UNIVERZITA PARDUBICE

FAKULTA EKONOMICKO-SPRÁVNÍ

BAKALÁŘSKÁ PRÁCE

2022 Kopytin Dmytro

Univerzita Pardubice

Fakulta ekonomicko-správní

Zabezpečení technologické firmy proti kyberšpionáži

Bakalářská práce

2022 Kopytin Dmytro

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Dmytro Kopytin**
Osobní číslo:	**E20824**
Studijní program:	**B0688A140004 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Zabezpečení technologické firmy proti kyberšpionáži**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je navrhnout zabezpečení technologické firmy proti kyberšpionáži.

Osnova:
- Popis stávajících způsobů kyberšpionáže a způsoby ochrany před ní.
- Formulace specifik technologických firem.
- Navržení zabezpečení modelové technologické firmy proti kyberšpionáži.

Rozsah pracovní zprávy: **Cca 35 stran.**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

BAŠTA, P., KOLOUCH, J. *CyberSecurity*. CZ.NIC, 2019. ISBN: 978-80-88168-31-7.
BELOUSOV, A., SOLODUKHA, V. *Základy kybernetické bezpečnosti*. Normy, koncepce, metody a prostředky zajištění. Moskva: Technosféra, 2021. ISBN 978-5-94836-612-8.
KATORIN, J., et al. *Velká encyklopedie průmyslové špionáže*. 2. dopl. vyd. Petrohrad: Polygon, 2000. ISBN 5-89173-106-1.

Vedoucí bakalářské práce: **doc. Ing. Miloslav Hub, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2022**
Termín odevzdání bakalářské práce: **30. dubna 2023**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

RNDr. Ing. Oldřich Horák, Ph.D. v.r.
vedoucí ústavu

V Pardubicích dne 1. září 2022

Prohlašuji:

Práci s názvem Zabezpečení technologické firmy proti kyberšpionáži jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny seznamu použité literatury

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně nebo doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 29.02. 2023

Dmytro Kopytin

Poděkování

Chtěl bych poděkovat vedoucímu mé bakalářské práce panu doc. Ing. Miloslavovi Hubovi, Ph.D., za poskytnuté cenné rady, odborné vedení, vstřícnost a trpělivost, které mi pomohly vypracování mé bakalářské práce. A chtěl bych poděkovat mé rodině a kamarádům za podporu a trpělivost během mého studia na univerzitě,

Anotace

Tato práce se zabývá zabezpečením technologické firmy před kyberšpionáží. V úvodu práce jsou vysvětleny základní pojmy a principy kyberšpionáže a jsou popsány různé techniky, které mohou být použity k neoprávněnému sběru informací o firmě a jejích zákaznících. Dále jsou analyzovány bezpečnostní hrozby, kterým může být technologická firma vystavena, včetně phishingu, ransomware a útoků na sítě. V další části práce jsou popsány různé nástroje a technologie, které mohou být použity pro detekci a prevenci kyberšpionáže, jako jsou firewally, antivirové programy, šifrování a správa hesel. V závěru práce jsou prezentována doporučení, jak ochránit technologickou firmu před kyberútoky, včetně pravidelné aktualizace softwaru a hardwaru, pravidelného zálohování dat, zavedení bezpečnostní politiky, pravidelného školení zaměstnanců a monitorování kyberbezpečnosti. Cílem této práce je poskytnout technologickým firmám ucelený přehled o kyberšpionáži a navrhnout účinná opatření pro zlepšení jejich kyberbezpečnosti.

Klíčová slova

Kybernetická bezpečnost, kybernetická špionáž, hacker

Title

Securing a technology company against cyberespionage

Annotation

This work deals with the security of a technological company against cyber espionage. The introduction explains the basic concepts and principles of cyber espionage and describes various techniques that can be used for unauthorized collection of information about the company and its customers. The work further analyzes security threats that a technological company may face, including phishing, ransomware, and network attacks. In the next section, various tools and technologies that can be used for detecting and preventing cyber espionage are described, such as firewalls, antivirus programs, encryption, and password management. In the conclusion, recommendations are presented on how to protect a technological company against cyber attacks, including regular software and hardware updates, regular data backups, implementing security policies, regular employee training, and monitoring of cyber security. The aim of this work is to provide technological companies with a comprehensive overview of cyber espionage and suggest effective measures to improve their cyber security.

Keywords

Cyber security, cyber espionage, hacker

Obsah

Seznam obrazků

Seznam zkratek a značek

ACC – Avigilon Control Center

AD – Active Directory

CIA – Central Intelligence Agency

DNS – Domain Name Service

ICMP – Internet Control Message Protocol

IKT – Informační kybernetické systémy

ISO – International Organization for Standardization

IT – Informační technologie

KZ – Kyberzločin

NIST – Národního institutu pro standardy a technologie

PTPC – Pomocné technické prostředky a systémy

TCP – Transmission Control Protocol

TPPI – The Perforated Plate Interceptor

UDP – User Datagram Protocol

Úvod

Kybernetická bezpečnost hraje zásadní roli v životě moderní informační společnosti, ve které je většina pracujících zaměstnána výrobou, skladováním, zpracováním a realizací různých informací. Obecně platí, že v rámci kybernetické bezpečnosti dnes rozumíme soubor různých konceptů, doktrín, strategií, metod a prostředků na ochranu před útoky útočníků (hackerů) na počítače, servery, informační systémy, datové sítě, mobilní zařízení atd.

Téma "Zabezpečení technologické firmy proti kyberšpionáži" je důležité a aktuální v moderním světě, kde kyberútoky na počítačové systémy a sítě se stávají stále běžnějšími a ničivějšími. Firmy, zejména technologické, které pracují s důvěrnými informacemi, musí zajistit bezpečnost svých systémů a dat, aby se chránily před potenciálními hrozbami.

K zajištění bezpečnosti počítačových systémů technologických firem je nutné přijímat různá opatření, jako je využívání technických, právních a organizačních opatření k prevenci kyberútoků. To může zahrnovat použití multifaktorové autentizace, šifrování dat, sledování sítě, ochranu před škodlivými programy, vytváření právních politik a postupů pro ochranu práv a důvěrných informací, pravidelné ověřování zranitelnosti systémů a sítí a také školení a zvyšování povědomí zaměstnanců o kyberbezpečnosti. Organizace, které nezajistí dostatečnou ochranu svých systémů a dat, se mohou stát obětí kyberútoků a utrpět vážné ztráty v podobě úniku důvěrných informací, finančních ztrát a poškození reputace. Proto zajištění bezpečnosti informačních systémů a dat je důležitým faktorem pro technologické firmy, které chtějí ochránit své obchodní operace a nadále růst v konkurenčním prostředí.

1. Klasifikace, způsoby a objekty kyberšpionáže

1.1. Typy kyberšpionáže a kyberzločinců

Kyberšpionáž zahrnuje neoprávněné a nezákonné získání přístupu ke chráněným informacím s různými cíli [1]. Toto se děje obcházením počítačových bezpečnostních systémů a často se používají speciální spyware, hardwarové a softwarové trojské koně. Hacking bezpečnostních systémů se provádí přes internet a místní sítě, stejně jako fyzický přístup. V mnoha zemích je kyberšpionáž považována za trestný čin, ale kvalifikace jednotlivých skutků jako kyberšpionáže závisí na konkrétních okolnostech případu. V závislosti na cílech může být kyberšpionáž rozdělena do následujících kategorií [2]:

- politická kyberšpionáž;
- ekonomická kyberšpionáž;
- vojenská kyberšpionáž;
- smíšená kyberšpionáž.

Pod ekonomickou kyberšpionáží se obecně rozumí jak krádež přímo finančních informací, tak snaha nelegálně proniknout do databáze s inovativním vývojem v oblasti vědy, techniky, průmyslu včetně know-how.

Jako další kritérium pro klasifikaci kyberšpionáže se používají následující úrovně [3]:

- mezinárodní;
- státní;
- regionální.

S tím, jak se tento jev neustále zvětšuje, roste ve světě i stupeň jeho nebezpečí. Většina aktivních hackerských skupin a seskupení se obvykle neomezuje pouze na rámce jedné země.

Kyberšpionáž je také klasifikována podle předmětu útoku. Akce útočníků mohou být namířeny proti [4]:

- vysoce postavených jednotlivců,
- podniky, korporace, průmyslové podniky,
- státní struktury, včetně obranných útvarů.

Klasifikace kyberšpionáže různými odborníky se provádí i z jiných důvodů: v závislosti na velikosti způsobené škody, způsobech dopadu, délce trvání v čase, počtu zapojených osob, právních důsledcích apod.

Hrozby mohou pocházet z tajných služeb a hackerských skupin. U kriminálních živlů není kyberšpionáž samoúčelná, ale součástí jejich činnosti jsou skupiny působící z ideologických a (nebo) materiálních důvodů.

Kyberšpionáž může zahrnovat i fyzickou infiltraci, ale v posledních letech se až 90 % všech útoků provádí prostřednictvím internetu nebo místních sítí [5]. Vládní organizace jsou zvláště zranitelné na svých oficiálních webových stránkách, firemních blogech, webových stránkách zaměstnanců a osobních účtech. Ochrana serverů je rovněž velmi důležitá. Kyberzločinci monitorují činnosti velkých IT společností jako Microsoft nebo Apple, aby mohli využít odhalených zranitelností a obejít bezpečnostní opatření. Pravděpodobnost útoku se zvyšuje s rostoucí popularitou dané služby nebo organizace. Sledují činnost prostřednictvím velkých vyhledávačů, sociálních sítí, poslů, známých portálů a také služeb jako Google, YouTube, Facebook a Skype, které také představují potenciální nebezpečí.

1.2. Způsoby provádění kyberšpionáže

Existují různé způsoby, jak se provádí kyberšpionáž, zahrnující následující [6]:

Phishing

Phishing je technika sociálního inženýrství, která se používá ke získávání důvěrných údajů. Může být prováděna prostřednictvím e-mailů, webových stránek sociálních sítí nebo komunikačních aplikací. Například hacker může zaslat e-mail, který vypadá legitimně, ale ve skutečnosti žádá o přihlašovací údaje k účtu.

Malware

Malware může být využito k získání důvěrných informací. Například trojské programy mohou zaznamenávat vše, co uživatel na klávesnici zadá, a spyware může shromažďovat informace o tom, jak uživatel používá počítač.

Kybernetická špionáž

Kybernetická špionáž představuje proces získávání důvěrných informací s využitím technických prostředků, jako jsou programy pro vzdálený přístup a špionážní aplikace. Například kyberšpióni mohou využít software pro vzdálený přístup k získání přístupu k vzdálenému počítači a shromažďování informací.

Objekty kyberšpionáže mohou být různé a závisí na cíli kyberšpiónů. Mezi nejčastější objekty patří [7]:

Korporace

Korporace jsou objekty kyberšpionáže, protože obsahují velké množství důvěrných informací, jako jsou finanční údaje a patenty. Kyberšpióni mohou usilovat o získání přístupu k těmto informacím a využít je pro své účely.

Vlády

Vlády jsou objekty kyberšpionáže, protože obsahují důvěrné informace, jako jsou státní bezpečnostní tajemství a vojenské informace. Kyberšpióni mohou usilovat o získání přístupu k těmto informacím a využít je pro své vlastní zájmy.

Individuální uživatelé

Individuální uživatelé mohou také být objektem kyberšpionáže. Hackeři se mohou pokusit získat přístup k osobním informacím, jako jsou čísla sociálního zabezpečení a bankovní údaje, aby je použili k podvodným účelům.

Veřejné organizace

Veřejné organizace mohou také být objektem kyberšpionáže. Tyto organizace obsahují důvěrné informace, jako jsou osobní údaje, zdravotnictví a finance. Kyberšpióni se mohou pokusit získat přístup k těmto informacím, aby je použili k podvodným účelům nebo je prodali na černém trhu.

1.3. Klasifikace kyberzločinců

Jako kyberzločinci jsou obvykle klasifikováni podle typu zločinu, kterého se dopouštějí, a podle jejich motivace. Mezi běžné typy kyberzločinců patří [8]:

- Hacker: Osoba s technickými znalostmi a schopnostmi, která používá počítačové systémy k neoprávněnému vstupu do cizích počítačových sítí nebo k poškozování či odcizování dat. Hacker může být bílý, šedý nebo černý.
- Malware autor: Osoba, která vytváří škodlivý software, jako jsou viry, trojské koně nebo spyware, a distribuuje ho na počítačových systémech bez svolení uživatele.
- Phisher: Osoba, která používá sociální inženýrství k získání citlivých informací, jako jsou hesla nebo bankovní údaje, od uživatelů internetových služeb. Phishing útoky se obvykle

provádějí pomocí falešných e-mailů, které vypadají, jako by byly posílány legitimními organizacemi.

- Spamovací gang: Skupina lidí, kteří se specializují na rozesílání nevyžádaného e-mailu (spam). Tento typ kyberzločinců používá často botnety, což jsou sítě počítačů, které jsou ovládány z dálky.
- Ransomware autor: Osoba, která vytváří škodlivý software, který kóduje data na počítači oběti a následně požaduje výkupné za jejich obnovení. Ransomware útoky jsou obvykle velmi účinné, protože poškozený uživatel nemůže přistoupit k datům bez zaplacení výkupného.

Kyberzločinci jsou také klasifikováni podle jejich motivace, jako jsou finanční zisk, politické nebo ideologické přesvědčení, nebo pouhé uspokojení z neoprávněného vniknutí do cizích počítačových sítí. Bez ohledu na to, jak jsou kyberzločinci klasifikováni, jsou považováni za hrozbu pro bezpečnost počítačových systémů a dat v celosvětovém měřítku..

1.4. Podrobný postup typového kybernetického útoku

Prvním krokem při vytváření seznamu (inventáře) sítě je zjištění doménových jmen a souvisejících sítí, které jsou spojené s danou organizací. Doménová jména jsou klíčové pro určení přítomnosti organizace na internetu a mohou být považována za síťové ekvivalenty názvu společnosti. Existuje mnoho databází, které lze pro tyto účely dotazovat, aby se získaly potřebné informace [9].

Různé dotazy mohou poskytnout různé informace. Většina informací, které útočníci používají na začátku útoku, se týká následujících typů požadavků:

- **organizační** – zobrazuje všechny informace týkající se konkrétního společnost;
- **vysokopecní** – zobrazí všechny informace týkající se konkrétní domény;
- **síťový** – zobrazuje všechny informace týkající se konkrétní sítě nebo na jednu IP adresu;
- **kontaktní** – zobrazuje všechny informace týkající se konkrétní osoby, obvykle-odpovědného zaměstnance organizace.

Druhym krokem po identifikaci přidružených domén je provést dotazy v DNS (Domain Name Service). DNS je rozptýlená databáze používaná k převodu IP adres na názvy síťových počítačů a naopak. Pokud je DNS nakonfigurován bez ohledu na bezpečnostní požadavky, mohou být důležité informace o organizaci snadno získány. Zone transfer, tj. přenos zónového souboru, je

nejslabším bodem pro kyberzločince. Zone umožňuje sekundárnímu řídícímu serveru aktualizovat svůj databázový server na základě požadavků primárního řídícího serveru, aby zvýšil spolehlivost DNS v případě, že selže primární jmenný server. Obvykle by mělo být přenos zóny DNS povoleno pouze na sekundárních DNS serverech. Bohužel je však mnoho DNS serverů nakonfigurováno nesprávně a umožňuje získání kopie zóny každému, kdo o ni požádá.

Třetím krokem po identifikaci sítí se útočník pokouší identifikovat jejich topologii, stejně jako potenciální přístupové cesty.

Snímání

Pokud je rekognoskace vyhledáváním zdrojů informací, skenování je zjišťováním zranitelností systémů. Během rekognoskace dostane útočník: jména a telefony zaměstnanců, rozsahy IP adres, servery DNS a e-maily. Nyní určuje, které systémy jsou dosažitelné z Internetu, pomocí nástrojů pro kontrolu rozsahu ping, skenování portů a automatizovaných prostředky výzkumu.

Skenování portů

Použitím rozsahového snímání ICMP nebo TCP najde útočník fungující (živé) systémy a zároveň shromažďuje některé užitečné informace. Poté začne skenovat porty každého systému. Skenování portů je proces připojení k portům TCP a UDP zkoumaného systému za účelem zjištění provozních služeb nebo stavu portu

Listening (poslech).

Identifikace "naslouchacích portů" je důležitá při určování typu operačního systému a použitých aplikací. Aktivní služby "naslouchání" mohou umožnit neoprávněnému uživateli přístup k systémům s nesprávnou konfigurací nebo k verzím softwarových produktů se známými slabými místy v ochraně.

Čtvrtý krok spočívá v mapování a plánování budoucích kroků kyberzločince, kde si stanovuje konkrétní cíle a motivy svého útoku. Po tomto kroku následuje fáze spáchání trestného činu, kdy se již útočník dopouští porušení právních předpisů ČR a dalších zemí.

Pátý krok se zaměřuje na získání přístupu k cílovému objektu. Kyberzločinec s určitými cíli a motivy musí překonat ochranné systémy objektu a získat přístup k zájmovým informacím s minimálními právy. Poté, co získá přístup k objektu s omezenými právy, útočník pomocí specializovaných nástrojů rozšiřuje své pravomoci.

Šestý krok představuje konečný cíl vícestupňového útoku - krádež informací. Po rozšíření svých pravomocí útočník uskuteční krádež informací, která byla cílem jeho útoku.

2. Problémy s identifikací zločinců a jejich zákazníků

2.1. Potenciální hrozby

Jedním z hlavních cílů kybernetické bezpečnosti v každé společnosti je identifikovat útočníka a pochopit jeho motivy, včetně toho, kdo za útokem stojí. I když proces řešení těchto úkolů využívá nejmodernější technologie a vědecké pokroky, stále jde spíše o umění než o vědu. Je logické, že před přijetím opatření na základě kybernetického útoku je důležité zjistit, kdo ho spáchal a proč. Nicméně to vyvolává celou řadu problémů, včetně toho, jak odstrašit útočníka. Americká strategie kybernetické bezpečnosti navrhuje ripish-trest jako nátlakové opatření, ale útočník by měl být odstrašen ještě před prvním úderem odvety. Další potenciální agresoři, jako státy, musí být přesvědčeni, že trestající stát přesně ví, kdo je útočník. Útok na "špatný" cíl (osobu nebo organizaci) ničí princip omezování a může vést k vytvoření nového nepřítele [14]. Ostatní "potenciální agresoři" - státy - by měli být přesvědčeni, že "odstrašující" (trestající) stát přesně ví, kdo je napadl. Útok na "nesprávný" cíl (osobu, organizaci) nejen porušuje logiku "principu omezení" (pokud nevadí "nevinnost" - proč být "nevinný"?), ale také vytváří nového nepřítele.

Namísto toho, aby se zapojil do kybernetické války (proti "původnímu" útočníkovi), může "odstrašující" stát nyní "potrestat" (donutit) dva aktéry kybernetických útoků. Druhým problémem je strana (stát), která byla mylně označena jako "původní útočník". "Obránce" by měl nejen přesvědčit, ale také přesvědčit "třetí strany", že definice "agresora" byla provedena "správně" a uvést relevantní argumenty, které nezávislí odborníci (rozhodčí soud) mohou zvážit. Nicméně, nejdůležitější v této záležitosti je, aby samotný "útočník" pochopil, že identifikace jako "agresor" byla provedena bezchybně. Pokud totiž věří, že skutečně napadený objekt se vrátil jen "odhadem" nebo že měl své "skryté motivy" pro "kybernetický útok", pak bude pravděpodobně pokračovat v podobných útocích, bez ohledu na to, zda bude nadále vystaven stejnému "trestu". Potřeba přesvědčit "třetí strany" o správnosti definice "agresora" závisí, jak by se dalo říci, na "důležitosti" těchto "třetích osob".

2.2. Identifikovani zdroj kybernetického útoku

Pracuje se na druhém vydání renomovaného experta na mezinárodní právo tzv. tallinnského manuálu [15], který se zaměřuje na použití mezinárodního práva při kybernetických konfliktech. První verze manuálu zdůvodňovala možnost fyzické reakce na kyberútok. NATO na něm pracuje již několik let.

V současné situaci je zvláště důležité správně identifikovat zdroj kybernetické hrozby, aby nedocházelo k nechtěným důsledkům, jako je rozpoutání válečného konfliktu nebo zbytečné prodlení s přípravou na obranu. Je nutné stanovit skutečného pachatele, aby mohly být využity diplomatické, politické a právní páky k odvrácení agrese. Identifikace pachatele také umožní vytvořit účinnou obrannou strategii a plánovat obranné akce. Pokud je pachatelem stát, musí se přistoupit k odvetným opatřením jinak, než v případě, kdy je hrozba způsobena nestátním aktérem. Tyto opatření mohou být diplomatického a právního charakteru a jejich volba závisí na identifikaci a analýze kroků, které má stát k dispozici. Identifikace uzlu, ze kterého je prováděn kyberútok, je klíčová pro určení, zda se jedná o soukromou osobu či organizaci a kdo jim poskytuje internetové služby. Dále je nutné znát fyzické umístění tohoto uzlu a nastavení, až po operační systém a aplikace, které jsou používány. Tyto informace umožní odhalit jazykovou a národní příslušnost útočníka.Ideální je, pokud v rámci této práce bude možné vyvodit závěry o motivech spáchaných činů. Definice motivace je však již "akrobacií" v oblasti identifikace speciálních operací v kyberprostoru a pouze technickými prostředky není možné tento úkol vyřešit.

Dnes existuje celá řada společností na světě, které se specializují pouze na tuto oblast. Můžete uvést některé příklady úspěšných identifikačních operací, které provedli [10]:

- **Cylance**, která studovala kampaň íránských hackerů;
- **Partneři**, kteří odhalili operaci Newscaster (Telecommentátor), která také pocházela z Íránu;
- **Kaspersky Lab**, který odhalil kampaně maska a Červený říjen;
- **Skupina-IB**, která našla stopu Islámského státu při útocích na mnoho ruských organizací;
- **BAE Systems**, která zkoumala útoky na ukrajinské počítače a našla na nich ruské otisky prstů;
- **Check Point**, který odhalil libanonskou hackerskou skupinu Volatile Cedar (létající cedr);
- **Taia Global**, která navzdory všeobecnému přesvědčení, že společnost Sony byla napadena hackery ze Severní Koreje, dokázala, že společnost Sony byla stále napadena z Ruska

2.3. Hlavní problémy při řešení problému identifikace zdroje kybernetických útoků

V oblasti kybernetických útoků existuje řada technických, metodologických, organizačních a právně morálně etických problémů. Technické problémy se týkají především nemožnosti

jednoduché identifikace zdroje útoků, bez ohledu na to, zda jsou realizovány formou útoků typu DDoS, pronikáním skrz ochranné bariéry, rozesíláním škodlivého kódu přes e-maily, nebo infikací webů a flash disků, přes které se Malware dostane do firemní sítě.

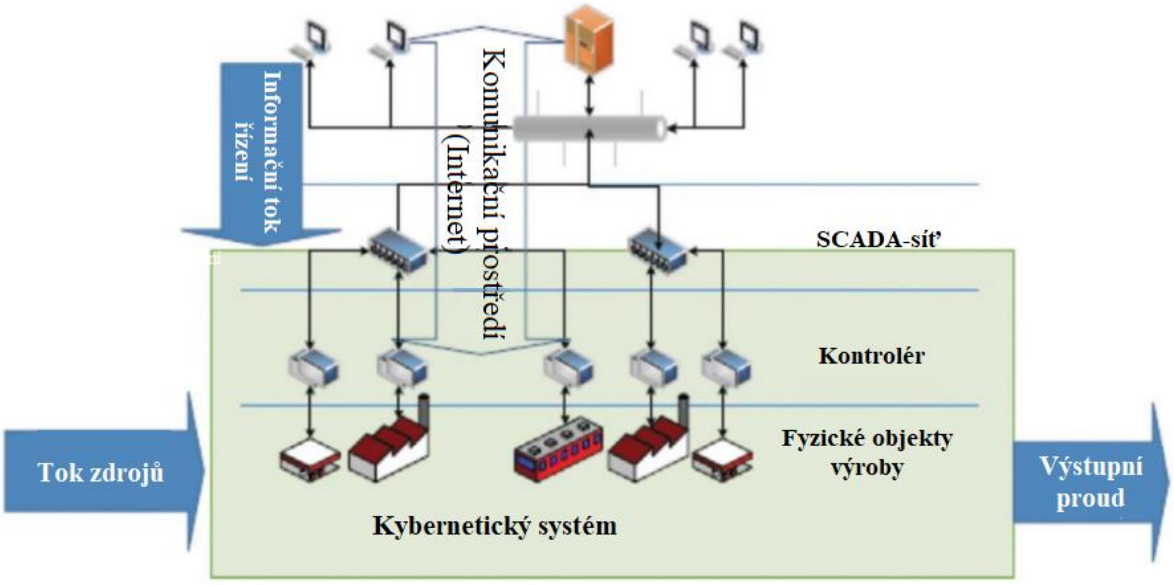
Při vytváření moderního internetu v letech 1960-1970 nebyla potřeba jednoznačné identifikace celého řetězce datových paketů z bodu A do bodu B brána v úvahu. Navíc samotná povaha internetové technologie zahrnuje decentralizaci a distribuci. To, co nás posledních 40 let bavilo, se teď začíná obracet proti nám. Jak můžeme identifikovat skutečného autora síťového paketu, který nám dorazil do počítače, pokud je možné technicky změnit adresu odesílatele? Všechny známé verze protokolu IP v zásadě neumožňují jednoznačnou identifikaci a autentizaci iniciátora připojení (i když se již dlouho vedou diskuze o internetovém pasu, který by umožnil identifikovat každého uživatele, který vstoupí na internet).

Nedostatek potřebných atributů verze protokolu IPv4 pro určení místa zdroje útoku není jedinou překážkou v dnešní době. Útočník může použít libovolný proxy server nebo anonymizér, aby skryl svou skutečnou polohu. V případě takového útoku bude zdrojem adresy útoku server prostředníka namísto skutečné adresy útočníka. Tyto servery jsou umístěny v různých národních segmentech internetu, což umožňuje útočníkovi provádět útok z různých geografických oblastí. Situaci dále zhoršuje skutečnost, že útočník může pronajmout speciální servery, které skrývají jeho skutečnou adresu. Tyto servery mohou být mnoho - 5, 10, 100 - což způsobuje dynamicky se měnící prostorové charakteristiky útoku, které se zásadně liší od běžných útočných zbraní. Jaderná hlavice může dynamicky měnit svou polohu, ale velmi pomalu, pokud ji vozíte speciálním vozidlem nebo vlakem. V tomto případě jsou však její zeměpisné souřadnice omezeny hranicemi jednoho státu nebo bloku. V kybernetických útocích se geografické umístění útočníka může rychle měnit, přičemž útok může být realizován z různých kontinentů během několika minut nebo dokonce sekund. Pokud se podíváte na e-mail obsahující hrozby nebo škodlivý kód, identifikace skutečného odesílatele může být téměř nemožná, pokud si to útočník nepřeje. K identifikaci zdroje útoku je potřeba projít řetězcem všech uzlů, kterými poštovní zpráva prošla, a ty mohou být v různých zemích a jurisdikcích. Když se jedná o škodlivý software a soubory, ty neobsahují žádné podpisy autora, které by pomohly identifikovat útočníka. Vědci musí prozkoumat velké množství informací a použít technickou analýzu k určení zdroje útoku s určitou pravděpodobností. Například společnost Cylance shromáždila a prozkoumala více než 8 GB dat, 80 000 souborů a záznamů o registraci na uzlech obětí při operaci s názvem "řeznický nůž" a až poté byla schopna s určitými výhradami prohlásit, že za útokem stojí Írán [11]. Nicméně technická analýza nikdy nedokázala určit, zda za touto operací stál stát nebo soukromá iniciativa.

3. Specifika kybernetické bezpečnosti technologických podniků

3.1. Funkce v oblasti řízení a zabezpečení průmyslových infrastruktur

V dnešní době je mnoho různých rizik spojených s řízením a provozem kritické infrastruktury. Každá společnost, která poskytuje datové služby nebo vyrábí software a zařízení pro správné fungování této infrastruktury, je povinna posoudit všechna možná rizika a identifikovat zranitelnosti. Důležitou součástí jsou však hrozby kybernetické bezpečnosti, které se objevily relativně nedávno. Tyto hrozby jsou především spojeny se systémy řízení fyzikálních procesů. Síť řadičů, kteří shromažďují data z fyzikálních objektů a generují přímé řídící signály, může být zranitelná kvůli vestavěnému software obsahujícímu softwarové trojské koně (malware). V oblasti elektrické energie je situace ještě složitější, protože moderní technologie umožňují vytvářet mikročipy (mikroprocesory) pro regulátory s vestavěnými hardwarovými trojskými koňmi, kteří mohou být kdykoli ovládáni zvenčí na příkaz "hostitele" nebo dokonce na základě interního algoritmu vloženého přímo do čipu [12]. Na obrázku 1 tak můžete vidět vizuální strukturu takové firmy. Tyto regulátory jsou obvykle spojeny v síti SCADA systémů, které spolu komunikují přes podnikovou síť a působí jako interoperabilní prostředí, často v globální síti (Internet).



Obrázek 1: Struktura moderní digitální výroby

Zdroj: [1]

Počítačová automatizace výrobních infrastruktur vedla ke sloučení (integraci) výkonných modulů a modulů interoperability systémů a to zase vedlo ke změně na digitální komunikaci,

sdílení a řízení týmů. Dříve každý prvek výrobního systému představoval samostatnou součást s vlastním řídicím okruhem, jehož řídící funkce byly definovány podle teorie automatizovaného řízení a typů zpětné vazby. V současnosti takové prvky nejsou jednoduché.

Termín kybernetický objekt (nebo kybernetický systém jako soubor objektů) se používá k prezentaci výrobních a technologických schémat, které integrují různé druhy energie a informační a telekomunikační prostředí, které zajišťuje výměnu mezi součástmi a udržitelné fungování celého systému monitorováním a automatizovaným řízením.[13] Koncepční struktura kybernetického systému tak zahrnuje následující prvky:

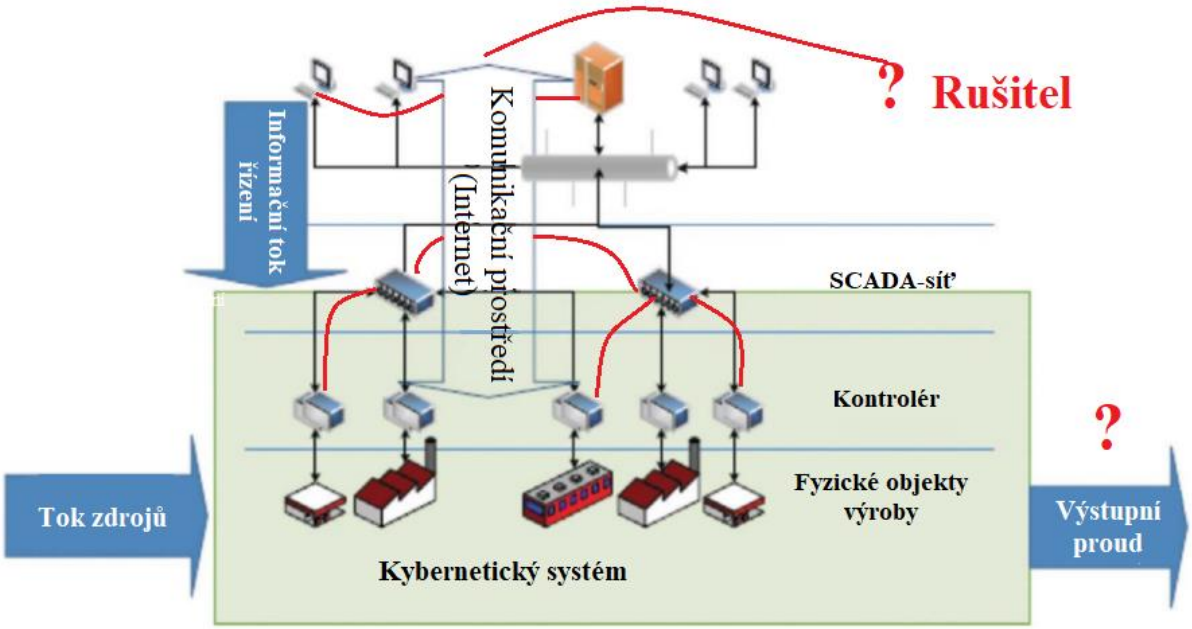
- sada vzájemně propojených fyzických komponent, které implementují konkrétní technologický proces;
- sada vzájemně propojených informačních komponent s různými stupni automatizace provádění řízení procesu;
- komunikační prostředí, které zajišťuje přenos informací uvnitř systému a výměnu informací s okolím, stejně jako přenos řídících týmů výkonným mechanismům.

Vzhledem k integraci fyzických, informačních a komunikačních složek v moderním kybernetickém systému jsou funkce řízení prováděny prostřednictvím informačního dopadu, zatímco v tradičních systémech automatického řízení regulace byla fyzická hodnota základem řídící funkce. Digitalizace průmyslu přinesla nové problémy související s poskytováním informační a kybernetické bezpečnosti. Jednotný kyberprostor, sestávající z interoperabilních systémů založených na společných, univerzálních protokolech a principech vzdáleného řízení, vede k tranzitnímu uzavření všech fungujících komponent, což umožňuje uzavřít prostřednictvím smyček digitální interakce všechny řídicí systémy výrobní, finanční a sociální sféry. Celosvětová dostupnost zařízení v kyberprostoru vyvolává problém udržení udržitelného provozu moderní výroby v prostředí náhodných počítačových havárií a cílených počítačových útoků, které mají dlouhodobý a těžko zjistitelný dopad na řízení technologických procesů.

3.2. Hlavní bezpečnostní rizika digitální výroby

Poslední roky jsou charakterizovány narůstajícím množstvím závažných případů kybernetických útoků, které se především zaměřují na technologické procesy. Podle publikovaných statistik z roku 2017 [19] tvořily průmyslové objekty více než 20 % všech hlášených cílů kybernetických útoků. Na druhé straně oblasti jako jsou sociální sítě, hostingové služby, zpravodajské weby a mobilní telekomunikační společnosti, dohromady představovaly méně než 13% všech zaznamenaných incidentů.

Jak ukazuje obrázek 2, moderní útočníci, kteří působí skrze telekomunikační kanály nebo mají přístup k informačním zdrojům firemní sítě, jsou schopni ovlivňovat výrobu jako celek.



Obrázek 2: Nové možnosti narušení bezpečnosti průmyslových podniků

Zdroj: [1]

Dalším kanálem, který útočníci využívají k organizování útoků, je schopnost ovlivňovat digitální řídicí komponenty, jako jsou sítě a regulátory. Podle údajů z SecurityLab.ru z roku 2020 se útočníkům podařilo získat přístup k osobním údajům uživatelů služby LastPass, a tím k mnoha účetním systémům, včetně výrobních systémů. V různých incidentech byly použity různé průnikové kanály, jako jsou viry v obrázcích na legitimních webových stránkách, zranitelnosti nalezené v smartphonu společnosti Samsung a dokonce i elektrická interference v paměti DRAM. Více než 20% incidentů pochází z internetových sítí. Je důležité zdůraznit, že se mění i celkový charakter útoků na kybernetické systémy. V digitální výrobě jsou typické cílené útoky, při jejichž přípravě a provádění se útočníci někdy spoléhají na odborníky v příslušných průmyslových odvětvích. Útočníci používají různé metody a "vektory" útoků najednou, aby dosáhli komplexní expozice. Tyto útoky zahrnují nejen různé technické metody, ale i metody založené na sociálním inženýrství. Mění se také účel samotného útoku - útočníci chtějí přímo ovlivnit probíhající technologické procesy, nikoliv pouze získat data. V současné době jsou odborníci na kybernetickou bezpečnost těmito hrozbami znepokojeni více než únosy dat.

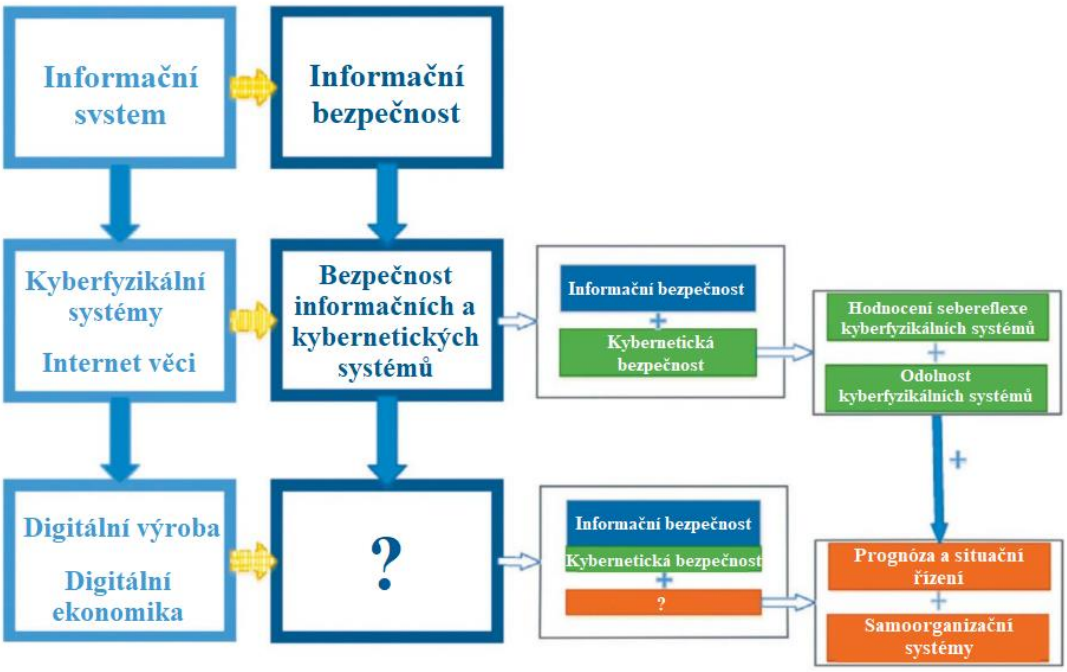
Rozsáhlé využívání cloudových systémů a systémů s nejasným perimetrem souvisí s vývojem následujících hrozeb kybernetické bezpečnosti [14].

- Hrozby zaměřené na využití výpočetního výkonu cloud pro řešení problémů vetřelce (např. brute force hesla a cache) nebo maskovat zdroj dopadu na jiné objekty.
- Hrozby zaměřené na platformy, infrastruktury a uživatelů cloud ze strany ostatních uživatelů cloud nebo z Internetu.
- Nástup systémů "inteligentního domu", nebo obecněji vzhled internetu věcí, vedl k možnosti narušení bezpečnosti osobního prostoru v podobě:
- Použití domácích zařízení pro pronikání do osobních počítačů a mobilních telefonů.
- Ohrožení života a zdraví uživatelů (porušení domácích zařízení může vést k požárům, otravám atd.).

V poslední době dochází k výraznému nárůstu počtu incidentů v oblasti kybernetické bezpečnosti souvisejících s automatizovanými systémy řízení technologických procesů (ASUTP), což je způsobeno trendem integrace těchto systémů s podnikovými informačními sítěmi. Téměř polovina zaznamenaných případů narušení automatizovaných systémů řízení technologických procesů pochází z podnikové sítě. Často se jedná o útoky zaměřené na vydírání, průmyslovou špionáž nebo sběr osobních údajů, jako jsou čísla PIN bankovních karet nebo sociální informace. Nové hrozby také zahrnují zachycení řízení a vnucování řídících algoritmů, vyhledávání zranitelností a sociálního inženýrství. Bohužel méně než 2 % podniků, které byly napadeny, hlásí incidenty, a odborníci v oblasti ASUTP často přeceňují úroveň ochrany svých systémů [15]. Tyto nové cíle útoků, spolu s novými penetračními mechanismy a objekty, vyžadují nové přístupy k zajištění bezpečnosti průmyslových systémů v digitální době výroby.

Digitalizace moderního průmyslu, jehož nedílnou součástí je i Energetika, prochází několika fázemi charakterizovanými různým stupněm přenosu lidských funkcí do počítačového systému. V počátečních fázích to bylo vyjádřeno stupněm automatizace výrobní sféry spočívající v automatizaci workflow, procesů sběru a zpracování informací a jejich přípravě v příslušném formátu pro uživatele.

Postupná integrace s počítačovými systémy přinesla přenos odpovědnosti za tvorbu řešení od lidských operátorů k automatizovaným systémům. Tento proces vyžadoval intenzivní vývoj metod a prostředků umělé inteligence, jako například expertních systémů, rozhodovacích a předpovědních systémů. Vzhledem k transformaci tradiční výroby a nástupu digitální výroby se také změnily požadavky na informační bezpečnost, což vedlo k vzniku konceptu kybernetické bezpečnosti a kyberfyzikálních systémů. Digitální výroba však přináší značnou složitost při tvorbě modelů ohrožení systémů, zejména kvůli velkému počtu uživatelů, součástí a integrací výrobních procesů. Tradiční modely útoků nejsou pro tyto systémy použitelné a předpovídání dopadů útoků je obtížné až nemožné, zejména kvůli neustálému vývoji technologií a integracím



Obrázek 3: Transformace požadavků na bezpečnost výroby

Zdroj: [1]

3.3. Hlavní zranitelnosti průmyslových informačních komunikačních systémů

Zranitelnost průmyslových IKT systémů představuje hlavní téma odborníků na kybernetickou bezpečnost z celého světa. To je důsledkem vědomí naléhavosti řešení tohoto problému a nedostatku vhodných nástrojů k jeho řešení. V USA byly zavedeny průkopnické opatření, jako jsou laboratoře, testovací stanoviště a místa pro průmyslové IKT systémy, průmyslová aliance pro kybernetickou bezpečnost a program kybernetické bezpečnosti v chemickém průmyslu. V roce 2003 provedly národní laboratoře Sandia hodnocení zranitelnosti systémů IKT s důrazem na systémy řízení a automatizace používané v kritických infrastrukturách. Většina bezpečnostních zranitelností v energetické infrastruktuře spočívá v nedostatečné definici citlivosti a zabezpečení dat, nedostatku bezpečnostního obvodu a nedostatečné ochraně dat a služeb pro ověřené uživatele. Řešení těchto zranitelností zahrnuje zvyšování povědomí o nových hrozbách, vývoj spolehlivého a efektivního řízení bezpečnosti a řešení bezpečnostních zranitelností prostřednictvím integrace ochranných technologií. Bezpečnost řídicích systémů v elektroenergetice je závislá na mnoha heterogenních kategoriích prvků, jejichž pokus o systematizaci byl proveden v práci [16]. Mnoho z těchto zranitelností vzniká kvůli nedostatečné správě zabezpečení a neefektivní správě, což může být způsobeno nevědomostí samotných administrátorů v automatizaci, kteří nebyli dostatečně školeni v oblasti bezpečnosti při umisťování moderních informačních technologií do řídicích systémů.

Systémová data

Zabezpečení systému zaměřené na data se zaměřuje na zachování dostupnosti, autenticity, integrity a soukromí dat. Zachování těchto atributů zajišťuje, že celý systém funguje spolehlivě.

Správa zabezpečení

Materiál tvrdí že "administrativní složka systému řízení zahrnuje takové neautomatizované funkce, jako je dokumentace postupu. Zásadním prvkem dokumentace je bezpečnostní politika systému, která stanoví cíle a odpovědnosti za bezpečnost."

Stavitelství

Architektura řídicích systémů v elektroenergetice odkazuje na svou specifickou hierarchii správy a ukládání dat.

4. Analýza firmy a základní bezpečnostní kroky

Abychom mohli pracovat podrobněji, provedeme analýzu těchto metod na příkladu vymyšlené společnosti "AAA". Společnost "AAA" je zaměřena na výrobu softwaru pro údržbu kritické infrastruktury a má velkou odpovědnost za zabezpečení a dodržování vysokých standardů bezpečnosti. Vzhledem k tomu, že tato společnost pracuje s citlivými a důvěrnými informacemi, je zásadní, aby všichni zaměstnanci dodržovali přísné požadavky na mlčenlivost a bezpečnost. V současné době má společnost "AAA" více než 200 zaměstnanců, kteří se specializují na různé oblasti, jako je vývoj softwaru, design, testování, implementace a technická podpora. Společnost se snaží udržovat vysokou úroveň kvalifikace svých zaměstnanců, aby mohla poskytovat nejlepší služby a produkty na trhu.

Princip práce společnosti "AAA" spočívá v tom, že poskytuje komplexní řešení pro své zákazníky, které zahrnuje nejen výrobu a dodávku softwaru, ale také jeho implementaci, školení zaměstnanců a technickou podporu. Společnost "AAA" také spolupracuje s dalšími dodavateli a partnery, aby mohla poskytnout svým zákazníkům nejlepší možné služby. V rámci společnosti "AAA" se klade velký důraz na bezpečnost a ochranu citlivých informací. Je nutné provádět důkladný proces ověření všech zaměstnanců a pravidelně je školit v oblasti bezpečnosti. Společnost také používá šifrování a další bezpečnostní opatření pro ochranu dat a informací svých zákazníků. Celkově lze říci, že společnost "AAA" je významným hráčem na trhu s výrobou softwaru pro údržbu kritické infrastruktury a věnuje se vysoké úrovni bezpečnosti a ochrany informací. Vzhledem k vysoké odpovědnosti a nutné mlčenlivosti v tomto segmentu je nutné zajistit a dodržovat vysoký standard bezpečnosti v rámci společnosti. Pro zajištění komplexní bezpečnosti je třeba zavést určité bezpečnostní opatření [17], [18]:

- **Vytvoření politiky bezpečnosti informací**: Je nutné vytvořit dokumenty, které by popisovaly hlavní principy a pravidla týkající se bezpečnosti informací v rámci společnosti. Tyto dokumentz by mělz stanovit pravidla pro hesla, přístup k síti, instalaci softwaru atd.
- **Zajištění fyzické bezpečnosti**: Je důležité zajistit, aby servery a zařízení byly umístěny v bezpečném prostoru. Měly by být zavedeny zavést systémy kontroly přístupu, aby byl omezen přístup k serverovně a dalším citlivým oblastem.
- **Školení a zvyšování povědomí**: Je důležité školit naše zaměstnance v pravidlech bezpečnosti a zvyšovat jejich povědomí v oblasti kybernetické bezpečnosti. Měly by být pořádny školení a semináře, aby naši zaměstnanci věděli, jak rozpoznat a předcházet kybernetickým útokům.

- **Pravidelné aktualizace bezpečnostního systému**: Společnost by měla neustále aktualizovat bezpečnostní systém, včetně softwaru a hardwaru, aby se ochránila před novými druhy kybernetických hrozeb.
- **Práce s ostatními společnostmi**: Mělo by být spolupracováno s ostatními společnostmi v daném průmyslu, aby bylo vyměňovano informace o hrozbách a společných přístupech k kybernetické bezpečnosti. To může pomoci být informován o nejnovějších hrozbách a efektivních způsobech ochrany.
- **Bezpečnostní audit a vývoj plánu akcí v případě porušení bezpečnosti**: Měli bychom pravidelně provádět bezpečnostní audit, aby byla zkontrolována shoda našeho bezpečnostního systému s normami a naší politikou bezpečnosti informací. To nám pomůže identifikovat zranitelnosti a přijmout opatření k jejich odstranění. Vývoj plánu akcí v případě porušení bezpečnosti měli bychom vypracovat plán akcí, který by určoval, jak reagovat na porušení bezpečnosti, včetně oznámení internímu týmu a orgánům práva.

4.1. VYTVOŘENÍ POLITIKY BEZPEČNOSTI INFORMACÍ

Společnost "AAA" se snaží zajistit bezpečnost informací v souladu s mezinárodními standardy a doporučeními, jako jsou ISO 27001, NIST SP 800-53 a CIS Critical Security Controls [19].

Důvěrnost

Důvěrné informace by měly být chráněny před neoprávněným přístupem. V společnosti AAA je kladen velký důraz na zachování důvěrnosti informací, které jsou majetkem společnosti nebo jejích klientů. Veškeré informace musí být zpracovávány a uchovávány v souladu s principy důvěrnosti. Vedení společnosti a zaměstnanci bezpečnostního oddělení mají plný přístup ke všem informacím společnosti. Různá oddělení společnosti mohou mít přístup pouze k informacím, které jsou nezbytné pro plnění svých pracovních povinností. Například vývojáři softwaru mají přístup pouze k informacím, které jsou nezbytné pro vývoj a testování softwaru, který vyvíjejí. Zaměstnanci oddělení prodeje mají přístup pouze k informacím o produktech společnosti, které jsou nezbytné pro jejich prodej a marketing.

Zaměstnanci oddělení technické podpory mají přístup pouze k informacím, které jsou nezbytné pro poskytování technické podpory zákazníkům, a zaměstnanci oddělení financí mají přístup pouze k informacím, které jsou nezbytné pro řízení financí společnosti.

Všichni zaměstnanci jsou povinni dodržovat politiku důvěrnosti společnosti a nezveřejňovat informace chráněné důvěrností třetím stranám bez příslušného povolení. V případě porušení politiky důvěrnosti mohou být zaměstnanci disciplinárně stíháni a dokonce i trestně stíháni.

Integrita

Informace by měly být chráněny před změnou nebo zničením bez povolení. To zahrnuje kontrolu verzí, ověřování integrity dat a ochranu před škodlivými programy. V rámci bezpečnostní politiky společnosti AAA je integrita informací také důležitým aspektem. Integrita informací znamená, že informace musí být chráněna před neoprávněnými změnami nebo zničením.

Pro zajištění integrity informací používáme různá bezpečnostní opatření, jako jsou instalace systémů kontroly integrity, zálohování dat, kontrola přístupu a autentizace uživatelů.

Zaměstnanci, kteří mají přístup k informacím, jsou povinni dodržovat bezpečnostní politiku společnosti a neprovádět neoprávněné změny v informacích ani je nezničit. Pokud během práce s informacemi dojde k jakýmkoli změnám nebo chybám, zaměstnanci jsou povinni o tom neprodleně informovat odpovědnou osobu.

V případě porušení integrity informací mohou být zaměstnanci podrobeni disciplinárnímu řízení a dokonce i trestnímu stíhání. Také přijímáme opatření pro obnovu integrity informací v případě jejich porušení, například obnovou z datových záloh.

Dostupnost

Informace by měla být dostupná pouze těm, kteří na to mají právo. Měla by být dostupná během pracovní doby zaměstnance a při potřebě i mimo pracovní dobu. Dostupnost informací je také důležitým aspektem bezpečnostní politiky společnosti AAA. Pro zajištění dostupnosti informací přijímáme opatření zaměřená na minimalizaci rizik spojených s nedostupností, jako jsou výpadky služeb, poruchy zařízení a mimořádné události, jako jsou požáry a přírodní katastrofy.

Používáme rezervování zařízení, duplikaci dat a zálohování napájení, aby zajišťovali nepřetržitou funkčnost našeho systému, i v případě vzniku havarijních situací. Pravidelně také testujeme zařízení a sítě, abychom zjistili možné zranitelnosti a rizika.

Společnost také poskytuje přístup k informacím pouze zaměstnancům, kteří skutečně potřebují přístup k informacím k plnění svých pracovních povinností. Kromě toho školí zaměstnance, jak správně zacházet s informacemi a jak zabránit jejich náhodnému smazání nebo poškození. V případě problémů s dostupností informací rychle reagujeme na události, obnovujeme funkčnost systému a navracíme přístup k informacím pro zaměstnance. Pokud nedostupnost

informací nastane kvůli vnějším faktorům, jako jsou například povětrnostní podmínky nebo technické problémy u poskytovatele služeb, také přijímáme opatření k včasnému informování zaměstnanců a klientů o možných zpožděních v zpracování informací. Pravidelně jsou analyzováno a vylepšováno naše procesy a bezpečnostní opatření pro zajištění nejvyššího stupně dostupnosti a ochrany informací.

4.2. ZAJIŠTĚNÍ FYZICKÉ BEZPEČNOSTI

Fyzická bezpečnost je důležitou součástí zabezpečení informačního systému společnosti AAA. Kromě technických opatření a vzdělávání zaměstnanců je nutné zajistit bezpečnost prostor, ve kterých se informační systém a další kritické systémy společnosti nacházejí.

Pro zajištění bezpečnosti prostor je nutné stanovit přístupová práva a řídit přístup do prostor pomocí různých bezpečnostních prvků, jako jsou například kamerové systémy, detektory pohybu nebo zabezpečené brány a dveře. Dále je třeba provádět pravidelné kontroly bezpečnostních opatření a testování odolnosti prostor proti různým druhům útoků.

Jedním z možných systémů videonahrávání, který by se dal použít pro společnost AAA, je systém Avigilon Control Center (ACC). Jedná se o vysokovýkonný systém videonahrávání, který poskytuje vysokou kvalitu záznamu a rychlý přístup k záznamům v reálném čase.Systém ACC také obsahuje funkci analýzy videodat, která umožňuje automaticky detekovat bezpečnostní porušení a upozornit operátora. Kromě toho systém ACC disponuje funkcemi škálovatelnosti a správy několika kamer, což ho činí ideální volbou pro společnost AAA s mnoha objekty k sledování a potřebou monitorovacího systému.

Zabezpečení fyzického prostoru je v případě společnosti AAA zvláště důležité, protože její software a zařízení se používají v kritických infrastrukturních systémech. Proto je nezbytné zajistit, aby prostor nebyl narušen neoprávněnými osobami nebo útočníky, kteří by mohli získat přístup k důležitým systémům a datům. Pro zajištění fyzické bezpečnosti je třeba také zajistit odpovídající zabezpečení při přepravě zařízení a materiálů a při nakládání s nimi v rámci společnosti. K tomu patří například používání zabezpečených vozidel, které jsou vybaveny GPS sledováním a dalšími bezpečnostními prvky, nebo zabezpečených skladovacích místností pro zařízení a materiály.

Pro firmu AAA, která se zabývá výrobou softwaru a zařízení pro různé společnosti, by bylo možné použít nákladní automobily pro dopravu zařízení a součástek na výrobní plochy. Jedním z příkladů nákladních automobilů, které lze použít, je Mercedes-Benz Actros. Tento automobil má velkou nosnost a vynikající vlastnosti průchodnosti, což umožní doručovat zařízení

a součástky na jakékoliv místo, včetně obtížně dostupných oblastí a podmínek s špatnou silniční infrastrukturou. Kromě toho má Mercedes-Benz Actros možnost ovládání pomocí dálkového monitorovacího systému, což poskytuje další bezpečnost a kontrolu nad nákladem v reálném čase. Tento automobil má také vysokou ekonomičnost a ekologičnost, což umožní společnosti AAA snížit náklady na palivo a snížit negativní vliv na životní prostředí.

Důležitým aspektem zajištění bezpečnosti informačního systému společnosti je spolupráce s externími specialisty a službami, které mohou poskytnout pomoc při ochraně před kybernetickými útoky a průmyslovou špionáží. Je také nutné navázat spolupráci se zaměstnanci zákonových orgánů pro operativní reakci na možné incidenty.

4.3. ŠKOLENÍ A ZVYŠOVÁNÍ POVĚDOMÍ

Základním cílem této programu je naučit personál společnosti "AAA" pravidla informační bezpečnosti, která umožní zabezpečit klíčové zdroje společnosti a ochránit důvěrné informace před kyberútoky a průmyslovým špionážem. Vzdělávací program by měl obsahovat několik fází, z nichž každá bude zaměřena na dosažení určitých cílů.

První fází programu bude výuka základů informační bezpečnosti. V této fázi bude personál společnosti seznámen s hlavními termíny, pravidly a principy, které jsou základem informační bezpečnosti. Například personál by měl být obeznámen s pojmy "důvěrnost", "integrita" a "dostupnost" informací a také s tím, jak tyto principy mohou být porušeny a jaké důsledky to může mít pro společnost.

Druhou fází bude výuka personálu základů kyberbezpečnosti. V této fázi bude personál seznámen s typy kyberhrozeb, které mohou společnost ohrožovat, a také s metodami ochrany informací před těmito hrozbami. Například personál by měl být obeznámen s hlavními typy škodlivého softwaru (virů, červů, trojských koní) a také s tím, jak zabránit infekci počítače a jaké kroky podniknout v případě zjištění škodlivého kódu.

Třetím krokem programu bude vzdělávání zaměstnanců v pravidlech bezpečného používání elektronické pošty. V této fázi budou zaměstnanci seznámeni s hlavními pravidly, která je třeba dodržovat při používání elektronické pošty. Například zaměstnanci by měli být obeznámeni s tím, jak vytvářet spolehlivá hesla, jak ověřovat pravost zpráv a jak zabránit úniku důvěrných informací prostřednictvím elektronické pošty.

Čtvrtým krokem programu bude vzdělávání zaměstnanců v pravidlech používání internetu. V této fázi budou zaměstnanci seznámeni s hlavními pravidly, která je třeba dodržovat při používání internetu. Například zaměstnanci by měli být obeznámeni s tím, jak se vyhnout

připojení k otevřeným Wi-Fi sítím, jaké údaje je třeba udržovat v bezpečí, jak zabránit úniku informací prostřednictvím sociálních sítí a messengers.

Pátým krokem programu bude vzdělávání zaměstnanců v pravidlech bezpečnosti při práci s důvěrnými informacemi. V této fázi budou zaměstnanci seznámeni s hlavními pravidly, která je třeba dodržovat při práci s důvěrnými informacemi. Například zaměstnanci by měli být obeznámeni s tím, jak skladovat důvěrné informace, jak zabránit úniku informací přes internet, jak kontrolovat přístup k informacím a jak reagovat na potenciální porušení bezpečnosti informací.

Takto navržený program školení zaměstnanců v oblasti zabezpečení informačního systému společnosti "AAA" je zaměřen na dosažení určitých cílů, každý z nich bude směřovat k zlepšení bezpečnosti informačního systému společnosti a ochraně důvěrných informací před kyberútoky a průmyslovou špionáží. Realizace tohoto programu umožní zvýšit úroveň bezpečnosti společnosti "AAA" a snížit riziko úniku důvěrných informací. Pro úspěšnou realizaci programu je nutné věnovat patřičnou pozornost každé fázi, pravidelně aktualizovat materiály a provádět testování, aby bylo zajištěno, že zaměstnanci plně rozumí a dodržují pravidla bezpečnosti.

K hodnocení účinnosti programu lze použít různé metody, jako jsou průzkumy zaměstnanců a zprávy o únicích informací. Průzkumy pomohou posoudit úroveň porozumění a dodržování pravidel bezpečnosti mezi zaměstnanci a zprávy o únicích informací umožní posoudit účinnost programu při prevenci úniků. Kromě toho je pro zajištění vysoké úrovně bezpečnosti informačního systému společnosti "AAA" také nutné používat moderní technologie ochrany informací, jako jsou antivirová softwarová řešení, bezpečnostní monitorovací systémy a podobně. Je také nutné pravidelně testovat systémy na průnik a provádět audit bezpečnosti informačního systému společnosti.

4.4. PRAVIDELNÉ AKTUALIZACE BEZPEČNOSTNÍHO SYSTÉMU

Je důležité zajistit a dodržovat vysoký standard bezpečnosti uvnitř společnosti při výrobě softwarového vybavení pro různé společnosti zajišťující kritickou infrastrukturu. V tomto kontextu je nutné stanovit požadavky a kritéria pro výběr softwaru a hardwaru.

Za prvé je třeba zohlednit bezpečnost při výběru jakéhokoli softwaru nebo hardwaru. Dodavatelé softwaru a hardwaru by měli poskytnout úplnou dokumentaci o bezpečnosti, včetně výsledků bezpečnostních testů a hodnocení zranitelností. Za druhé je nutné zajistit, aby dodavatelé softwaru a hardwaru splňovali standardy bezpečnosti a důvěrnosti stanovené v odvětví. Za třetí

je důležité zhodnotit spolehlivost a stabilitu softwaru a hardwaru. Je třeba vybírat stabilní a spolehlivé softwary a hardwary, které pracují bez poruch. Za čtvrté je vhodné upřednostňovat snadné používání softwaru a hardwaru, aby klienti mohli snadno pracovat s naším zařízením bez dalších nákladů na vzdělávání. Za páté je třeba vybírat dodavatele softwaru a hardwaru, kteří poskytují operativní technickou podporu, aby bylo možné rychle a efektivně řešit vznikající problémy.

Cisco Firepower Threat Defense:

Cisco Firepower Threat Defense je komplexní řešení pro ochranu sítě, které disponuje širokou paletou funkcí pro detekci a prevenci hrozeb, včetně ochrany před škodlivým softwarem, DDoS útoky, útoky na aplikace, phishing a dalšími typy hrozeb. Toto software má flexibilní a škálovatelnou architekturu, která umožňuje snadno jej integrovat do různých sítových infrastruktur. Kromě toho je rozhraní pro správu jednoduché na používání, což usnadňuje práci s programem a zjednodušuje nastavení bezpečnosti. Vysoký výkon a široká škála možností nasazení činí Cisco Firepower Threat Defense nejlepší volbou pro zajištění bezpečnosti kritické infrastruktury společností.

Abychom si ověřili, že jsme zvolili nejlepší možnost, srovnáme tento software s konkurencí. Zvažme tři konkurenční produkty: Check Point, Fortinet a Palo Alto Networks a porovnejme je s Cisco Firepower Threat Defense.

Check Point:

Check Point je jedním z nejznámějších produktů v oblasti informační ochrany, který nabízí multifunkční bezpečnostní platformu pro prevenci hrozeb, včetně firewallů, systémů detekce útoků a správu hrozeb. Nicméně, v porovnání s Cisco Firepower Threat Defense, Check Point může být méně efektivní při detekci a prevenci bezpečnostních hrozeb, protože jeho systémy mohou být méně přesné. Check Point také může být dražší a nemá tak rozsáhlou funkcionalitu jako u Cisco Firepower Threat Defense, včetně síťové inteligence a flexibilnějších mechanismů správy bezpečnostních politik.

Fortinet:

Fortinet je integrovaná bezpečnostní platforma, která zahrnuje firewally, systémy detekce útoků, antiviry a mnoho dalšího. Fortinet může být cenově dostupnější než Cisco Firepower Threat Defense, ale může být méně efektivní při detekci a prevenci bezpečnostních hrozeb. Fortinet také může mít menší měřítkovatelnost než Cisco Firepower Threat Defense a nemá tak rozsáhlou

funkcionalitu jako u Cisco, jako je správa hrozeb a flexibilnější mechanismy správy bezpečnostních politik.

Palo Alto Networks:

Palo Alto Networks je integrovaná bezpečnostní platforma, která zahrnuje firewally, systémy detekce útoků, systémy ochrany koncových zařízení a správu hrozeb. Palo Alto Networks může být účinnější při detekci a prevenci bezpečnostních hrozeb než Check Point a Fortinet, ale může být dražší než Cisco Firepower Threat Defense. Také může mít menší měřítkovatelnost než Cisco Firepower Threat Defense a nemá tak rozsáhlou funkcionalitu jako u Cisco, jako je správa hrozeb a flexibilnější mechanismy správy bezpečnostních politik.
Jako software by bylo doporučeno použití systému ochrany informací před vnějšími hrozbami a průnikem do sítě, například Cisco Firepower Threat Defense.

Obrázek 4: Cisco Firepower Threat Defense

Zdroj: [20]

Pokud jde o hardware pak bylo rozhodnuto orientovat se na následující požadavky a kritéria při výběru hardware pro naši společnost:

- Spolehlivost: Je důležité, aby serverové zařízení bylo spolehlivé a mělo vysokou dostupnost, aby se zabránilo ztrátě dat a výpadkům v práci.
- Bezpečnost: Serverové zařízení by mělo mít mnoho bezpečnostních funkcí, jako je hardwarové šifrování dat, ochranu před škodlivým softwarem a mechanismy pro kontrolu přístupu.
- Výkon: Je důležité, aby zařízení bylo výkonné a mohlo rychle a efektivně zpracovávat velké objemy dat.

- Škálovatelnost: Společnost může růst, takže je důležité mít možnost škálování serverového zařízení v budoucnosti.
- Cena: Cena by měla odpovídat uvedeným požadavkům a kritériím, aby se zajistilo nejefektivnější využití rozpočtu společnost

Při srovnávání Dell PowerEdge s HP ProLiant, Cisco UCS a IBM System X lze identifikovat následující klíčové faktory:

- Spolehlivost a dostupnost: Všechny čtyři hardware poskytují vysokou úroveň spolehlivosti a dostupnosti, avšak Dell PowerEdge má dodatečné funkce, jako např. lepší kontrolu chyb paměti a vylepšenou podporu clusteringu, které zvyšují spolehlivost a dostupnost.
- Bezpečnost: Všechny čtyři hardware nabízejí bezpečnostní funkce, avšak Dell PowerEdge má dodatečné funkce, jako např. hardwarové šifrování dat, ochranu před škodlivým softwarem a možnost vzdálené správy.
- Výkon: Všechny čtyři hardware mají vysoký výkon, ale Dell PowerEdge může zajistit vyšší rychlost zpracování dat díky použití nejmodernějších technologií zpracování a paměti.
- Škálovatelnost: Všechny čtyři hardware mohou být škálovány, ale Dell PowerEdge má flexibilnější architekturu, která umožňuje snadnější škálování systému s růstem společnosti.
- Cena: Cena na všechny čtyři hardware může výrazně lišit v závislosti na konfiguraci a funkcích. Nicméně Dell PowerEdge nabízí výhodný poměr cena a kvalita, což může být důležitým faktorem pro společnosti s omezeným rozpočtem.

Na základě srovnání bylo rozhodnuto, že Dell PowerEdge je nejlepší volbou, protože nabízí širší spektrum funkcí, vyšší výkon a lepší flexibilitu při škálování, což umožňuje společnosti lépe odpovídat jejím potřebám. Kromě toho výhodný poměr cena a kvalita dělá z Dell PowerEdge atraktivní volbu pro společnosti s omezeným rozpočtem.

Obrázek 5: Rozšiřitelný dvousocketový věžový server PowerEdge T430

Zdroj: [21]

Celkově použití systému ochrany informací Cisco Firepower Threat Defense a serverů Dell PowerEdge zajistí spolehlivou ochranu společnosti "AAA" před vnějšími hrozbami a průnikem do sítě, a také zajistí důvěrnost přenosu dat a spolehlivost ukládání informací.

Kromě výše zmíněných systémů bylo také zvažováno použití bezpečnostního řešení pro správu a monitorování, jako je například Splunk Enterprise Security. Tento systém zajišťuje centralizovanou správu logů, monitorování událostí a detekci bezpečnostních incidentů v reálném čase. Pomáhá rychle identifikovat a odstraňovat zranitelnosti v systému, zabránit útokům a skrytí informací a zlepšit účinnost a efektivitu bezpečnostního týmu.

Také bylo bych doporučováno použití řešení pro správu přístupu, jako je Okta Identity Cloud. Tento systém zajišťuje automatizovanou kontrolu přístupu k informacím a aplikacím, což pomáhá zabránit neoprávněnému přístupu k důležitým informacím. Poskytuje také zprávy o aktivitách uživatelů a podporuje multifaktorovou autentizaci, což zvyšuje úroveň bezpečnosti. Použití systému pro správu a monitorování bezpečnosti a systému pro kontrolu přístupu pomůže zabezpečit maximální bezpečnost informací uvnitř společnosti "AAA" a zabránit únikům informací a neoprávněnému přístupu k nim.

4.5. PRÁCE S OSTATNÍMI SPOLEČNOSTMI

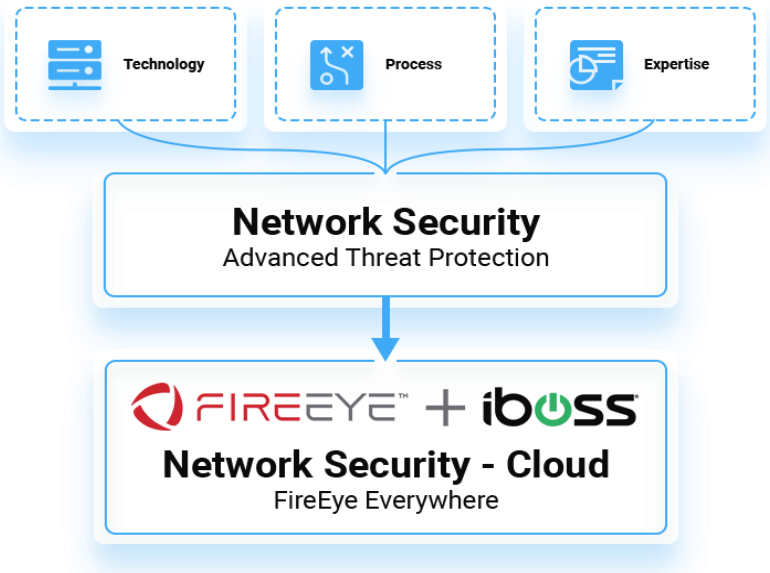
Zde je návrh tří firem, které by mohly pomoci zlepšit bezpečnost společnosti "AAA", která se zabývá výrobou softwaru pro zařízení určená pro různé společnosti, které se věnují údržbě kritické infrastruktury. Vzhledem k vysoké odpovědnosti a nutnosti zachování důvěrnosti v této oblasti je nezbytné zajistit a udržovat vysokou úroveň bezpečnosti uvnitř společnosti. Zvláště

důležitým faktorem je předcházení všem možným pokusům o průmyslovou a kyberšpionáž s cílem ukrýt klíčový duševní vlastnictví.

Níže uvedené firmy by mohly být potenciálními kandidáty pro spolupráci s AAA. Při výběru společnosti pro poskytnutí služeb souvisejících s bezpečností je důležité zvážit mnoho faktorů, jako jsou zkušenosti s podobnými projekty, odbornost, certifikace, renomé v odvětví, cena a další. Mezi nejdůležitější patří zkušenosti společnosti s podobnými projekty, odbornost a certifikace zaměstnanců, používané kryptografické protokoly a algoritmy, dostupnost a kvalita technické podpory a také schopnost poskytnout bezpečné řešení v souladu s nejnovějšími bezpečnostními standardy.

První doporučenou firmou je Accenture Security. Accenture je jednou z největších a nejuznávanějších firem na světě v oblasti kybernetické bezpečnosti. Jejich služby zahrnují strategické poradenství, řízení kybernetické bezpečnosti a zajištění souvisejících technologií. Accenture má velký tým odborníků na kybernetickou bezpečnost, kteří mohou pomoci společnosti "AAA" s ochranou před průmyslovou a kyberšpionáží.

Další společnost, která by byla nabídnuta, je Cylance. Nabízejí inovativní řešení pro zajištění bezpečnosti založené na umělé inteligenci a strojovém učení. Jejich produkty zahrnují systémy pro detekci hrozeb a prevenci útoků, stejně jako řešení pro ochranu koncových bodů a cloudů. Cylance má zajímavý seznam klientů, včetně mnoha společností zabývajících se údržbou kritické infrastruktury, jako jsou plynové a energetické společnosti. Pracují také s vládními a vojenskými organizacemi, což svědčí o vysoké úrovni důvěry, kterou si získali. Nakonec bych bylo doporučena společnost FireEye, která je lídrem v oblasti kybernetické bezpečnosti. Nabízejí širokou škálu produktů a služeb pro detekci a prevenci kybernetických útoků, stejně jako řešení pro vyšetřování incidentů v oblasti kybernetické bezpečnosti. FireEye má obrovské zkušenosti s prací s firmami.



Obrázek 6: Příklad práce FireEye

Zdroj: [22]

Výběr dodavatele zabezpečení sítě a serverů AAA by měl zohlednit mnoho faktorů, včetně zkušeností firmy s podobnými projekty, certifikace, kvalifikace zaměstnanců, používané technologie, kvalita technické podpory a další. Výše uvedené společnosti by mohly být vhodnými kandidáty pro spolupráci s AAA v oblasti bezpečnosti IT. Každá z těchto společností má vynikající zkušenosti v této oblasti a může nabídnout rozmanité řešení pro zabezpečení sítě, serverů, kryptografických protokolů a algoritmů. Zvážení této spolupráce může přinést mnoho výhod pro AAA, včetně zvýšení bezpečnosti, snížení rizika kybernetických útoků a ochranu důvěrných dat a klíčového duševního vlastnictví.

4.6. BEZPEČNOSTNÍ AUDIT A VÝVOJ PLÁNU AKCÍ V PŘÍPADĚ PORUŠENÍ BEZPEČNOSTI

Posoudit existující politiky a postupy bezpečnosti, aby se zjistilo, do jaké míry odpovídají nejlepším praxím v odvětví. To může zahrnovat kontrolu toho, jak efektivně společnost spravuje přístup ke svým systémům a datům, jaké systémy monitorování a řízení přístupu jsou používány, jak jsou prováděny kontroly na zranitelnosti a další.

- Provést testování penetrace, aby se určilo, jak dobře jsou systémy společnosti chráněny před kybernetickými útoky. Takový test může zahrnovat pokusy o průnik do systému pomocí různých metod, například prostřednictvím prolomení hesel nebo použití škodlivých programů.

- Zkontrolovat bezpečnostní opatření, která jsou používána k ochraně fyzických objektů společnosti, jako jsou serverovny nebo laboratoře. Například zkontrolovat přítomnost systémů řízení přístupu, kamerových systémů, ochrany atd.
- Zkontrolovat přítomnost bezpečnostních politik pro zaměstnance společnosti, včetně požadavků na používání složitých hesel, opakované ověřování identity, pravidelné školení zaměstnanců v základech informační bezpečnosti atd.
- Posoudit, jak společnost spravuje svá data, včetně ochrany před úniky, ukládání dat a výměnu informací mezi zaměstnanci společnosti.
- Zkontrolovat přítomnost mechanismů detekce a reakce na bezpečnostní incidenty, jako jsou kybernetické útoky nebo úniky dat, a zkontrolovat účinnost těchto mechanismů.
- Zkontrolovat přítomnost zálohování dat a obnovu po bezpečnostních incidentech.
- Zkontrolovat dodržování právních předpisů v oblasti informační bezpečnosti, které mohou zahrnovat požadavky na ochranu dat, povinnost oznámení o bezpečnostních porušeních atd.
- Posoudit celkovou bezpečnostní kulturu v společnosti, včetně míry povědomí o bezpečnostních rizicích mezi zaměstnanci a jejich chování vůči informacím a systémům společnosti.

Pokud existuje definovány hlavní kroky bezpečnostní auditu, můžeme se podívat na konkrétní kroky k vytvoření akčního plánu v případě porušení bezpečnosti.

- Izolace infikovaných zařízení: Pokud se objeví bezpečnostní hrozba, prvním krokem by byla izolace infikovaných zařízení od firemní sítě, aby se zabránilo šíření škodlivých programů.
- Hodnocení úrovně hrozby: Dalším krokem by bylo hodnocení úrovně hrozby, aby se určil rozsah problému a nutné kroky k jeho odstranění.
- Oznámení odpovědným osobám: Po určení úrovně hrozby bych okamžitě oznámil odpovědným osobám, kteří by měli být informováni o situaci, včetně vedení společnosti a bezpečnostní služby.
- Provádění vyšetřování: Po oznámení odpovědným osobám bych prováděl vyšetřování, aby zjistil, jak došlo k porušení bezpečnosti a jaké kroky musí být přijaty k odstranění hrozby v budoucnosti.
- Odstranění hrozby a obnovení: Po dokončení vyšetřování bych se pustil do odstranění hrozby a obnovy bezpečnostního systému společnosti, aby se zabránilo opakování podobných incidentů.

5. Hodnocení nákladů a účinnosti bezpečnosti

Pro hodnocení efektivity výdajů na bezpečnost nutné zohlednit veškeré výdaje a náklady na zajištění bezpečnosti společnosti. Zde jsou některé z nich:

- Mzdy a cestovné náklady zaměstnanců bezpečnostní služby.
- Vybavení a softwarové zabezpečení pro zajištění bezpečnosti počítačových systémů a sítí.
- Fyzická ochrana budovy a infrastruktury společnosti, včetně kamerových systémů a přístupových kontrol.
- Poradenské služby a školení zaměstnanců v otázkách bezpečnosti.
- Výdaje na bezpečnostní audity a penetrační testování k odhalení zranitelností našich systémů.

Nutno také zohlednit potenciální náklady na možné bezpečnostní incidenty, jako je krádež duševního vlastnictví nebo porušení bezpečnosti našich systémů, které mohou vést ke ztrátě dat a pověsti společnosti.

Pro hodnocení efektivity našich výdajů na bezpečnost můžeme použít metriky, jako je ROI (návratnost investic) a TCO (celkové náklady vlastnictví). ROI yxistuje možnost vypočítat porovnáním výdajů na bezpečnost s ekonomickým prospěchem, který získáme při prevenci potenciálních hrozeb. TCO nám umožní zhodnotit celkové náklady na bezpečnost naší společnosti, včetně nákladů na nákup vybavení, instalaci a podporu bezpečnostního systému. Takže pro hodnocení efektivity výdajů na bezpečnost společnosti "AAA" nutno zohlednit veškeré výdaje na bezpečnost a náklady na prevenci potenciálních hrozeb a použít metriky ROI a TCO k posouzení výsledků našich investic do bezpečnosti.

5.1. Hodnocení ROI

Pro zajištění bezpečnosti v rámci společnosti byla realizována následující opatření:

- Instalace systému řízení přístupu s použitím přístupových karet a biometrických údajů za 1 076 450 Kč.
- Vývoj a zavedení monitorovacího systému událostí v síti za 1 722 320 Kč.
- Pravidelné provádění penetračních testů pro odhalení zranitelností v systémech společnosti za 1 507 030 Kč ročně.
- Školení zaměstnanců v pravidlech informační bezpečnosti za 645 870 Kč.
- Celkové náklady na zabezpečení společnosti činily 6 458 700 Kč.

Avšak díky implementaci těchto opatření byly předcházeny následující hrozby:

- Potenciální prolomení sítě společnosti, které by mohlo vést k úniku důvěrných informací a ztrátám ve výši 10 764 500 Kč.
- Kybernetický útok na servery společnosti, který by mohl vést k výpadku poskytování služeb zákazníkům a ztrátám ve výši 4 305 800 Kč.
- Interní přístup k důvěrným informacím, který by mohl vést k úniku klíčové intelektuální vlastnosti a ztrátám ve výši 2 152 900 Kč.

Díky opatřením zajišťujícím bezpečnost společnost "AAA" ušetřila 17 223 200 Kč. ROI činí 266,67 % ((17 223 200 / 6 458 700) * 100 %). To znamená, že za každou utracenou korunu na bezpečnost přináší společnosti 2,67 Kč ekonomického přínosu.

5.2. Hodnocení TCO

Pro hodnocení bezpečnosti společnosti "AAA" pomocí metody Total Cost of Ownership (TCO) je třeba zohlednit všechny náklady související s bezpečností, včetně kapitálových a provozních nákladů. Kapitálové náklady zahrnují náklady na pořízení hardwaru a softwaru, stejně jako náklady na nastavení bezpečnostních systémů. Provozní náklady zahrnují náklady na školení zaměstnanců, údržbu a aktualizaci bezpečnostních systémů.

Pro společnost "AAA" mohou kapitálové náklady na zajištění bezpečnosti zahrnovat:

- Pořízení a instalaci systému kontroly přístupu za 1 076 450 Kč.
- Pořízení a instalaci systému sledování událostí na síti za 1 722 320 Kč.

Provozní náklady na zajištění bezpečnosti mohou zahrnovat:

- Pravidelné penetrační testy pro odhalení zranitelností v systémech společnosti ve výši 1 507 030 Kč ročně.
- Školení zaměstnanců o pravidlech informační bezpečnosti za 645 870 Kč ročně.
- Náklady na údržbu a aktualizaci bezpečnostních systémů ve výši 1 076 450 Kč ročně.

Celková částka kapitálových nákladů činí 2 798 770, zatímco celková výše provozních nákladů činí 3 229 350 Kč ročně. Celkové náklady na bezpečnost společnosti za tříleté období (dobu analýzy) budou činit 12 486 820 Kč.

Nicméně díky implementaci bezpečnostních opatření byly předejity následující hrozby:

- Potenciální prolomení sítě společnosti, které by mohlo vést ke ztrátě důvěrných informací a ztrátě ve výši 10 764 500 Kč.

- Kybernetický útok na servery společnosti, který by mohl vést k výpadku služeb pro zákazníky a ztrátě ve výši 4 305 800 Kč.
- Interní přístup k důvěrným informacím, který by mohl vést ke ztrátě klíčové duševního vlastnictví a ztrátě ve výši 2 152 900 Kč.

Takto lze celkový ekonomický efekt opatření na zajištění bezpečnosti společnosti AAA vyčíslit jako rozdíl mezi získanými výhodami a náklady na bezpečnost. V případě TCO to umožní vyhodnotit širší spektrum nákladů, zahrnující nejen přímé, ale i nepřímé a skryté náklady na bezpečnost. To umožní lépe posoudit skutečné náklady na bezpečnost a porovnat je s dosaženými výhodami.

Některé náklady, které lze zahrnout při výpočtu TCO pro bezpečnost společnosti AAA, zahrnují:

- Náklady na pořízení a aktualizaci softwaru pro zajištění bezpečnosti, jako jsou antivirové programy, software pro ochranu před hackerskými útoky atd.
- Náklady na školení zaměstnanců v oblasti informační bezpečnosti, aby zvýšili svou odbornost v oblasti zajištění bezpečnosti a snížili pravděpodobnost chyb.
- Náklady na údržbu zařízení pro zajištění bezpečnosti, jako jsou firewally, systémy pro detekci vniknutí atd.
- Náklady na monitorování bezpečnosti, včetně platby personálu zodpovědného za monitorování a zařízení pro monitorování.
- Náklady na pravidelné provádění bezpečnostních auditů, včetně platby služeb externích konzultantů a zařízení pro auditování.

Celkově TCO umožňuje vidět komplexnější obraz nákladů na bezpečnost, včetně nepřímých a skrytých nákladů, a porovnat je s výhodami získanými z opatření na zajištění bezpečnosti. To umožňuje lépe posoudit účinnost opatření na zajištění bezpečnosti a určit, jaké kroky je třeba podniknout k zlepšení bezpečnosti společnosti.

Závěr

V rámci této bakalářské práce se zaměřovala na problematiku kyberšpionáže a možnosti ochrany technologické firmy před tímto typem útoků. Nejprve byla provedena klasifikace a popis různých typů kyberšpionáže. Dále se zabývala problémy s identifikací zločinců a jejich zákazníků, včetně potenciálních hrozeb a hlavních problémů při řešení tohoto problému.

V další části se zaměřovalo na specifiku kybernetické bezpečnosti v technologických firmách, včetně bezpečnostních rizik digitální výroby a zranitelností průmyslových informačních komunikačních systémů. Následně byla provedena analýza firmy a navrhly se základní bezpečnostní kroky, jako bylo vytvoření politiky bezpečnosti informací, zajištění fyzické bezpečnosti, školení a pravidelné aktualizace bezpečnostního systému.

V poslední části bylo provedeno hodnocení nákladů a účinnosti bezpečnostních opatření pomocí hodnocení ROI a TCO. Na základě zjištění bylo doporučeno, aby technologické firmy věnovaly zvýšenou pozornost kybernetické bezpečnosti a přijaly opatření k ochraně svých informačních systémů před kyberšpionáží. Bezpečnostní opatření by měla být pravidelně aktualizována a zaměřena na identifikaci potenciálních hrozeb a zranitelností průmyslových informačních komunikačních systémů. Výsledkem těchto opatření bude snížení rizik spojených s kybernetickými útoky a zvýšení bezpečnosti celého podniku.

Celkově lze tedy konstatovat, že tato bakalářská práce poskytuje ucelený pohled na problematiku kyberšpionáže a navrhuje řadu konkrétních opatření pro zabezpečení technologické firmy. Pokud by tato opatření byla implementována a dodržována, mohla by tato firma efektivně snížit rizika spojená s kyberšpionáží a ochránit své podnikání před negativními dopady kybernetických útoků.

Použitá literatura

1. BELOUSOV, A a A SOLODUKHA. *Základy kybernetické bezpečnosti. Normy, koncepce, metody a prostředky zajištění*. Moskva: Technosféra, 2005. ISBN 978-5-94836-612-8.
2. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model*. [online]. 2006. [cit. 2022-10-16]. Dostupné z: http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R1.pdf
3. *Základní metody zabezpečení informací* [online]. 2020, 20.05.2020 [cit. 2023-01-30]. Dostupné z :https://www.smartsoft.ru/blog/osnovnye_metody_obespechenija_informatsionnoj_bezopasnosti/
4. GULOMOV, Sherzod a Nurlat MAMAJEV. *Analýza metod a prostředků detekce kybernetických hrozeb ve velkých datech* [online]. 28.04.2022, 5 [cit. 2023-02-07]. Dostupné z: https: econferencezone.org
5. Jak zajistit informační bezpečnost ve společnosti: kompletní průvodce od A do Z. *Kickidler* [online]. 24.02.2022 [cit. 2023-01-10]. Dostupné z: https://www.kickidler.com/ru/info/kak-obespechit-informacztionnuyu-bezopasnost-v-kompanii.html
6. JAKOVLEV, V, A SHAMKIN a A BEZBOGOV. *Metody a prostředky ochrany počítačových informacÍ* [online].Tambov: Nakladatelství TGTU, 2006 [cit. 2023-02-01]. ISBN 5-8265-0504-4. Dostupné z: https://www.tstu.ru/book/elib/pdf/2006/shamkin2.pdf
7. KASPERSKYCLUB DAILY. Kyberšikana a legální malware. *Kaspersky* [online]. 2021 [cit. 2022-12-21]. Dostupné z: https://www.kaspersky.ru/blog/legal-malware-counteraction/5539//
8. OSTAPENKO, A, J LYSOV a J KATORIN. *Velká encyklopedie průmyslové špionáže*. 2. dopl. vyd. Petrohrad: Polygon, 2000. ISBN 5-89173-106-1.
9. MCDERMOTT, Roger. *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic*. Tallin: International Centre for Defence and Security, 2004.
10. *Řízení bezpečnosti podnikání* [online]. 2021 [cit. 2023-02-09]. Dostupné z: https://bbooster.online/stati/upravlenie-bezopasnostyu-biznesa.html
11. SKOROBOGATOV S. *Hardware assurance and its importance to national ecurity*, 2012 [cit. 2023-01-10]. Dostupné z: http://www.cl.cam.ac.uk/sps32/secnews.htm

12. SOSNIN, A. *Management bezpečnosti podnikání* [online]. Moskva: Evropska univerzita, 2003 [cit. 2023-01-25]. Dostupné z: https://mybook.ru/author/aleksandr-krishtalyuk/upravlenie-bezopasnostyu-biznesa/read/
13. SOSNIN, A. *Management bezpečnosti podnikání* [online]. Moskva: Evropska univerzita, 2003 [cit. 2023-01-25]. Dostupné z: https://mybook.ru/author/aleksandr-krishtalyuk/upravlenie-bezopasnostyu-biznesa/read/
14. STOUFFER, K, J GILSINN a J FALCO. *Bezpečnost IT pro průmyslové řídicí systémy: specifikace požadavků a testování výkonu*. Crystal City, Virginie: Homeland Security Symposium & Exhibittion, 2004.
15. TIMOFEEV, V a V SOLODKY. *Technická ochrana informací s omezený přístup* [online]. 1. Charkov: Charkov Národní univerzita radioelektroniky, 2013 [cit. 2023-02-01]. ISBN 978-966-7735-62-3. Dostupné z: https://openarchive.nure.ua/server/api/core/bitstreams/cb351e0b-7a2a-474d-82c5-1177519d2a5e/content
16. ANDRIANOV, V., S. GOLDUJEV a V. GOLOVANOV. *Zajištění informační bezpečnosti podniku* [online]. Petrohrad: Alpina Pablishers, 2021 [cit. 2023-01-11]. ISBN 9785457275775. Dostupné z: https://www.litres.ru/book/v-b-golovanov/obespechenie-informacionnoy-bezopasnosti-biznesa-5020392/
17. BOHULICKÁ, N. a M. KUČEROV. *Bezpečnostní modely počítačových systémů* [online]. Vologda: Litres, 2021 [cit. 2023-01-12]. ISBN 9785043596987. Dostupné z: https://www.litres.ru/mihail-kucherov/modeli-bezopasnosti-komputernyh-sistem-65802786/
18. RSI SECURITY. 5 data security methods for large businesses. *Rsisecurity* [online]. 16.12.2019 [cit. 2023-02-01]. Dostupné z: https://blog.rsisecurity.com/5-data-security-methods-for-large-businesses/
19. GOLL, Jan. Z norem řízení bezpečnosti informací se postupně vytrácí řada užitečných věcí. *Tzb-info* [online]. 05.2019 [cit. 2023-02-03]. Dostupné z: https://www.systemonline.cz/sprava-it/normy-rizeni-bezpecnosti-informaci.html
20. *Exkalibr* [online]. [cit. 2023-02-15]. Dostupné z: https://www.exkalibr.sk/cisco-asa-5506-x-firewall-edition-bezpecnostni-zarizeni-8-portu-gbe_d76836.html
21. *Kvan* [online]. [cit. 2023-02-15]. Dostupné z: https://kvan.tech/configurator/dell/T630/
22. *Iboss* [online]. [cit. 2023-02-15]. Dostupné z: https://www.iboss.com/iboss-and-fireeye-cloud-network-security/