírá data, respektive generuje záznamy síťových toků. Appliance se může pochlubit propustností 7,5 Gbps a je možné na něj napojit dva 10 Gbps interface na monitoring pomocí XFP portu. O chod se stará 16Gb paměť.

---

1 https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.6/com.ibm.qradar.doc/c_hwg_app_overview_m3.html

2 https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.6/com.ibm.qradar.doc/c_hwg_app_oview.html

- **QRadar 1501** je appliance pracující jako event collector, sbírá logovací události, které jsou zasílány od koncových zařízení a aplikací a předává je např. QRadaru 1628, který se pak stará o processing událostí.

- **QRadar 1628** je dedikovaný škálovatelný event procesor, který v sobě skrývá jak Event collector tak Event Processor a samozřejmě interní úložiště pro události. QRadar 1628 potřebuje pro svůj zdárný chod připojení na appliance QRadar 3128 (Console). Appliance zvládá až 40000 EPS (*Event per second*).

- **QRadar 1728** je dedikovaný flow procesor, schopný díky své škálovatelností zvýšit počet FPM (*Flow per minute*). Appliance obsahuje Flow processor, Flow Collector a interní úložiště pro datové toky. Při upgradované licenci je schopen zpracovat až 1 200 000 FPM, které posléze ukládá do 128Gb úložiště.

- **QRadar 1805** je appliance, která dohromady kombinuje jak Event Processor, tak Flow Processor za účelem zvládání většího počtu událostí a toků. Typově se jedná o kombinaci výše zmíněných appliance QRadar 1628 a 1728. Navíc od již zmíněných procesorů obsahuje také interní úložiště. Toto komplexní řešení má ale nevýhodu v relativně nízkém výkonu, konkrétně 5000 EPS a 200 000 FPM u upgradované verze. Velikost uložiště je 64 GB.

- **QRadar 3128 Console** je appliance užívaná pro centralizovanou správu událostí a datových toků, profilace síťového chování a identifikace potenciálních bezpečnostních hrozeb. Zmíněné řešení je možné rozšířit o jednu či více appliance (Event processor 1628, Flow processor 1728 a Flow processor1828).

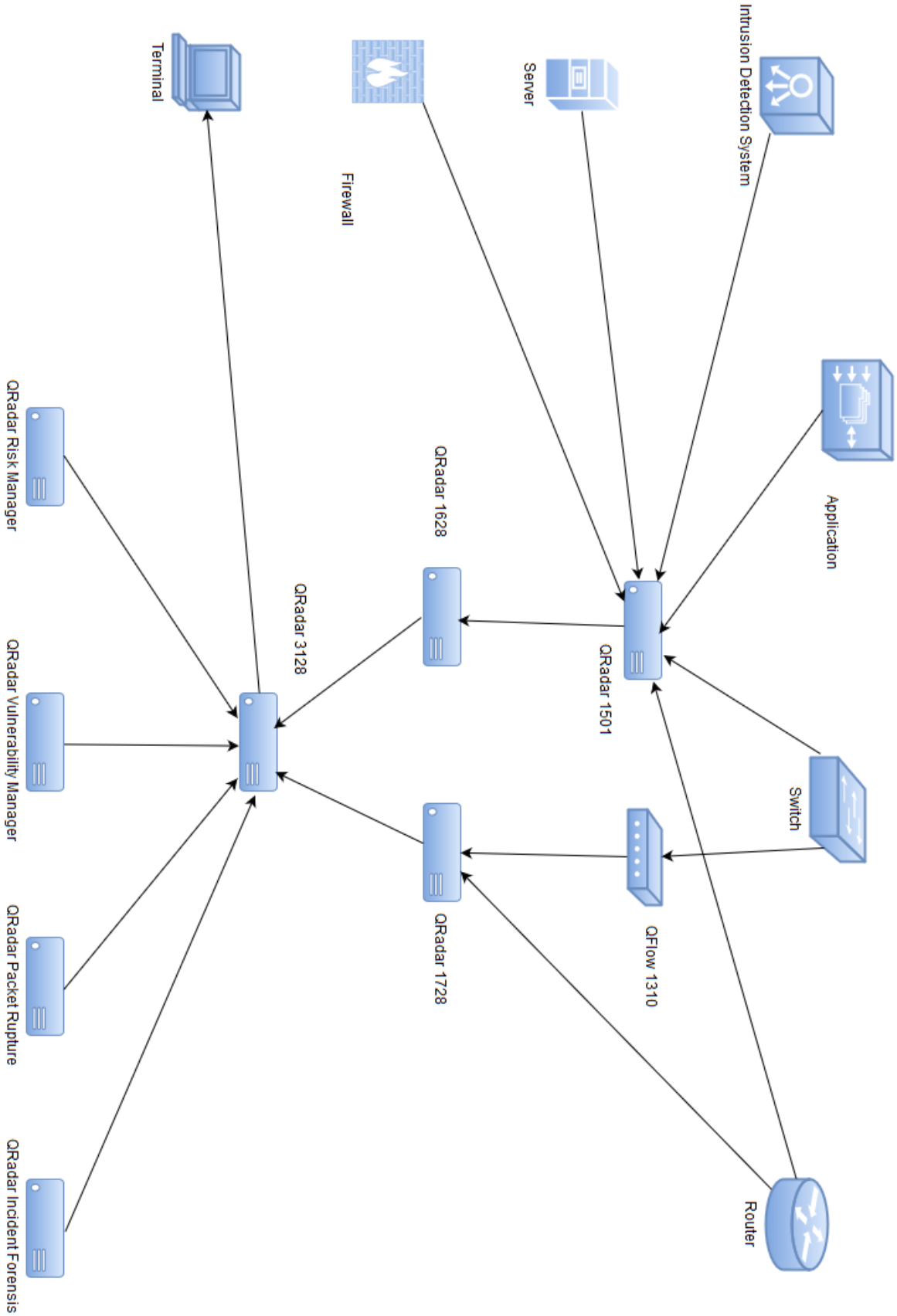
- **QRadar Vulnerability Manager** je nadstavbová komponenta pro definování zranitelnosti. Provádí skenování a report na potencionálně slabých místech v podnikové informační infrastruktuře. Manager nabízí správu workflow pro

software, appliance a virtuální appliance, plně integrované s QRadarem. Zařízení nejprve provede scan všech síťových součástí, ať už vevnitř nebo vně sítě organizace, následně provede komplexní reporting s návrhy na zlepšení zranitelných míst. Obsahem skenování může být až 32 768 prvků, při užití upgradované verze. Součástí je opět interní úložiště čítající kapacitu 64 GB.

- **QRadar Risk Manager** je další nadstavbová komponenta zvyšující funkcionalitu QRadaru. Nabízí plně integrovaný management rizik, řešení zranitelných míst a také automaticky nabízí řešení pro tato rizika. Díky těmto schopnostem přináší do QRadaru komplexní řešení pro veškerý rizikový a incident management, jejich následující vizualizaci a reporting. Pro tyto účely mu slouží 64 GB velké úložiště.

- **QRadar Incident Forensis** je nadstavbovou komponentou zabývající se především zpětným zmapováním akcí potencionálního útočníka, tak jak šly krok za krokem, provedení hloubkového šetření podezřelých bezpečnostních incidentů - to vše za účelem zvýšení efektivity práce bezpečnostních týmů a rovněž jako preventivní opatření, aby se podobné útoky v budoucnu neopakovaly.

- **QRadar Packet Capture** slouží jako volitelná nadstavba pro QRadar Incident Forensis, za účelem skladování dat v případě, kdy žádné jiné zařízení schopné zachytávání packetů (PCAP) není dostupné. Jedná se tedy o appliance zabývající se kolekcí datového toku. Pro účely odchytávání dat z forenzních procesů má k dispozici úložiště o kapacitě 128 Gb. (*IBM QRadar Security Intelligence Platform v7.2.6*, 2015)



Obrázek 10 - Distribuovaná fyzická architektura QRadar M4 rack server, vlastní zpracování

Výše je demonstrována jak kolekce toku dat (QFlow 1310) tak příjem logů z aplikací do kolektoru (QRadar 1601), nasbíraná data jsou pak dále procesována přes Flow Collector (QRadar 1728) a Event Collector (1628). Zpracované informace z dat jdou pak do console QRadaru (QRadar 3128), kterému v rozhodovacích a jiných esenciálních procesech napomáhají další logické komponenty – Risk manager, Vulnerability manager, atd. Koncový výstup je pak prezentován uživateli pomocí user interface Terminálu.

Systémové požadavky IBM QRadar SIEM

Níže bude uveden přehled obsahující systémové požadavky pro jednotlivé druhy appliance. Systémové požadavky jsou relevantním faktorem, pokud je třeba vzít v potaz implementaci na vlastní hardware, případně využití možnosti virtuální appliance. Při využití komplexního řešení od IBM je zaručeno, že hardware bude odpovídat nárokům kladeným od softwaru.

Rozdíl mezi fyzickým a virtuálním appliance tkví především v rozdílu výkonu jednotlivých druhů appliance. Virtuální appliance je několikanásobně výkonnostně slabší než jeho fyzický ekvivalent.

TABULKA xx28 porovnání

Zařízení	CPU	RAM	Úložiště	Šasi
QRadar 3128 **QRadar 1628** **QRadar 1728**	2 x E5-2680V2, 2.8 GHz, 10Core, 25 MB Cache	128 GB	48 TB	xSeries 3650 M4 BD
QRadar 1501	1 x Intel Xeon processor E5-2630V2, 2.6 GHz, 6 Core, 15MB Cache	24 GB	1,2 TB	xSeries 3550 M4
QFlow 1310	1 x E5-2630V2, 2.6 GHz, 6 Core, 15MB Cache	16 GB	300 GB	xSeries 3550 M4

(*Lenovo Components*, 2016)

Funkční model IBM QRadar SIEM je výhodný z důvodu přehledného zobrazení logických prvků v infrastruktuře tak, aby byla hlouběji definována jejich funkcionalita.

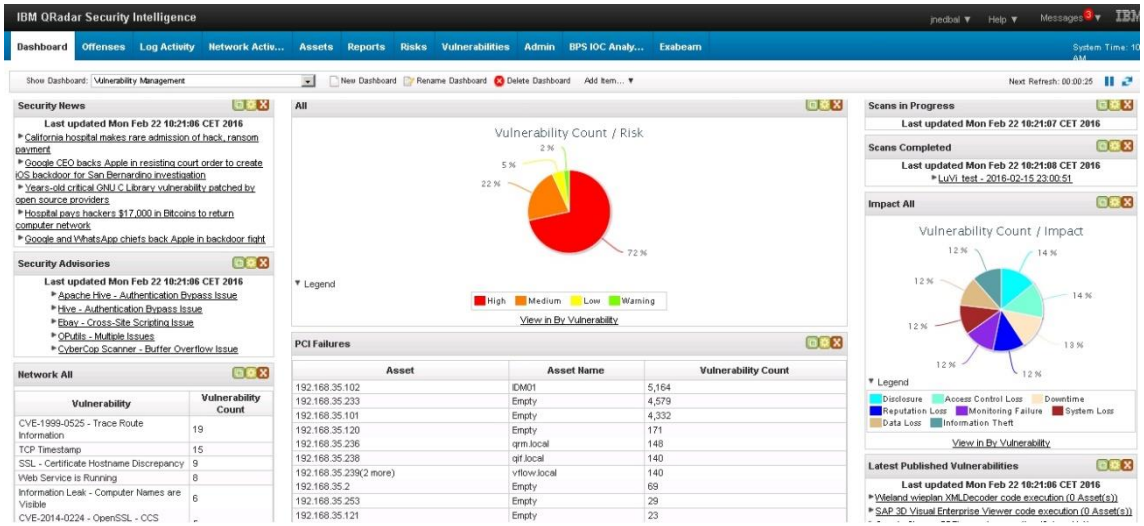
V kontextu logické infrastruktury lze nalézt níže uvedené logické komponenty:

- Event processor
- Event collector
- Flow collector
- Console
- Magistrate
- Data Node (Storage)

Event processor má na starosti zpracování událostí, která jsou sbírána z jednoho či více kolektorů. Event processor koreluje informace získané z událostí a prezentuje v oblasti, která je s konkrétním typem události asociovaná. Nasbírané informace z událostí jsou podrobeny analýze na základě předem daných podmínek a pravidel. Po terminaci tohoto procesu jsou data předána Magistrate.

QRadar QFlow Collector je komponenta, jejíž prací je pasivní sběr toku dat tak, jak plynou přes porty. Je schopen sbírat data, respektive datový provoz a získávat informace ze 4. nebo až 7. ISO/OSI vrstvy. Kolektor také podporuje kolekci externích datových toků, které se liší v závislosti na výrobci, avšak slovo „Flow," je ve většině případů obsaženo v názvu protokolů. Flow v tomto kontextu znamená kooperaci a komunikaci dvou jedinečných IP adres a portů, využívající shodný komunikační protokol. Nejznámější komunikační protokol je vytvořen společností CISCO a nese název NetFlow.

QRadar Console poskytuje uživatelské rozhraní pro komponenty QRadaru. Rozhraní nabízí uživateli datový tok, různé druhy náhledů – přes filtrování, offense, důležité informace a administrativní funkce, to vše v reálném čase.



Obrázek 11- Ukázka user interface IBM Security QRadar, vlastní zpracování

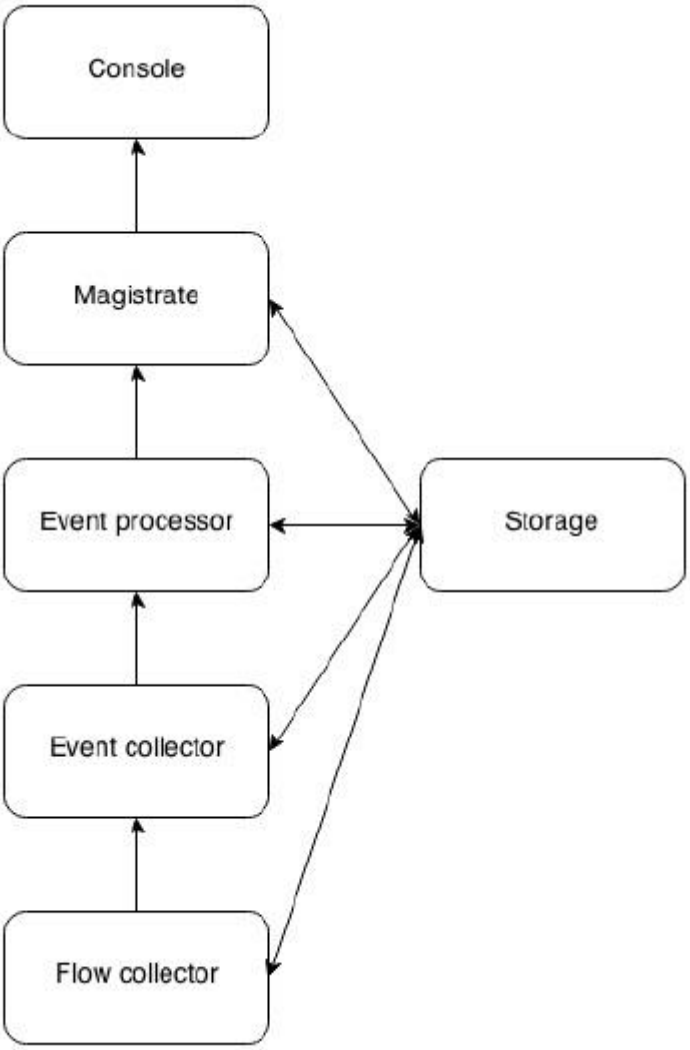
Magistrate je služba, jež běží na konzoli QRadaru. Poskytuje klíčové procesy komponentů. Poskytuje správu pohledů, reportů, varování a analýz datového toku a bezpečnostních událostí, které vyžadují zvýšenou pozornost. Magistrate nechá události projít přes vytvořená pravidla. Pokud událost splňuje podmínky některého z pravidel, je generována adekvátní odpověď, která je definována v konkrétním pravidle. Bezpečnostní incidenty jsou seřazeny podle magnitude – číselná hodnota, která je součtem několika faktorů. Jmenovitě je to počet přijatých událostí, závažnost, relevance a důvěryhodnost.

QRadar Event Collector má za úkol sběr událostí z lokální a vzdálených zdrojů logů tyto události pak normalizuje. Během tohoto procesu dochází také k rozpoznávání typu události a jeho následnému mapování na QRadar Identifier (QID) jednou z komponent Magistrate. Nakonec kolektor sváže identické události k sobě, aby šetřil systémové užívání a zašle informace o událostech do Event Processoru.

.

Data Node (Storage) umožňuje novým i stávajícím logickým komponentám QRadaru přidávat úložiště a zvětšovat kapacitu v případě potřeby. Data Node urychluje rychlost vyhledávání v systému díky možnosti ponechat více dat bez komprese. V rámci QRadaru se nejčastěji používá jako úložiště databázový systém IBM DB2. (*IBM Security QRadar*, 2016)

Po definování jednotlivých logických komponent z funkčního pohledu bude demonstrována jejich kooperace za účelem lepšího porozumění celému konceptu.



Obrázek 12- Kooperace v rámci logické architektury IBM QRadar SIEM, převzato a upraveno (IBM Corporation, s. 135)

5 Kalkulace (servery, dispozice, ekonomický aspekt)

V rámci poslední probírané kapitoly budou demonstrovány konkrétní kalkulace na pořízení distribučního řešení pro dvě tuzemské firmy. Z důvodu zachování citlivých informací budou záměrně opomenuty jejich jména či jiné charakteristické vlastnosti, které by mohly vést k určení. Typově však lze říci, že se bude jednat o standardní nasazení řešení pro střední firmu v bankovním sektoru a druhé řešení je implementováno na malou firmu ze zdravotnického sektoru.

Záměrně jsou užity logické prvky QRadaru, i když je možná implementace SIEM řešení také na jiný hardware než ten, který je nabízen od společnosti IBM.

Definování dílčích pojmů souvisejících s rozdílem mezi malou a střední firmou bylo pokryto v kapitole *Výběr produktu pro implementaci v prostředí středního podniku.*

Implementace SIEM řešení pro střední firmy je relativně běžným procesem, naproti tomu implementovat toto řešení také na malou firmu není až tak obvyklé, i když se tento trend bude zřejmě zvětšovat. S rostoucí potenciální možností bezpečnostního incidentu, nezbude malým organizacím nic jiného, než si také pořídit bezpečností řešení, které těmto pokusům zamezí. Útočník se totiž může domnívat, že snáze získá citlivé informace ze systému menších organizací, které mnohdy stránku internetové bezpečností opomíjí.

V závěru kapitoly budou obě implementace porovnány.

Celý proces implementace distribuovaného SIEM řešení zahrnuje mimo samotnou implementaci na organizační infrastrukturu také několik kroků, které jsou provedeny ještě před samotnou implementací. Bez těchto kroků nelze řešení implementovat požadovaným způsobem, respektive zachovat všechny faktory stanovené organizací.

1. Analýza a popis prostředí
    - Seznam zařízení
    - Kalkulace
2. Návrh komponentů QRadar + licence

Analyzování veškerých dílčích faktorů relevantních pro chod řešení nebo organizaci samotnou je stěžejním krokem v celém procesu. Předem musí být známy co nejpřesnější údaje týkající se počtu zařízení zasílajících data do QRadaru. Bez těchto čísel není možné vytvoření kalkulace potřebného výkonu a bez kalkulace nelze navrhnout konkrétní distribuované řešení. Řešení tvořené bez řádné analýzy by nemuselo výkonnostně stačit na přijímaný objem dat nebo naopak může být zbytečně výkonné a organizace mohla pořídit finančně méně náročné řešení.

Návrh konkrétního řešení a sestavení logických QRadaru probíhá vždy v souladu s kalkulací a organizační politikou. Řešení je navrženo takovým způsobem, aby vždy mělo výkonnostní i kapacitní rezervu pro případ náhlého překročení vypočítaného limitu. Z pravidla jsou čísla získaná z kalkulace navýšena o dvacet procent, což představuje dostatečnou záruku, proti těmto náhlým rizikovým situacím, ve většině případů.

5.1 Střední organizace z bankovního sektoru

Nyní bude demonstrován proces implementace distribuovaného SIEM řešení v prostředí středního podniku. Tento podnik je situován v bankovním sektoru.
Střední organizace je definována počtem zaměstnanců v rozmezí 50 až 250 lidí.

1. **Analyzování prostředí**

Jako úplně první je třeba zjistit čísla zásadní pro pozdější kalkulace a návrh logické struktury řešení. V tomto kontextu je stěžejní počet zaměstnanců a také počet zákazníků, se kterými firma spolupracuje.
Velmi důležitou informací je fakt, že IT infrastruktura této firmy je rozdělena do dvou geografických lokalit, z toho důvodu je vyžadován sběr událostí z obou těchto míst. Pro implementaci QRadaru je možné použití fyzického i virtuálního řešení, v tomto případě bude užito distribuované fyzické řešení, neboť to bylo jedním z požadavků organizace.

V rámci analýzy je nutné definovat co nejpřesněji počet zařízení, která zasílají svoje události do QRadaru.

Zařízení generující log záznamy	**Počet**
Unix server	20
Windows server	150
Databáze	20
Síťové zařízení	10
Aplikace	4
Zařízení generující flow záznamy	
Flow sondy	2

Tabulka 3- Seznam zařízení- střední firma, vlastní zpracování

Tato tabulka nereflektuje celkový počet prvků v infrastruktuře, ale pouze takový seznam prvků, který je natolik významný, že stojí za to, je do SIEM systému připojit a zmínit je.

Na základě této tabulky předpokládaného počtu zařízení bude vytvořena kalkulace za účelem zjištění potřebného výkonu pro kolekci a procesování eventů a flow. Kromě výkonnostního aspektu se zde řeší také požadavky na úložiště. Velikost úložiště se odvíjí od několika faktorů. Prvním je objem dat (událostí a flow), které do systému přicházejí a tím druhým je délka, po jako je nutné data skladovat např. pro potřebu auditování.

Za zmínku také stojí, že veškeré hodnoty budou na závěr navýšeny o 20%, aby bylo zajištěno pokrytí při náhlém výkyvu / přesahu stanovených hodnot.

	Device Type	Qty.	EPS Factor	EPS Rate
Event Sources	Windows Active Directory Servers	4	15	60
	Windows IIS and Exchange Servers	10	10	100
	Windows General Purpose Servers	132	2	264
	UNIX and Linux Servers	20	0,5	10
	DNS / DHCP Servers	4	15	60
	Antivirus Servers	2	20	40
	Database Servers	20	1	20
	Proxy Servers	2	25	50
	Large Firewalls	2	150	300
	Small Firewalls		20	0
	IDS, IPS and DAM		5	0
	VPN	4	5	20
	Routers and Switches	2	0,25	1
				0
				0
Additional Event Sources				0
				0
				0
				0
	Total Log Sources	202	Total EPS License	925

Obrázek 13- Kalkulace EPS- střední podnik, vlastní zpracování

Na přiloženém obrázku lze přehledně vidět, jakým způsobem probíhá výpočet EPS pro SIEM řešení. Na základě dříve zjištěného počtu zařízení, pro které je pevně definován počet EPS, je spočteno celkové konkrétní číslo potřebné pro účely této organizace. Hodnota EPS pro střední firmu byla spočtena na hodnotu 925.

	Device Type	Qty.	Flow Factor	Flow Rate
Flow Sources	Total Workstations on Network	220	10	2 200
	Total Servers on Network	146	120	17 520
	FPM - Layer 4 Total			19 720
	QFlow FPM (based on bandwidth			0
	Total FPM License			19 720

Obrázek 14- Kalkulace FPM- střední podnik, vlastní zpracování

Kalkulace pro celkový počet FPM je tvořena následujícím způsobem. Pro přesné stanovení této hodnoty je nutné vědět celkový počet pracovních stanic na síti. Ze seznamu zařízení je znám fakt, že toto řešení bude obsahovat dvě flow sondy. První sonda bude umístěna na perimetr, a to tak, aby zachytávala síťový provoz vnitřní sítě do internetu a naopak. Druhá sonda je umístěna v určité VLAN, kde monitoruje vnitřní komunikaci, která je směrována na kritické servery. Celkové číslo pro servery na síti odpovídá počtu serverů, které si organizace přeje monitorovat. V tomto případě se jedné o všechny Windows servery (Active directory, IIS and Exchange a General Purpose), tedy 146 serverů pro monitoring.
Celkové nároky na FPM jsou rovny 19 720.

Nyní jsou známy hodnoty objemu dat potřebných pro toto řešení. Dalším logickým krokem je výpočet nároků na úložiště. Požadavkem organizace byla schopnost uchování dat po dobu **6 měsíců**, což je interval, po kterém probíhá auditování. Veškerá čísla asociovaná s nároky na úložiště jsou proto násobeny šesti. Postup pro výpočet úložiště je totožný jak pro nároky flow, tak událostí.

Event Storage		
Average Event Size		Number of days uncompressed
1 000		14
Daily (bytes) Normalized	Daily (bytes) Raw	Events per Day
15 975 360 000	79 876 800 000	79 876 800
Weekly (bytes) Normalized	Weekly (bytes) Raw	Events per Hour
111 827 520 000	559 137 600 000	3 328 200
Monthly (bytes) Normalized	Monthly (bytes)	Events per Min.
479 260 800 000	2 396 304 000 000	55 470
Monthly (TB) Normalized	Monthly (TB) Raw	Events per Sec.
0	2,18	925
Auditing requirements	13	

Obrázek 15- Kalkulace úložiště, EPS- střední podnik, vlastní zpracování

Na přiloženém obrázku jsou demonstrovány nároky pro normalizované a surové události přicházející do systému. Hodnota normalizovaných událostí však není pro proces výpočtu úložiště zásadní. Je nutné počítat nároky ze surových dat, neboť hodnoty po normalizaci mohou být zavádějící a mohou se měnit v závislosti na několika faktorech.

Pro výpočet velikosti úložiště je nutné znát několik hodnot. Prvním z nich je průměrná velikost události přicházející do systému. Tato hodnota je stanovena na 1000 bajtů, což je defaultní hodnota pro většinu událostí. Při užití nestandartních událostí, které jsou velikostně větší, je logicky nutné počítat také s nárůstem celkových nároků na úložiště. Druhou hodnotou je počet dní, kdy mají obdržená data zůstat v dekompresi. Nestlačená data mají řádově několikrát větší velikost, ale vyhledávání potřebných informací v těchto datech je velmi rychlé. Naproti tomu komprimovaná data jsou objemově menší, ale rychlost vyhledávání informací v těchto datech je markantně snížena. Časový interval, po kterém jsou data kompresována, se odvíjí od toho, kolik dní zpětně je nejčastěji potřeba pro analýzu obdržených dat. Pokud je maximálním intervalem zpětného hledání týden, je zbytečné používat interval vyšší a naopak. Tato optimalizace může ušetřit organizaci další náklady na úložiště a častější komprese zajistí rychlejší výměnu nepotřebných dat za ty potřebné.

Pro střední firmu byla hodnota potřebná pro skladování událostí stanovena na 2,18 TB za měsíc. S ohledem na nároky skladování je celková hodnota 13,08 TB.

Shodným způsobem bude vypočtena kapacita úložiště potřebného pro flow.

Flow Storage		
Average Flow Size	QFlow Capture Size	Number of days uncompressed
200	100	14
Daily (bytes) Normalized	Daily (bytes) Raw	Flows per Day
1 135 872 000	5 679 360 000	28 396 800
Weekly (bytes) Normalized	Weekly (bytes) Raw	Flows per Hour
7 951 104 000	39 755 520 000	1 183 200
Monthly (bytes)	Monthly (bytes)	
34 076 160 000	170 380 800 000	
Monthly (TB) Normalized	Monthly (TB) Raw	Flows per Min.
0,03	0,1550	19 720
Auditing requirements	1,1157	

Obrázek 16- Kalkulace úložiště, FPM- střední podnik, vlastní zpracování

Pro kalkulaci nároků na kapacitu úložiště pro Flow je nutné znát kromě hodnoty FPM také několik dalších hodnot. První hodnotou je průměrná velikost segmentu datového toku, což je defaultně nastaveno na hodnotu 200 bajtů. Další důležitá hodnota je definována jako QFlow Capture Size, což je velikost zprávy, která je zaslána při reportingu jednoho flow záznamu. Velikost tohoto atributu je nastavena na 100 bajtů. Třetí hodnotou je, tak jako v případě EPS, počet dní, kdy data zůstanou nekomprimovaná. I zde je hodnota stlačení dat nastavena na 14 dní.

Měsíční nároky na kapacitu úložiště pro flow je 0,16 TB. Pro interval šesti měsíců je hodnota rovna 1,12 TB.

Kalkulace pro nároky na SIEM řešení jsou nyní kompletní. Posledním krokem je zvětšení všech zjištěných výsledků o 20% rezervu, což je dostatečné pro prevenci proti náhlým výkyvům.

EPS requirements total	1109,4
FPM requirements total	23664
Auditing requirements total	16,81

Obrázek 17- Kalkulace total requirements- střední podnik, vlastní zpracování

Pro tento podnik bude nutné navrhnout takové řešení, aby bylo schopné zpracovávat alespoň 1110 EPS, 23 664 FPM a mělo kapacitu úložiště kolem 17 TB.

Po dokončení procesu kalkulace, kdy byly zjištěny parametry potřebné pro fungování SIEM řešení, bude vytvořen návrh distribuovaného řešení splňující tato kritéria.

2. Návrh komponentů QRadaru + licence

Než bude možné přejít k samotnému návrhu konkrétních appliance, je nutné se zamyslet, jak bude vypadat logická struktura komponent tohoto řešení. Než však bude možné tento návrh vytvořit, je nutné být obeznámen se seznamem potřebných logických komponent.

Toto řešení bude obsahovat následující prvky:

- Console
- Event processor
- Event collector
- Flow collector
- Flow processor

Konkrétní appliance vyhovující co nejvíc výkonnostním požadavkům, jsou zmíněny níže.

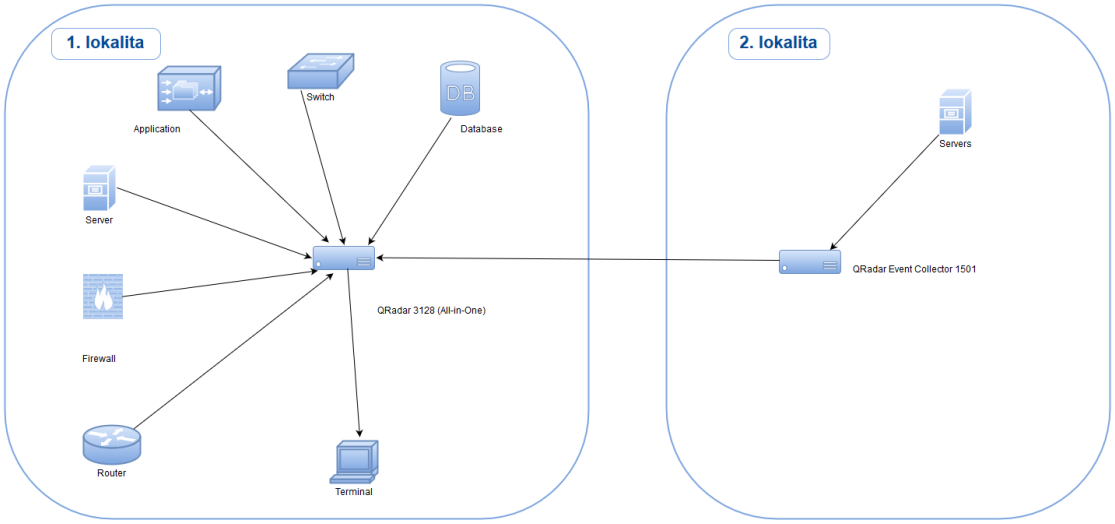
1.Lokalita *Logická komponenta*	*Konkrétní appliance*	2.Lokalita *Logická komponenta*	*Konkrétní appliance*
Console	QRadar 3128 (All-in-One)	Event Collector	QRadar Event Collector 1501
Flow Processor			
Flow Collector			
Event Processor			
Event Collector			
Capacity increase license	Up to 2,5k EPS		

Obrázek 18 - Konkrétní výběr appliance, střední firma, vlastní zpracování

Pro celkový sběr a procesování byla vybrána fyzická appliance **QRadar 3128 (All-in-One),** které v rámci své funkcionality vymezuje vše potřebné. Tato appliance je schopná v základní verzi výkonu 1000 EPS, 25 000 FPM a pro účely úložiště je připraveno 48 TB (z čehož je 40 TB využitelných). Co se týče výkonnostních aspektů na flow a skladovacích nároků na Storage, je zmíněné zařízení ideální a s rezervou splňuje tyto požadavky.
Nicméně při porovnání s kalkulací je vidět, že výkon pro kolekci a procesování událostí není dostatečný. Z toho důvodu bude nutné dokoupit licenci upgradující tuto appliance na úroveň, kdy je schopna výkonu 2500 EPS namísto dřívějších 1000 EPS. Tuto fyzickou appliance je možné škálovat až na úroveň, kdy je schopna zpracovat 15000 EPS a 300000 FPM. Takto výkonná licence však není pro infrastrukturu středního podniku potřeba.

Pro druhou lokaci, kde je potřeba sběr událostí ze serverů bude použit kolektor **QRadar Event Collector 1501**, který svým výkonem zaručí včasný sběr a dopravení událostí do All-in-one appliance v první lokaci, kde budou události zpracovány.

Hlavním problémem zde bylo rozdělení infrastruktury do dvou geograficky oddělených lokalit, přičemž organizace vyžaduje sběr událostí z obou těchto lokalit. Z toho důvodu vypadá struktura komponent a appliance následujícím způsobem.



Obrázek 19 - Logická struktura komponent, střední podnik, vlastní zpracování

Jak je možné vidět z přiloženého obrázku, veškeré procesování probíhá v první lokaci, kde je lokalizováno také souhrnné řešení QRadar 3128 (All-in-one). Toto zařízení mimo jiné přijímá nasbírané události z druhé lokace, odkud mu je zasílá kolektor událostí QRadar Event Collector 1501. All-in-one appliance se postará o veškeré procesy asociované se zpracováním dat a tyto data předá do terminálu (Console), kde s nimi může pracovat koncový uživatel. (*IBM Security QRadar SIEM*, 2016)

Po prvotní analýze, zjištění počtu zařízení, kalkulace dílčích výkonnostních atributů, návrhu struktury logických komponent a výběru konkrétní appliance splňující veškeré požadavky, zbývá už pouze finální kalkulace za SIEM řešení.

Licence	Price (EUR)
IBM Security QRadar Core Appliance XX28 G2 Appliance Install Appliance + Subscription and Support 12 Months	84534
IBM Security QRadar SIEM All-in-One 31XX Install License + SW Subscription & Support 12 Months	79226
IBM Security QRadar SIEM Event Capacity Increase from 1K to 2.5K EPS Install License + SW Subscription & Support 12 Months	62049
IBM Security QRadar Event Collector 1501 G2 Appliance Install Appliance + Subscription and Support 12 Months	16019
Total (EUR)	**241828**
Total (CZK) 30.3.2015	**6529356**

Obrázek 20- Finální kalkulace za SIEM řešení, střední podnik, vlastní zpracování

Ceny vycházejí z oficiálního ceníku vydaného firmou IBM, který je aktualizován několikrát do roka. Cena komponent nebo appliance se odvíjí od několika faktorů. Prvním je, zda se jedná o appliance fyzickou či virtuální, dále je důležité, jak je konkrétní model aktuální (v kalkulaci je užita nejnovější appliance pro Event collector nesoucí název G2). Je nutné zmínit, že pokud je při implementaci užito komponentů od IBM, je výsledná cena podstatně vyšší, než za kolik by se dalo řešení pořídit při použití alternativ. V reálném světě je možný nákup licencí QRadaru, které jsou pak aplikovatelné na kompatibilní komponenty jiných firem (např. HP). Z demonstrativních důvodů byly užity striktně komponenty dodávané společností IBM.

5.2 Malá organizace ze zdravotnického sektoru

Druhá z porovnávaných organizací se zabývá zajištěním služeb ve zdravotnickém sektoru, Tak jako mnoha jiným organizacím veřejné správy, bylo i této nařízeno zdokonalení internetové bezpečnosti, podle zákona o kybernetické bezpečnosti, vydaného v lednu 2015. Konkrétní podmínky jsou k nahlédnutí v přiložené kopii zákona. Tato organizace spadá do intervalu vymezeného pro malý podnik, respektive má počet zaměstnanců více jak 10, ale zároveň méně než 50.
Proces implementace bude totožný jako u středního podniku.

- **Analyzování prostředí**

V první fázi je nutné zjistit veškeré cifry asociované s pozdějším návrhem konkrétního řešení. Mezi známými čísly je počet zaměstnanců a počet zákazníků spolupracujících s organizací.
Organizace má veškerou IT infrastrukturu situovanou v jedné geografické lokaci, tudíž nebude třeba vymýšlet složité SIEM řešení.
Pro implementaci bude užito fyzické řešení, dle přání organizace.

V rámci analýzy je nutné definovat co nejpřesněji počet zařízení, která zasílají svoje události do QRadaru.

Zařízení generující log záznamy	**Počet**
Unix server	3
Windows server	12
Databáze	2
Síťové zařízení	3
Aplikace	4
Zařízení generující flow záznamy	
Flow sonda	1

Tabulka 4 - Seznam zařízení- malý podnik, vlastní zpracování

V tabulce jsou zobrazeny pouze ty zařízení, která jsou důležitá pro zapojení do SIEM řešení i pro samostatné zmínění v tabulce.

Pomocí této tabulky budou následně vypočteny hodnoty kritické pro návrh adekvátního SIEM řešení. Nejprve budou definovány konkrétní hodnoty pro EPS, následně pro FPM a nakonec pro kapacitní nároky úložiště.

Veškeré hodnoty získané v procesu kalkulace budou na závěr navýšeny o 20%, aby byla zajištěna dostatečná rezerva pro náhlé výkonnostní výkyvy.

	Device Type	Qty.	EPS Factor	EPS Rate
Event Sources	Windows Active Directory Servers	2	15	30
	Windows IIS and Exchange Servers		10	0
	Windows General Purpose Servers	10	2	20
	UNIX and Linux Servers	3	0,5	2
	DNS / DHCP Servers	2	15	30
	Antivirus Servers		20	0
	Database Servers	2	1	2
	Proxy Servers		25	0
	Large Firewalls	2	150	300
	Small Firewalls		20	0
	IDS, IPS and DAM		5	0
	VPN	1	5	5
	Routers and Switches	4	0,25	1
				0
				0
Additional Event Sources				0
				0
				0
				0
	Total Log Sources	26	Total EPS License	390

Obrázek 21- Kalkulace EPS- malý podnik, vlastní zpracování

Pro potřeby malého podniku, na základě kalkulace z počtu zjištěných zařízení zasílajících data do QRadaru, bylo zjištěno, že je potřeba výkon 390 EPS.

	Device Type	Qty.	Flow Factor	Flow Rate
Flow Sources	Total Workstations on Network	45	10	450
	Total Servers on Network	13	120	1 560
	FPM - Layer 4 Total			2 010
	QFlow FPM (based on bandwidth			0
	Total FPM License			2 010

Obrázek 22- Kalkulace FPM- malý podnik, vlastní zpracování

Jak je vidět výše, do sítě je zapojeno 45 pracovních stanic. Síťový provoz stanic vně a do firemní sítě bude analyzovat flow sonda umístěná na perimetru.
Druhá flow sonda bude umístěna takovým způsobem, aby byla schopna zachytit komunikaci stanic s Windows General Purpose servery a UNIX servery.
Celkové nároky na flow jsou rovny 2010 FPM.

Poté, co jsou známy požadavky na EPS a FPM, je dalším krokem pomocí těchto čísel zjistit, jaké jsou nároky na kapacitu úložiště při zachování těchto parametrů.
Ještě před samotnou kalkulací je nutné zmínit, že interval auditování je v tomto případě **3 měsíce**, nikoliv 6 měsíců jako to bylo u středního podniku.

Event Storage		
Average Event Size		Number of days uncompressed
1 000		14
Daily (bytes) Normalized	Daily (bytes) Raw	Events per Day
6 730 560 000	33 652 800 000	33 652 800
Weekly (bytes) Normalized	Weekly (bytes) Raw	Events per Hour
47 113 920 000	235 569 600 000	1 402 200
Monthly (bytes) Normalized	Monthly (bytes)	Events per Min.
201 916 800 000	1 009 584 000 000	23 370
Monthly (TB) Normalized	Monthly (TB) Raw	Events per Sec.
0	0,92	390
Auditing requirements	2,755	

Obrázek 23- Kalkulace úložiště, EPS- malý podnik, vlastní zpracování

Průměrná velikost události je 1000 byte, což je defaultní hodnota pro většinu událostí chodících do QRadaru. Interval, po kterém jsou přijatá data kompresována, je roven 14 dnům. I v tomto případě se pro potřeby výpočtu užívá hodnot surových dat, nikoliv normalizovaných. Celkové nároky na skladování událostí jsou 0,92 TB/ měsíc, respektive 2,8 TB na celý interval auditování.

Flow Storage		
Average Flow Size	QFlow Capture Size	Number of days uncompressed
200	100	14
Daily (bytes) Normalized	Daily (bytes) Raw	Flows per Day
115 776 000	578 880 000	2 894 400
Weekly (bytes) Normalized	Weekly (bytes) Raw	Flows per Hour
810 432 000	4 052 160 000	120 600
Monthly (bytes)	Monthly (bytes)	
3 473 280 000	17 366 400 000	
Monthly (TB) Normalized	Monthly (TB) Raw	Flows per Min.
0,00	0,02	2 010
Auditing requirements	0,047	

Obrázek 24- Kalkulace úložiště, FPM- malý podnik, vlastní zpracování

Pro kalkulaci kapacitních nároků pro flow je, kromě samotného čísla FPM, nutné vědět také další stěžejní atributy. Průměrná velikost segmentu datového toku je 200 bytů, což je defaultní a nejčastější velikost příchozích segmentů. Pod pojmem QFlow Capture Size je rozuměna velikost zprávy, která bude zaslána během reportu. Tato velikost je pro jeden flow záznam a je nastavena na 100 bajtů. Poslední důležitá hodnota je počet dní, po kterém budou data stlačena, aby bylo uvolněno místo pro nově příchozí segmenty. Tak jako v případě EPS, i zde je hodnota nastavena na 14 dní.
Měsíční nároky na kapacitu úložiště pro flow je 0,016 TB. Pro interval 3 měsíců je hodnota rovna 0,47

Po provedení kalkulací nároků na úložiště jsou již všechny potřebné hodnoty známy. Je však ještě nutné tyto hodnoty zvětšit o 20%, jako prevenci proti problémům během náhlého výkyvu. Finální čísla vypadají následujícím způsobem.

EPS requirements total	468
FPM requirements total	2412
Auditing requirements total	3,36

Obrázek 25- Kalkulace total requirements, vlastní zpracování

Vzniklé řešení bude schopné výkonu alespoň 468 EPS, 2412 FPM a bude mít kapacitu úložiště 3,4 TB. Ze zjištěných hodnot bude čerpáno během druhé části implementace, respektive při návrhu distribuovaného řešení.

- **Návrh řešení QRadaru + licence**

Před samotným vytvořením konkrétního návrhu řešení pomocí appliance a licencování musí být nejprve vyřešeno, jak bude vypadat logická struktura. Pro sestavení logické struktury je potřeba znát seznam logických komponent, bez kterých řešení nebude fungovat. Prvním krokem v procesu návrhu bude tedy zjištění seznamu potřebných logických komponent.

- Console
- Event processor
- Event collector
- Flow collector
- Flow processor

Na základě všeobecného seznamu komponent vzniká schopnost definovat konkrétní appliance pro fyzické distribuované řešení.
Zmíněné řešení bude rozebráno níže.

Logická komponenta	*Konkrétní appliance*
Console	QRadar 3105 (All-in-One)
Flow Processor	
Flow Collector	
Event Processor	
Event Collector	

Obrázek 26- Konkrétní výběr appliance- malý podnik, vlastní zpracování

Pro kolekci a procesování událostí i datových segmentů byla vybrána fyzická appliance **QRadar 3105 (All-in-One)**, ta je v rámci své funkcionality schopna pokrýt veškeré výkonnostní i kapacitní nároky podnikem kladené.
Zmíněná appliance je schopná v základní verzi výkonu 1000 EPS, 25 000 FPM a pro účely úložiště je připraveno 9 TB místa, z čehož je využitelných 6,2 TB.
Tyto výkonnostní a kapacitní aspekty dalece překračují požadavky na řešení pro tuto organizaci, nicméně je nutné si uvědomit, že při zachování užití appliance a komponent pouze od společnosti IBM, se jedná o nejlepší možnou volbu v poměru cena/výkon. (*IBM Security QRadar SIEM*, 2016)

Po definování konkrétní appliance už zbývá pouze finální vyčíslení za All-in-One appliance.

Licence	Price (EUR)
IBM Security QRadar Core Appliance XX05 G2 Appliance Install Appliance + Subscription and Support 12 Months	31748
IBM Security QRadar SIEM All-in-One 31XX Install License + SW Subscription & Support 12 Months	79226
Total (EUR)	**110974**
Total (CZK) 30.3.2015	**2996298**

Obrázek 27- Kalkulace za řešení- malý podnik, vlastní zpracování

Ceny vycházejí z oficiálního ceníku vydaného firmou IBM, který je aktualizován několikrát do roka. Cena komponent nebo appliance se odvíjí od několika faktorů. Prvním je, zda se jedná o appliance fyzickou či virtuální, dále je důležité, jak je konkrétní model aktuální (v kalkulaci je užita nejnovější appliance pro Event collector nesoucí název G2). Je nutné zmínit, že pokud je při implementaci užito komponentů od IBM, je výsledná cena podstatně vyšší, než za kolik by se dalo řešení pořídit při použití alternativ. V reálném světě je možný nákup licencí QRadaru, které jsou pak aplikovatelné na kompatibilní komponenty jiných firem (např. HP). Z demonstrativních důvodů byly užity striktně komponenty dodávané společností IBM.

6 Shrnutí výsledků

- **Porovnání řešení QRadaru pro oba podniky**

Při shrnutí a porovnávání obou řešení je nutné vzít v potaz několik komparativních atributů, které nemalým způsobem ovlivňují výsledná čísla a rozdíly napříč oběma podniky.

- Počet zaměstnanců
- Geologické rozdělení IT infrastruktury
- Fiskální aspekty a omezení podniku
- Počet zařízení přistupujících do systému
- Auditivní požadavky

Všechny zmíněné aspekty výrazně přispívají k tomu, proč je nutné v každém z demonstrovaných organizací užití diametrálně odlišného řešení.
Z těchto atributů jsou logicky odvozeny další aspekty, jejichž hodnota je přímo úměrná velikosti komparativních atributů.

Níže je znázorněna tabulka obsahující komparativní atributy a další aspekty, které byly natolik důležité, aby zde byly zobrazeny.

Komparativní atributy	Malý podnik	Střední podnik
Počet zaměstnanců	48	235
Geologické rozdělení IT infrastruktury	1 lokace	2 lokace
Počet zařízení přistupujících do systému	43	220
Auditivní požadavky	3 měsíce	6 měsíců
Počet EPS	468 EPS	1110 EPS
Počet FPM	2412 FPM	23664 FPM
Kapacitní nároky	3,36 TB	16,81 TB
Druh SIEM řešení	QRadar 3105 (All-in-One)	QRadar 3128 (All-in-One), QRadar Event Collector 1501, Event Capacity Increase from 1K to 2.5K EPS Install License
Cena za pořízení řešení (CZK)	**2 997 000**	**6 530 000**

Obrázek 28- Komparace podniků, vlastní zpracování

Jak je možné vidět z přiložené tabulky, počty zaměstnanců a těch, jež přistupují do systému, je skoro 5x více u střední firmy.

Rovněž je rozdíl, zda je infrastruktura rozdělena mezi více geografických lokací. Tato skutečnost požaduje další appliance v místě, kde je zbytek infrastruktury umístěn.

Počet zasílaných událostí do SIEM je pouze dvakrát větší, naproti tomu počet flow segmentů je větší takřka desetkrát. Tento fakt poukazuje na to, že počet zasílaných událostí lze rapidně navýšit, i když počet cílových zařízení není zdaleka takový, jako u středního podniku. To, co markantně ovlivňuje celkové nároky na EPS, je konkrétní druh zařízení. V případě malého podniku jsou čísla takto navýšena díky dvěma velkým firewallům, které zasílají velké množství událostí, a jejich počet je násoben indexem 150 EPS.

Velikost nároků na FPM se odvíjí především od počtu pracovních stanic, které jsou připojeny do sítě, a také od počtu serverů, které si organizace přeje sledovat pomocí flow sond.

Kapacitní nároky na úložiště jsou pětkrát větší u středního podniku, což je pouze logické, vezmou-li se v úvahu počty událostí a flow, které jsou ukládány. Tento rozdíl je také způsoben faktem, že interval pro audit, respektive pro uchování dat, je u středního podniku 6 měsíců. Interval u středního podniku je dvakrát delší než pro malý podnik.

Z čistě komparativních účelů je možné předpokládat, že by byl interval pro obě organizace shodný. V tomto případě by se rozdíl mezi nároky na obě úložiště zmenšil. Kapacitní nároky u malé organizace by dvakrát vzrostly, tj. na hodnotu 6,72 TB. Po změně intervalu délky auditování by výsledná čísla byla pouze 2,5 krát větší ve prospěch středního podniku.

Všechny výše zmíněné faktory způsobily, že výsledná cena řešení pro střední podnik je více jak dvakrát větší, než v případě malého podniku.

7 Závěr

Hlavním cílem bakalářské práce bylo provedení analýzy možností a přístupů SIEM, při zahrnutí co největšího možného počtu faktorů. Faktory lze definovat jako potřeby z hlediska technických a legislativních požadavků, případně logických vazeb napříč řešením. Aby bylo možné dosáhnout stanovených cílů, bylo nutností nastudování patřičné odborné literatury. Dalším cílovým požadavkem bylo demonstrování návrhu a implementace, kdy prvotním krokem v tomto procesů musí zákonitě být porozumění veškerým možným omezením. Tyto omezení by později mohly omezovat potřebné kroky v rámci implementace nebo bránit jejich provedení v rozsahu, v jakém byly zamýšleny. Dalším logickým krokem bylo studium doporučených postupů a návodů, které jsou v kontextu kybernetické bezpečnosti a SIEM řešení, definovány v rámci ISO Standardů 27k. Po porozumění problematice bezpečnosti následovalo studium legislativních omezení v tomto tématu. Pro tento účel byl jako zdroj zvolen Zákon o kybernetické bezpečnosti, který je svým obsahem nejblíže řešené problematice. Následovalo definování samotných principů SIEM a konkrétní aplikace IBM Security QRadar SIEM v rovině teoretické i praktické.

Analýza standardů a legislativních omezení ukázala, jak veliká je nutnost vlastnictví tohoto bezpečnostního řešení pro takřka každou firmu, jež operuje alespoň malou částí svého portfolia v kybernetickém světě. Je pravda, že díky Zákonu o kybernetické bezpečnosti jsou některé organizace seznámeny s možným rizikem, jaké jim při absenci bezpečnostního řešení hrozí. Tento zákon vytváří povinnost pouze pro firmy spadající do sektoru veřejné správy. Cílem této práce bylo mimo jiné také ukázat, jak je důležité vlastnictví takového řešení i pro všechny ostatní organizace, ať už se jedná o nadnárodní korporace nebo o malé podniky.

V obecné rovině lze říci, že demonstrovaný postup návrhu a implementace řešení je aplikovatelný na jakkoliv velkou organizaci. Za předpokladu, že budou respektovány dílčí faktory, které diferenciují různě veliké organizace, a bude použit postup definovaný

např. ve standardu ISO 27001, který popisuje postup pro zavedení efektivního systému řízení bezpečnosti informací.
Nutností je zmínění skutečnosti, že při implementaci takto komplexního řešení by měla implementace bez odborného vedení a asistence vždy být tou poslední a nejkrajnější možností. Pokud je řešení implementováno někým, kdo vlastní pouze povrchní a nekomplexní znalosti z tohoto odvětví, je vznik problému nebo neřešitelného bezpečnostního rizika ve většině případů pouhou otázkou času. Pokrytí celého portfolia hrozeb je procesem, který stále probíhá, je nutné mu věnovat notnou dávku času a přizpůsobovat ho vždy tak, aby byl aktuální pro odvedení bezchybné práce. Zastaralé bezpečnostní řešení je to samé, co žádné bezpečnostní řešení, pokud narazí na bezpečnostní hrozbu, která je za hranicí jeho kognitivních funkcí.

Při psaní této práce u mé osoby došlo k notnému prohloubení znalostí v kontextu bezpečnosti informací a zejména pak v kontextu SIEM systému. Získal jsem hlubší znalosti o celkové struktuře SIEM řešení i o tom, jakým způsobem funguje kooperace komponentů v tomto řešení. Praktické schopnosti a zkušenosti jsem získal díky tvorbě návrhu a implementování konkrétních řešení pro dvě zcela odlišné organizace. SIEM systémy, dle mého názoru, představují budoucnost bezpečnosti informací na internetu. Z toho důvodu jsem již několikrát v průběhu práce vyslovil předpoklad, že dříve nebo později, bude třeba, aby každá organizace s potřebou přehledu o své IT infrastruktuře, bude muset vlastnit adekvátní bezpečnostní řešení. Toto řešení bude sloužit jako prevence proti hrozbám a zároveň jako hlavní determinant úspěchu celé organizace.
Tento úsudek pramení z přesvědčení, že nyní jsou nejcennějším vlastnictvím informace. Pokud organizace o tyto cenné informace přijde například při kybernetickém útoku, může se rozloučit s konkurenceschopností na trhu a tudíž i s potencionálními zisky.

V budoucnu bych v tomto tématu velmi rád pokračoval, neboť mne velmi zajímá a kontext bezpečnosti informací je stále aktuálnější téma. Další zajímavé téma by bylo přenesení této technologie na korporace, které vlastní databáze čítající tisíce terabytů dat. Implementace pro tyto korporátní obry, které by bez těchto databázi přišly o svou tržní sílu, by bylo taktéž velmi zajímavé sledovat. Řešení SIEM v kontextu s Big Daty je bezpochyby dalším potenciálním podnětem k prošetření.

8 Seznam použité literatury

1) BRANDELOVÁ, Mary, 2011. *SIEM: Analýza protokolů (logů)*. COMPUTERWORLD [online]. roč. 2010, č. 2 [cit. 2016-02-05]. Dostupné z: http://computerworld.cz/securityworld/siem-analyza-protokolu-logu-47994

2) BURNHAM, John. *IBM Once Again Leads Gartner's Magic Quadrant for SIEM* [online]. 2015 [cit. 2016-02-18]. Dostupné z: https://securityintelligence.com/ibm-is-a-leader-again-in-2015-gartner-magic-quadrant-for-siem

3) GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ, 2009 *Podniková informatika*. 2., přeprac. a aktualiz. vyd. Praha: Grada. Expert (Grada). ISBN 978-80-247-2615-1.

4) HP CORPORATION, 2016. *HP components: HP ProLiant Gen8* [online].[cit. 2016-02-26]. Dostupné z: http://www8.hp.com/h20195/v2/GetPDF.aspx/c04128166.pdf

5) IBM CORPORATION, 2015. *EPS and FPM Limits* [online]. [cit. 2016-02-29]. Dostupné z: http://www-01.ibm.com/support/docview.wss?uid=swg21963963

6) IBM CORPORATION, 2015. *IBM QRadar: Security Intelligence Platform v7. 2. 6*. [online]. [cit. 2016-02-21]. Dostupné z: http://www-01.ibm.com/support/knowledgecenter/SS42VS_7.2.6/com.ibm.qradar.doc/qradar_IC_welcome.html?lang=cs

7) IBM CORPORATION, 2015. *IBM Security QRadar Components*, [online]. [cit. 2016-02-26]. Dostupné z: https://www-01.ibm.com/support/knowledgecenter/SS42VS_7.2.6/com.ibm.qradar.doc/shc_qradar_comps.html

8) IBM CORPORATION, 2015. *IBM Security QRadar SIEM: Virtual appliance overview* [online]. 2016 [cit. 2016-02-26]. Dostupné z: https://www-304.ibm.com/support/knowledgecenter/SS42VS_7.2.1/com.ibm.qradar.doc_7.2.1/c_siem_vrt_ap_ov.html

9) IBM CORPORATION, 2015. *Kooperace v rámci logické architektury IBM QRadar SIEM : IBM Security QRadar Version 7.2*

10) ISO 27000 DIRECTORY, 2009. *ISO/IEC 27004:2009* [online]. [cit. 2015-10-24]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/27004

11) ISO 27000 DIRECTORY, 2009. *ISO/IEC 27006:2007* [online]. 2009. [cit. 2015-10-24]. Dostupné z: http://csnonlinefirmy.unmz.cz/html_nahledy/36/80527/80527_nahled.htm

12) ISO 27000 DIRECTORY, 2011. *ISO 27005:2011: Risk management* [online]. [cit. 2015-10-25]. Dostupné z: http://www.iso27001security.com/html/27005.html) & (ISO 27005:2011: Risk management [online]. 2011. [cit. 2015-10-25]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/27005)

13) ISO 27000 DIRECTORY, 2011. *ISO 27007:2011: Guidelines for Information security management systems auditing* [online]. [cit. 2015-10-25]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/27007)

14) ISO 27000 DIRECTORY, 2011. *ISO 27007:2011: Guidelines for Information security management systems auditing* [online]. [cit. 2015-10-25]. Dostupné z: http://www.iso27001security.com/html/27007.html

15) ISO 27000 DIRECTORY, 2011. *ISO/IEC 27034: Relevantní dodatky* [online]. [cit. 2015-11-05]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/27034

16) ISO 27000 DIRECTORY, 2013. *ISO/IEC 27002: Code of practise. ISO 27k standards* [online]. [cit. 2015-10-04]. Dostupné z: http://www.iso27001security.com/html/27002.html#Section11

17) ISO 27000 DIRECTORY, 2013. *ISO/IEC 27044: SIEM* [online]. [cit. 2015-11-08]. Dostupné z: http://www.iso27001security.com/html/27044.html)

18) ISO 27000 DIRECTORY, 2014. *ISO/IEC 27004:2014: Measurement* [online]. [cit. 2015-10-24]. Dostupné z: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en

19) ISO 27000 DIRECTORY, 2014. *ISO/IEC 27033: ISO 27033-1- ISO 27033-6* [online]. [cit. 2015-10-28]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/27033

20) ISO 27000 DIRECTORY, 2015. *ISO/IEC 27002: Information security, CIA.* Wikipedia [online]. [cit. 2015-10-04]. Dostupné z: https://en.wikipedia.org/wiki/ISO/IEC_27002

21) ISO 27000 DIRECTORY, 2015. *ISO/IEC 27006:2015* [online]. [cit. 2015-10-24]. Dostupné z: https://www.iso.org/obp/ui/#iso:std:iso-iec:27006:ed-3:v1:en

22) ISO 27000 DIRECTORY, 2015. *ISO/IEC 27033: ISO 27033-1- ISO 27033-6* [online]. [cit. 2015-10-28]. Dostupné z: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_ics_browse.htm?ICS1=35&ICS2=040&

23) ISO 27000 DIRECTORY, 2015. *ISO/IEC 27033: ISO 27033-1- ISO 27033-6* [online]. [cit. 2015-10-28]. Dostupné z: http://www.iso27001security.com/html/27033.html)

24) ISO 27000 DIRECTORY, 2015. ISO/IEC 27034: *ISO/IEC 27034-1:2011* [online]. [cit. 2015-11-05]. Dostupné z:

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44378

25) ISO 27000 DIRECTORY, 2015.*ISO/IEC 27044: SIEM* [online [cit. 2015-11-08]. Dostupné z: http://www.itgovernanceonline.com/information-security/iso-27000-series/about-iso-27044/

26) ISO 27000 DIRECTORY, 2016. *IEC: About the IEC* [online]. [cit. 2016-02-04]. Dostupné z: http://www.iec.ch/about/?ref=menu

27) ISO 27000 DIRECTORY, 2016. *ISO: About ISO* [online]. [cit. 2016-02-04]. Dostupné z: http://www.iso.org/iso/home/about.htm

28) ISO 27000 DIRECTORY, 2016. *ISO: ISO Standard* [online]. [cit. 2016-02-04]. Dostupné z: http://www.iso.org/iso/home/standards.htm

29) JIRÁSKO, Tomáš, 2015. *Normy v IT - ČSN ISO/IEC 27000.* [online]. [cit. 2015-08-23]. Dostupné z: http://www.itbiz.cz/clanky/normy-v-it-csn-iso-iec-27000

30) KRČMÁŘ, Petr, 2013. *Zákon o kybernetické bezpečnosti: Obsah* [online]. [cit. 2015-11-14]. Dostupné z: http://www.root.cz/clanky/zakon-o-kyberneticke-bezpecnosti-co-v-nem-stoji/

31) LENOVO CORPORATION, 2015. *Lenovo Product Overview*, [online]. [cit. 2016-02-25]. Dostupné z: https://lenovopress.com/tips0851-system-x3550-m4-e5-2600-v2?cm_mc_uid=82656404685614558039634&cm_mc_sid_50200000=1456298394#processor-options

32) MALIŠ, Petr, 2015. *Zákon o kybernetické bezpečnosti: Právní aspekty* [online]. [cit. 2015-11-14]. Dostupné z*: http://www.systemonline.cz/it-security/pravni-aspekty-prijeti-zakona-o-kyberneticke-bezpecnosti.htm*

33) MILLER, David. 2011. *Security information and event management* (SIEM) implementation. New York: McGraw-Hill, ISBN 0071701095.

34) Průša, J., Ošťádal, B., Topolánek, M., 2006. *Analýzy č. 3 – úloha malých a středních podniků v evropských ekonomikách*, Praha: CEVRO – Liberálně-konzervativní akademie. ISSN 1801-3767)

35) RED HAT ENTERPRISE, 2016. *Linux Product Overview* [online]. [cit. 2016-02-26]. Dostupné z: http://www.redhat.com/en/files/resources/en-rhel-7-server-datasheet-12182617.pdf

36) RIVERA, Janessa. 2015. *Computer Fraud & Security: Building better data protection with SIEM*. ISSN 1361-3723. [cit. 2016-02-04]. Dostupné z: http://www.sciencedirect.com/science/journal/13613723/2016/1

37) ŠUTÁK, Martin, 2014. *Seriál o řízení bezpečnosti: ISMS.* [online]. [cit. 2015-08-28]. Dostupné z: http://www.chrantesidata.cz/cs/art/472-isms-serial-o-rizeni-bezpecnosti/#5dil

38) VAN DER MEULEN, Rob, 2015. *Gartner forecast: Proactive security*. *Gartner.com* [online]. Stamford, [cit. 2016-02-04]. Dostupné z: www.gartner.com/newsroom/id/2990717

39) VÍZNER, Lukáš, 2014. *Security information and event management v rámci cloudové infrastruktury* [online]. Hradec Králové, [cit. 2016-03-15]. Univerzita Hradec Králové. Vedoucí práce Mgr. Josef Horálek, Ph.D.

40) WHITMAN, Michael E a Herbert J MATTORD, 2012. *Principles of information security*. 4th ed. Boston, MA: Course Technology. ISBN 1111138214.

41) WOLTERS KLUVER ČR, 2014. *Zákon č.181/2014 ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů.* In: ASPI [právní informační systém]. Praha: Wolters Kluwer ČR [vid. 2015-11-12].)

9 Přílohy

1) Zákon o kybernetické bezpečnosti

Oskenované zadání práce