VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH MONITOROVÁNÍ SÍTĚ SPOLEČNOSTI
CORPORATE NETWORK MONITORING CONCEPT

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Jiří Hopp**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Viktor Ondrák, Ph.D.**
SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Student:	**Jiří Hopp**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2020/21

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává bakalářskou práci s názvem:

Návrh monitorování sítě společnosti

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Navrhnout management bezpečnosti.

Základní literární prameny:

DOSTÁLEK, L. Velký průvodce protokoly TCP/IP: bezpečnost. 2. aktualiz. vyd. Praha: Computer Press, 2003. 572 stran. ISBN 80-7226-849-X.

ENDORF, C., E. SCHULTZ a J. MELLANDER. Detekce a prevence počítačového útoku. Praha: Grada Publishing, 2005. 335 stran. ISBN 80-247-1035-8.

NORTHCUTT, S. Bezpečnost sítí: velká kniha. Brno: CP Books, 2005. 589 stran. ISBN 80-251-06-7-7.

THOMAS, M. T. Zabezpečení počítačových sítí bez předchozích znalostí. Brno: CP Books, 2005. 338 stran. ISBN 80-251-0417-6.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Sbírka zákonů České republiky, 2014.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2020/21

V Brně dne 28.2.2021

L. S.

Mgr. Veronika Novotná, Ph.D. ředitel	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Bakalářská práce se zabývá analýzou stavu monitorování kybernetických bezpečnostních událostí v instituci a analýzou bezpečnostních politik instituce. Na základě analýzy pak návrhy změn nastavení monitorovacích systémů, úprav bezpečnostních politik a návrhy dalších opatření, vedoucích ke zvýšení stavu bezpečnosti informací a bezpečnosti provozu informačních systémů v instituci.

Klíčová slova

Bezpečnost, informační bezpečnost, bezpečnostní politika, management bezpečnosti, kybernetická bezpečnostní událost, monitoring událostí, zálohování dat, nástroje monitorování

Abstract

The bachelor's thesis analyzes the state of cybersecurity events monitoring in the institution and the security policies of the institution. Based on the analysis suggests updates of the settings of cybersecurity monitoring systems, changes of the security policies, and other steps to increase the state of information security and information systems security in the institution.

Key words

Security, information security, security policy, security management, cybersecurity event, event monitoring, data backup, monitoring tools

Bibliografická citace

HOPP, Jiří. *Návrh monitorování sítě společnosti* [online]. Brno, 2021 [cit. 2021-05-15]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/132177. Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Viktor Ondrák.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 16. května 2021

…….

podpis studenta

Poděkování

Poděkování bych rád věnoval zejména Ing. Viktoru Ondrákovi Ph.D. za vedení mé bakalářské práce, užitečné rady, vstřícný přístup a odbornou pomoc při řešení mé bakalářské práce. Dále bych rád poděkoval svému nadžízenému a ostatním kolegům z instituce za praktické rady a zkušenosti, kterých jsem při práci s nimi nabyl. V poslední řadě bych chtěl poděkovat mým kamarádům, kamarádkám a rodině za motivaci při psaní mé práce.

OBSAH

ÚVOD

S různými novými technologiemi, které ve světě každoročně přibývají, přibývají také možné zranitelnosti a příležitosti pro útočníky. Počty počítačových útoků s každým rokem rostou. Není možné, aby byla síť stoprocentně bezpečná a předešlo se všem hrozbám, ale je možné dělat všechno proto, abychom tomuto riziku předcházeli.

Pro minimalizaci hrozícího nebezpečí je nutné zajistit monitoring sítě a vyhodnocování událostí. To s sebou přináší mnohá úskalí, jako jsou například falešně pozitivní a falešně negativní detekce. Je proto potřeba nejen samotného monitoringu, ale i správného vyladění detekčních systémů, aby byly systémy schopny včas zachytit hrozící nebezpečí a pomohly nám předcházet bezpečnostním incidentům.

Vzhledem ke dříve zmiňovanému rostoucímu počtu počítačových útoků, nových technologií a nových zranitelností již k zajištění bezpečnosti na síti nestačí běžná logická pravidla pro omezení provozu a je potřeba k obraně využívat moderních technologií, jako je umělá inteligence nebo strojové učení.

Pro instituci, která manipuluje s citlivými daty občanů, firem a daty jiných institucí je zajištění bezpečnosti informací a bezpečnosti provozu všech používaných informačních systémů stěžejní záležitostí.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Cílem práce je navrhnout management bezpečnosti organizace. Zejména pak monitoring událostí na síti a vyhodnocování, zda se jedná o bezpečnostní hrozby, nebo falešně pozitivní zprávy.

Dílčími cílemi práce jsou:

- vytvoření teoretického základu,
- analýza současného stavu bezpečnosti organizace a jejího nynějšího monitorování sítě,
- návrh opatření, vedoucích ke zvýšení stavu bezpečnosti informací a bezpečnosti provozu všech informačních systémů. Návrhy změn nastavení monitorovacích systémů pro detekci kybernetických bezpečnostních událostí.

Teoretická část bude zpracována na základě informací získaných z odborné literatury, případně budou využity informace dostupné na internetu. Informace v analytické části budou vycházet z konzultací se zaměstnanci, interních dokumentů instituce a z vlastních poznatků nabytých při výkonu zaměstnání. V praktické části budou zpracovány konkrétní návrhy opatření, vedoucích ke zvýšení bezpečnosti. A zejména návrhy změn systémů monitoringu.

1 TEORETICKÁ VÝCHODISKA PRÁCE

V této kapitole mé bakalářské práce se budu věnovat převážně základním pojmům z oblastí bezpečnosti počítačových sítí, jejich správy a bezpečnostními politikami, zpracovanými podle požadavků vyhlášky o kybernetické bezpečnosti. Tato kapitola je základem pro pochopení dále zpracovávaných témat.

1.1 Management sítě

Počítačová síť je spojením nebo sadou spojení mezi alespoň dvěma počítači, za účelem výměny dat mezi nimi. Sítě se pak skládají z komponent, kterými jsou jednotlivé propojené systémy, propojovací software, síťový hardware (např. přepínače), fyzická přenosová média a adresní systém, pro všechny výše uvedené komponenty [2, s. 27].

Při návrhu správně fungující sítě, je potřeba kombinace kompetentních lidí, chytře vymyšleného designu, správného hardware znalostí a zkušeností [5, s. 1].

Vedení podniků od sítí v dnešní době čekají stálou dostupnost a správnou funkčnost. Vznikají tak větší nároky na administrátory sítí, od kterých se očekává, že toto zajistí [5, s. 1].

S rostoucí velikostí sítě rostou i náklady na práci, související se správou systému. Tyto náklady rychle překročí náklady na automatizovaný software pro správu sítě. Proto má u každé větší sítě smysl o takovém softwaru přemýšlet, jelikož náklady na něj se brzy vrátí [2, s. 734].

1.1.1 Klasifikace FCAPS

Model FCAPS byl vytvořen skupinou International Telecommunication Union (ITU-T). Skupina ITU-T původně vytvořila Telecommunications Management Framework (TMN), ten později pro potřeby správy počítačových sítí rozšířen a vznikl model FCAPS [5, s. 2].

Jednotlivá písmena obsažená ve zkratce FCAPS znamenají Fault (chyba), Configuration (konfigurace), Accounting a Administration (účtování a správa), Performance (výkon) a Security (zabezpečení). [2, s. 734].

Původně organizace ISO zamýšlela vytvoření samostatných protokolů pro každou z pěti oblastí FCAPS, později se ukázalo, že by všechny oblasti mohly být podporovány jednotným protokolem [2, s. 735].

1.1.2 Modely správy

- **Správa chyb** - *„chybou je myšlena hardwarová nebo softwarová chyba, která vede k nežádoucímu výsledku"* [2, s. 736].

  Správa chyb se snaží zajistit čas chyby, příčinu chyby a poskytnout správci potřebné informace k odstranění příčiny chyby. Většina operačních systémů a aplikací nemá problém s vytvářením chybových hlášek, které mohou systémy pro správu chyb detekovat a zobrazovat. Problém může nastat při zjišťování příčiny chyby [2, s. 736].

  Systémy pro správu chyb detekují události, spojené s chybovými stavy, případně určují chyby na základě určitých množin událostí. Důležité události jsou zaznamenány do protokolu událostí, případně odeslány po síti (například protokolem SMTP) [2, s. 736].

  V každém systému je při vzniku chyby běžné, že nevznikne pouze jedna chybová událost, ale vzniknou i další události s chybou související. Balíčky pro správu chyb bývají napsány tak, aby dokázaly spolu související události seskupovat, toto je označováno jako korelace událostí a prvek toto zajišťující jako korelátor událostí. Systémy umí agregovat duplicitní chybové události, případně filtrovat a vyřazovat nerelevantní události, maskovat události, které jsou pouze následkem původní příčiny chyby a analyzovat hlavní (kořenové) příčiny [2, s. 738].

- **Správa konfigurace** - Správa konfigurace se snaží zajistit automatizované provádění opakujících se úloh, snížit složitost požadováním standardů a aktivně sledovat stav systémů. Týká se například správy nastavení počítačů a síťových zařízení, instalace a konfigurace systému (SCM), správa uživatelských účtů a skupin nebo aktualizace a opravy softwaru a systémů [2, s. 740].

  Stanovení standartů pro hardware a software používaných v síti je jednou z možností, jak dosáhnout menší složitosti a usnadnit správu konfigurace. Ke snížení úsilí na konfiguraci jednotlivých systémů je možné vytvořit referenční platformu v podobě otestovaného systému, který je možno posléze duplikovat nebo klonovat [2, s.740].

  Pro sledování stavu systémů využívá většina řešení konzoly, nebo řídící panely pro správu, s jejichž pomocí je možno spravovat systémy vzdáleně. Například Windows Server 2008 využívá konzoly Server Manager, která do hierarchické stromové struktury slučuje zobrazení z více různých nástrojů, jako je třeba Active Directory. Je tak možné spravovat místní i vzdálené systémy z jednoho prostředí, což šetří čas i námahu [2, s. 740-741].

Pro účely automatizace provádění opakujících se úloh (jako je například nasazení softwaru na systémy a pracovní stanice), balíky pro správu musí přidat nově pořízený software do svého itineráře a být schopny systém monitorovat. Balík se stará o instalaci agenta a zapisuje si potřebné vlastnosti, jakými jsou například názvy systémů uložené v adresářové službě nebo názvy instalovaných produktů a čísla jejich verzí. [2, s. 741-742].

Software pro správu konfigurace jsou schopny uchovávat stavy systému ve formě softwarových instalačních balíčků, nebo ve formě kontejnerů (bitových kopií) celých systémů. Nasazení pak probíhá obvykle spuštěním skriptu, který se odkazuje na bitovou kopii síťové složky a je schopen automaticky provést instalaci [2, s. 742-743].

- **Účtování a správa** - *„Funkce účtování, kterou nabízí nástroje pro správu sítě, se týká měření využití dat pro účely fakturace zákazníkům, nebo oddělením. Toto měření zajišťuje řádnou distribuci služeb nebo ověřuje, zda firma dodržela smlouvy o úrovni poskytovaných síťových služeb."* [2, s. 747].

  Funkce účtování jsou součástí různých protokolů, souhrnně označovaných jako AAA (autorizace, autentizace a accounting - účtování). Zástupci AAA protokolů jsou například RADIUS, TACACS a Diameters. O architektuře AAA a protokolu RADIUS bude více v kapitole Řízení přístupů [2, s. 748].

  Jelikož mnohé sítě nevyžadují funkci účtování, používá se při vyložení zkratky FCAPS namísto účtování (Accounting) správa (Administration), mezi její funkce by pak patřila například správa uživatelů a skupin, přístupy k prostředkům a důležitým síťovým nastavením. Funkce správy se do určité míry překrývá s dalšími části klasifikace FCAPS, např. se zabezpečením nebo konfigurací [2, s. 748].

- **Správa výkonu** - Měření výkonu sítě za standardních podmínek tvoří základ, s nímž lze posléze porovnávat budoucí změny. Monitory výkonu dokáží na síti měřit mnohé proměnné, mezi nejdůležitější patří například míra kolizí, míra chyb rámců a další míry týkající se provozu sítě. Monitory výkonu využívají systémových čítačů, kromě zachytávání a zaznamenávání událostí jsou tak schopny u některých událostí měřit například i frekvenci, trvání, hodnoty, nebo jiné parametry, které daný subsystém potřebuje měřit. V případě disků mohou čítače sledovat například přístupy k disku, objem přenesených dat nebo délku fronty. Díky těmto hodnotám jsme schopni optimalizovat výkon [2, s. 748-749].

- **Správa zabezpečení** - V nástrojích pro správu sítě nabízí správa zabezpečení prostředky, které uživatelům a skupinám povolují, nebo zamítají přístup k síťovým prostředkům (autentizace a autorizace byly už částečně popsány pod správou účtování v odstavci o RADIUS serveru). Zabezpečení sítě spoléhá na autentizaci uživatelů a systému a na ochranu dat například pomocí šifrování. Další kategorií služeb, které může software pro správu zabezpečení nabízet, je hodnocení a analýza rizik [2, s. 752].

1.2 Základní pojmy z oblasti bezpečnosti

1.2.1 Aktivum

Aktivum můžeme chápat jako libovolnou komponentu IS/ICT, která má pro organizaci hodnotu. Aktiva můžeme dělit na hmotná a nehmotná, přičemž hmotnými aktivy jsou například počítače, aktivní prvky síťové infrastruktury, kabelové rozvody, tiskárny a další zařízení. Nehmotnými aktivy může být firemní knowhow (pracovní postupy), datové soubory důležité pro provoz organizace, nebo třeba programové vybavení [18, s. 66].

1.2.2 Hrozba

Hrozbou se v terminologii bezpečnosti rozumí jakákoliv okolnost, nebo událost působící na zranitelné místo aktiva a může způsobit potencionální škodu na aktivu [18, s. 67].

Hrozby mohou být přírodní a fyzické, jako jsou živelné pohromy (povodně, vichřice, požáry), nebo nehody (poruchy v dodávce elektrického proudu, poruchy vodovodního potrubí). Hrozby také mohou být technické a technologické, jako jsou poruchy sítí, poruchy pracovních stanic, poruchy způsobené špatně nakonfigurovanými programy, nebo počítačovými viry a další. Dalším typem hrozeb mohou být hrozby způsobené lidmi, ať už úmyslně, či neúmyslně, přičemž hrozby způsobené neúmyslně tvoří většinou více než 50% všech hrozeb, které poškodí informační systémy nebo informační a komunikační technologie (dále jen IS/ICT) organizace [18, s. 67].

1.2.3 Bezpečnostní událost

„Kybernetickou bezpečnostní událostí (dále jen událost) je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací." (15).

1.2.4 Bezpečnostní incident

„Kybernetickým bezpečnostním incidentem (dále jen incident) je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.“ (15).

1.2.5 Zranitelnost

Za zranitelnosti se označují slabá místa aktiv. Dělí se na fyzické zranitelnosti, zahrnující budovy a místnosti s ICT vybavením, technické zranitelnosti a zranitelnosti programového vybavení, zranitelnosti nosičů dat, elektromagnetických zařízení, komunikačních systémů a kabelových rozvodů formou přerušení nebo odposlechem a zranitelnosti personální, plynoucí z úmyslného počínání osob, nebo nedbalosti [18, s. 67].

1.2.6 Protiopatření

Protiopatřeními se rozumí jakékoliv kroky, které mají za cíl zabránit, nebo zmírnit škody způsobené působící hrozbou [18, s. 67].

Protiopatřeními mohou být například uzamykání místností a zastřežení objektů, používání hesel a autentizace při přístupu do informačních systémů, nebo detailní testování systémů [18, s. 67].

Protiopatření se dají dělit na administrativní (směrnice, bezpečnostní politiky a dokumentace), fyzické (zastřežení budov, používání zámků, trezorů, čipových karet pro přístupy do místností) a technologické (například autorizace a autentizace při přístupech uživatelů do informačních systémů) [18, s. 67].

1.3 Bezpečnostní politika dle vyhlášky o kybernetické bezpečnosti

Bezpečnostní politika je právním dokumentem, který definuje, jakým způsobem organizace zajišťuje bezpečnost. Hlavním cílem bezpečnostní politiky je zachování kontinuity provozu organizace předcházením, nebo včasným podchycením a řešením bezpečnostních incidentů (17).

Podle vyhlášky č. 82/2018 Sb. – Vyhlášky o kybernetické bezpečnosti (dále jen vyhláška) se bezpečnostní politikou rozumí soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv (16).

Následující struktura bezpečnostních politik vychází z obsahu bezpečnostních politik podle přílohy č. 5 k vyhlášce (16).

Používaným pojmem v následujících bodech obsahu bezpečnostních politik bude povinná osoba, kterou se ve vyhlášce rozumí orgán, nebo osoba s povinností zavést bezpečnostní opatření podle zákona (16).

1.3.1 Politika systému řízení bezpečnosti informací

Podle vyhlášky má povinná osoba za úkol stanovit rozsah systému řízení bezpečnosti informací, ve kterém určí organizační části a aktiva, kterých se systém tyká. Stanovit cíle systému řízení bezpečnosti informací a na jejich základě pro stanovený rozsah zavést bezpečnostní opatření. Dále vytvořit a schválit bezpečnostní politiku, zajistit provedení auditu kybernetické bezpečnosti podle § 16, zajistit pravidelné vyhodnocování účinnosti systému řízení bezpečnosti informací a další (16).

1.3.2 Politika řízení aktiv

Čtvrtý paragraf vyhlášky stanovuje povinnosti povinné osoby při řízení aktiv. Povinná osoba stanoví metodiku pro identifikaci a hodnocení aktiv. Dále aktiva identifikuje a eviduje, určuje pro ně garanty. Hodnotí primární aktiva z hlediska důvěrnosti, integrity a dostupnosti a řadí je do jednotlivých úrovní hodnocení. Určuje vazby mezi primárními a podpůrnými aktivy. Podpůrná aktiva hodnotí zejména z hlediska těchto vazeb (16).

Také stanovuje přípustné způsoby používání aktiv a určuje způsob likvidace dat, provozních údajů, informací a jejich kopií, nebo fyzických nosičů těchto dat (16).

1.3.3 Politika organizační bezpečnosti

Podle vyhlášky by měly být v politice organizační bezpečnosti definovány bezpečnostní role, jejich práva a povinnosti, dále požadavky na oddělení výkonu činností jednotlivých bezpečnostních rolí a provozních rolí (16).

1.3.4 Politika řízení dodavatelů

Povinná osoba eviduje dodavatele, stanovuje pro ně pravidla a dodavatele prokazatelně písemně informuje o jejich evidenci, o pravidlech a dodržování těchto pravidel vyžaduje (16).

U významných dodavatelů navíc v rámci výběrového řízení provádí povinná osoba před uzavřením smlouvy hodnocení rizik. U uzavíraných smluv stanovuje způsoby realizace bezpečnostních opatření a určuje vzájemnou smluvní odpovědnost za zavedení a kontrolu opatření. Řídí rizika a v reakci na jejich zjištění zajišťuje jejich řešení (16).

1.3.5 Politika bezpečnosti lidských zdrojů

Hlavním cílem řízení personální bezpečnosti je, aby si všechny osoby, podílející se na provozu a správě informačních systémů (IS) byly vědomy svých povinností při práci s informačními systémy. Povinná osoba stanovuje plán rozvoje bezpečnostního povědomí, který definuje obsah a rozsah poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech z hlediska bezpečnosti. Zajišťuje jejich poučení, případně teoretická, nebo praktická školení. Povinná osoba také zajišťuje kontrolu dodržování definovaných opatření (16).

V případě ukončení smluvního vztahu s administrátory, nebo osobami zastávajícími bezpečnostní role musí zajistit předání jejich odpovědností (16).

1.3.6 Politika řízení provozu a komunikací

Povinná osoba zajišťuje bezpečný provoz informačního a komunikačního systému a stanovuje provozní pravidla a postupy, obsahující mimo jiná práva a povinnosti uživatelů, administrátorů a osob zastávajících bezpečnostní role, postupy pro řešení chybových stavů systému, postupy pro sledování kybernetických bezpečnostních událostí, pravidla pro ochranu před škodlivým kódem, řízení technických zranitelností, provádění zálohování, a pravidla pro zajištění bezpečnosti síťových služeb. Dále pak postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů, pravidla pro ochranu informací a dat v průběhu životního cyklu a postupy řízení a schvalování provozních změn (16).

Povinná osoba dodržuje stanovená pravidla a postupy a aktualizuje je v souvislosti s prováděnými a plánovanými změnami (16).

Povinná osoba musí zajistit oddělení vývojového, testovacího a provozního prostředí (16).

1.3.7 Politika řízení přístupu

Povinná osoba řídí přístup k informačnímu a komunikačnímu systému a přijímá opatření k zajištění ochrany přihlašovacích údajů a jejich zneužití neoprávněnou osobou (16).

V rámci řízení přístupu k informačnímu a komunikačnímu systému povinná osoba řídí přístup na základě skupin a rolí, každému uživateli a administrátorovi přidělí přístupová práva a jedinečný identifikátor, zavádí opatření pro řízení přístupu zařízení k informačnímu a komunikačnímu systému. Zavádí bezpečnostní opatření pro používání mobilních zařízení a dalších technických zařízení (16).

Dále povinná osoba omezuje přidělování oprávnění na úroveň nezbytně nutnou k výkonu náplně práce. Přiděluje a odebírá oprávnění na základě politiky řízení přístupu. Pravidelně přezkoumává přidělená oprávnění a role. V případě změny pozice nebo zařazení zajišťuje změnu nebo odebrání přístupových oprávnění. Odebírání a přidělování přístupových oprávnění dokumentuje (16).

1.3.8 Politika bezpečného chování uživatelů

Vyhláška o kybernetické bezpečnosti pod politiku bezpečného chování uživatelů řadí instrukce pro zabezpečení nakládání s aktivy, bezpečné použití přístupového hesla, používání e-mailu a přistupování na internet, bezpečný vzdálený přístup, chování na sociálních sítích a bezpečnost ve vztahu k mobilním zařízením (16).

1.3.9 Politika zálohování a obnovy a dlouhodobého ukládání

Podle přílohy č. 5 vyhlášky o kybernetické bezpečnosti by v bezpečnostní politice pro zálohování, obnovy a dlouhodobého ukládání měly být definovány požadavky na zálohování a obnovu, pravidla a postupy zálohování a dlouhodobého ukládání, pravidla a postupy obnovy záloh a pravidla a postupy testování zálohování a obnovy. Dále pak politika přístupu k zálohám a ukládaným informacím (16).

1.3.10 Politika bezpečného předávání a výměny informací

Pro politiku bezpečného předávání a výměny informací by měla politika dle struktury z vyhlášky definovat pravidla a postupy pro ochranu předávaných informací, způsoby ochrany elektronické výměny informací a pravidla pro využívání kryptografické ochrany (16).

Pravidla pro využívání kryptografické ochrany jsou blíže specifikována v jedné z následujících kapitol, politika bezpečného používání kryptografické ochrany.

1.3.11 Politika řízení technických zranitelností

Řízení technických zranitelností je ve struktuře vyhlášky popsáno pravidly pro omezení instalace programového vybavení, pravidly a postupy vyhledávání opravných programových balíčků, pravidla a postupy testování oprav a nasazení oprav programového vybavení (16).

1.3.12 Politika bezpečného používání mobilních zařízení

Podle struktury bezpečnostních politik z přílohy č. 5 vyhlášky patří do politik pravidla a postupy pro bezpečné používání mobilních zařízení a pravidla a postupy pro zajištění bezpečnosti zařízení, která povinná osoba nemá ve své správě (16).

1.3.13 Politika akvizice, vývoje a údržby

Povinná osoba s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního řeší řízení rizik podle § 5 vyhlášky, významné změny podle § 11 vyhlášky, stanovuje bezpečnostní požadavky a zahrnuje je do projektu akvizice, vývoje a údržby. Dále zajišťuje bezpečnost vývojového i testovacího prostředí a ochranu testovacích dat. Testuje bezpečnost před provedením významných změn (16).

1.3.14 Politika ochrany osobních údajů

Pro politiku ochrany osobních údajů vymezuje vyhláška mít v bezpečnostních politikách zpracovány charakteristiky zpracovávaných osobních údajů a popis přijatých a provedených technických a organizačních opatření (16).

1.3.15 Politika fyzické bezpečnosti

Povinná osoba podle vyhlášky předchází poškození, krádeži, či zneužití aktiv. Předchází přerušení poskytování služeb informačního a komunikačního systému (16).

Dále vymezí oblast perimetru fyzické bezpečnosti, ve které jsou umístěna technická aktiva a ve které jsou uchovávány informace. Pro oblast přijme opatření k zamezení neoprávněného vstupu, opatření k zamezení poškození a zajistí ochranu na úrovni objektů i v rámci objektu (16).

1.3.16 Politika bezpečnosti komunikační sítě

Pro ochranu bezpečnosti komunikační sítě spadající dle zákonu o kybernetické bezpečnosti pod sítě provozující informační systém kritické informační infrastruktury má povinná osoba povinnost zajistit segmentaci komunikační sítě, řízení komunikace v rámci sítě a perimetru komunikační sítě. Zajistit důvěrnost a integritu dat při vzdáleném přístupu, správě a při přístupu do sítě pomocí bezdrátových technologií. Blokuje nežádoucí komunikaci a pro řízení komunikace mezi segmenty sítě zajišťuje vhodným nástrojem ochranu integrity (16).

1.3.17 Politika ochrany před škodlivým kódem

Podle zákona a vyhlášky o kybernetické bezpečnosti má správce a provozovatel informačního, nebo komunikačního systému kritické informační infrastruktury, případně správce a provozovatel IS základní služby povinnost zajistit použití nástroje pro nepřetržitou automatickou ochranu koncových stanic, mobilních zařízení, serverů, datových úložišť a výměnných datových nosičů, komunikační sítě a jejich prvků a dalších zařízení. Dále monitorovat a řídit používání výměnných zařízení a datových nosičů, řídit automatické spouštění výměnných zařízení a datových nosičů, řídit oprávnění ke spouštění kódu a provádět pravidelnou aktualizaci nástroje pro ochranu před škodlivým kódem. Správce nebo provozovatel významného informačního systému se těmito požadavky řídí přiměřeně (16).

1.3.18 Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí

Podle vyhlášky o kybernetické bezpečnosti by měla být nastavena politika, ve které by byla definována pravidla a postupy nasazení nástroje pro detekci kybernetických bezpečnostních událostí. Dále pak postupy pro vyhodnocování a reagování na detekované události a pravidla a postupy pro optimalizaci nastavení takových nástrojů (16).

Nástroj musí zajistit ověření a kontrolu přenášených dat v rámci komunikační sítě, mezi sítěmi a na perimetru komunikační sítě a blokovat nežádoucí komunikaci (16).

Dále přiměřeně v závislosti na důležitosti aktiv zajišťuje správce a provozovatel informačního, nebo komunikačního systému kritické informační infrastruktury, případně správce a provozovatel informačního systému základní služby detekci kybernetických bezpečnostních událostí v rámci koncových stanic, mobilních zařízení, serverů, datových úložišť a vyměnitelných datových nosičů, aktivních prvků na síti a obdobných aktiv (16).

1.3.19 Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Podle zákona a vyhlášky je správce a provozovatel informačního, nebo komunikačního systému kritické informační infrastruktury, případně správce a provozovatel informačního systému základní služby povinen používat nástroj pro sběr a nepřetržité vyhodnocení kybernetických bezpečnostních událostí. Nástroj musí umožňovat sběr a vyhodnocování událostí, jejich agregaci na základě souvislostí a osobám zodpovídajícím za bezpečnost poskytovat informace o detekovaných událostech. Dále nástroj musí umožňovat aktualizaci nastavení pravidel pro omezení počtu falešně pozitivních vyhodnocení, nastavení pravidel včasného varování a využití informací získaných nástrojem pro optimální nastavení bezpečnostních opatření informačního a komunikačního systému (16).

Vyhláška dále definuje potřebu zaznamenávat události, záznamy chránit před neoprávněným čtením a jakýmikoliv změnami a zajistit synchronizaci jednotného času nejméně jednou za 24 hodin. Uchovávat tyto záznamy po dobu 12 měsíců u provozovatelů významných informačních systémů a po dobu 18 měsíců v případě správce a provozovatele informačního, nebo komunikačního systému kritické informační infrastruktury a správce a provozovatele informačního systému základní služby (16).

1.3.20 Politika bezpečného používání kryptografické ochrany

Povinná osoba má povinnost používat pro ochranu aktiv aktuálně odolné kryptografické algoritmy a klíče na základě doporučení Národního úřadu pro kybernetickou a informační bezpečnost. Používat systém pro správu klíčů a certifikátů, který zajistí generování, distribuci, ukládání, změny, omezení platnosti, zneplatnění certifikátů a likvidaci klíčů a podporuje kontrolu a audit. Cílem opatření je zajištění důvěrnosti, integrity a dostupnosti dat (16).

1.3.21 Politika řízení změn

Povinná osoba zjišťuje možné dopady změn u informačního a komunikačního systému a určuje významné změny. V případě významných změn dokumentuje jejich řízení, zpracovává analýzu rizik, snaží se o snížení nepříznivých dopadů spojených se změnami, aktualizuje bezpečnostní politiku a dokumentaci, zajistí možnost testování změn a případnou možnost navrácení změn do původního stavu (16).

Správce a provozovatel informačního, nebo komunikačního systému kritické informační infrastruktury, případně správce a provozovatel IS základní služby dále podle výsledků analýzy rizik rozhoduje o provedení penetračních testů, nebo testování zranitelností. Povinná osoba, která je správcem nebo provozovatelem významného informačního systému se požadavky tohoto bodu řídí přiměřeně (16).

1.3.22 Politika zvládání kybernetických bezpečnostních incidentů

Povinná osoba podle vyhlášky zavede proces detekce kybernetických bezpečnostních událostí (dále jen událost) a zvládání kybernetických bezpečnostních incidentů (dále jen incident). Stanoví postupy detekce a vyhodnocování událostí a incidentů a koordinace a zvládání incidentů. Definuje postupy pro identifikaci, sběr, získání a uchování podkladů pro analýzu incidentů (16).

Povinná osoba dále zajišťuje, aby jak administrátoři a osoby zastávající bezpečnostní role, tak uživatelé, dodavatelé a další zaměstnanci oznamovali neobvyklé chování informačního a komunikačního systému a podezření na jakékoliv zranitelnosti (16).

Také zajišťuje prošetření událostí, zda-li mají být klasifikovány jako incidenty podle § 31 vyhlášky. U incidentů zajistí zvládání podle stanovených postupů, snaží se o odvrácení, nebo minimalizaci dopadu incidentů, vede o incidentech a jejich řešení záznamy, prošetřuje příčiny incidentů a hlásí incidenty podle § 32 na NÚKIB (16).

1.3.23 Politika řízení kontinuity činností

V rámci řízení kontinuity činností stanovuje povinná osoba práva a povinnosti administrátorů a osob zastávajících bezpečnostní role. Provádí hodnocení rizik a analyzuje dopady incidentů na kontinuitu činností (16).

Podle hodnocení rizik a analýzy dopadů pak určuje minimální úrovně poskytovaných služeb, přijatelných pro užívání, provoz a správu informačního a komunikačního systému, doby obnovení chodu těchto služeb a dobu, za kterou musí být zpětně obnovena data po incidentu nebo selhání. Podle těchto cílů stanovuje politiku řízení kontinuity činností. Plány kontinuity činností a havarijní plány vypracuje, pravidelně aktualizuje a testuje (16).

1.4 Nástroje zabezpečení

1.4.1 Antivir

Antivirový program neboli antivir, je počítačový software, sloužící k nalezení a odstranění počítačových virů a dalšího škodlivého softwaru (malware). Antivir buď vyhledává na disku počítače sekvenci odpovídající příznaku viru z databáze virů, nebo detekuje podezřelou aktivitu programu, což by mohlo označovat infekci (19).

1.4.2 Proxy

Proxy servery můžou být druhem firewallu, nebo programem. Jejich fungování spočívá v dělání role „prostředníka“ mezi klientem vnitřní sítě a připojením do sítě internet. V případě že proxy server povolí připojení na daný server, otevře k serveru druhé spojení jménem původního hostitele, na druhé straně přijímá data ze serveru a poskytuje je zpět původnímu klientovi ve vnitřní síti [3, s. 93].

1.4.3 Firewall

Firewall je bezpečnostní zařízení, umístěné na hraně internetového připojení, které sleduje a případně filtruje veškerý provoz, který jím prochází [3, s. 134].

Firewall je schopen blokovat příchozí i odchozí provoz podle jeho zdroje nebo cíle a nebo třeba konfigurací zpřístupňovat zdroje vnitřní sítě definováním výjimek, například pro webový server. Firewall by také měl být schopen oznamovat průběh svých činností, například zaznamenávat své aktivity na syslog servery [3, s. 140].

1.4.4 Virtuální privátní síť (VPN)

Síť VPN tvoří chráněnou relaci nad nechráněnými kanály, jako je např. Internet. Po připojení pomocí VPN se zařízení připojené zvnějšku chová, jako by bylo připojené ve vnitřní síti. Dá se využít pro práci z domova, práci na cestách, nebo třeba k připojení obchodních partnerů, nebo dodavatelů do vnitřní sítě [6, s. 13].

1.5 Řízení přístupů

1.5.1 Autentizace

Autentizace je ověřování totožnosti uživatelů, nebo jednotlivých komunikačních entit. Totožnost uživatelů se dá ověřit třemi různými způsoby, a to na základě toho:

- **kdo jsou** – k identifikace se používá otisků prstů, dlaní, skenování obličeje,
- **co mají** – k identifikaci se používá například fyzických klíčů, nebo karet,
- **co znají** – k identifikaci se používá hesel, pinů, identifikačních čísel, které uživatel zná [4, s. 517].

1.5.2 Autorizace

Po fázi autentizace nastává fáze autorizace, která určuje, jaká práva a přístupy k síťovým zdrojům, službám datům a operacím bude uživatel mít [4, s. 519].

1.5.3 Účtování

Účtování (Accounting) je poslední složkou architektury ochrany přístupu do systému. Účtování zodpovídá za zaznamenání každého přístupu a každé činnosti uživatele v systému [4, s. 519].

1.5.4 Radius

Zkratka vzniklá z anglického Remote Authentication Dial-in User Service. Jedná se o síťový protokol, starající se o ověření vzdálených uživatelů. Funguje na bázi RADIUS serverů, které mohou být ve velikosti od pár uživatelů až po velké servery pro tisíce uživatelů, nasazené například i u poskytovatelů internetových služeb [2, s. 802].

V rámci autentizace sever RADIUS zajistí identifikaci uživatele a povolí nebo zakáže jeho připojení. Servery RADIUS jsou schopny udržovat kopie síťových účtů uživatel, ale z hlediska bezpečnosti je doporučené, aby server RADIUS předával autentizační informace jiným serverům [2, s. 802].

V rámci autorizace *„server RADIUS určuje přístupová práva a oprávnění, která může uživatel v síti mít. Autorizace rovněž určuje typ připojení, které může klient RADIUS poskytovat, jako například připojení PPP nebo Telnet.”* [2, s. 802].

V rámci účtování server RADIUS, jelikož uchovává podrobné protokoly událostí, je schopen poskytovat údaje pro účely fakturace nebo účtování [2, s. 802].

1.5.5 Digitální certifikát

Datová struktura, která nese informace o identitě svého majitele. Majitelem může být fyzická osoba, právnická osoba, nebo třeba server. Je určen k ověřování elektronického podpisu, šifrování dat a zajištění integrity dat (9).

1.5.6 Šifrování dat

„Šifrování dat je proces, kterým se nezabezpečená elektronická data převádí za pomoci kryptografie na data šifrovaná, čitelná pouze pro majitele dešifrovacího klíče. Šifrování dat slouží k jejich ochraně proti nežádoucímu zjištění cizí osobou a uplatňuje se při ukládání dat i při jejich přenosu včetně telekomunikace“ (10).

1.5.7 Doména

Doména je logickým seskupením síťových počítačů, sdílejících databázi údajů o uživatelských účtech, zabezpečení a další. Po připojení k doméně máme k dispozici všechny serverem poskytované zdroje (v závislosti na nastavených právech pro připojený účet) [20, s. 68].

1.5.8 Active Directory

Microsoft Active Directory (AD) je nejčastěji používanou adresářovou strukturou dnešní doby. AD tvoří širokou spravovatelnou třídu objektů. Uživatelé a účty jsou objekty organizovaně umístěné v adresáři, kterým mohou být přidělována různá oprávnění [2, s. 564].

1.5.9 Skupinové zásady

Služba Active Directory umožňuje vytvoření obecných zásad, které mohou být použity na doménu, nebo na určitou skupinu v adresářové struktuře AD. Skupinové zásady mohou být měněny pomocí editoru objektů zásad skupiny (Group Policy Object Editor) [2, s. 556].

1.6 Zálohování dat

Vzhledem k tomu, že kdykoliv může i přes konstrukční vlastnosti moderních serverů dojít k poruše disku s daty, případně o data na disku přijít jiným způsobem, je nezbytné provádět zálohování dat [20, s. 129].

Zálohování může vycházet z principů funkčnosti diskových polí RAID, případně se mohou data archivovat na páskové jednotky. Pásky pak bývají z důvodů bezpečnosti přeneseny do jiné místnosti [20, s. 129].

1.6.1 Typy zálohování

Typem zálohování se rozlišuje, jestli se zálohují pokaždé všechna data, nebo jen data, která se změnila [20, s. 130].

Typy zálohování jsou:

- **Full backup** (úplná záloha) – zálohují se všechny soubory, velké objemy zálohy [20, s. 131],
- **Differential backup** (rozdílová záloha) – zálohují se pouze soubory, které byly od poslední zálohy vůči záloze full backup změněny. Pro obnovení je potřeba i poslední záloha metody full backup [20, s. 131].
- **Incremental backup** (přírůstková záloha) – zálohují se pouze soubory, které se změnily od okamžiku jakékoliv poslední zálohy, pro obnovu jsou nutné všechny předchozí přírůstkové zálohy [20, s. 131].

1.6.2 Strategie zálohy

Je zbytečné zálohovat data, která máme na instalačních médiích a v případě ztráty je můžeme doinstalovat. Pro úsporu místa na záložním médiu bychom mělo zálohovat pouze data takovýchto aplikací [20, s. 131].

Zálohovat bychom měli v době, kdy se s daty zrovna nepracuje, vhodné by proto bylo provádět zálohy mimo pracovní dobu (při denním provozu například v noci) [20, s. 132].

1.6.3 Obnova dat ze zálohy

Úspěšná obnova je stěžejním bodem celého procesu zálohy dat. Měli bychom provádět pokusnou obnovu dat, abychom měli jistotu, že v případě nouze budou zálohy fungovat [20, s. 93].

1.7 Detekce a prevence vniknutí

1.7.1 Co je to IDS

Intrusion Detection System (IDS) *„IDS může být definován jako soubor nástrojů, metod a zdrojů, které nám pomáhají identifikovat, zpřístupnit a hlásit neautorizované a neschválené síťové aktivity"* [1, s. 36].

Útoky se mohou vyskytnout ve všech sítích. IDS se snaží tyto útoky odhalovat, případně jim zamezovat. Sledují provoz v síti pomocí sond, které sbírají pakety přenášené v síti a vyhodnocují jej podle znalostních databází známých útoků. V případě nalezení útoku reagují obvykle upozorněním správci sítě, ale mohou reagovat i aktivně, např. zablokováním komunikace. [4, s. 77]

Systémy IDS pracují v síťové vrstvě OSI modelu. IDS analyzují pakety, zda-li nejsou v síťovém provozu přítomny specifické vzory. Jestliže je shledáno, že se vzor vyskytuje, zaznamená se do souboru výstraha a v závislosti na těchto datech může být učiněna odpovídající odezva. Testováním přítomnosti specifických vzorů jsou IDS podobné antivirovým softwarům, ve kterých se užívají známé signatury za účelem rozeznání potencionálně zhoubných provozních vzorů [1, s. 37].

1.7.2 Co je to IPS?

Prevenční systémy IPS (Intrusion Prevention System) brání v úspěšném dokončení útoku. Systémy IPS spolupracuje s IDS, přičemž výrobci zpravidla oba mechanismy kombinují [3, s. 262].

IPS se v sítích zařazují sériově (nejsou pasivní) a proaktivně blokují narušení [1, s. 41].

1.7.3 Analýza IDS a IPS

Existuje mnoho možných datově analytických koncepcí pro analytický stroj, pro jejich pochopení je vhodné si proces analýzy narušení rozdělit do 4 fází: [1, s. 45].

1. Předzpracování

   Krok, ve kterém jsou data získaná ze senzorů IDS nebo IPS organizována pro účely klasifikace, například převedením do předem daného kanonického formátu, nebo strukturované databáze [1, s. 45].

   Po zformátování dat jsou data rozdělena do příslušných klasifikací. Ty závisí na použitých analytických schématech. Například v případě detekce založené na pravidlech, klasifikace bude zahrnovat pravidla a deskriptory vzorů. V případě detekce anomálií obdržíme statistické profily založené na různých algoritmech, kde je normální uživatelské chování znormováno a jakékoliv chování vně této klasifikace je označeno jako anomální [1, s. 45].

2. Analýza

   V analytické fázi je každý záznam porovnán s databází vzorů a je buď uznán jako narušení, nebo je ignorován [1, s. 45].

3. Odezva

   Ve fázi odezvy se projevuje rozdíl mezi IDS a IPS. Zatímco u IDS je výstraha obdržena až po případné incidenční události, u IPS je senzor řazen sériově a můžeme pomocí automatické odpovědi získat prevenci v reálném čase [1, s. 45].

4. Vyladění

   V poslední fázi se řeší doladění systémů IDS nebo IPS v závislosti na přesnosti předchozích detekcí. Vyladění dává správcům možnost snížit množství falešně pozitivních zpráv, je proto důležitou součástí úspěšné detekce a prevence narušení [1, s. 46].

1.7.4 Porovnání IDS a IPS

IDS i IPS mají oba své místo v bezpečnosti sítě, nelze říci, že by IPS nahradilo IDS a IDS se stalo minulostí [1, s. 51].

Naopak, IDS a IPS jsou oddělené technologie, které se mohou vzájemně doplňovat [1, s. 49].

Ačkoliv některé IDS systémy mají možnost reagovat vyřazením nebo resetem TCP, nejsou stejné jako systémy IPS. IPS zařízení jsou umisťovány sériově a všechny pakety jimi musí projít. U IDS je paket odeslán k analýze na vnitřní rozhraní, pak je vyslána výstraha a vygenerována odezva. Čekací doba na odezvu, oproti tomu, kdyby byla odezva v reálném čase, má často za důsledek selhání odezvy [1, s. 50].

Vzhledem k tomu že jsou IPS umisťovány sériově, vytváří tak úzká místa (úzká hrdla) v síti [1, s. 50].

Kvůli tomu, že IPS na narušení přímo reaguje mohou vzniknout v případě falešně pozitivních výsledků vážné problémy. Není proto vhodné používat IPS ve všech případech. [1, s. 50].

1.7.5 Terminologie

U systémů detekce vniknutí se můžeme setkat se čtyřmi typy zpráv. Skutečně pozitivní, falešně pozitivní, skutečně negativní a falešně negativní. (11) [1, s. 50].

Skutečně pozitivní – Reálný útok, který vyvolá alarm v IDS.

Falešně pozitivní – Alarm v IDS, který není na základě reálného útoku, ale je způsobem příliš citlivým nastavením IDS. Je potřeba, aby organizace svůj IDS vyladila tak, aby omezila počty falešně pozitivních zpráv zaplavujících IDS a mohla se tak ve výsledcích IDS lépe orientovat.

Skutečně negativní – Nedošlo k útoku, ani nebyl vyvolán žádný alarm.

Falešně negativní – V takovémto případě IDS selhalo odhalit skutečný útok. Může být zapříčiněno nesprávným odladěním výjimek falešně pozitivních zpráv v IDS.

1.8 Logy

1.8.1 Co je to log

Log je soubor se záznamem jednotlivých událostí, které se staly v monitorovaném systému nebo na síti. Každý záznam obsahuje informace vztahující se k určité události jako například čas, zdroj, podrobnější popis události a další. V minulosti se logy používali zejména k ladění chyb, ale s postupem času nabyly mnohem větší důležitosti a začaly se využívat k dalším účelům jako je optimalizace výkonu systémů a sítě, sledování činností uživatelů a poskytování užitečných dat při vyšetřování podezřelých aktivit [12, s. 2-1].

1.8.2 Syslog

Syslog je protokol, který byl v roce 2001 popsán dokumentem RFC 3164 a později aktualizován dokumentem RFC 5424. Dokumenty také popisují formát syslogových zpráv. Protokol syslog nabízí způsob, jakým mohou aplikace posílat informace o událostech přes síť na syslogové servery. Syslog nabízí oddělení aplikací generujících logy, systémů ukládajících logy a aplikací nabízejících správu a analýzu logů. Protokol syslog je simplexový a nenabízí potvrzení doručení zpráv, je možné že některé zprávy mohou být po cestě ztraceny [13] [14].

1.8.3 Správa logů

Správa logů (log management) může být pro organizaci důležitý z několika ohledů. Pomáhá zajistit, že logy budou ukládány s dostatečnou mírou detailu na dostatečně dlouhou dobu. Analýza logů pomáhá při řešení bezpečnostních incidentů, podvodných aktivit, nebo při řešení chybových stavů v systémech. Kromě interních potřeb organizace, je často schraňování logů vyžadováno i například zákonem, nebo různými standardy [12, s. 2-7].

1.8.4 Logovací servery

Někteří klienti generující logy poskytují svá data logovacím serverům po síti, jiní poskytují serverům možnost připojit se k nim a získat kopie logovacích souborů. Data jsou serverům poskytována buď v reálném čase, téměř reálném čase, nebo v plánovaných časových rozmezích podle objemu dat. Logy pak mohou být ukládány buď přímo na logovacím serveru, nebo v oddělených databázích [12, s. 3-1].

Topologie logovacích serverů může být i rozmanitější než pouze jeden logovací server, starající se jak o analýzu, tak uchovávání logů. Více logovacích serverů může odděleně zajišťovat například sběr logů, analýzu, krátkodobé ukládání logů a dlouhodobé ukládání logů. Taktéž mohou poskytovat v systému redundanci pro případ, že nějaký ze serverů přestane fungovat [12, s. 3-1].

Více logovacích serverů může být řazeno i způsobem, že se některé servery budou starat pouze o sběr logů z různých míst a centrálním logovacím serverům poté přeposílat všechna, nebo jen některá data [12, s. 3-1].

1.8.5 Analyzátory logů

Ve většině organizací jsou za analýzu logů zodpovědní administrátoři, kteří ale obvykle musí řešit spoustu dalších věcí a analýze logů přikládají nízkou prioritu. Často je analýza logů považována za neefektivní a zabírající příliš mnoho času na to, jaké benefity z ní vychází. Aby analýza logů měla smysl, měli by být zodpovědní administrátoři školeni k jejímu efektivnímu provádění a měli by mít k dispozici potřebné nástroje síťového zabezpečení, jako jsou například host-based IDS a SIEM [12, s. 2-10].

Jednou z podstatných funkcí nástrojů analýzy je korelace událostí. Korelace událostí (event correlation) napomáhá administrátorům vidět v událostech širší souvislosti, kterých by si při běžném prohlížení logů nevšimnuli. Korelace událostí spojuje logy například na základě časových razítek, IP adres, typu události, nebo různých statistických metod [12, s. 3-4].

Analyzátory také umožňují zobrazení logů ve formě čitelné pro člověka. Logy z různých zdrojů totiž mohou nabývat různých podob a aby se s nimi dalo dále dobře pracovat, je třeba je konvertovat a normalizovat. Při normalizaci se data konvertují do konzistentního formátu, aby se usnadnily následné analýzy. Například časové razítko z jednoho zdroje může být ve 12hodinovém formátu (2:34:56 P.M. EDT) zatímco časové razítko z jiného zdroje ve 24hodinovém formátu (14:34) a časové pásmo zapsáno zvlášť (-0400) v jiném poli [12, s. 3-4].

1.9 SIEM

Security information and event management (SIEM) software je typem softwaru pro centralizované logování, který využívá jednoho, nebo více logovacích serverů pro analýzu záznamových souborů a jeden, nebo více serverů pro jejich uchovávání [12, s. 3-9].

Různé SIEM produkty nabízejí dva různé způsoby sběru logů z generátorů logů, a to buď s agentem, nebo bez agenta. V případě využití způsobu sběru logů bez agenta se buď servery autentizují ke každému zařízení a logy si z něj samy vytahují (pull) nebo zařízení samy posílají logy na příslušný server (push). V případě využití agenta nainstalovaného na logovaném zařízení jsou data před odesláním na SIEM server filtrována, agregována a normalizována [12, s. 3-9].

Výhodou metody s nainstalovaným agentem jsou menší objemy dat po filtrování, agregaci a normalizaci, takže i menší objemy dat, které se přenášejí po síti. Naopak výhodou metody bez agenta může být, že není třeba instalovat, nastavovat a starat se o program agenta. Nevýhodou pak může být nutnost autentizace u každého logovaného zařízení, což nemusí být v některých případech možné [12, s. 3-9].

Produkty SIEM obvykle nabízejí správcům další užitečné funkce. Jednou z nich je například grafické rozhraní designované pro ulehčení analýzy potencionálních problémů a zobrazení dat týkajících se daného problému. Dále mohou produkty nabízet databázi známých zranitelností, které mohou správci využít ve svůj prospěch, nebo třeba funkci korelace událostí, která přiřazuje vyšší prioritu útokům cílícím na zranitelná místa, nebo důležitější zařízení. [12, s. 3-10].

2 ANALÝZA SOUČASNÉHO STAVU

V této části bakalářské práce uvedu základní informace o instituci, popíšu síťovou infrastrukturu v instituci a dále se budu zabývat analýzou současného stavu monitoringu síťových událostí v instituci. Informace z této části práce poslouží jako podklady pro praktickou část.

2.1 Základní informace o instituci

Z důvodu anonymizace a utajení informací o instituci uvedu pouze, že se jedná o orgán veřejné moci (OVM), přesněji státní instituci (dále jen instituce).

2.2 Povinnosti OVM v oblasti kybernetické bezpečnosti

Pro subjekty, jejichž systémy, služby, nebo sítě mají zásadní význam pro fungování státu, vyplývají ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti specifické povinnosti k zavedení bezpečnostních opatření. Zákon se vztahuje na povinné osoby, které provozují kritickou informační infrastrukturu, nebo významný informační systém. Při vyhlášení stavu kybernetického nebezpečí se okruh subjektů s povinností provádět protiopatření zvětšuje. Opatření mohou být preventivní, nebo reaktivní a organizační, nebo technické povahy (15).

Instituce popisovaná v této práci spadá pod § 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti jako správce a provozovatel významného informačního systému (15).

2.3 Bezpečnostní politiky organizace

Informace o bezpečnostních politikách instituce budou v této kapitole stejně jako v teoretické části strukturovány podle přílohy č. 5 k vyhlášce č. 82/2018 Sb. – Vyhlášce o kybernetické bezpečnosti (16).

Informace pocházejí z bezpečnostních politik a vnitřních směrnic instituce. Konkrétněji se v instituci bezpečnostní politiky informačních systémů instituce řídí dokumenty na třech úrovních.

První úrovní jsou politiky. Ty jsou tvořeny Bezpečnostní politikou IS, Bezpečnostní politikou ISVS a Bezpečnostní politikou ISMS.

Bezpečnostní politika IS obsahuje standardy definující úroveň bezpečnosti v konkrétních oblastech IT. Tento dokument se řídí zejména vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti.

Bezpečnostní politika ISVS (informačních systémů veřejné správy) stanovuje konkrétní pravidla a zásady pro zajištění bezpečnosti informačních systémů podle zákona č. 365/2000 Sb., o ISVS, potažmo vyhlášky č. 529/2006 Sb., o dlouhodobém řízení ISVS.

Bezpečnostní politika ISMS stanovuje rámec řízení bezpečnosti informací v souladu s normou ČSN ISO/IEC 27001, potažmo s požadavky kybernetického zákona a souvisejících prováděcích právních předpisů. V tomto dokumentu jsou definovány základní oblasti rizik, která mohou ohrozit důvěrnost, integritu a dostupnost aktiv instituce a omezit poskytování služeb instituce.

Druhou úrovní jsou bezpečnostní směrnice, obsahující bezpečnostní směrnice pro bezpečnostního správce ISVS.

Třetí úrovní jsou pak ostatní dokumenty, jako příručky a technická dokumentace, pro uživatele i správce informačních systémů.

2.3.1 Politika systému řízení bezpečnosti informací

V instituci je osobou zodpovědnou za zpracování a schválení veškeré dokumentace týkající se bezpečnosti bezpečnostní ředitel, případně jím delegovaný manažer kybernetické bezpečnosti, nebo bezpečnostní správce.

2.3.2 Politika řízení aktiv

Primárním aktivem jsou data a informace. Informační aktiva se rozlišují na tři stupně, pro které platí různé požadavky na ochranu, a to stupně veřejné, interní a citlivé. Každé informační aktivum má definovaného vlastníka, přípustné použití a je klasifikováno do příslušné kategorie a klasifikačního stupně.

Garant aktiva je odpovědný za zajištění rozvoje, použití a bezpečnosti aktiva. Podílí se na hodnocení aktiv z hlediska jejich bezpečnosti. Role garanta aktiva je taktéž závazná pro správce významného informačního systému dle kybernetického zákona.

2.3.3 Politika organizační bezpečnosti

Rozdělení bezpečnostních rolí:

Bezpečnostní ředitel – řídí činnost bezpečnostního výboru, řídí rozvoj bezpečnosti informačních systémů a řídí bezpečnost k dalším orgánům veřejné moci, které informační systémy využívají.

Manažer kybernetické bezpečnosti – zajišťuje činnosti delegované bezpečnostním ředitelem, přičemž nesmí být pověřen výkonem rolí odpovědných za provoz informačních systémů. Vede vyšetřování bezpečnostních incidentů v informačních systémech, provádí kontroly bezpečnostních politik, sleduje a vyhodnocuje hrozící rizika a navrhuje protiopatření. Řídí a kontroluje činnost bezpečnostních správců instituce. Role manažera kybernetické bezpečnosti je závazná pro správce významného informačního systému dle kybernetického zákona.

Bezpečnostní správce IS – sleduje stav bezpečnosti IS a prověřuje události týkající se jeho bezpečnosti. Vypracovává bezpečnostní dokumentaci pro IS.

Součástí pracovní náplně bezpečnostního ředitele, manažera i správce je být v kontaktu se zájmovými skupinami zaměřenými na bezpečnost.

Prosazování bezpečnostních pravidel a účast na řešení bezpečnostních incidentů má v rámci svého útvaru a u svých podřízených každý vedoucí pracovník. Každý vedoucí pracovník je povinen poskytovat bezpečnostnímu řediteli veškerou podporu v oblasti bezpečnosti informací.

Přidělení rolí bezpečnostního ředitele a manažera kybernetické bezpečnosti konkrétním osobám určuje nejvyšší vedení. O přidělení role bezpečnostního správce IS rozhoduje bezpečnostní ředitel.

2.3.4 Politika řízení dodavatelů

Na straně instituce je definován garant služby, dodávané třetí stranou, který má znalosti potřebné k posouzení konkrétní dodávané služby.

Od externích dodavatelů jsou požadovány zprávy o poskytovaných službách, nejvýše v měsíčních intervalech a požadovány zprávy o bezpečnostních událostech, týkajících se dodávaných služeb.

2.3.5 Politika bezpečnosti lidských zdrojů

Každé osoba podílející se na provozu a správě informačních systémů jsou při vzniku pracovního vztahu přidělena přístupová práva k datům a prostředkům výpočetní techniky odpovídající pracovnímu zařazení.

Všechny smlouvy uzavřené se zaměstnanci instituce obsahují ustanovení o odpovědnosti za bezpečnost informací. Tato ustanovení se týkají zaměstnanců v pracovním poměru, zaměstnanců v poměru služebním i externích subjektů, podílejících se na provozu a správě informačních systémů.

Při ukončení či změně pracovního vztahu jsou osobám odejmuta či pozměněna přístupová práva k informacím, software a prostředkům výpočetní techniky IS, a to ke konkrétnímu datu. Dále u všech osob podílejících se na provozu a správě informačních systémů byl zajištěn závazek mlčenlivosti o údajích významných z hlediska bezpečnosti i po ukončení pracovního vztahu.

Všichni zaměstnanci jsou před započetím používání informačního systému povinni potvrdit seznámení se se směrnicemi.

Identity management (IDM) je v instituci řešen za pomoci dedikovaného softwaru. Některé další oprávnění a přístupy, zejména když se jedná o výjimky, jsou pak řešeny například přímo v Active Directory, nebo na file serveru.

2.3.6 Politika řízení provozu a komunikací

Jednotlivé pravomoci a odpovědnosti spojené s bezpečným provozem se vážou k bezpečnostním rolím, již blíže popsaným v kapitole politiky organizační bezpečnosti.

Postupy, požadavky a standardy bezpečného provozu tak jako většinu ostatní dokumentace vypracovává bezpečnostní správce a schvaluje bezpečnostní ředitel, při zpracování dokumentů se musí řídit zákonem a vyhláškou o kybernetické bezpečnosti.

Představitelé jednotlivých bezpečnostních rolí se řídí svými odpovědnostmi z bezpečnostních politik a v tomto ohledu jsem neodhalil žádný nedostatek.

2.3.7 Politika řízení přístupu

Základní strategie řízení přístupů uživatelů i správců k informačním systémům spočívá v instituci ve výchozím blokování všech přístupů a postupným povolováním tam, kde je to vyžadováno.

Přístupy uživatelů k aktivům informačních systémů musí být v souladu se zákony ČR a v souladu s vnitřními předpisy instituce.

Přístupová oprávnění je schopen hlídat nástroj Varonis, blíže popsaný v kapitole nástrojů pro detekci událostí.

V případě, že uživatel narušuje bezpečnost informačních systémů, má bezpečnostní ředitel právo mu přístup zablokovat.

O přístup k jednotlivým komponentám používaných informačních systémů žádají uživatelé pomocí helpdesku prostřednictvím svého nadřízeného. Oprávněnost požadavků na přístup ověřuje správce ICT u bezpečnostního správce.

2.3.8 Politika bezpečného chování uživatelů

Zaměstnanci jsou povinni ukládat pracovní data pouze na zálohované síťové disky, je zakázáno taková data ukládat na lokální disky počítačů. Ve spolupráci s ICT mají zaměstnanci povinnost zajistit neobnovitelnou likvidaci dat, klasifikovaných jako citlivá nebo interní, ze zařízení, před předáním zařízení jiné osobě.

Zvláštní kategorií jsou poté osoby s přístupy k utajovaným informacím. Tato problematika se řídí zákonem č. 412/2005 Sb. O ochraně utajovaných informací a o bezpečnostní způsobilosti. Tyto osoby musí projít bezpečnostní prověrkou zajišťovanou Národním bezpečnostním úřadem.

Každý uživatel pracující v instituci je povinen zúčastnit se každoročního bezpečnostního školení, zaměřeného zejména na phishingové e-maily.

Taktéž má každý uživatel po nástupu do zaměstnání povinnost projít kurzem Základy kybernetické bezpečnosti, poskytovaným Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB).

2.3.9 Politika zálohování a obnovy a dlouhodobého ukládání

„Zálohou se rozumí data uložená na médiu pro zálohování jako jeden celek.“

Zálohy fileserverů probíhají 2x denně, a to o půlnoci a v poledne.

Jedna záloha týdně obsahuje veškerá data uložená na serveru nutná pro obnovu provozního stavu. Pro každý server a aplikace na něm je vždy k dispozici alespoň jedna záloha.

Minimálně jedna záloha měsíčně musí být verifikována, pokud se jako záložní médium používá magnetická páska a pokud se pro zápis používá pouze jedna zapisovací hlava.

Zálohy mají kopii, které jsou uloženy na magnetických páskách a umístěny v trezoru, v jiné serverové místnosti, než jsou tvořeny. Pro bezpečnost serverových místností platí kritéria, popsaná v jedné z dalších kapitol.

Pravidla a postupy testování zálohování a obnovy v politikách jasně definovány nejsou. Pravidla přístupů k zálohám také jasně definována nejsou.

2.3.10 Politika bezpečného předávání a výměny informací

Uživatelé mají skupinovými politikami zakázané připojovat k počítačům USB flash disky, CD, DVD a jiná vyměnitelná média. V případě, že takové médium obdrží a potřebují pracovat s jeho obsahem, jsou instruování požádat součinnost IT, kteří médium zkontrolují na přítomnost virů a jeho obsah uživateli nahrají na síťový disk.

Data v tiskových frontách na tiskových serverech jsou přístupna pouze osobě, která data tiskne. Vytištění dokumentů je umožněno pouze autorizované osobě po autorizaci přístupovou kartou u tiskárny.

Jsou definovány osoby, které mají právo zveřejňovat veřejně přístupné informace o informačních systémech. Dále je zakázáno na veřejně přístupných systémech publikovat telefonní čísla, která oficiálně nepatří subjektům podílejících se na správě a provozu informačních systémů. Povoleno je pouze zveřejňování jmen oficiálních statutárních zástupců instituce.

Pravidla používání kryptografické ochrany dat, požadované vyhláškou o kybernetické bezpečnosti jsou definována v politice bezpečného používání kryptografické ochrany, o které píšu v jedné z následujících kapitol.

2.3.11 Politika řízení technických zranitelností

Uživatelům instituce se podle vnitřních směrnic zakazuje instalovat programy nebo provádět jiné změny v konfiguraci počítače, které by vedly k nežádoucímu chování zařízení, nebo vedly k nežádoucímu chování sítě.

Uživatel smí s technickým vybavením instituce manipulovat pouze na všeobecné uživatelské úrovni. Zásahy do techniky a sítí provádí pouze správa ICT.

Z technického hlediska je instalace programů částečně blokována zákazem zápisu do složek Program Files a Program Files (x86) pod uživatelským účtem a znemožnění uživatelům všech instalací, které vyžadují oprávnění správce.

Instalace rozšíření do používaného prohlížeče Google Chrome jsou blokovány skupinovými politikami a povoleny jsou jen explicitně definované výjimky, které se dají nainstalovat za využití účtu místního správce.

Z praktického pohledu vím, že jsou uživatelé schopni nainstalovat si některé menší programy do složek, kam zápis povolen mají. Blokování těchto instalací není technicky vyřešeno a omezuje se pouze ve směrnicích.

Pro opravy programového vybavení je politikou vyžadováno, aby při instalaci nové verze software byl pro případ potřeby připraven návrat k funkční verzi tohoto software.

2.3.12 Politika bezpečného používání mobilních zařízení

Uživatel, který má k dispozici služební mobilní zařízení, je podle směrnic povinen zařízení alespoň jedenkrát do měsíce přinést pracovníkům správy ICT ke kontrole zabezpečení a aktualizací.

Informace klasifikované jako citlivé mohou na mobilních zařízeních, jako jsou notebooky, tablety, nebo mobilní telefony, opustit prostory instituce pouze v šifrované podobě.

Instituce využívá programu pro šifrování disků všech zařízení, která opustí budovu instituce. Uživatelé, kterým se tato zařízení předávají, mají povinnost si při předání nastavit heslo, které musí zadat při každém spuštění šifrovaného služebního PC, nebo notebooku.

Pro služební mobilní telefony a tablety platí, že si pro ně uživatel při převzetí musí nastavit dostatečně silné heslo.

2.3.13 Politika akvizice, vývoje a údržby

Pro každou aplikaci je před jejím nákupem, nebo vývojem specifikována doba platnosti licence, rozsah licence, omezení licence, přístupy ke zdrojovým kódům, možnosti úprav zdrojových kódů pracovníky instituce, případně externími subjekty.

Všechny nové systémy, nebo změny systémů stávajících jsou z hlediska bezpečnosti posuzovány manažerem kybernetické bezpečnosti.

2.3.14 Politika ochrany osobních údajů

Jednotlivé typy osobních údajů, oprávnění přístupu k nim, lhůty k jejich zpracování, informace o předávání údajů jiným příjemcům, nebo předávání do zahraničí jsou podrobně definovány v interních dokumentech instituce v sekci GDPR.

2.3.15 Politika fyzické bezpečnosti

Všechny příjezdové cesty a vstupy k budově instituce jsou sledovány kamerovým systémem. Používané kamery jsou vzdáleně spravovány. Záběry vybraných kamer jsou pak promítány pracovníkům ostrahy jednotlivých budov, kteří mají za úkol sledovat, zda-li nedochází k nějaké podezřelé aktivitě nebo narušení bezpečnosti. Záznamy z kamer jsou ukládány a po určitou dobu zachovány. Pracovníci ostrahy také provádějí periodické obchůzky a kontroly prostor uvnitř i vně budovy.

Většina dveří je chráněna elektronickými zámky, které se odemknou privilegovaným zaměstnancům po přiložení přístupové karty. Pracovníci ostrahy mají dále na monitorech zobrazeny výstupy z aplikace, která umožňuje řízení a monitorování událostí a integruje v sobě EZS (elektronická zabezpečovací signalizace) a EPS (elektronická požární signalizace). Pracovníci ostrahy v aplikaci vidí stavy jednotlivých čidel a jsou systémem upozorněni například na jakékoliv násilné otevření dveří bez použití karty, nebo jiné rozpojení čidel v zastřežených místnostech v budově.

Dále podle bezpečnostních politik platí speciální pravidla budov i místností pro servery. Budovy musí mít pevnou konstrukci, aby do nich nebylo možno proniknout bez užití vysokého stupně násilí. Servery musí být umístěny v takových prostorech, které jsou fyzicky odděleny od ostatních prostor a omezí se tak přístup pouze pro oprávněné osoby. Všechny požadavky pro bezpečné umístění serverů jsou splněny.

2.3.16 Politika bezpečnosti komunikační sítě

Všechna koncová zařízení v jednotlivých kancelářích připojená k vnitřní síti instituce jsou ověřována protokolem RADIUS. Každý uživatel se k počítači přihlašuje doménovým účtem, který je spravován v Active Directory, odkud také zařízení dostává doménové politiky omezující povolené činnosti uživatele a zvyšující bezpečnost.

V politice je dále uvedeno, že musí být zajištěna deaktivace nevyužitých přípojných míst. To sice administrátoři dodržují a při odstranění zařízení z místnosti mají povinnost zneaktivnit zásuvku odpojením v serverové místnosti, ale někdy se může stát, že k odpojení nedojde.

Dostupnost síťových služeb na síti je automaticky testována a v případě nedostupnosti důležité služby jsou o této situaci informováni administrátoři vygenerovaným e-mailem.

Politika dále doporučuje pro všechna zařízení zajistit monitorování změn přiřazených hardwarových a logických adres síťových karet. Změna přiřazení IP nebo MAC adresy by totiž mohla znamenat, že v připojeném zařízení byla změněna síťová karta, nebo že se někdo pokouší falšovat totožnost při přístupu na síť.

Hlídání IP adres ani MAC adres jako takové sice v síti neprobíhá, využívá se ale RADIUS ověřování, přičemž zařízení, které není v doméně známo, spadne do odlišné VLAN, odkud není schopno případně způsobit žádné škody.

Stav a výkon serverů a jednotlivých aplikací je monitorován v System Center Operations Manager (SCOM).

Pod politiku bezpečnosti komunikační sítě patří i řízení přístupu uživatel, kde je cílem předcházet neoprávněným přístupům uživatelů k informačním systémům. Pro ověření identity uživatelů musí být využit takový autentizační mechanizmus, který podporuje vícefaktorovou autentizaci. Práva uživatelů v informačních systémech jsou vždy odvozena od identifikace daného uživatele. Uživatelská hesla musí být dlouhá nejméně 8 znaků (u významných informačních systémů 12 znaků), obsahovat písmeno, číslici a speciální znak. Hesla jsou platná po dobu 3 měsíců. Pro administrátory pak platí ještě vyšší nároky na komplexnost hesel.

Dále politika vyžaduje, aby vzdálená připojení byla šifrovaná, aby byla při vzdáleném přístupu požadována minimálně stejná míra autentizace jako při přístupu z vnitřní sítě, aby měl připojovaný uživatel aktualizovaný systém a používal antivirový program.

Pro vzdálené přístupy se v instituci používá aplikace, která podporuje vícefaktorovou autentizaci a šifrované spojení. Všechna zařízení půjčovaná uživatelům jsou chráněna antivirovým řešením a pro zařízení v osobním vlastnictví uživatelů platí, že musí podobnou ochranou disponovat.

Všechna tato opatření se zdají být v pořádku a jsou v instituci dodržována.

2.3.17 Politika ochrany před škodlivým kódem

Každá pracovní stanice má nainstalované vzdáleně spravovatelné antivirové řešení. Aktualizace antivirového software a virových databází na stanicích probíhá automaticky. Používané řešení umožňuje kontrolu jednotlivých souborů, kontrolu vyměnitelných médií, kontrolu spouštěných programů, automatický start se startem operačního systému a další.

2.3.18 Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí

Postupy reagování na bezpečnostní incidenty jsou dány v bezpečnostní politice, kde je definováno, kdo a jak incidenty prošetřuje, za řešení bezpečnostních incidentů je zodpovědný bezpečnostní ředitel.

Obecné postupy řešení detekovaných bezpečnostních událostí však nikde definovány nejsou. Taktéž pravidla a postupy nasazení nástrojů a pravidla a postupy jejich nastavení a optimalizace nikde definovány nejsou. Budu se proto k tomuto tématu vracet v další části mé práce, kde navrhnu doplnění bezpečnostních politik o tyto nedostatky.

Nástroje používané v organizaci:

- **GreyCortex Mendel IDS:** Nástrojem, kterým se budu v práci zabývat nejintenzivněji je produkt Mendel od Brněnské společnosti GreyCortex.
  Jedná se o nástroj k analýze síťového provozu schopný detekovat hrozby na základě známých signatur, poznat nežádoucí síťovou komunikaci a aktivitu uživatelů, infikované stanice a síťové útoky.
  Kromě rozlišování skrz známé signatury disponuje GreyCortex Mendel i komponentou NBA (Network Behaviour Analysis), která analyzuje datové toky skrz strojové učení a je schopna odhalit i nové, nebo neznámé hrozby a útoky i bez známých signatur.
  GreyCortex Mendel je také schopen zobrazovat datové toky na síti a vyhodnocovat korelace mezi událostmi.
  Tak jako jiné nástroje detekce a prevence vniknutí je GreyCortex Mendel schopen reagovat na vzniklé události a zabránit počítačovému útoku, než stihne způsobit škody.

- **Nástroj používaný k hlídání přístupů:** Používaný nástroj sleduje normální chování jednotlivých uživatelů sítě a je schopen zaslat výstrahu, případně zamezit komunikaci v případě, že by se vyskytla podezřelá aktivita. Také dokáže sledovat kam mají jednotliví uživatelé přístup a pomáhá nám jednoduše tyto přístupy upravovat.

2.3.19 Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Záznam událostí: Je nasazen nástroj, sledující na serverech výskyt událostí významných z hlediska bezpečnosti (auditní záznamy) tak, jak to vyžaduje bezpečnostní politika.

Zaznamenávány jsou všechny potřebné typy událostí a to například: změny uživatelských účtů a skupin, neúspěšně pokusy o přihlášení, výskyt škodlivého kódu, start a zastavení informačních systémů, změny konfigurace komponent informačních systémů, změny systémového času na NTP serverech, ruční změny času na komponentách informačních systémů.

Nástroje používané v organizaci:

- **SIEM:** Používaný nástroj je proaktivní SIEM, analyzující chování koncových uživatel a zařízení a aktivitu na síti. Nástroj používá umělou inteligenci a machine learning a je schopen detekovat známé i neznámé hrozby. Instituce jej používá zejména k monitoringu serverů.
- **Grafická nástavba pro SIEM:** Open source nástroj nastavený na míru tak, aby ve webovém prohlížeči zobrazoval grafické výstupy využitím údajů z nasbíraných logů.

Ochrana záznamů: Základní záznamy jsou uchovávány po dobu 3 měsíců a v případě významných informačních systémů pod správou instituce dle vyhlášky po dobu 12 měsíců.

Synchronizace času: Čas všech zařízení provozujících informační systémy, podporujících časovou synchronizaci je pravidelně automaticky synchronizován s určenými časovými servery.

Nástroje, které se starají o sběr záznamů, jejich agregaci a korelaci podle souvislostí a varování administrátorů nasazené jsou. Problém vidím v tom, že ačkoliv je to v politice uvedeno, není nijak hlídáno, aby určitý správce tyto záznamy denně analyzoval.

V politikách je definováno, že je potřeba události zaznamenávat, zaznamenané události vyhodnocovat a jak záznamy uchovávat. Není, ale konkrétně definováno, jak tyto události vyhodnocovat a jak se starat o nastavení implementovaných nástrojů.

2.3.20 Politika bezpečného používání kryptografické ochrany

Je využíváno kryptografických metod, algoritmů a klíčů, které jsou podle doporučení na internetových stránkách NÚKIB aktuálně považovány za odolné.

Dále je využíváno systému správy klíčů a certifikátů, který je schopen zajistit generaci, distribuci, uchování, změn, omezení platnosti, zneplatnění certifikátů a likvidaci klíčů a který umožňuje kontrolu a audit.

V instituci se pro interní použití využívá certifikátů z vlastní certifikační autority a uznávaných certifikátů jiných certifikačních autorit.

V případě certifikátů vlastní certifikační autority je správa prováděna na serveru instituce a v případě certifikátů jiných certifikačních autorit v zákaznických portálech daných autorit.

2.3.21 Politika řízení změn

Od dodavatelů informačních systémů jsou požadovány provozní dokumentace revidované alespoň jednou ročně, nebo v případě každé významné změny.

Dále je vyžadováno oddělení vývojového, testovacího a produkčního prostředí všech aplikací, které jsou součástí informačních systémů během celého životního cyklu aplikace. Musí být zajištěno, aby práva přístupu k vývojovému, respektive testovacímu prostředí nebyly automaticky sdílené s právy přístupu do produkčního prostředí a naopak.

Při změně jakékoliv části IS je požadováno vypracování dokumentace změny obsahující údaje jako popis změny, důvod, kdo změnu odsouhlasil, koho se změna dotkne, plán změny, plán testování a postup případné obnovy do funkčního stavu.

2.3.22 Politika zvládání kybernetických bezpečnostních incidentů

Za šetření bezpečnostních incidentů je v instituci zodpovědný bezpečnostní ředitel. Ten vyhodnotí závažnost incidentu, zajistí opatření k nápravě jeho důsledků a zamezí opakování události. Případně v rámci plnění povinností vyplývajících ze zákona o kybernetické bezpečnosti oznamuje incident podle vzoru formuláře z přílohy č. 8 vyhlášky o kybernetické bezpečnosti na NÚKIB určenou formou.

2.3.23 Politika řízení kontinuity činností

Je požadováno, aby bylo prováděno a dokumentováno hodnocení rizik, analýza možných dopadů kybernetických bezpečnostních incidentů a posouzení rizik souvisejících s ohrožením kontinuity činností instituce. Za provedení těchto úkonů je zodpovědný bezpečnostní ředitel.

Minimální úroveň poskytovaných služeb přijatelná pro užívání, provoz a správu informačních systémů, doba obnovení chodu minimální úrovně systémů, a bod obnovy dat jako časové období, během kterého musí být zpětně obnovena data po bezpečnostním incidentu nebo po selhání jsou definovány v politice řízení kontinuity činností, kterou schvaluje bezpečnostní ředitel.

K revizi plánů obnovy dochází jednou za 12 měsíců, nebo v případě závažné změny prostředí IS, plány obnovy jsou testovány jednou za 2 roky.

2.4 Další nalezené bezpečnostní problémy

2.4.1 Přihlašování do systému GreyCortex Mendel

Při analýze jsem zjistil, že se do systému všichni správci přihlašují stejným účtem „Administrator“.

Myslím si, že podle politik bezpečnosti komunikační sítě je tohle nedostačující a vyžaduje změnu. V současné době totiž není možné dohledat, kdo provedl změny v nastavení systému

2.4.2 Přístup do systému GreyCortex Mendel instituce z vnější sítě

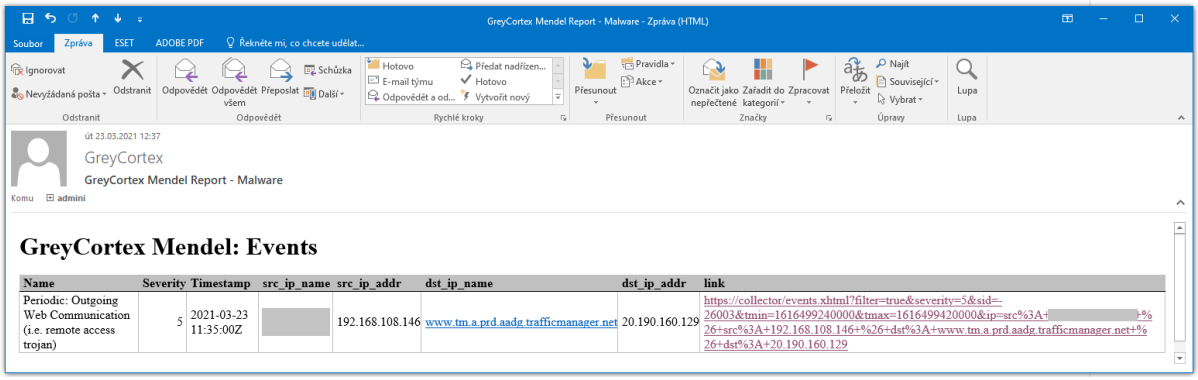
Při komunikaci s externisty ze support týmu GreyCortex bylo zjištěno, že jsou schopni do systému přistupovat z vnější sítě, bez použití VPN, jako tomu je v případě ostatních informačních systémů.

Ačkoliv se pro přístup do systému z vnější sítě musí přistupující stále autentizovat, je povolený přístup zvenčí chybějící vrstvou bezpečnosti, která by se dala vylepšit.

2.4.3 Doladění výstražných emailů generovaných GreyCortex Mendel IDS

Systém GreyCortex Mendel je v instituci momentálně nastaven tak, aby generoval výstražné e-maily a rozesílal je administrátorům v případě, že se objeví událost vyhodnocena se závažností (severity) 5, nebo vyšší.

E-maily mohou obsahovat různé typy informací, které se dají nastavit v systému pod účtem správce. Jednou z obsažených položek v e-mailu je link, který by měl po kliknutí otevřít webové rozhraní systému GreyCortex Mendel s podrobnostmi o dané události.



Obrázek č. 1: Výstražný e-mail ze systému GreyCortex Mendel
(Zdroj: dle výřezu sestavy programu GreyCortex Mendel)

Tento link je bohužel momentálně generován tak, že po kliknutí nepřesměrovává na korektní adresu, ale na název kolektoru.

2.5 Požadavky organizace

V současné době se e-mailové schránky administrátorů plnily varovnými e-maily, které pro ně v množství falešně pozitivních zpráv neměly vypovídající hodnotu. Manažer kybernetické bezpečnosti instituce od mé bakalářské práce očekává návrhy nastavení systémů monitoringu, zejména IDS, tak, aby se snížily počty falešně pozitivních zpráv a bylo tak možné se v dashboardech IDS a varovných e-mailech lépe orientovat. Cílem těchto změn je dosažení zvýšení bezpečnosti informací a bezpečnosti provozu všech informačních systémů v instituci. Dále pak požaduje poukázat na případně další nalezené bezpečnostní problémy zejména v rámci analýzy bezpečnostních politik.

2.6 Shrnutí analýzy

Vzhledem ke každoročnímu růstu nových zranitelností a příležitostí pro počítačových útok není možné zabezpečit síť proti všem hrozbám. Můžeme se ale snažit tomuto riziku předcházet. Aby se minimalizovalo riziko, že takový útok úspěšně proběhne, monitoring sítě je nezbytný.

Jelikož instituce již využívá několik systémů, monitorující různé oblasti sítě a zajišťující zabezpečení. Bude mým snažením spíše než navrhovat zabezpečení nová, správné nastavení stávajících systémů tak, aby se v nich dalo snadno orientovat a v případě náznaku podezřelých aktivit nebo nových hrozeb si jich v systému jednoduše všimnout a dokázat na ně reagovat. Když je totiž systém zahlcen množstvím falešně pozitivních záznamů o hrozbách, je pro správce velmi obtížné se v systému a množství informací orientovat.

Při analýze jsem narazil na několik problémů s nastavením IDS, jako je problém s účty správců IDS, problém s příchozími varovnými e-maily a v neposlední řadě již zmiňovaný problém s množstvím falešně pozitivních zpráv.

Z analýzy dále vyplynulo, že v instituci neexistují jednoznačná pravidla správy IDS. Budu se proto této problematice dále věnovat v následující části práce a navrhnu aktualizaci bezpečnostních politik, aby obsahovaly pravidla správy IDS.

V instituci také chybí pravidla postupy vyhodnocování záznamů z nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí a pravidla a postupy nastavení a optimalizace nástroje.

V bezpečnostních politikách instituce je dle mého názoru nedostatečně popsána politika přístupu k zálohám a ukládaným informacím a postupy testování zálohování a obnovy.

3 VLASTNÍ NÁVRHY ŘEŠENÍ

V kapitole vlastních návrhů řešení se budu věnovat návrhu konkrétních opatření, vedoucích ke zvýšení stavu bezpečnosti informací a bezpečnosti provozu všech informačních systémů.

Z analýzy současného stavu jsem zjistil, že si instituce v oblasti bezpečnosti nevede špatně a většinu potřebných náležitostí splňuje, i tak se ale najdou části bezpečnostních politik, které by si zasloužily revizi a vylepšení.

Projdu jednotlivé nedostatky bezpečnostních politik, odhalené v analytické části práce a případně navrhnu jejich úpravy, změny, nebo doplnění o chybějící informace.

Dále se budu věnovat nastavení nástroje pro detekci kybernetických bezpečnostních událostí, aby byla zvýšena jeho využitelnost tím, že nastavím některá nová pravidla pro falešně pozitivní zprávy a zvýším tak přehlednost systému.

Nakonec navrhnu některá další opatření k problémům, na které jsem narazil při nastavování nástroje pro detekci kybernetických bezpečnostních událostí a dalších dílčích systémů a částí, se kterými jsem se při řešení setkal, nebo je využíval.

3.1 Návrh aktualizací bezpečnostních politik

V této kapitole reviduji a navrhnu řešení některých nedostatků v bezpečnostních politikách instituce.

3.1.1 Návrhy změn v politice nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí

V závislosti na analýze bezpečnostních politik a doporučeních (případně požadavcích) vyhlášky navrhuji, aby byly v bezpečnostní politice, nebo jiném dokumentu přidány postupy řešení detekovaných bezpečnostních událostí, definována pravidla a postupy nasazení nástrojů detekce a pravidla a postupy jejich optimalizace.

Za aktualizaci bezpečnostních politik, případně vytvoření nového dokumentu je podle politik oddělení povinností zodpovědný bezpečnostní správce. Já se v této kapitole budu zabývat návrhem obsahu, který by nová dokumentace mohla obsahovat.

Pravidla a postupy nasazení nástroje pro detekci kybernetických bezpečnostních událostí:

V návrhu tohoto bodu bych navrhnul vycházet z bezpečnostní politiky řízení provozních změn. To znamená, že zodpovědná osoba vypracuje dokumentaci změny, kde uvede zejména popis a důvod změny, identifikaci rizik spojených se změnou a metody řízení těchto rizik. Dále by měla osoba zpracovat plán průběhu změny (projekt).

Dále bych navrhnul, aby nasazení nástroje proběhlo mimo provozní hodiny instituce, nejlépe ve večerních hodinách, nebo v den pracovního klidu. Nástroj by měl být nejdříve otestován v testovacím prostředí a před nasazením nového nástroje do ostrého provozu musí být připravena záloha pro případný návrat do původního funkčního stavu informačních systémů.

Postupy řešení detekovaných bezpečnostních událostí:

V tomto bodě bych navrhoval následující strukturu:

- Bezpečnostní správce, případně delegovaný administrátor operativně prošetří zjištěnou událost.
- Událost klasifikuje do jedné z kategorií: reálná hrozba, nebo falešně pozitivní zpráva.
- V případě nutnosti se poradí v tomto pořadí s: bezpečnostním správcem, manažerem kybernetické bezpečnosti, nebo externím specialistou.
- V případě, že je událost kategorizována jako reálná hrozba, postupuje podle bezpečnostní politiky zvládání kybernetických bezpečnostních incidentů.

Pravidla a postupy pro optimalizaci nastavení nástroje pro detekci kybernetických bezpečnostních událostí:

Navrhuji, aby byla jasně definována přesná časová rozmezí, kdy odpovědný správce provede důkladnější než každodenní analýzu záznamů IDS. Taktéž bude zodpovědný za kontrolu již nastavených pravidel pro určení falešně pozitivních zpráv a v případě jejich zastaralosti, o jejich úpravu, nebo smazání.

Každé nastavené pravidlo v aktuálně používaném nástroji pro detekci kybernetických bezpečnostních událostí (aktuálně systému GreyCortex Mendel), bude s dostatečnou srozumitelností popsáno adekvátním názvem. Případně budou další detaily uvedeny v poli „description“.

Tyto změny mají za cíl zajistit, že se v systému bude možné jednoduše a přehledně orientovat. A to i v případě, že by aktuálně zodpovědný správce měl být nahrazen správcem jiným.

O provedení této analýzy informuje zodpovědný správce svého nadřízeného e-mailem. Navrhuji, aby tato analýza probíhala jednou měsíčně.

Dále by měl existovat dokument, ve kterém by bylo definováno, kdo ze správců je zodpovědný za správu IDS GreyCortex Mendel a ostatních nástrojů monitoringu a kdo jej nahradí v případě jeho delší nepřítomnosti, nebo odstoupení z funkce.

3.1.2 Návrhy změn v politice využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Za vypracování dokumentace konkrétních pravidel a postupů je podle politik oddělení povinností zodpovědný bezpečnostní správce IS. Já se v této kapitole budu zabývat navržením obsahu, který by tato dokumentace měla obsahovat.

Ačkoliv je v politikách určeno, že by mělo vyhodnocení událostí probíhat na denní bázi, ne vždy je to kvůli množství ostatních povinností administrátorovi umožněno, navrhuji, aby byl každý den vyhrazen čas, kdy se zodpovědná osoba může této činnosti věnovat a z nástroje pro vyhodnocení událostí je využito maximum.

Pravidla a postupy pro evidenci a vyhodnocení kybernetických bezpečnostních událostí:

V tomto bodě bych navrhoval strukturu podobnou struktuře vyhodnocení detekovaných událostí z minulé kapitoly:

- Bezpečnostní správce, případně delegovaný administrátor denně ve stanovenou dobu prochází záznamy o událostech.
- V případě, že nalezne bezpečnostní událost, která ho zaujala, prošetří ji.
- Událost klasifikuje do jedné z kategorií: reálná hrozba, nebo falešně pozitivní zpráva.
- V případě nutnosti se poradí v tomto pořadí s: bezpečnostním správcem, manažerem kybernetické bezpečnosti, nebo externím specialistou.
- V případě, že je událost kategorizována jako reálná hrozba, postupuje podle bezpečnostní politiky zvládání kybernetických bezpečnostních incidentů.
- Vede záznamy o významných šetřených událostech, ke kterým se může on, případně další správci v budoucnu vracet.

Pravidla a postupy pravidelné aktualizace pravidel pro vyhodnocení kybernetických bezpečnostních událostí:

Nastavení a vyladění nástroje pro vyhodnocování kybernetických bezpečnostních událostí není jednorázová záležitost, ale nastavení je třeba pravidelně aktualizovat.

Měl by být stanoven interval, kdy se zodpovědný administrátor hlouběji, nad rámec každodenní analýzy, zamyslí nad nastavenými pravidly nástroje a aktualizuje je. Navrhuji, aby k tomu docházelo jednou měsíčně.

Pravidla a postupy pro optimální nastavení bezpečnostních vlastností nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí:

Je třeba definovat, jaký typ událostí nás zajímá a chceme se jimi zabývat. Události, které pro administrátory nemají hodnotu takového charakteru, že by se rozhodli je okamžitě řešit, mohou být obvykle označeny za falešně pozitivní, nebo alespoň nemusí pokaždé aktivovat výstrahu, když se v systému objeví.

Je dobré projít výchozí pravidla nastavená v systému od dodání, zbavit se nepotřebných pravidel a namísto nich vytvořit pravidla na míru pro dané prostředí. To pomůže ke snížení počtu falešně pozitivních zpráv a usnadní orientaci v systému.

Zodpovědný administrátor by dále měl při analýze zaznamenaných událostí v systému nastavovat závažnost událostí, které se zdají být zbytečnými na nižší. V systému pak snadněji uvidí nové záznamy událostí s vyšší závažností, namísto událostí se závažností nízkou, které mohou být obvykle ignorovány.

V případě že administrátor shledá zaznamenanou událost za falešně pozitivní, měl by kromě ignorování výstrahy zajistit vytvoření pravidla pro falešně pozitivní záznam, aby se toto stejné hlášení neopakovalo a výstrahy měly větší smysl.

3.1.3 Návrh změn v politice zálohování a obnovy a dlouhodobého ukládání

Z analýzy současného stavu vyplynulo, že v dokumentaci není jasně popsaná politika přístupu k zálohám a ukládaným informacím. A dále postupy testování zálohování a obnovy.

V této kapitole se budu zabývat návrhem obsahu těchto politik, za konečné zpracování politik je podle oddělení odpovědností zodpovědný bezpečnostní správce IS.

Politika přístupu k zálohám a ukládaným informacím

Vzhledem k tomu, že jsou zálohy ukládány na magnetických páskách, které jsou uloženy v trezoru umístěném v zabezpečené místnosti navrhuji, aby bylo v politikách doplněno, že pravidla přístupů k zálohám vycházejí z pravidel přístupů do serverových místností a trezoru, k jehož přístupu určuje oprávnění bezpečnostní ředitel.

Pravidla a postupy testování zálohování a obnovy

Testování obnovitelnosti záloh by bylo v reálném prostředí nákladné a složité, nemusí to být naštěstí nezbytný krok. Testovat obnovy záloh je možné i administrativně, a to hledáním postupů a míst, odkud budou obnovy procesů, stanovených jako stěžejních, probíhat.

V politikách by mělo být uvedeno, kdo a jak se o testování stará. Je důležité, aby testování plánu obnovy prováděli jiné zaměstnanci než ti, kteří se starají o samotné zálohování.

3.1.4 Návrh změn v politice bezpečnosti komunikační sítě

Navrhuji, aby bylo v bezpečnostní politice ukotveno, že je potřeba v určitém časovém intervalu hloubkově zkontrolovat nevyužitá přípojná místa a postarat se o jejich deaktivaci.

Ačkoliv mají administrátoři povinnost se o deaktivaci přípojných míst starat operativně a průběžně, někdy se stane, že na deaktivaci zapomenou.

Proto navrhuji, aby jednou ročně proběhla důkladná analýza a deaktivace nevyužitých míst.

3.2 Návrhy řešení dalších nalezených bezpečnostních problémů

3.2.1 Přihlašování do systému GreyCortex Mendel

Systém GreyCortex Mendel nabízí několik možností autentizace včetně přejímání účtů z doménového řadiče (LDAP), nebo autentizaci pomocí protokolu Kerberos.

Z důvodu bezpečnosti navrhuji pro každého ze správců, přistupujících do systému GreyCortex Mendel využívat minimálně lokálně vytvořený osobní účet, opatřený osobním, nesdíleným heslem o dostatečné komplexitě.

Lokální účet se dá vytvořit v nastavení GreyCortex Mendel pod účtem „Administrator“.

Další z výhod oddělených účtů pro každého správce je, že v případě provedení změn v systému bude dohledatelné, kdo změny provedl.

Poslední výhodou tohoto opatření, kterou zmíním, je záložka „Incidents“, ve které je možno v systému GreyCortex Mendel oznámit nalezený incident a označit jej k dalšímu řešení. Při oznámení incidentu je možné k němu přiřadit v záložce „Assignee“ osobu, která se bude řešením incidentu zabývat.

U zaznamenaných incidentů je pak v kartě „Incident detail“ možno k incidentu přidávat komentáře a komunikovat tak v diskuzi s ostatními správci, případně i s členy support týmu společnosti GreyCortex.

3.2.2 Přístup do systému GreyCortex Mendel instituce z vnější sítě

Situaci jsem konzultoval s bezpečnostním správcem IS, který je podle politik odpovědný za kontrolu oprávnění přístupů do IS a činností vyplývajících z bezpečnostních politik. Přednesl jsem mu informaci o volném přístupu do systému GreyCortex Mendel z vnější sítě a navrhoval přístup omezit pouze z vnitřní sítě, případně za použití VPN.

Po konzultaci jsme se rozhodli přístup ponechat, ale omezit jej nastavením pravidla výjimky na firewallu, pouze pro IP adresu support týmu.

3.2.3 Doladění výstražných emailů generovaných GreyCortex Mendel IDS

Po prozkoumání tohoto problému jsem se dozvěděl, že Mendel do odkazu vkládá název kolektoru a bohužel systém funkcionalitu změny tohoto nastavení momentálně neumožňuje.

Možným řešením ze strany instituce by bylo nastavení DNS záznamu tak, aby k názvu kolektoru byla přiřazena vnitřní adresa, na které se nachází rozhraní systému Mendel.

Dále bych chtěl poukázat na aktuálně nastavenou hodnotu závažnosti pro vygenerování výstražného e-mailu. Ze zkušeností vím, že u většiny událostí se závažností 5 a nižší se jedná o falešně pozitivní výstrahy. Navrhuji proto, aby byla hranice, od které se budou generovat výstražné e-maily zvýšena na 6.

3.3 Ladění IDS GreyCortex Mendel

Hlavním bodem ladění dashboardů bude rozlišení a určení falešně pozitivních zpráv pro zpřehlednění systému.

Cílem určování falešně pozitivních zpráv je eliminace zobrazení událostí, u kterých systém mylně vyhodnotil, že by se mohlo jednat o události nebezpečné, aby se síť zdála být čistou a nebyly následně přehlédnuty případné nové události.

3.3.1 Periodická komunikace na adresy spadající pod Microsoft

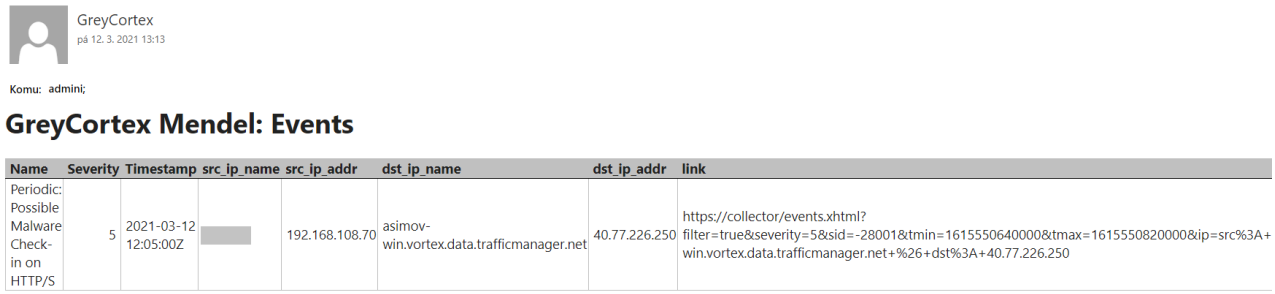
Podle aktuálních nastavení našeho GreyCortex Mendel IDS se v případě objevení události, která byla vyhodnocena se závažností 5 nebo více, vygeneruje varovný email, který se rozešle všem administrátorům.

V případě této události začaly přicházet emaily poukazující na periodickou komunikaci k prozkoumání, jelikož periodická komunikace může být náznakem přítomnosti nějakého malware.

Kromě přítomnosti malware může ale periodická komunikace znamenat dotazy na update, synchronizaci dat, nebo třeba aktualizace stránky v aplikacích, jako je například počasí. Z tohoto důvodu je tyto zjištění nutno prověřit a v případě, že se jedná o legitimní komunikaci, vytvořit pravidlo určující falešně pozitivní zprávu.

Z emailu lze vyčíst, že komunikace probíhá ze zařízení s vnitřní adresou 192.168.108.70 na adresu 40.77.226.250, označenou jako asimov-win.vortex.data.trafficmanager.net.

Systém události této periodické komunikace přiřadil závažnost 5. Dále by mělo jít z emailu využít přiloženého odkazu k přechodu do systému s automaticky předvyplněným polem filtrování na konkrétní událost, to ale bohužel nefunguje, jak by mělo a budu to řešit v jedné z následujících kapitol.



GreyCortex
pá 12. 3. 2021 13:13

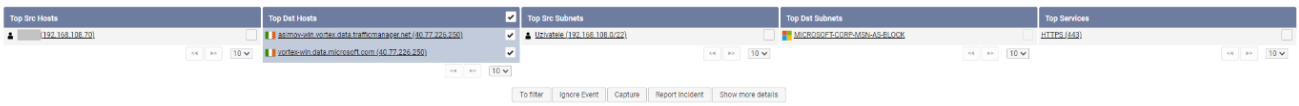
Komu: admini;

GreyCortex Mendel: Events

Name	Severity	Timestamp	src_ip_name	src_ip_addr	dst_ip_name	dst_ip_addr	link
Periodic: Possible Malware Check-in on HTTP/S	5	2021-03-12 12:05:00Z		192.168.108.70	asimov-win.vortex.data.trafficmanager.net	40.77.226.250	https://collector/events.xhtml?filter=true&severity=5&sid=-28001&tmin=1615550640000&tmax=1615550820000&ip=src%3A+win.vortex.data.trafficmanager.net+%26+dst%3A+40.77.226.250

Obrázek č. 2: Varovný email z GreyCortex Mendel IDS
(Zdroj: vlastní zpracování dle výřezu sestavy programu GreyCortex Mendel)

Pro více informací o dané události můžeme přejít do systému, obvykle použitím přiloženého odkazu v emailu, v tomto případě manuálním dohledáním události.

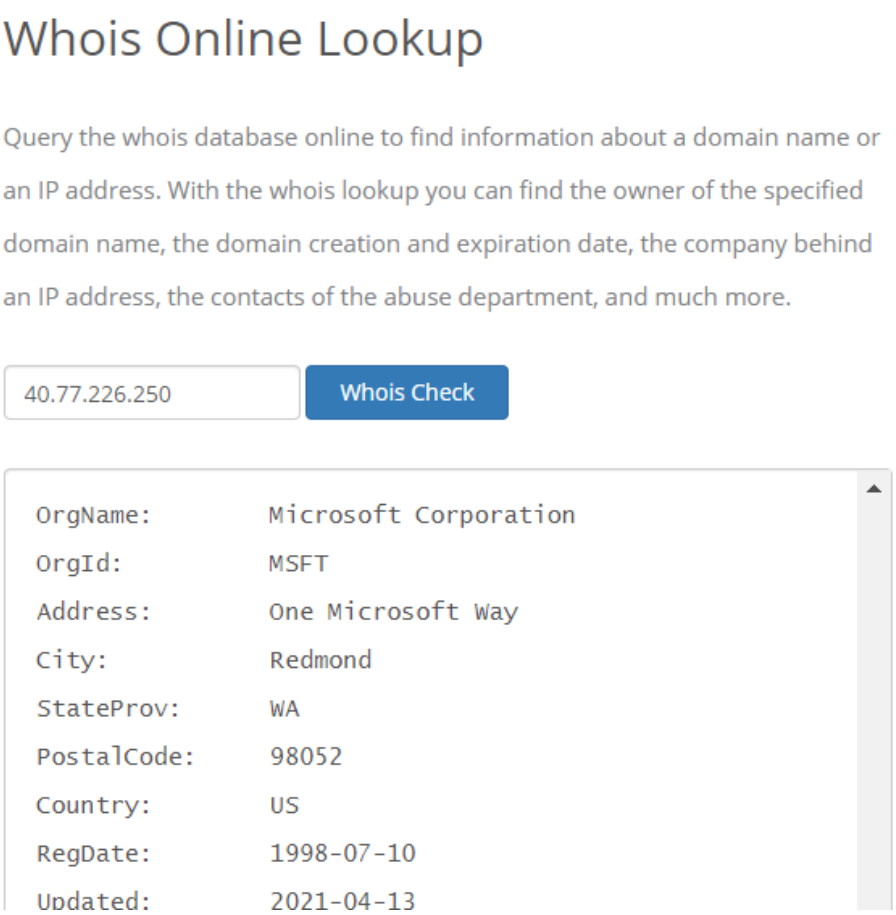


Obrázek č. 3: Podrobnosti o události kumunikace na adresu Microsoftu v systému GreyCortex Mendel
(Zdroj: vlastní zpracování dle výřezu sestavy programu GreyCortex Mendel)

Pro ověření legitimnosti domén a IP adres se dají využít webové stránky jako jsou například ipvoid.com, nebo virustotal.com.

Se znalostí vnitřní sítě organizace jsem schopen určit, že zdrojová adresa 192.168.108.70 se nachází ve VLAN určené pro pracovní stanice běžných uživatelů, která je definována pro podsíť 192.168.108.0/22.

Cílovou IP adresu jsem zkontroloval ve webové službě ipvoid.com a zjistil, že cílová adresa patří společnosti Microsoft.

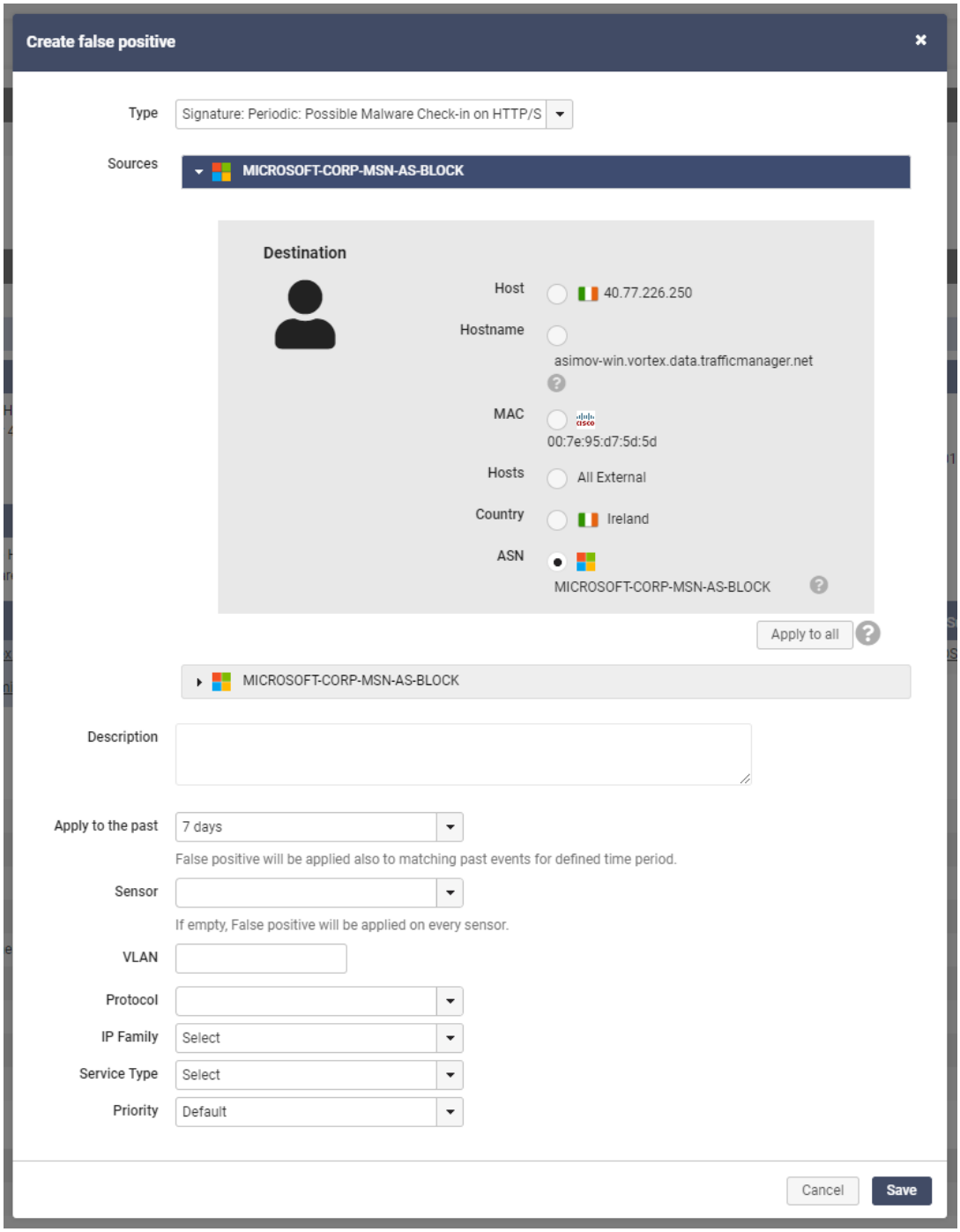


Obrázek č. 4: Kontrola podezřelé adresy na ipvoid.com
(Zdroj: vlastní zpracování dle výřezu zobrazení webu ipvoid.com)

Po kontrole cílové adresy a zjištění, že jde o ověřené Microsoft servery, na které bývají zařízeními s operačním systémem Windows odesílány telemetrické údaje, lze předpokládat, že se jedná o falešně pozitivní zjištění a bezpečnou komunikaci. Tudíž jsem se rozhodl tuto událost definovat jako false positive.

Označení události jako false positive je v systému Mendel poměrně jednoduché a dá se definovat pomocí zdrojové adresy, cílové adresy, služby, nebo portu. U zdrojových a cílových adres se dá dále zvolit, zda-li chceme definovat IP adresu, MAC adresu, hostname, nebo třeba ASN.

Po zvolení „Ignore event“ se zobrazí vyskakovací okno s nabídkou nastavení pravidla pro definici falešně pozitivního záznamu. Vzhledem k tomu, že může podobná komunikace probíhat na více různých IP adres patřících Microsoftu, rozhodl jsem se zvolit označení celého Microsoft ASN - MICROSOFT-CORP-MSN-AS-BLOCK, čili autonomního systému zahrnujícího skupiny rozsahů IP adres pod společnou správou Microsoftu. Stisknutím tlačítka „Save“ se nastavení pravidla aplikuje.

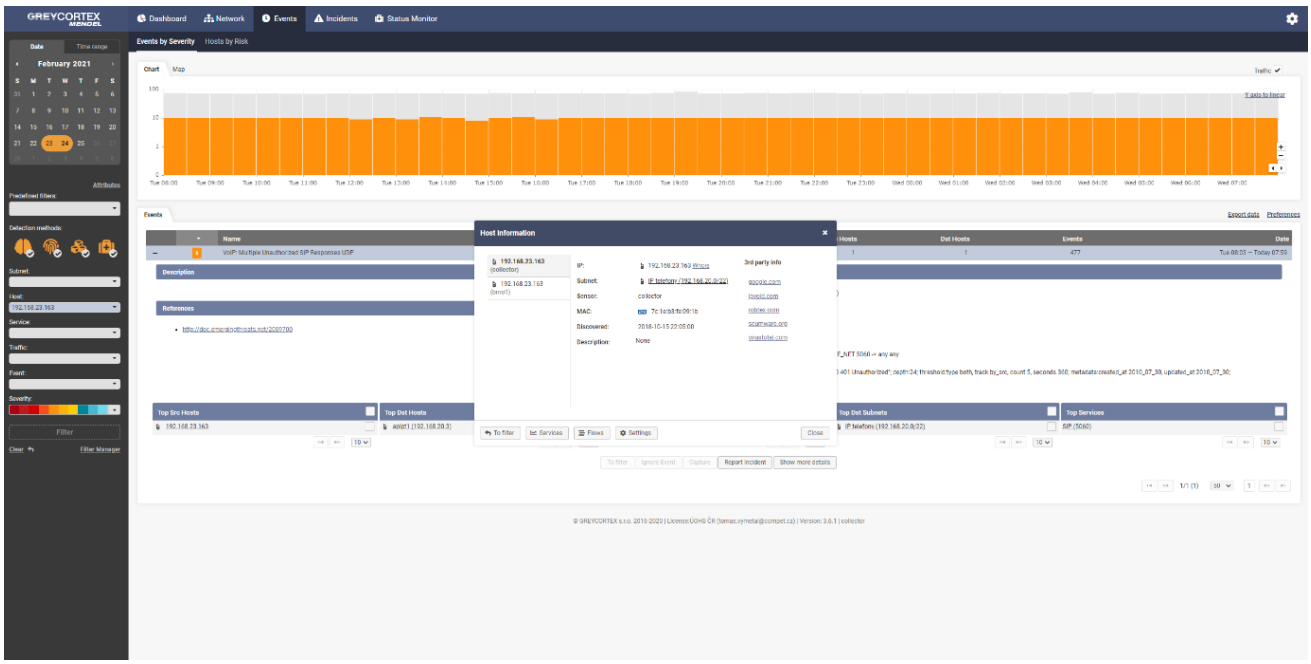


Obrázek č. 5: Vytvoření pravidla falešně pozitivního záznamu v systému GreyCortex Mendel.
(Zdroj: vlastní zpracování dle výřezu sestavy programu GreyCortex Mendel)

Podobně jako pro ASN MICROSOFT-CORP-MSN-AS-BLOCK jsem vytvořil pravidla pro ASN Microsoft Corporation a AKAMAI-AS, které také bývají využity pro telemetrii Microsoftu.

3.3.2 Periodická komunikace dveřníku

Další z alarmujících událostí o probíhající periodické komunikaci jsem si v systému GreyCortex Mendel všiml poměrně jednoduše, jelikož ji systém přiřadil závažnost 6.



Obrázek č. 6: Podrobnosti o události komunikace dveřníku v GreyCortex Mendel
(Zdroj: vlastní zpracování dle výřezu sestavy programu GreyCortex Mendel)

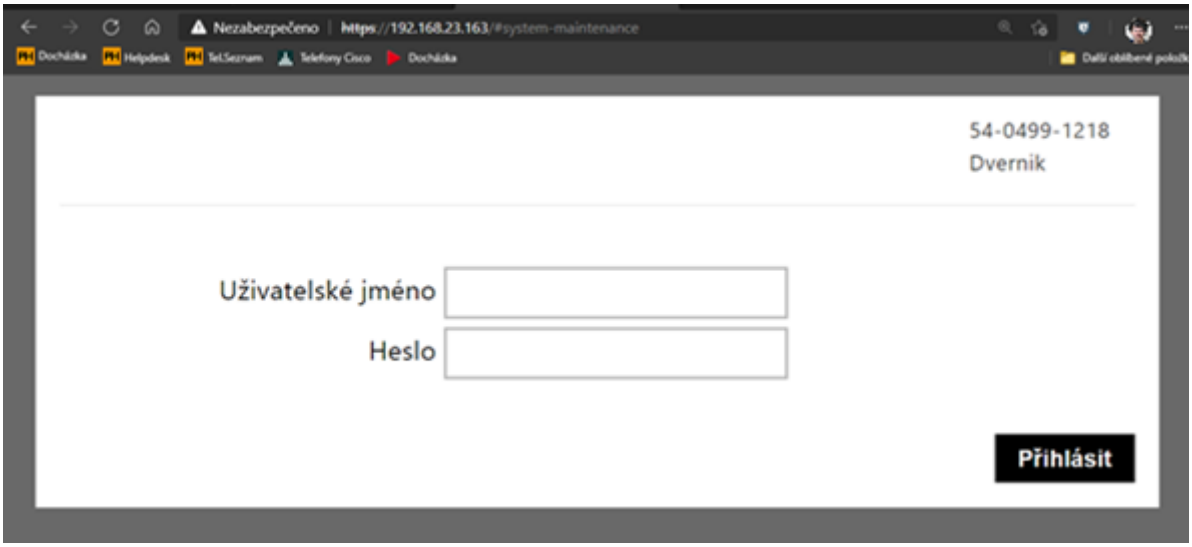
Po zobrazení podrobností o události v GreyCortex Mendel vidím, že tato komunikace probíhá z vnitřní adresy instituce 192.168.23.163 na taktéž vnitřní adresu instituce 192.168.20.3.

Pro zjištění, co za adresami stojí, jsem nahlédl do sdílené tabulky v Microsoft Excel, kterou používá oddělení ICT k evidenci IP adres. Zjistil jsem, že zdrojová adresa náleží dveřníku kanceláře v jedné z budov instituce. Cílová adresa pak náleží Call Manageru.

Vzhledem k tomu že se jedná o dveřník snažící se komunikovat s Call Managerem, je pravděpodobnější, že se jedná o chybový stav, nebo miskonfiguraci, než že by se jednalo o známku malware.

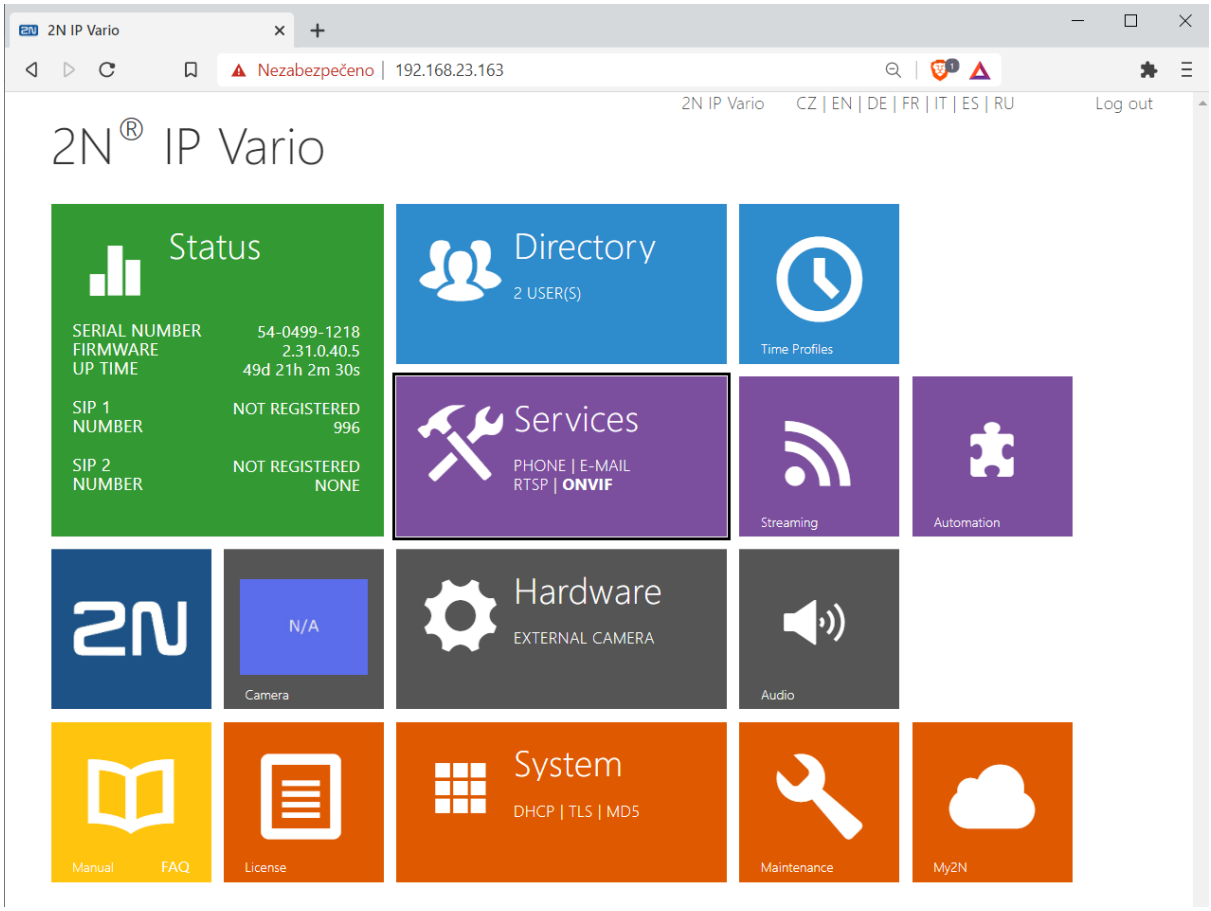
I přes to že se nejedná o malware, je v takovýchto případech lepší, než slepě označit událost jako falešně pozitivní, pokusit se vyřešit problém tam, kde je jeho příčina. Omezí se tak přílišné zahlcení systému IDS pravidly, která by do budoucna neměla užitek, kromě filtrování chybové komunikace dveřníků.

Při pokusu o vyřešení problému se pokusím přihlásit přímo do nastavení dveřníku přes webové rozhraní z IP adresy dveřníku.



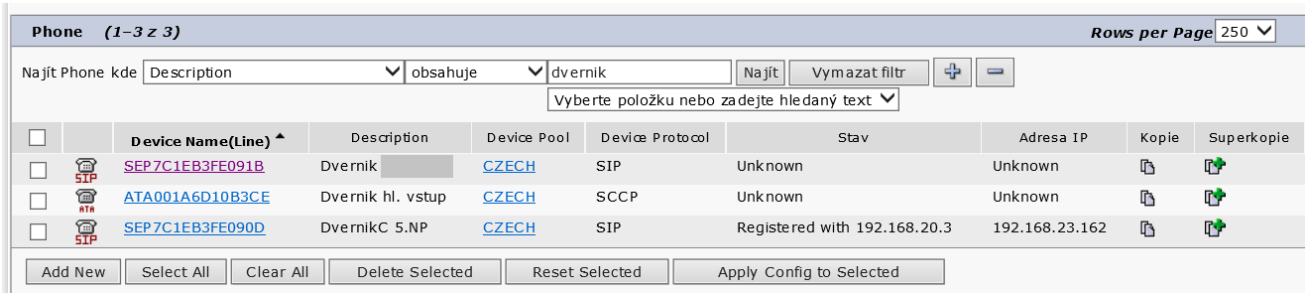
Obrázek č. 7: Přihlášení do webového rozhraní dveřníku
(Zdroj: vlastní zpracování dle výřezu webového rozhraní dveřníku)

Po přihlášení do webového rozhraní správy dveřníku již vidím, o jaký dveřník se přesně jedná a také vidím, že dveřník není zaregistrovaný ke call manageru.



Obrázek č. 8: Webové rozhraní dveřníku
(Zdroj: vlastní zpracování dle výřezu webového rozhraní dveřníku)

Dalším krokem, který jsem podstoupil bylo vyhledání dveřníku přímo v Call Manageru, ke kterému se dveřník neúspěšně snaží zaregistrovat.



Obrázek č. 9: Dveřníky v Call Manageru
(Zdroj: vlastní zpracování dle výřezu sestavy Call Manageru)

Daný dveřník jsem našel a zjistil, že ačkoliv jej Call Manager na síti vidí, opravdu k němu není zaregistrovaný. Zajímavostí bylo, že dveřník stejného typu, s IP adresou 192.168.23.162, nacházející se v pátém patře budovy, se k Call Manageru úspěšně zaregistroval.

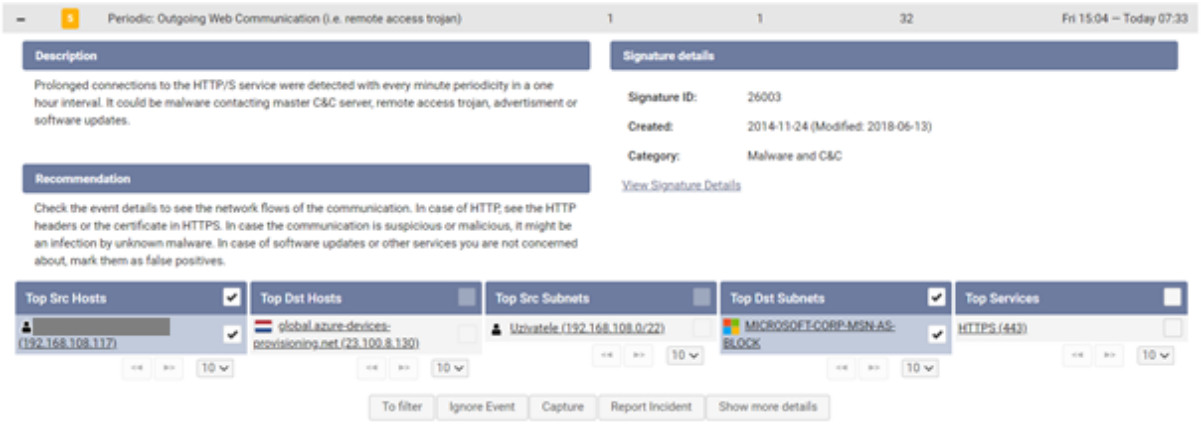
Porovnal jsem proto nastavení obou dveřníků jak v Call Manageru, tak v jejich webových rozhraních. Nastavení jsem sladil podle funkčního dveřníku, ale problém to nevyřešilo. Taktéž jsem problémový dveřník po záloze jeho nastavení resetoval do továrního nastavení a z oficiálních stránek výrobce dveřníku jsem stáhl nejnovější verzi firmware a aktualizoval jej. Bohužel ani to problém nevyřešilo.

Po dohodě s vedením jsme se rozhodli odložit řešení problému s dveřníkem do doby, než bude zrealizován přechod na nový Call Manager, k čemuž dojde v průběhu tohoto roku.

Prozatím jsem komunikaci dveřníku s Call Managerem označil v IDS jako falešně pozitivní zprávu.

3.3.3 Periodická komunikace telekonferenčního zařízení

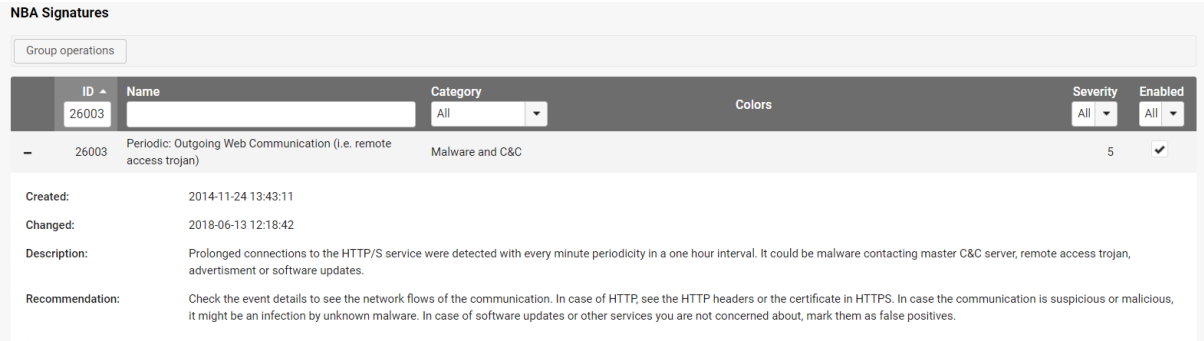
Dalším zařízením, které v systému IDS vyvolává každou minutu záznam o periodické komunikaci a ztěžuje tak orientaci v systému bylo poměrně nově nainstalované telekonferenční zařízení.



Obrázek č. 10: Podrobnosti o události komunikace telekonferenčního zařízení v GreyCortex Mendel
(Zdroj: vlastní zpracování dle výřezu sestavy programu GreyCortex Mendel)

Ačkoliv by se mohlo zdát, že událost vypadá stejně jako událost periodické komunikace na Microsoft servery řešené v jedné z předchozích kapitol, tato událost nebyla vyfiltrována pomocí dříve nastaveného pravidla, jelikož systém GreyCortex Mendel rozeznal jiný druh rozpoznávacího vzorku hrozby.

V systému je možno zobrazit podrobnosti o daném vzorku kliknutím na „View Signature Details“, případně dohledáním v Settings->Detection->NBA Signatures. V této záložce Mendel i doporučuje kroky, které je dobré podstoupit pro rozlišení, zda se jedná o falešně pozitivní zprávu.



Obrázek č. 11: Detaily vzorku – Periodic: Outgoing Web Communication
(Zdroj: vlastní zpracování dle výřezu sestavy programu GreyCortex Mendel)

Po kontrole nového zařízení na přítomnost malware a původu cílové IP adresy, patřící taktéž Microsoftu, jsem se rozhodl zprávu také označit jako falešně pozitivní.

ZÁVĚR

Ve své bakalářské práci jsem se zabýval návrhy k vylepšení managementu bezpečnosti organizace v oblasti bezpečnostních politik a vyhodnocení událostí. Kde mým hlavním snažením bylo navrhnout opatření, vedoucí ke zvýšení bezpečnosti informací a bezpečnosti provozu všech informačních systémů, zabývat se změnami nastavení systémů pro sledování kybernetických bezpečnostních událostí na síti a vyhodnocovat, zda se jedná o bezpečnostní hrozby, nebo falešně pozitivní zprávy.

V první části práce jsem uvedl základní teoretická východiska, vysvětlující základní pojmy z oblasti počítačových sítí a bezpečnosti informačních a komunikačních technologií.

V analýze současného stavu jsem se zabýval zejména analýzou bezpečnostních politik instituce vycházejících z vyhlášky 82/2018 Sb. o kybernetické bezpečnosti a zákona 181/2014 Sb. o kybernetické bezpečnosti. Zároveň jsem se v analýze současného stavu snažil odhalit nedostatky instituce v oblasti bezpečnosti informací a bezpečnosti provozu všech informačních systémů, poukázat na chybějící pravidla správy nástrojů pro detekci kybernetických bezpečnostních událostí a další nastavení, která by stála za vylepšení.

V návrhové části jsem se pak zabýval návrhy konkrétních úprav bezpečnostních politik, ladění nastavení nástroje GreyCortex Mendel pro detekci kybernetických bezpečnostních událostí a návrhy změn dalších nastavení a nedostatků objevených v rámci analýzy současného stavu.

Jelikož se mi podařilo naplnit stanovených cílů mé práce, a byť jen minimálně zvednout úroveň bezpečnosti informací a bezpečnosti provozu všech informačních systémů instituce, považuji mé snažení za úspěšné.

SEZNAM POUŽITÉ LITERATURY

[1] ENDORF, Carl, Eugene SCHULTZ a Jim MELLANDER. Detekce a prevence počítačového útoku. Přeložil Ivo BLACHOWICZ. Praha: Grada Publishing, 2005. 335 stran. ISBN 80-247-1035-8.

[2] SOSINSKY, Barrie A.. *Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]*. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.

[3] THOMAS, Thomas M.. *Zabezpečení počítačových sítí bez předchozích znalostí*. Brno: CP Books, 2005. ISBN 80-251-0417-6.

[4] DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP: bezpečnost. Praha: Computer Press, 2003. ISBN 80-7226-849-X.

[5] SHIELDS, G. The Shortcut Guide to Network Management for the Mid-Market [online]. Realtimepublishers.com, 2007. ISBN 978-1-9314-9172-3. Dostupné z: https://www.realtimepublishers.com/chapters/1197/sgnmm-1.pdf

[6] NORTHCUTT, Stephen. Bezpečnost sítí: velká kniha. Brno: CP Books, 2005. ISBN 80-251-0697-7.

[9] Digitální certifikát – WikiKnihovna. [online]. Poslední změna 9. Prosinec 2021 09:49[cit. 2021-05-05]. Dostupné z: https://wiki.knihovna.cz/index.php?title=Digit%C3%A1ln%C3%AD_certifik%C3%A1t

[10] Šifrování dat [online]. San Francisco (CA): Wikimedia Foundation, Poslední aktualizace 29. prosinec 2020 19:50 [cit. 2021-05-06]. Dostupné z https://cs.wikipedia.org/wiki/%C5%A0ifrov%C3%A1n%C3%AD_dat

[11] *Intrusion Detection System* [online]. San Francisco (CA): Wikimedia Foundation, Poslední aktualizace 12. únor 2019 06:10 [cit. 2021-03-25]. Dostupné z: https://cs.wikipedia.org/wiki/Intrusion_Detection_System

[12] KENT, Karen. SOUPPAYA, Murugiah. Guide to Computer Security Log Management: Recommendations of the National Institute of Standards and Technology [online]. Gaithersburg: NIST, Září 2006. 72 s. SP800-92. Dostupný z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

[13] RFC 3164. The BSD syslog Protocol [online]. C. Lonvick. August 2001. [cit. 2021-02-27]. Dostupný z: https://www.ietf.org/rfc/rfc3164.txt

[14] RFC 5424. The Syslog Protocol [online]. R. Gerhards. March 2009. [cit. 2021-02-27]. Dostupný z: https://www.ietf.org/rfc/rfc5424.txt

[15] ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Sbírka zákonů České republiky [online]. 2014, částka 75. Dostupný také z: https://www.zakonyprolidi.cz/cs/2014-181

[16] ČESKO. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: Sbírka zákonů České republiky [online]. 2018, částka 43. Dostupný také z: https://www.zakonyprolidi.cz/cs/2018-82

[17] Bezpečnostní politika (Security policy) - ManagementMania.com. [online]. Copyright © 2011. Poslední změna 20-06-2018 [cit. 2021-04-05]. Dostupné z: https://managementmania.com/cs/bezpecnostni-politika-security-policy

[18] DOUCEK, P. Bezpečnost IS/ICT a proces globální integrace. AT&P Journal. 2005, č. 1, s. 65 - 68. ISSN 1335-2237.

[19] *Antivirový program* [online]. San Francisco (CA): Wikimedia Foundation, Poslední aktualizace 10. listopad 2020 09:38 [cit. 2021-04-05]. Dostupné z: https://cs.wikipedia.org/wiki/Antivirov%C3%BD_program

[20] HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. Praha: Computer Press, 2001, p. 69. ISBN 80-7226-566-0.

SEZNAM POUŽITÝCH OBRÁZKŮ