Univerzita Pardubice

Fakulta ekonomicko-správní

Metody detekce kybernetických útoků a hrozeb v podnikovém prostředí

Bakalářská práce

2024 Martin Bureš

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Martin Bureš**
Osobní číslo:	**E21579**
Studijní program:	**B0688A140004 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Metody detekce kybernetických útoků a hrozeb v podnikovém prostředí**
Zadávající katedra:	**Ústav matematiky a kvantitativních metod**

Zásady pro vypracování

Cílem práce je popis kybernetických útoků a hrozeb v podnikovém prostředí a souhrn metod jejich detekce a prevence. Budou uvedeny příklady detekovaných útoků a vyplývajících hrozeb z praxe. V praktické části budou popsány kybernetické hrozby pro vybranou firmu včetně zlepšovacích návrhů do budoucna.
Osnova:

- Metody kybernetických útoků.
- Druhy detekce a prevence kybernetických útoků.
- Hrozby ve vybrané firmě.
- Navrhované metody prevence útoků.

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

Seznam doporučené literatury:

HUB, Miloslav. Bezpečnost a ochrana informací v prostředí internetu. Pardubice: Univerzita Pardubice, 2013. ISBN 978-80-7395-701-8.
KIZZA, Joseph Migga. Guide to computer network security. Fourth edition. Cham, Switzerland: Springer--Verlag, 2017. Computer communications and networks. ISBN 978-3-319-55605-5.
MITNICK, Kevin D. a William L. SIMON. Umění klamu: nejslavnější hacker na světě. Gliwice: Helion, c2003. ISBN 83-7361-210-6.
SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380--765-8.
SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7.

Vedoucí bakalářské práce: **Mgr. Jana Heckenbergerová, Ph.D.**
Ústav matematiky a kvantitativních metod

Datum zadání bakalářské práce: **1. září 2023**
Termín odevzdání bakalářské práce: **30. dubna 2024**

L.S.

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

Ing. et Ing. Martin Lněnička, PhD. v.r.
garant studijního programu

V Pardubicích dne 1. září 2023

Prohlášení

Prohlašuji:
Práci s názvem Metody detekce kybernetických útoků a hrozeb v podnikovém prostředí jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v 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 a 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
30. 4. 2024

Martin Bureš v. r.

Poděkování

Tímto bych rád poděkoval své vedoucí práce Mgr. Janě Heckenbergerové, Ph.D. za její cennou pomoc a odborné rady, které mi pomohly ve vypracování této práce. Dále bych chtěl také poděkovat Ing. Luďkovi Tichému ze společnosti ČEZ Distribuce, a.s. za jeho ochotnou pomoc a všechny poskytnuté materiály. Nakonec bych rád poděkoval svým rodičům, přítelkyni a Vojtovi, Vítovi a Lukášovi za jejich trpělivost a podporu.

Anotace

Tato práce je věnována popisu metod obrany proti kybernetickým útokům. Jsou zde uvedeny příklady kybernetických útoků i způsoby, jak se proti nim bránit. Praktická část práce obsahuje podrobný popis bezpečnostního systému reálné firmy, včetně jednotlivých nástrojů, bezpečnostní politiky, i návrhů do budoucna.

Klíčová slova

bezpečnost, kybernetické útoky, kyberprostor, internet, sítě

Title

Methods of detecting cyberattacks and threats in a business environment

Annotation

This work deals with describing methods of protection against cyberattacks. There are given examples of cyberattacks and ways of how to defend against them. The practical part of this work contains an in depth description of a security system of a real company, including individual tools, security policy and suggestions for the future.

Keywords

security, cyberattack, cyberspace, internet, networks

Obsah

SEZNAM OBRÁZKŮ 5

ÚVOD 10

1 KYBERNETICKÝ ÚTOK 11

1.1 Útočník 11
1.2 Zranitelné místo 12
1.3 Hrozba 12
1.4 Motivy kybernetických útoků 13
1.5 Typy a dělení útoků 14
1.5.1 Dělení útoků dle škody 14
1.5.2 Dělení útoků dle cíle 15
1.5.3 Dělení útoků dle provedení 15
1.6 Malware 17

2 METODY A DRUHY KYBERNETICKÝCH ÚTOKŮ 18

2.1 Necílené útoky 18
2.1.1 Phishing 18
2.1.2 Internetový bot 19
2.2 Cílené útoky 19
2.2.1 Prolamování hesel 19
2.2.2 Sociotechnika 20
2.2.3 Útoky zevnitř 21

3 DRUHY DETEKCE A PREVENCE KYBERNETICKÝCH ÚTOKŮ 23

3.1 Monitoring 23
3.2 Nástroje kybernetické bezpečnosti 24
3.2.1 Antiviry 24
3.2.2 Firewally 24
3.3 Analýza rizik 25
3.3.1 Identifikace aktiv 26
3.3.2 Stanovení hodnot aktiv 26
3.3.3 Identifikace hrozeb 26
3.3.4 Analýza hrozeb a zranitelností 26
3.3.5 Výpočet ztráty 27
3.4 Proškolení zaměstnanců 27
3.5 Postupy v případě krize 28

4 KYBERNETICKÉ HROZBY VE SPOLEČNOSTI ČEZ 30

4.1 Četnost útoků 30
4.1.1 Necílené útoky 30
4.1.2 Útoky řešené automaticky 30
4.1.3 Útoky řešené manuálně 30
4.1.4 Kybernetické incidenty 31
4.2 Druhy kybernetických hrozeb 31
4.2.1 DDoS útok 31
4.2.2 Ransomware 32
4.2.3 Vnitřní hrozby 33

5 BEZPEČNOSTNÍ POLITIKA A BEZPEČNOSTNÍ OPATŘENÍ SPOLEČNOSTI ČEZ 34

5.1 PDCA cyklus 34
5.2 Bezpečnostní role 35
5.3 Pasivní prvky obrany 36

5.3.1 Sytém IDS ... *36*
5.3.2 Systém IPS ... *36*
5.3.3 Systém IDR ... *37*
5.4 Aktivní prvky obrany ... 37
5.4.1 SIEM ... *38*
5.4.2 Nadstavba SOAR ... *39*
5.4.3 Anti-DDoS ... *40*
5.5 Dokumentace ... 41
5.5.1 Systémy ISMS ... *41*
5.5.2 Konfigurační databáze CMDB ... *41*
5.6 Zabezpečení zevnitř ... 42
5.6.1 Řízení identit ... *42*
5.6.2 Klasifikace dokumentů ... *42*
5.6.3 Školení zaměstnanců ... *43*
5.7 Krizové řešení ... 45
6 NAVRHOVANÉ METODY PREVENCE ÚTOKŮ ... 46
6.1 Navrhované nástroje ... 46
6.1.1 EDR ... *46*
6.1.2 XDR ... *47*
6.2 Provádění analýzy rizik ... 48
6.3 Zavádění nových nástrojů ... 49
6.3.1 Hardening ... *49*
6.3.2 Penetrační testy ... *49*
ZÁVĚR ... 50
SEZNAM ZDROJŮ ... 51
Použitá literatura ... 51
Elektronické zdroje ... 51

Seznam obrázků

Obrázek 1: Informační tok; Zdroj: vlastní, na základě [2] ... 15
Obrázek 2: Útok přerušením; Zdroj: vlastní, na základě [2] ... 16
Obrázek 3: Útok odposlechem; Zdroj: vlastní, na základě [2] ... 16
Obrázek 4: Útok modifikací; Zdroj: vlastní, na základě [2] ... 16
Obrázek 5: Útok přidáním hodnoty; Zdroj: vlastní, na základě [2] ... 17
Obrázek 6: Bastion host mezi vnitřní a vnější sítí; Zdroj: vlastní, na základě [5] ... 25
Obrázek 7: PDCA cyklus; Zdroj: [17] ... 35
Obrázek 8: Porovnání vývoje OWASP Top Ten mezi roky 2017 a 2021; Zdroj: [16] ... 40

Seznam zkratek a značek

AD – Active Directory

BCM – Business Continuity Management

BCP – Business Continuity Plan

BIA – Business Impact Analysis

CMDB – Configuration Management Database

DDoS – Distributed Denial of Service

DLP – Data Loss Prevention

DoS – Denial of Service

DRP – Disaster Recovery Plan

EDR – Endpoint Detection and Response

IDM – Identity Management

IDR – Intrusion Detection and Response

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

ISMS – Information Security Management Systems

MITRE ATT&CK – Adversarial Tactics, Techniques, and Common Knowledge

PAM – Privileged Access Management

PDCA – Plan, Do, Check, Act

PIM – Privileged Identity Management

SIEM – Security Information and Event Management

SOAR – Security Orchestration, Automation and Response

SOC – Security Operation Center

XDR – Extended Detection and Response

Úvod

V dnešní době, internetové éře, kdy čím dál tím víc aspektů každodenního života probíhá za obrazovkou, si lze podnik bez jakékoliv digitální přítomnosti představit jen těžko. Byť jen v podobě webových stránek, internetové reklamy, či dokonce celého výplatního systému, většina firem v České republice nějakým způsobem proniká do digitální sféry, ať už za účelem přilákání nových zákazníků nebo jen k uchování soukromých firemních dat. S každým dalším krokem integrace do digitálního prostředí ovšem roste i riziko cíleného kybernetického útoku, tedy hrozby, že se někdo pokusí napadnout firemní systém a způsobit v něm škody.

Každá firma a podnik se tedy musí zamyslet nad tím, jak se před kybernetickými hrozbami chránit a jak zabezpečit svoje firemní zdroje a aktiva před vnějšími i vnitřními útoky. Tomuto riziku čelí všechny organizace od těch nejmenších podniků až po velké mezinárodní společnosti. Tato bakalářská práce je zaměřena především na metody prevence a detekce kybernetických útoků a je strukturována do několika velkých kapitol.

V kapitole **Kybernetický útok** jsou definované základní termíny používané v kybernetické bezpečnosti včetně popisu útočníka a jeho motivací, vysvětlení pojmů hrozba a zranitelné místo, stejně jako představení základních typů kybernetických útoků a škodlivého kódu.

Kapitola **Metody a druhy kybernetických útoků** už se zaměřuje na konkrétní způsoby, kterými může útočník napadnout firemní systém nebo jakým způsobem dokáže přimět samotné zaměstnance firmy, aby mu přístup do systému sami poskytli.

První část této práce nakonec uzavírá kapitola **Druhy detekce a prevence kybernetických útoků**, která se zaměřuje na konkrétní ochranné nástroje i celkové bezpečnostní praktiky, které pomáhají kybernetické útoky odhalovat a předcházet jim.

V druhé části práce je pak na praktickém příkladě dopodrobna rozebraný bezpečnostní systém skupiny ČEZ Distribuce, a.s., velké celostátní energetické firmy. Jsou zde představeny unikátní hrozby, kterým musí firma takového rozsahu čelit, způsoby a konkrétní nástroje, pomocí kterých těmto hrozbám čelí a celková bezpečnostní infrastruktura, na které je celý systém postavený. V závěru práce jsou také poskytnuty navrhované nástroje, které by se daly v budoucnu použít a rozepsané procesy, které musí každý nový bezpečnostní prvek podstoupit, než je spuštěn do provozu.

1 Kybernetický útok

Před rozdělením kybernetických útoků do různých typů je vhodné definovat si, co to vlastně **kybernetický útok** je a určit si význam několika důležitých pojmů. Pod termínem útok se běžně rozumí využití **zranitelného místa** informačního systému firmy, ať už úmyslné či neúmyslné, které vede ke škodě na firemních aktivech. Aktivem se rozumí cokoliv, co má pro subjekt hodnotu, která může být snížena působením hrozby. Podle rozsahu škod se útoky dají dělit na útoky významné (takové, kde je škoda na aktivech vysoká) a na útoky nevýznamné (takové, kde je rozsah škod velmi nízký). [2] [3] [19]

Samotný pojem **kybernetický útok** pak znamená jakýkoliv útok odehrávající se v síti. Tento termín se začal používat až někdy v druhém desetiletí 21. století a do té doby sloužil pro označení útoků na výpočetní technologie výraz počítačový útok. Počítačovým útokem se rozumí útok nejen na počítač jako celek, ale i na jakoukoliv jeho část, ať už je to hardware, software, či uchovávaná data. [4]

Útok na data je nejběžnějším typem útoku a může být proveden na data uložená i na jiném nosiči dat, jako jsou třeba flash disky či jiné externí paměti, a zároveň i na data v době jejich přenosu prostřednictvím sítě. [4]

Dnes už se ovšem souhrnně používá termín **kybernetický útok**, který označuje útok na jakékoliv zařízení v síti se svojí vlastní IP adresou, tedy nejen počítače, ale i jakékoliv jiné zařízení, které umí komunikovat s ostatními prvky v **kyberprostoru**. Pojmem **kyberprostor** se pak rozumí prostor tvořený počítačovou sítí a jejími jednotlivými prvky. [4]

1.1 Útočník

Kybernetickým útočníkem, někdy také nazývaným hackerem, se rozumí osoba, která takový **kybernetický útok** vykoná, ať už úmyslně nebo neúmyslně. Útočníci se dají rozdělit na základě jejich schopnosti napáchat škody, a to na útočníky slabé, střední a velké síly. Schopnost napáchat škody se odvíjí přímo od útočníkových zkušeností. Jednoduchý **kybernetický útok** může za pomocí pár programů provést prakticky kdokoliv, na rafinovanější útoky už je ovšem potřeba se v kybernetické bezpečnosti firmy vyznat. [2] [19]

Útočníci mohou mít mnoho důvodů kybernetický útok provést a k dosažení svých cílů volí všechny možné metody. Ti zkušenější navíc před každým pokusem o útok provádí

průzkum prostředí, do kterého se chystají vniknout, a podle toho přizpůsobí svůj přístup. [19]

1.2 Zranitelné místo

Zranitelným místem se v oblasti digitální bezpečnosti rozumí slabina v informačním systému, která může být útočníkem využita k napáchání škod. Podstata takové slabiny může spočívat v několika různých faktorech. **Zranitelná místa** vznikají běžně jako následek nějakého selhání, ať už přehlédnutí nedostatku v systému během jeho návrhu. Dalším důvodem vzniku zranitelného místa může být zanedbání pečlivé konstrukce systému nebo jeho správného provozu. [2]

Běžně rozlišujeme různé druhy podstaty zranitelného místa:

- **Fyzická podstata** zranitelného místa spočívá v nedostatku zabezpečení fyzických komponentů informačního systému. Může tím být například nevhodné umístění serveru na místě, ke kterému má útočník snadný přístup a mohl by ho tak snadno poškodit.
- Zranitelné místo s **přírodní podstatou** nastává v případě nedostatku ochrany systému před přírodními jevy, jakými jsou například zemětřesení, záplavy, blesk či sněhová bouře. Pravděpodobnost výskytů takových jevů se sice může zdát nízká, ale i přírodní jev může firmě způsobit rozsáhlé škody, proto se nesmí opomíjet.
- Do **fyzikální podstaty** zranitelného místa jsou zařazována nebezpečí jako vyzařování nebo i útoky na komunikaci.
- Nejdůležitějším zranitelným místem je ovšem **lidský faktor**. Lidé jsou nejzranitelnější součástí každého informačního systému a jejich zahrnutí je nevyhnutelné. Této slabině je třeba věnovat zvláštní péči, jelikož lidé dělají chyby mnohem častěji než stroje a pro útočníka tak mnohdy bývají snazším cílem.

  [1] [2]

Výskyt zranitelného místa v systému způsobuje, že některé vlivy prostředí pro něj znamenají **hrozby**.

1.3 Hrozba

Hrozbou se v informační bezpečnosti rozumí možnost využití **zranitelného místa** systému k útoku za účelem způsobení škody. Je to tedy aktivita, událost, či osoba, která může

mít negativní dopad na firemní aktiva a způsobit škodu. Výše této potenciálně utrpěné škody se nazývá dopad hrozby. Ten může být odvozen od absolutní hodnoty potenciálních škod, které zahrnují i znovuobnovení řádné činnosti a odstranění následků škod. Existují dva hlavní typy hrozeb – objektivní a subjektivní. [2] [3]

Pod **objektivní hrozbou** se rozumí taková, která hrozí všem firmám. Nachází se tu hrozby přírodní (například požár či záplava), fyzikální a technické (například porucha hardwaru). [2]

Subjektivní hrozby jsou takové, které se týkají konkrétní firmy. Taková hrozba může být buď neúmyslná, způsobená nechtěně či omylem, jako například když špatně proškolený zaměstnanec způsobí výpadek serveru; nebo úmyslná, kterou má na svědomí útočník, ať už vnitřní (nespokojení zaměstnanci), či vnější. [2]

Další důležitou charakteristikou hrozby je její úroveň. Ta se hodnotí podle tří následujících faktorů: **nebezpečnosti**, **přístupu** a **motivace útočníka**. Mírou **nebezpečnosti** hrozby se rozumí její schopnost způsobit škodu. Faktor **přístupu** znamená pravděpodobnost toho, že se působení hrozby dostane až k aktivu. **Přístup** může být vyjádřen také frekvencí výskytu hrozby. Posledním rozhodujícím faktorem je **motivace útočníka**, který se odvíjí od útočníkova zájmu iniciovat hrozbu vůči danému aktivu. [3]

1.4 Motivy kybernetických útoků

I když bezpečnostní hrozba může přijít z přírodního zdroje či neúmyslných lidských chyb, většina hrozeb a následných útoků v kyberprostoru jsou způsobeny nelegálními či kriminálními aktivitami pocházejících ať už zevnitř, či zvenku. Federální úřad pro vyšetřování (FBI) v USA roztřídil možné motivace kybernetických útočníků do následujících skupin: terorismus, vojenská špionáž, **ekonomická špionáž**, zacílení Národní informační infrastruktury (National Information Infrastructure), **odplata**, **nenávist**, **proslulost**, **finanční zisk** a **ignorance**. [5]

Toto rozdělení bylo vytvořeno primárně za účelem celkové národní bezpečnosti, nikoliv pro podnikové prostředí, proto pro účely této závěrečné práce nebudou skupiny terorismus, vojenská špionáž a zacílení Národní informační infrastruktury dál rozepsány. [5]

Ekonomická špionáž je ve své nejčistší formě útokem na obchodní tajemství a slouží k účelu nelegálního získání konkurenčně významných skutečností napadené firmy. [5]

Existuje mnoho důvodů vedoucích ke kybernetické **odplatě.** K těm závažnějším patří například nespokojenost s velkými firmami, nesouhlas s rozhodnutími vlády a mnohé podobné, které mohou vést jedince či skupinu jedinců k útoku na politické či jiné systémy, které vnímají jako nespravedlivé a škodlivé. Většina důvodů k odplatě je ovšem mnohem všednějších, jako například zamítnutá žádost o povýšení, vyhazov z práce a další situace zahrnující rodinné či osobní problémy. [5]

Nenávist jako motiv vždy proudí a je založena na odporu jedince či skupiny jedinců ke konkrétní rase, náboženství či pohlaví. Na základě toho tito jedinci zvažují **kybernetický útok** na firmu vedenou osobami či zaměstnávající osoby, vůči kterým je tato nenávist vedená. [5]

Vidina **Proslulosti** v kybernetické sféře je motiv převážně mladých hackerů, kteří touží prokázat svoje hackerské znalosti a kompetence a proniknutím do zabezpečeného systému si tak vybudovat respekt mezi svými vrstevníky. [5]

Finanční zisk je motivem mnoha útočníků, kteří za svoje útoky chtějí získat peněžní odměnu. Ta může pocházet už předem od někoho, kdo si hackerské služby pronajme, aby získal nějaké legálně nedostupné informace, nebo prodejem nelegálně získaných dat konkurenci. [5]

Ignorance jako motivace ke kybernetickému útoku může mít mnoho podob, jedná se ovšem často o začátečnické chyby v bezpečnosti způsobené nezkušenými či neproškolenými uživateli, kteří mohou nevědomky využít slabého místa v informačním systému, což může vést k napáchání škod na firemních aktivech. [5]

1.5 Typy a dělení útoků

Kybernetické útoky samotné se pak dají dělit do několika skupin na základě různých kritérií. Mezi nejběžnější rozdělení patří dělení dle záměru (na úmyslný či neúmyslný útok), dělení dle škody, dle cíle útoku a dle provedení. [2]

1.5.1 Dělení útoků dle škody

Útoky dělené dle rozsahu škod se dělí na útoky s malou škodou a na útoky s velkou škodou.

Útoky s malou škodou se označují také jako nevýznamné útoky. Takové útoky bývají často automatické a necílené na jeden konkrétní objekt, jako například různé druhy

spamů. Takových útoků v kyberprostoru probíhá spousta a větší firma jim musí čelit prakticky neustále. [2]

Naproti tomu **útoky s velkou škodou** nebo také významné útoky bývají hlavně cílené, provedené za účelem napáchat škody na nějakém konkrétním objektu. K jejich provedení už je ale potřeba zkušenější a schopnější útočník, proto k nim nedochází až tak často. [2]

1.5.2 Dělení útoků dle cíle

Kybernetický útok může být zacílený na několik rozdílných komponentů systému, na základě útočníkova záměru. V tomto směru rozpoznáváme **útok na hardware**, **útok na software** a **útok na data**. [2]

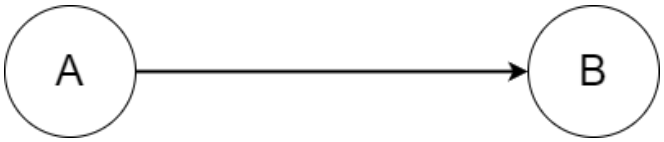
Útokem na hardware se rozumí útok na jakoukoliv fyzickou součást systému. Může jím být například záměrné přehlcení serveru, způsobené tak, aby přestal fungovat a tím zamrazil celý informační systém.

Útok na software je naproti tomu útok na programové vybavení systému, za jehož účelem může stát například neoprávněné vpuštění útočníka dovnitř.

A v poslední řadě **útok na data** je už cílený na samotné zabezpečené informace, které takovýmto útokem chce útočník buď získat pro vlastní užitek nebo narušit jejich integritu, aby zamezil jejich řádnému použití oprávněnými zaměstnanci firmy.

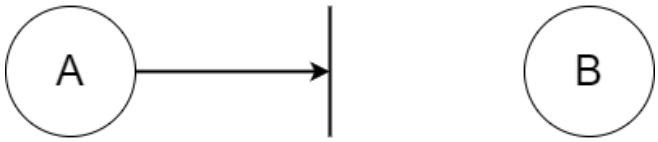
1.5.3 Dělení útoků dle provedení

Útok ve své podstatě nějakým způsobem narušuje tok informací. Běžný informační tok přenáší v prostředí informačního systému informace od zdroje k uživateli a útoky tento přenos mohou nějakým způsobem tento přenos měnit nebo blokovat. **Chyba! Nenalezen z droj odkazů.** [2]



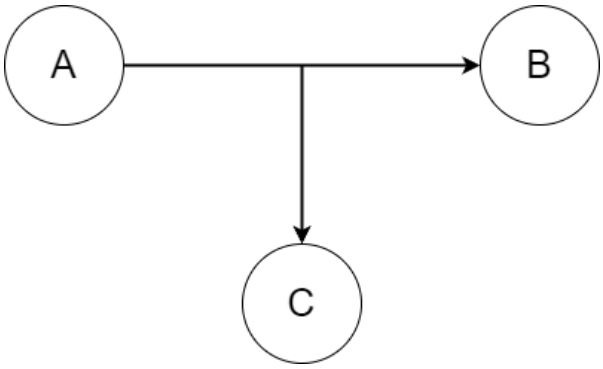
Obrázek 1: Informační tok; Zdroj: vlastní, na základě [2]

Útok přerušením nebo také útok na dostupnost informační tok kompletně zablokuje, tak, že informace vysílaná zdrojem nedorazí k cíli a uživatel tak dané informace nedostane. [2]



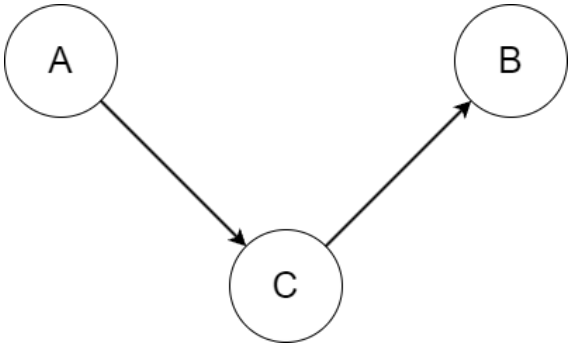
Obrázek 2: Útok přerušením; Zdroj: vlastní, na základě [2]

Naproti tomu během **útoku odposlechem** čili útokem na důvěrnost informace k uživateli neporušeně dorazí, avšak dorazí také k neoprávněnému útočníkovi, který tento útok provedl. Pokud útočník takto zachytí citlivá data, může být tento druh útoku velice účinný. [2]



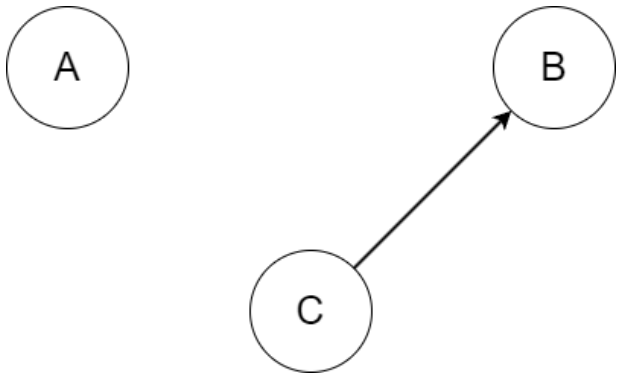
Obrázek 3: Útok odposlechem; Zdroj: vlastní, na základě [2]

Při **útoku modifikací** útočník odchytí informace zaslané od zdroje, poupraví (modifikuje) je a takto upravenou informaci odešle dál uživateli. Sám tak obdrží původní nezměněnou informaci a zároveň tím dezinformuje oprávněného uživatele. Proto se tento útok nazývá také jako útok na integritu dat. [2]



Obrázek 4: Útok modifikací; Zdroj: vlastní, na základě [2]

A nakonec **útokem přidáním hodnoty** útočník pouze posílá uživateli svoje nesprávné či neautentizované informace bez toho, aniž by nějak narušil přítok informace ze zdroje. Tento druh útoku slouží buď pro dezinformaci oprávněného uživatele nebo pro falešnou autentizaci svého vlastního informačního toku. Tento druh bývá nazývaný také jako útok na autenticitu a integritu. [2]



Obrázek 5: Útok přidáním hodnoty; Zdroj: vlastní, na základě [2]

1.6 Malware

Kybernetické útoky také mohou mít různé druhy záměru. Některé kybernetické útoky, převážně **útoky na data**, se soustředí na získání nějaké utajované informace, jiné zas na pouhé poškození napadeného prvku pomocí šíření **malwaru**. Pod pojmem **malware** se rozumí počítačový program určený k poškození počítačového systému. Typickými příklady **malwaru** jsou různé druhy **virů**, **trojských koní**, **spywaru** a podobně. [2]

Počítačový **virus** je nejtypičtějším příkladem **malwaru**. Jedná se o počítačový program, který po svém spuštění nakazí ostatní spustitelný software a začne v počítači provádět škody. Může se stejně jako každý jiný software přenášet po internetu či po datových nosičích. Existují různé typy **virů**, které se od sebe liší svojí nenápadností, způsobu páchání škod nebo i ve schopnosti sami sebe modifikovat. [2] [25]

Trojský kůň je pak konkrétní druh počítačového **viru**, který je skrytou součástí počítačového programu, který se tváří jako užitečný software, při spuštění ale provádí zároveň i před uživatelem skrytou činnost, která je pro něj nežádoucí. [2]

Další typy malwaru jako jsou třeba **spyware** či **adware** se liší svým úkolem. Spyware má například za úkol sledovat počínání uživatele napadeného stroje, kdežto **adware** ho zase zasypává spoustou reklam. Existuje mnoho různých druhů **malwaru** a počítačových **virů** a útočníci stále vymýšlejí a vytvářejí nové. [2]

2 Metody a druhy kybernetických útoků

Existuje spousta způsobů, kterými může útočník napadnout firemní kyberprostor. Metoda, kterou je kybernetický útok proveden, se nazývá **vektor útoku**, který popisuje, kudy je daný útok veden a co je jeho cílem. A právě na základě cíle se dají všechny kybernetické útoky rozdělit do dvou základních skupin, na **cílené** a na **necílené**. Jednotlivých **vektorů útoků** ovšem existuje spousta a s přibývajícím časem útočníci vymýšlejí stále nové, proto jsou v této práci zmíněné pouze ty nejběžnější a nejznámější. [19]

2.1 Necílené útoky

Necíleným útokem se rozumí takový útok, který směřuje na velký počet uživatelů a nezáleží při něm na tom, komu způsobí škody. Všechny uvedené metody se ovšem dají použít i pro útok na jeden konkrétní cíl. Tyto útoky z pravidla nebývají příliš rafinované a nevyžadují od útočníka mnoho zkušeností, můžou ale být zákeřné, pokud na ně není firemní bezpečnostní systém připraven.

2.1.1 Phishing

Phishing je typickým příkladem necíleného kybernetického útoku. Název pochází od anglického slova pro rybaření, fishing, a stejně jako rybář útočník při provádění tohoto útoku nahodí návnadu a čeká, jestli se na ní někdo chytí. Návnada může mít podobu například falešného e-mailu, takzvaného **spamu,** který je posílán hromadně a vybízí příjemce k zadání svých přihlašovacích údajů, třeba za záminkou obnovení účtu. [24]

Falešný e-mail sloužící k metodě **phishing** může vypadat například takto:

Vážený uživateli,

Vzhledem ke změnám v systému naší e-mailové služby by se mohlo stát, že vaše aktuální e-mailová schránka bude automaticky smazána. Pokud s touto změnou nesouhlasíte, zašlete nám do 3 dnů svoje přihlašovací údaje na adresu hesla@seznam.cz.

Váš

Tým Seznam

Útočník se přitom snaží, aby zasílaný **spam** vypadal oficiálně a podobal se opravdovým e-mailům, které příjemce čas od času obdrží. Pokud příjemce falešné výzvě

vyhoví a útočníkovi přihlašovací údaje zašle, poskytne mu tak plný přístup k jeho e-mailové schránce. Jelikož k **phishingu** nepotřebuje útočník žádné zvláštní zkušenosti či nástroje, jedná se o velice běžný, přesto však účinný útok.

2.1.2 Internetový bot

Internetovým **botem** se rozumí automatický počítačový program, který pro svého uživatele vykonává nějakou předem stanovenou opakovanou činnost. Ne vždy musí tito **boti** nutně sloužit jako prostředek k útoku, můžou například sbírat informace o nějaké webové stránce nebo moderovat komentáře pod příspěvky. [25]

Dají se ovšem využít útočníky k různým druhům útoků, ať už se jedná o **phishing**, kdy **boti** zasílají automaticky hromadné **spamy**, či třeba jen zahlcení komentářů vlastní reklamou nebo nevhodným obsahem pro způsobení reputační škody firmě, která stránku vlastní.

Obzvlášť škodliví boti také mohou přenášet **malware**, například v podobě počítačových červů, kteří dokážou z napadených počítačů rozesílat tento škodlivý software dál. Tato nakažená zařízení mohou vytvořit síť zvanou **botnet**, která je používaná k návazným útokům, jakými jsou rozesílání spamu či **DDoS** útok. [2] [25]

2.2 Cílené útoky

Naproti necíleným útokům pak stojí **cílené útoky**, tedy takové, u kterých má útočník zvolený konkrétní cíl, který chce napadnout. Jelikož se útočník může přizpůsobit konkrétním bezpečnostním systémům obránce, bývají tyto už útoky o něco složitější a rafinovanější. S narůstající mírou bezpečnosti ovšem taky narůstají požadavky na útočníkovy znalosti a zkušenosti, aby dokázal bezpečnostní systémy napadeného subjektu obejít.

2.2.1 Prolamování hesel

Nejpřímější způsob cíleného útoku je pokus o prolomení přístupového hesla k nějakému uživatelskému účtu. Tímto účtem může být pracovní či soukromý e-mail, firemní účet používaný k přístupu do interního systému nebo i administrátorský účet správce sítě. Skrz ně by útočník dostal přístup k soukromým věcem, utajovaným dokumentům a v horších případech i k nastavení sítě. Existuje mnoho způsobů a metod, dle kterých může útočník heslo prolomit, proto by se zabezpečení hesel nemělo podceňovat.

Nejzákladnější metodou je přitom takzvaná metoda **útoku hrubou silou**. Ta spočívá v odhadu hesla pomocí softwaru, který postupně zkouší zadávat všechny možné kombinace

písmen, čísel a znaků, dokud se takto vygenerovaný řetězec nebude rovnat uživatelskému heslu. V principu je to jen otázka času, kdy software uživatelské heslo uhodne. Čím kratší heslo je, tím rychleji půjde uhodnout. Proto se vždy preferuje zvolit si co nejdelší heslo, jelikož čas na jeho uhodnutí se může pohybovat v rámci týdnů, což už se ve většině případů útočníkovi nevyplatí. [2]

Slovníková metoda je podobně jako metoda hrubého útoku způsob, kterým se dá přístupové heslo uhodnout. Ovšem místo toho, aby software zadával zcela náhodné znaky, zkouší postupně vkládat běžně používaná slova. Vzhledem k tomu, že většina uživatelů si volí snadno zapamatovatelná hesla, jakými jsou „*heslo*“, „*password*“, „*12345*“, či svoje vlastní křestní jméno, bývá tato metoda často úspěšná. Pokročilejší programy navíc dokážou slova kombinovat, střídat velká a malá písmena, a dokonce i vyměňovat některá písmena za číslice, což je taky běžně rozšířený jev ve výběru hesel. Proto se vždy doporučuje volit takové heslo, jehož význam nic neznamená a vložit do něj i čísla a jiné složitější znaky. [2]

Existuje ještě další řada různých metod, které dělají prolomování hesel jednodušší. Některé dokážou například odhadnout délku hesla či místo a četnost použití čísel. Proto se při volbě správného uživatelského hesla nesmí zanedbávat základní bezpečnostní pravidla, jakými jsou vytvoření dostatečně dlouhého hesla bez jednoznačného významu. Je vhodné také ve firmě zavést způsob dvoufázového ověřování, napojené na zaměstnancův e-mail, čí telefonní číslo. Zanedbání těchto kroků totiž útočníkovu práci dost usnadní a nebude mít problém dostat se k utajovaným informacím.

2.2.2 Sociotechnika

Jedny z nejzákeřnějších kybernetických útoků, se kterými se člověk může setkat, ovšem výpočetní techniku využívají minimálně. Naproti tomu využívají **sociotechniku**, také nazývanou sociální inženýrství. Ta je úzce spojená s metodou **phishing** Kevin Mitnick, označovaný jako nejznámější hacker na světě, popisuje **sociotechniku** jako *„ovlivňování a přesvědčování lidí s cílem oklamat je tak, aby uvěřili, že **sociotechnik** je osoba s totožností, kterou předstírá a kterou si vytvořil pro potřeby manipulace“*. [1]

Šikovný **sociotechnik** tak dokáže jen třeba pomocí mobilního telefonu přelstít důvěřivého zaměstnance, který mu pak sám ochotně nadiktuje přístupová hesla do informačního systému nebo mu pošle důvěrné dokumenty, jelikož si o útočníkovi myslí, že je také zaměstnancem firmy. Obejde přitom veškeré firewally, ověřovací zařízení a další

nástroje kybernetické bezpečnosti a využije u toho jen zaměstnancovi neopatrnosti. K dosažení svého cíle navíc může používat i metody phishingu. [1] [19]

Útočník přitom běžně působí jako charismatický a sebevědomý člověk. Správný **sociotechnik** si před pokusem o útok nejprve provede důkladný průzkum firmy, na kterou se rozhodl zaútočit. Pomocí něj si pak dokáže získat perfektní znalosti firmy, firemních procesů, a třeba i správného použití firemní terminologie a žargonu, a díky nim si plně vybudovat zaměstnancovu důvěru. [1] [2]

Budování důvěry může také spočívat ve vykonání nějaké služby pro daného zaměstnance. **Sociotechnik** tak může schválně vytvořit zaměstnanci nějaký problém (nebo si ho klidně jen vymyslet) a pomůže mu ho vyřešit. Zaměstnanec v něm pak vidí kolegu a nepřemýšlí už nad tím, zda do firmy doopravdy patří. [1]

Takto vybudovanou důvěru útočník využije k získání nějaké důvěrné informace, kterou mu poté důvěřivý zaměstnanec rád poskytne. Tato informace už může být to, pro co **sociotechnik** přišel, nebo mu jen může pomoci dostat se hlouběji do systému či zase oklamat někoho jiného. [1]

Proti neproškoleným a neopatrným zaměstnancům můžou být sociotechnické metody velice účinné, jelikož útočníci se zaměřují převážně na lidské slabiny, jakými jsou důslednost, snaha zapadnout, podřídit se autoritě anebo třeba i snaha pomoci. [2]

2.2.3 Útoky zevnitř

Další část kybernetické bezpečnosti, která by se v podnikovém prostředí neměla opomíjet, je ochrana před svými vlastními zaměstnanci. Z výzkumů stále vychází najevo, že největší hrozbou pro firmu v jakékoliv oblasti je její vlastní personál. Ten má k dispozici vnitřní přístup do firmy a s tím spojené vědomosti o firemních technologiích, zdrojích, vybavení a systémech. [5] [23]

Už v roce 1997 provedla účetní firma Ernst & Young průzkum s 4226 IT manažery po celém světě o bezpečnosti jejich sítí. Z jejich odpovědí vyšlo najevo, že 75 % všech manažerů věří, že autorizovaní uživatelé a zaměstnanci představují pro podnik bezpečnostní hrozbu. 43 % všech respondentů navíc nahlásilo, že mají zkušenosti se škodlivou činností od vlastního personálu. [5]

Právě díky jejich snadnému přístupu do firemní sítě je toto riziko stále aktuální. Zaměstnanec, obzvlášť bývalý zaměstnanec, může mít totiž širokou řadu různých motivů

proč na svoji vlastní firmu zaútočit, ať už jde o pomstu, třeba kvůli odmítnutí zvýšení platu nebo vyhození z práce, či o jednoduchou snahu si přivydělat. Proto je zásadní chybou toto riziko zanedbávat, nešifrovat citlivá data na zaměstnaneckých počítačích nebo neodebírat přístupová práva po jejich odchodu. [5]

3 Druhy detekce a prevence kybernetických útoků

I když metod a postupů, jakými může útočník napadnout firemní aktiva je mnoho, proti každému známému kybernetickému útoku existují opatření, které mu dokážou zabránit, anebo zcela předejít. Ať už se jedná o konkrétní nástroje a služby či o celkovou bezpečnostní politiku firmy a její přístup k ochraně, existuje mnoho způsobů, jak se před napadením firmy bránit.

3.1 Monitoring

Monitoring neboli pozorování, je jednou z nejdůležitějších součástí kybernetické bezpečnosti. Jedná se neustálé sledování všech prvků systému, monitorování veškerých aktivit a s tím spojené nahlašování všech anomálií. **Monitoring** se také stará o ukládání všech informací o těchto aktivitách pro případnou rekonstrukci nezvyklých událostí a vystopování původu chyb či útoků. [2]

Monitoring se nepoužívá pouze jako ochrana před vnějšími útoky, ale také jako kontrola správného chodu vnitřních aktivit systému. Při jakékoliv poruše se díky němu dá zjistit, co se porouchalo, kdy, a proč.

Pro zavedení **monitoringu** ve firemní síti se používá široká škála programů a nástrojů, které mají za úkol pozorování neobvyklých či podezřelých aktivit, sledování všech uživatelů provádějících změny, automatickou rekonfiguraci nastavení, hlášení o hrozbách i tvorbu příslušné dokumentace. [2]

Monitoring může neobvyklou aktivitu rozpoznávat, tedy detekovat, na základě dvou hlavních metod:

- Metoda detekce útoku založená **na znalostech** porovnává aktuální chod sítě a jejích prvků s databází všech známých útoků. Pokud nalezne shodu mezi aktuálním chodem a databází, vyhodnotí aktivitu v síti jako útok. Databázi útoků je však třeba pravidelně aktualizovat, aby zahrnovala i nejnovější metody kybernetických útoků. Tato metoda také poskytuje ochranu pouze před známými útoky.
- Metoda detekce útoku založená **na chování** oproti tomu využívá statistických metod k odhadnutí správnosti chování sítě. Systém se umí sám učit a zdokonalovat a dokáže díky tomu poskytnout ochranu i před neznámými hrozbami.

  [2]

3.2 Nástroje kybernetické bezpečnosti

K obraně proti kybernetickým útokům slouží spousta nástrojů, které se zavádějí pro ochranu firemních systémů. Některé nástroje kybernetické bezpečnosti mohou být specializované, soustředící se pouze na obranu proti jedinému typu útoku, jiné zase počítač chrání před mnohými druhy hrozeb a snaží se ho chránit plošně.

Nástrojů kybernetické bezpečnosti existuje celá řada a stále se vyvíjejí nové, proto jsou v této práci uvedeny pouze ty nejznámější a nejrozšířenější.

3.2.1 Antiviry

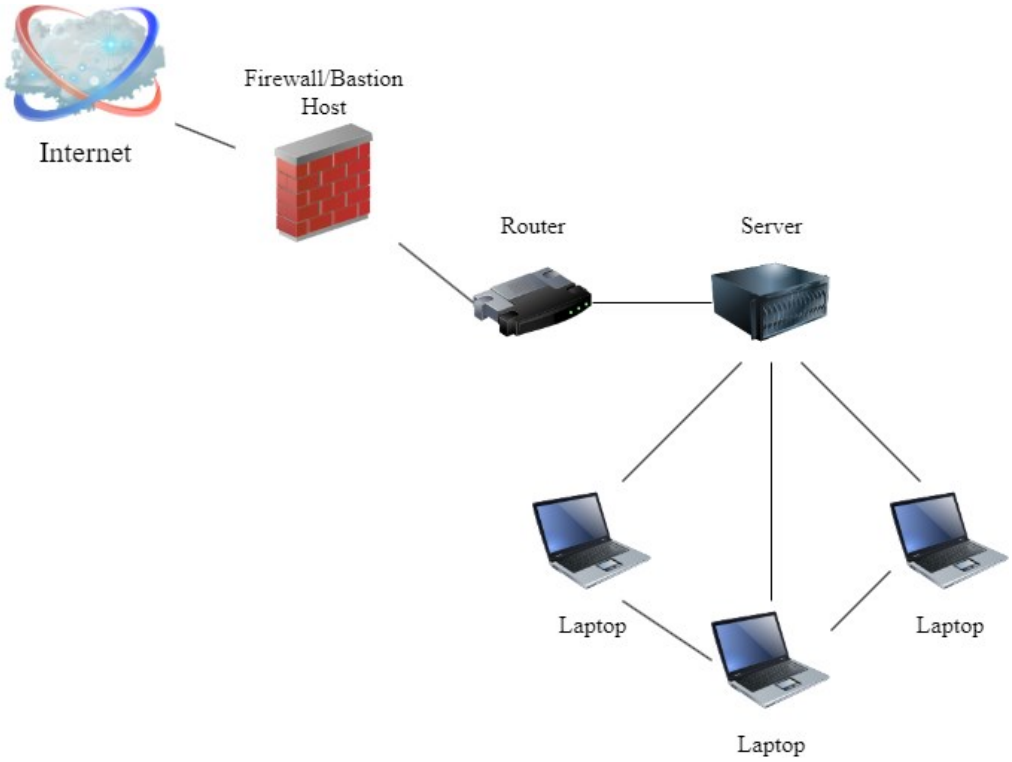
Jako hlavní ochranou proti počítačovým virům se používají takzvané **antiviry**. **Antivirus** je počítačový program, jehož primárním cílem je detekovat, blokovat a eliminovat **malware** všeho druhu. Proti některým zákeřnějším druhům malwaru se používají specializované typy antivirů, například proti **spywaru** se běžně používá takzvaný antispyware. [2]

3.2.2 Firewally

Firewall je bezpečnostní mechanismus, který má za úkol ochránit soukromou počítačovou síť. Tento nástroj může být zapojen ve formě hardwaru, softwaru, či kombinací obou. Hlavním úkolem tohoto nástroje je monitorovat příchozí i odchozí provoz v síti a filtrovat datové pakety, které nejsou v souladu s nastavenými pravidly sítě. [5]

Některé **firewally** takto vyfiltrované pakety rovnou zahazují, ty kvalitnější je ovšem ukládají v bezpečném prostředí a o těch nejnebezpečnějších informují administrátora sítě. Díky tomu tak může administrátor na tuto hrozbu přiměřeně reagovat a zavést tak třeba další doplňující opatření. [5]

V mnohých případech se **firewall** instaluje na počítačích speciálně určených pro tuto činnost, které oddělují vnější síť s tou vnější, a každý síťový provoz tak musí jít skrz ně. Tyto stroje se běžně označují jako **bastion host** (opevněný hostitelský počítač). [5]



Obrázek 6: Bastion host mezi vnitřní a vnější sítí; Zdroj: vlastní, na základě [5]

3.3 Analýza rizik

Analýza rizik je analýza prováděná za účelem řízení rizika. Dle normy ISO/IEC 27000:2017 je **analýza rizik** chápána jako *„proces pochopení povahy rizika a stanovení úrovně rizika.“* [3] Díky ní se dají posoudit **hrozby**, kterým firma čelí, navrhnout bezpečnostní opatření v obraně proti těmto **hrozbám** a s jistotou vypočítat, zda bude nově zavedené bezpečnostní opatření výhodné, a zda se jeho zavedení firmě vyplatí. Měla by se proto provádět při každé závažnější změně v bezpečnostním systému. [3]

Existují dvě základní skupiny metod **analýzy rizik**, které se používají. Jsou jimi **kvantitativní** metody a **kvalitativní** metody **analýzy rizik**.

- **Kvalitativní** metoda je založena na popisu závažnosti dopadu rizika a pravděpodobnosti jeho výskytu. Pro popis svých hodnot využívá čísla v určitém rozsahu (například <1 až 10>) nebo je popisuje slovně (<malé, střední, velké>). Tato metoda se používá pro svoji jednoduchost a rychlost, bývá ovšem mnohem subjektivnější a její výsledky nemusí věrně odrážet realitu.

- Naproti tomu **kvantitativní** metoda využívá exaktních matematických výpočtů k dosažení přesnějších výsledků. Pro všechny své hodnoty používá číselné ohodnocení a dopad bývá vyjádřen ve finančních termínech (například 12 000 Kč). Výsledky této metody bývají mnohem přesnější, je ovšem mnohem náročnější na zpracování.

- V praxi se také často používá kombinace **kvalitativních** a **kvantitativních** metod. Tyto kombinované metody vychází z číselných údajů, využívají ale i kvalitativní ohodnocení pro lepší přiblížení údajů ke skutečnosti.

  [2] [3]

Řádná **analýza rizik** se provádí postupně v následujících krocích, které by měly zajišťovat kvalitu analýzy a udržet jí určitý standard.

3.3.1 Identifikace aktiv

Prvním krokem u vytváření rizikové analýzy je vždy identifikace aktiv. Jedná se o vytvoření seznamu všech aktiv, které leží uvnitř předem stanovené hranice analýzy rizik, a které ohrožuje nějaké riziko. Při zapisovaní každého aktiva se uvede jeho název a umístění. Takto zvolená aktiva mohou být hmotná i nehmotná a rozdělují se na základě stanoveného měřítka. [3]

3.3.2 Stanovení hodnot aktiv

Dalším krokem je přidělení peněžní hodnoty každému aktivu. Posuzování velikosti této hodnoty je založeno na výši škody, ke které by došlo v případě zničení či ztracení tohoto aktiva. Velmi důležité také je rozlišit, zda se jedná o jedinečné aktivum, nebo zda je snadno nahraditelné. V tomto kroku se také při vysokém počtu aktiv některá aktiv seskupují dohromady podle různých hledisek, aby se vytvořily skupiny aktiv s podobnými vlastnostmi. Tato skupina dále vystupuje jako pouze jedno aktivum. [3]

3.3.3 Identifikace hrozeb

Následně se provede takzvaná identifikace hrozeb, během které se sepíšou hrozby, které pro daná aktiva přicházejí v úvahu. Během toho se vychází z vlastních zkušeností, z různých průzkumů, z online statistik a podobně. [3]

3.3.4 Analýza hrozeb a zranitelností

V dalším kroku jsou pak ke každé hrozbě jsou přidělena náležitá aktiva, které by daná hrozba mohla ohrozit. Stanoví se také úroveň hrozby vůči každému aktivu a úroveň

zranitelnosti aktiva vůči této hrozbě. Bere se zde v úvahu pravděpodobnost výskytu hrozby, hodnota aktiva a škoda, kterou by daná hrozba na aktivu napáchala. [3]

3.3.5 Výpočet ztráty

Posledním krokem analýzy rizik je konečný výpočet ztráty. Ztráta se počítá s každou dvojicí hrozby a aktiva zvlášť a je výsledkem součinu pravděpodobnosti výskytu hrozby a velikostí potenciální ztráty na aktivu. Takto vypočítaná předpokládaná roční ztráta je jasným ukazatelem míry nebezpečí každé hrozby. [3]

Při zavádění nového systému či změny nastavení se vždy odhadne nová pravděpodobnost výskytu hrozby, která po zavedení nové změny nastane. Tato nová pravděpodobnost se vynásobí s potenciální ztrátou a zjistí se tak nová ztráta po zavedení změny. Tato nově vytvořená ztráta se porovná s původní ztrátou a pokud je jejich rozdíl vyšší než náklady na zavedení nové změny, vyplatí se nové opatření zprovoznit. V opačném případě se tato nová změna nevyplatí. [2]

3.4 Proškolení zaměstnanců

Při řízení firemní bezpečnosti se nesmí zanedbat ani příprava všech zaměstnanců na případ pokusu o útok. Právě na nich z velké části záleží na tom, zda útoky na firmu budou úspěšné, či ne. Nejenom správci bezpečnostních systému se totiž můžou stát cílem útoku, nýbrž i ostatní pracovníci se můžou stát terčem útočníka, který by se je snažil obejít a zneužít u toho jejich nepřipravenost.

V první řadě by měl být každý zaměstnanec firmy informován o bezpečnostních krocích používaných k volbě kvalitního uživatelského hesla. Správné heslo by mělo být přiměřeně dlouhé, aby zabránilo metodě **útoku hrubou silou** a nemělo by mít podobu nějakého běžně používaného termínu, aby znemožnilo použití **slovníkového útoku**. Zároveň by také mělo střídat velká a malá písmena a mimo ně obsahovat i různé neobvyklé znaky a číslice. Mnoho firem proto při vytváření uživatelských účtu k nim zároveň generují i hesla, která splňují všechny náležité bezpečnostní požadavky. Důležitým faktorem také je, aby si zaměstnanec toto heslo zapamatoval a nenechával ho uložené na nějakém dostupném místě, například napsané na lístečku u počítače či v textovém souboru na ploše. [1]

Další útok, před kterým by měl každý pracovník na pozoru, je jakýkoliv útok provedený pomocí metody **phishing** za využití **sociotechniky**. Nepřipravený zaměstnanec by totiž mohl být snadno oklamán podvodný e-mailem či telefonátem a mohl by vyzradit své přihlašovací údaje či nějaké firemní tajemství. Tyto útoky navíc bývají přímo zacíleny

na nepozorné členy personálu a plně využívají zrádného lidského faktoru. Měl by tedy být kladen důraz na ostražitost před všemi podezřelými či neobvyklými zprávami a u každé neobyčejné žádosti by si měl pracovník ověřit její věrohodnost u někoho z bezpečnostního týmu. Hlášení by měl podat i v případě, že například podvodný e-mail prohlédne a ignoruje ho. [1]

Nejlepší způsob, pomocí kterého zaměstnancům vštěpit zásady bezpečnosti a zvýšit jejich povědomí o kybernetických útocích, je přidělit jim povinná bezpečnostní **školení**, která pracovníky nějakým způsobem informují o bezpečnostních rizicích a naučí je, jak se proti nim bránit a předcházet jim. Důležitým krokem řádného **školení** by také mělo být následné otestování jejich nově nabitých vědomostí. Může mít mnoho různých podob, nejběžněji se vyskytuje jako elektronický online test, který zaměstnanec může vyplnit kdekoliv. Školení by také neměla být jednorázová záležitost a místo toho by se měly vědomosti personálu pravidelně testovat a kontrolovat, aby se předešlo případným narušením zevnitř. [1]

3.5 Postupy v případě krize

I přes všechny možné nástroje a bezpečnostní opatření ale stále hrozí každé firmě riziko, že jeden z útoků bude úspěšný a naruší integritu systému nebo napáchá nějaké jiné škody. Proto musí mít připravené plány, jak se s takovou krizí vyrovnat a snažit se přitom pokračovat ve firemních procesech.

Jednou z věcí, kterou by firma měla podstoupit, je plánování **kontinuity podnikových procesů** (BCP) nebo také řízení **kontinuity činnosti organizace** (BCM). Jde o naplánování akcí provedených bezprostředně po úspěšném útoky či jiné škodlivé události za účelem minimalizace ztrát a co nejrychlejšímu obnovení běžného chodu. Všechny tyto akce musí být řádně zdokumentované a dostupné, aby se daly v případě potřeby najít a použít. [2]

BCM se používá výhradně v případech kdy napáchaná škoda nezastaví procesy kompletně, nýbrž pouze jen omezí funkci celé infrastruktury či přístup ke zdrojům. Pro případ opravdu velké katastrofy, kdy jsou všechny procesy zcela přerušeny, bývá vytvořen ještě **plán obnovy po pohromě** (DRP). Ten už využívá mnohem drastičtějších kroků k co nejrychlejšímu obnovení chodu firmy a používá se opravdu jen v nejnutnějších případech. [2]

Základem všech obnovovacích plánu jsou **zálohy** všech dat, programů i systémů, které mají být pravidelně aktualizovány, aby se daly v případě potřeby použít. Ty jsou uložené na vzdáleném místě od opravdových systému, aby se k nim útočník snadno nedostal a nenapadl je. Díky nim stačí někdy napadený systém či data pouze přehrát uloženou zálohou a opravit je tak. [2]

4 Kybernetické hrozby ve společnosti ČEZ

Praktická část bakalářské práce se zabývá popisem kybernetických hrozeb a bezpečnostních opatření společnosti ČEZ, pro přiblížení reálného fungování firmy a využití teoretických poznatků v praxi. Veškeré materiály byly poskytnuty panem Ing. Luďkem Tichým, vedoucím odboru kybernetické bezpečnosti a ochrany dat skupiny ČEZ Distribuce, a.s.

4.1 Četnost útoků

Skupina ČEZ Distribuce je jakožto velkou firmou a předním energetickým výrobcem ideálním cílem pro útočníky všeho druhu. Ať už se jedná o necílené útoky nebo o velký kybernetický incident, čelí skupina ČEZ prakticky neustále hrozbám všeho druhu.

4.1.1 Necílené útoky

Velká společnost typu ČEZ čelí hned po vstupu do kyberprostoru různým útokům prakticky neustále. Hned po připojení k internetu je taková firma zasypána prakticky nekonečnou hromadou různých automatických **botů** a **spamů**, sloužících útočníkům k automatickému sběru dat a nalezení slabých míst v systému firmy. Takové necílené útoky nemají sice na společnost s dobrým zabezpečením sebemenší vliv, ale přesto slouží jako ukázka nebezpečí v kyberprostoru, a i jako varování malým firmám.

4.1.2 Útoky řešené automaticky

Automatické necílené útoky ale ovšem nejsou jedinou hrozbou, které společnost takového dosahu čelí. Zhruba jednou nebo dvakrát do týdne společnost napadne nějaký druh cíleného útoku za účelem způsobit škodu už této konkrétní firmě. Takové běžné útoky ale nepředstavují pro dobře zabezpečenou firmu žádné větší riziko a bývají řešeny automaticky pomocí zavedených systémů bez pomoci operátora.

4.1.3 Útoky řešené manuálně

S nějakými většími nebo „zajímavějšími“ útoky se pak ČEZ potýká přibližně jednou za měsíc. Takovéto vzácnější útoky bývají mířené třeba na nějaký konkrétní produkt nebo část systému, je tedy evidentní, že tyto útoky mají předem dobře určený cíl či záměr. Takovými útoky už se operátoři zabývají a zkoumají je, například odkud vedou, co je přesně jejich účelem a podobně. Tento druh výskytu útoků ovšem pořád bývá systémem či operátory podchycen a nenapáchá ve firmě žádnou škodu.

4.1.4 Kybernetické incidenty

Nejvážnějším a rizikově nejvýše ohodnoceným útokem, ke kterému může dojít a který může kriticky narušit infrastrukturu systému, je takzvaný kybernetický incident. Za těmito útoky už stojí vysoce sofistikovaný a zkušený útočník s jasně daným cílem a schopností narušit integritu i tak dobře zabezpečené velké společnosti, jakou je skupina ČEZ.

K těmto útokům dochází už velmi zřídka a zcela nepravidelně, některé roky nezaznamenají útok takového rozsahu ani jednou, ale například v roce 2023 takový útok proběhl rovnou dvakrát. Během těchto incidentů útočníci využili špatného vnitřního nastavení v systému, ale naštěstí se oba útoky podařilo odchytit, než stačily napáchat značné škody.

4.2 Druhy kybernetických hrozeb

Stejně jako všechny ostatní firmy čelí skupina ČEZ každodenně mnoha kybernetickým hrozbám. Jelikož se ale jedná o velkou celostátní energetickou společnost, hrozí jí i závažnější a rafinovanější útoky, než jsou viry, prolomování hesel, či spamy. Může se totiž stát ideálním cílem pro vysoce zkušené útočníky, kteří si jejím napadením můžou vydělat značnou sumu peněz. Proto je zde věnována kapitola několika speciálním typům útoků, kterým musí společnost čas od času čelit, spolu s opatřeními, která jsou

4.2.1 DDoS útok

Útok typu **DoS** (Denial of Service) nebo také **DDoS** (Distributed Denial of Service) je speciálním typem útoku, jejímž úkolem je přetížením narušit nebo poškodit síť, webovou stránku, či jinou síťovou službu. Pro provedení tohoto útoku si útočník nejprve zajistí silnou konektivitu a výkonný superpočítač a pomocí skriptu začne na zacílenou online službu zasílat nevyžádané požadavky. Špičkové **DDoS** útoky dokážou požadavky vysílat až v řádech terabitů za sekundu, takže napadený prvek zcela zahltí. [20]

Napadený stroj se pak pod tlakem může dostat do takzvaného **deterministického stavu** a zpřístupnit útočníkovi věci, které by neměl, například nějaký síťový port. Lepší **DDoS** útoky navíc na zvolenou IP adresu dokážou útočit z celého světa pomocí koordinované sítě strojů výpočetní techniky. Tato síť se nazývá **botnet** a jedná se o síť počítačů, nakažených virem nebo jiným malwarem, které bez vědomí svého oprávněného uživatele dokážou odesílat požadavky. Posílání takového velkého objemu dat je ovšem finančně náročné, proto si útočníci služby **DDoS** běžně pouze pronajímají na určitou dobu, a proto jsou tyto útoky časově omezené. [4]

Tento typ útoků se většinou používá k otestování kvality napadeného stroje a bezpečnostního systému firmy. Sekundárním cílem bývá někdy jednoduše znepříjemnit obránci život. Útok **DDoS** často funguje právě u webových stránek, které pak útočník může pozměnit dle libosti, vložit na ně například nevhodný obsah a způsobit tak firmě takzvaný **defacement**, tedy vizuální změnu webové stránky za účelem způsobit firmě reputační škodu. Útok DDoS proto může být nebezpečný, pokud je bezpečnost systémy zanedbaná, ovšem při správném nastavení by neměl způsobit větší škody.

Příkladem takového **DDoS** útoku je napadení na systém přihlášek na střední školy v únoru 2024, který se sice podařilo odrazit, přesto ovšem zpomalil chod webových stránek a vyvolal tím frustraci u starostlivých rodičů a reputační škodu systému DiPSy. [21]

Dalším příkladem je široký útok na státní weby, například na České dráhy, provedený v roce 2022. Během nich se útočník snažil získat co nejvíc informací o nastavení perimetru. Za pomocí **DDoS** útoku se mu podařilo shodit servery a při opětovném nabootovávání těchto serverů odečítal data, z čehož si dokázal odvodit nastavení informačního systému a zjistil tak i třeba, kolik má systém paměti. [22]

4.2.2 Ransomware

Útok pomocí **ransomwaru** či také vyděračského softwaru je druh útoku, při kterém útočník napadne data nebo systém škodlivým softwarem, který tyto data zašifruje či zablokuje, dokud jejich majitel není ochotný zaplatit za ně výkupné. Ransomware se podobně jako virus šíří pomocí spamů či skrz počítačovou síť a může majiteli zcela znepřístupnit jeho vlastní systém nebo ho zašifrovat takovým způsobem, že se v něm sám nevyzná. [28]

Po takovém nakažení obvykle majitel obdrží zprávu s odkazem na zaplacení sumy výkupného, aby dal útočník jeho systém opět do pořádku. Tyto odkazy navíc bývají i časově omezené a majitel tak může na vyplacení výkupného mít třeba jen deset hodin. V případě **ransomwaru** je pro zkušené útočníky atraktivnější napadat velké společnosti, jelikož ty jsou schopné zaplatit vysoké sumy peněz a obnovit tak svůj provoz. Pokud navíc tyto firmy spravují služby nezbytné pro řádný chod společnosti, jako například energetická skupina ČEZ, jsou mnohem ochotnější výkupné včas a co nejrychleji zaplatit.

Aktuálním případem použití **ransomwaru** byly rozsáhlé útoky na nemocnice kolem roku 2022. Zde útočníci zjistili, že bezpečnostní systémy ve zdravotnictví jsou zanedbané, a přitom chrání velice citlivé a cenné informace, tedy jsou ideálním cílem kybernetického

útoku. Právě kvůli podstatě uchovávaných informací byly zdravotnické organizace s porovnáním se společnostmi v jiných odvětvích ochotny nejčastěji výkupné zaplatit, a to v 61 % všech případů. [29]

Tento druh útoku je tedy velice aktuální a vysoce nebezpečný, jelikož firmě běžně způsobí obrovské škody. Může se totiž také samozřejmě stát, že ani po zaplacení výkupného útočník svůj ransomware ze systému nestáhne a bezpečnostní tým ho i tak bude muset od základů sestavit znovu.

4.2.3 Vnitřní hrozby

Velká společnost typu ČEZ musí být zároveň na pozoru před svými vlastními zaměstnanci. S vysokým počtem pracovníků totiž nebezpečí útoku zevnitř stoupá, jelikož je těžší všechny manuálně kontrolovat, jestli firmě nepůsobí nějaké škody.

Způsobů, kterými může zaměstnanec svou vlastní organizaci poškodit, je mnoho, stejně jako motivů způsobit škodu záměrně. Například zaměstnanec nespokojený se svým platem může začít využívat firemní aktiva pro vlastní účely, krást firemní prostředky nebo dokonce automaticky odvádět příjmy firmy do vlastního bankovního účtu.

Škodu ovšem mohou snadno napáchat i bývalí zaměstnanci. Pokud třeba byli ze svého zaměstnaní vyhozeni, mohou se pokusit skrz svůj bývalý firemní účet stáhnout klasifikované dokumenty, které pak chtějí prodat konkurenci. Běžně také perfektně znají firemní procesy a vyznají se v interním systému, pokus o útok pro ně proto může být jednodušší.

Kontrolovaní musí být i samotní členové bezpečnostního týmu, jelikož ti se nejlépe orientují v bezpečnostním systému firmy a mohou znát jeho slabé stránky. V některých případech si mohou dokonce vytvořit i přístupová „zadní vrátka“ pomocí kterých se pak mohou nepozorovaně dostat do systému a napáchat tam škody. Tato hrozba je především nebezpečná v tom, že přichází z nečekaného směru a páchání škod může probíhat zcela nepozorovaně. Proto firma nesmí své zaměstnance nikdy podceňovat a v bezpečnosti musí brát ohledy i na ně.

5 Bezpečnostní politika a opatření společnosti ČEZ

Při takovém neustálém kybernetickém náporu ze všech stran a už ze samotné energetické podstaty činnosti firmy si skupina ČEZ nemůže dovolit, aby kybernetické útoky na jejich systémy byly úspěšné. Proto je zde zavedena celá řada bezpečnostních opatření, která dohromady pracují v dokonalém souladu a jsou řízeny centrálně.

Všechna zařízení, která skupině ČEZ chrání její informační systémy, se dají rozdělit na pasivní a aktivní prvky obrany. Pasivní prvky se starají o nepřetržitou obranu systému, kdežto ty aktivní reagují na konkrétní útoky, provedou jejich analýzu a použijí patřičné protiopatření.

5.1 PDCA cyklus

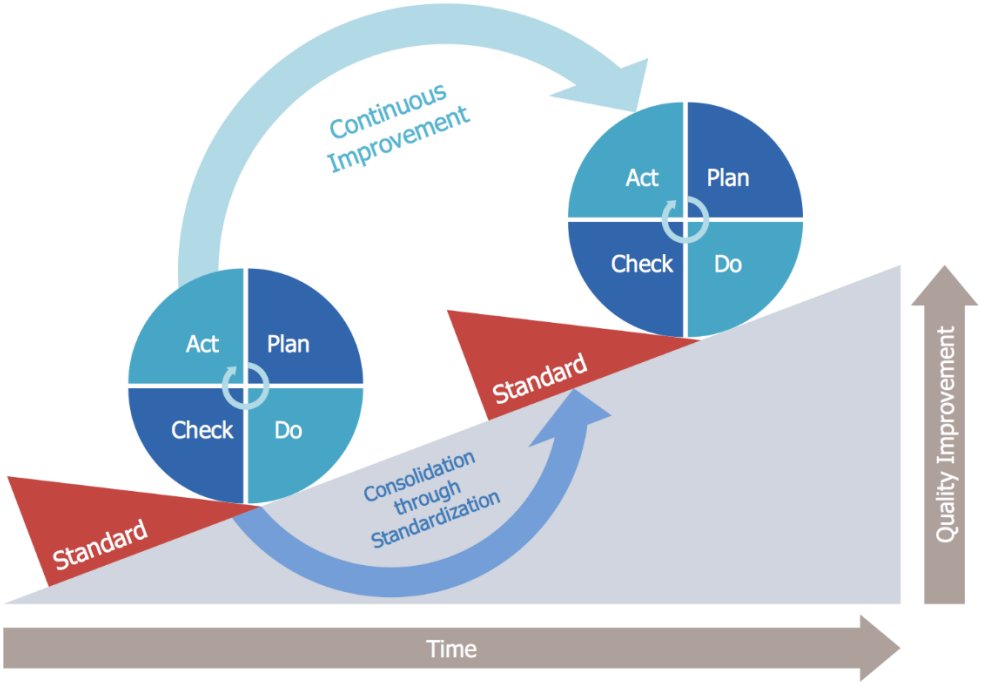
Celý bezpečnostní sytém stojí na principu řízení kvality, o který se stará takzvaný **PDCA cyklus**. Hlavní myšlenka tohoto cyklu spočívá v tom, že pokud v systému narazíme na chybu, tak ji opravíme. Základní část **PDCA cyklu** se sestává ze 4 kroků: **Plan**, **Do**, **Check** a **Action**.

- V prvním kroku **Plan** jde o naplánování budoucích cílů, kterých chceme dosáhnout. V tomto kroku se určí všechny potřebné úkoly a procesy, které vedou k dosažení stanoveného cíle. Zároveň s tím se vytyčí i způsob, dle kterého se bude kontrolovat, zda byly všechny cíle splněny. V rámci kybernetické bezpečnosti to znamená, že se vymyslí způsob, jakým bude případná chyba či slabé místo opraveno.

- V dalším kroku **Do** jsou pak všechny naplánovaného procesy provedeny za patřičné dokumentace všech kroků, podle které bude celý proces zkontrolován. V tomto bodě je kybernetická chyba opravena.

- Kontrola všech procesů probíhá právě v bodě **Check**. Během tohoto bodu testujeme, zda naše řešení pro opravu chyby funguje a zda nevyvolalo další problémy či slabá místa.

- Pokud kontrola proběhla úspěšně, cyklus postoupí do bodu **Act**. Zde už jde právě vytvořené řešení do produkce a začne se používat. Pořád je ovšem aktivně kontrolováno, zda funguje, jak má.



Obrázek 7: PDCA cyklus; Zdroj: [17]

Celý **cyklus PDCA** je nekonečný, neustále se pracuje na nových vylepšeních a všechny procesy jsou kontrolovány. Díky tomuto cyklu by se měla kybernetická bezpečnost neustále zlepšovat a s ubíhajícím časem by kvalita zabezpečení měla stoupat. Od této myšlenky se odvíjí celkové filozofické řízení bezpečnosti ve skupině ČEZ.

5.2 Bezpečnostní role

Bezpečnostní tým starající se o kybernetickou bezpečnost firmy, tvoří několik pozic, které spolu spolupracují a mají pevně danou hierarchii. Seznam pozic vedený svrchu obsahuje následující bezpečnostní role:

- Celý bezpečnostní tým řídí dle zákonu a ISO 27000 takzvaný **manažer kybernetické bezpečnosti.** Ten zodpovídá za celý bezpečnostní systém jako celek a schvaluje všechny nové nástroje a koncepční změny. Vedle něj stojí ještě **bezpečnostní ředitel**, ten má ovšem na starosti spíše fyzickou bezpečnost a systémy **ISMS** (systémy řízení bezpečnosti informací).

- Přímo pod ním je pozice **architekta kybernetické bezpečnosti**, který má za úkol udržovat danou koncepci bezpečnostního řešení pro celou firmu, pro její strategii i pro její produkty a zodpovídá za jednotlivé návrhy řešení.

- Další bezpečnostní rolí je takzvaný **bezpečnostní administrátor**. Ten už má na starosti konkrétní oblast kybernetické bezpečnosti, jako například řízení identit či řízení dokumentace.

- Poslední skupinu rolí pak tvoří **dohled**. To je tým fungující v pracovišti **SOC** (rozepsané v samostatné kapitole) a dělí se na další 3 úrovně. Těmi jsou **operátoři**, **analytici** a **kompetenční centrum**. Tyto role dohlíží na správný chod systému a v případě útoku na něj reagují a snaží se ho zastavit.

5.3 Pasivní prvky obrany

Pasivními prvky obrany, které jsou ve firmě zařízeny, jsou mimo jiné i běžně používané nástroje jako firewally, různé antiviry a spam filtry, a i samotné nastavení systému. Tyto prvky slouží k prvotní obraně před drobnými či automatizovanými útoky, kterými jsou například **spamy** či různí internetoví **boti**.

I když jsou tyto prvky obrany pro ochranu proti drobným útokům užitečné, sofistikovaný útočník by se přes ně s velkou pravděpodobností bez problémů dostal, proto jsou zavedeny i pokročilejší obranná zařízení.

5.3.1 Sytém IDS

Systém **IDS** (Intrusion Detection System) čili **systém pro detekci průniku** je nástroj síťové bezpečnosti, který monitoruje provoz v síti a zařízení k ní připojené, aby našel podezřelou aktivitu nebo porušení bezpečnostních pravidel sítě. [8]

Nalezené hrozby pak ve formě zprávy odešle bezpečnostnímu operátorovi v **bezpečnostním operačním středisku**, který se s hrozbou dokáže vypořádat. Systém IDS tak urychluje a automatizuje detekce síťových hrozeb a je napojen na aktivní prvek obrany **SIEM,** který kombinuje data z ostatních zdrojů a dokáže tak přesněji určit původ i místo kybernetického útoku.

5.3.2 Systém IPS

Se systémem **IDS** souvisí i systém **IPS** (Intrusion Prevention System), čili **systém pro prevenci průniku**, který se z IDS vyvinul a spolu s detekováním bezpečnostních hrozeb jim dokáže také předcházet.

Takto dokáže preventivně přímo blokovat podezřelý provoz, a i upevňovat bezpečnostní pravidla sítě skrz blokování neautorizovaných činností uživatelů. Díky tomu se **bezpečnostní operační středisko** může zabývat složitějšími útoky a systém se automaticky postará o ty jednodušší. **Chyba! Nenalezen zdroj odkazů.**

5.3.3 Systém IDR

Systém bezpečnosti **IDR** (Intrusion Detection and Response), čili **detekce a reakce na narušení,** je relativně nová kybernetická metoda, která na základě informací o identitách a jejich síťových privilegiích dokáže rozpoznat určité typy útoků (například ransomware) směřujících na firemní síť. [10]

Činí tak na základě porovnávání činnosti uživatele v síti s databází známých anomálií a řádným chováním uživatelů dle jejich privilegií. Tato databáze se díky umělé inteligenci neustále rozšiřuje a dělá tak celý systém stabilnější. Při nalezení škodlivé činnosti pošle **IDR** podobně jako **IDS** a **IPS** zprávu do aktivního prvku obrany **SIEM**, který pak podá hlášení bezpečnostním operátorům. Mimo to dokáže metoda **IDR** také chránit uživatelské údaje a díky maskovacím technologiím oklamat útočníkovi nástroje za pomocí falešných údajů a návnad. [9] [10]

5.4 Aktivní prvky obrany

Veškeré aktivní prvky obrany informačního systému řeší a ovládá pracoviště typu **SOC** (Security Operation Center), čili **bezpečnostní operační středisko**. Z tohoto pracoviště se řídí veškerá firemní bezpečnost.

Součástí **SOCu** je tým ve třech vrstvách, takzvané **L1**, **L2** a **L3**.

- Na první úrovni **L1** pracují takzvaní operátoři, kteří přijímají hlášení z obranného prvku **SIEM,** toto hlášení vyhodnocují dle zavedených metodik a hlášení buď vyřeší, nebo pošlou dál. První úroveň řeší výhradně jednodušší problémy a útoky, které jsou obecně známé a k jejichž řešení existují zavedené postupy. Pokud se operátor nedokáže sám s narušením vypořádat, odešle hlášení o úroveň výš.

- Na této další úrovni, **L2**, už působí analytici, kteří disponují určitými zkušenostmi potřebnými k řešení složitějších záležitostí. Ti se potýkají s komplexnějšími problémy a musí si umět poradit i se sofistikovanějšími útočníky. Zkoumají také, zda dané hlášení je opravdu kybernetický útok či zda se jedná pouze o false positive.

- Nad druhou úrovní už stojí pouze úroveň **L3**, kterému se také říká kompetenční centrum. Zde se provádí koncepční změny, které mají na starosti architekti. Pokud vyjde najevo nějaká nová zranitelnost, tito architekti ji napravují pomocí nějakého druhu systémového opatření, jakým je například změna architektury. Rozhodují také o přenastavení celého systému ke zvýšení jeho odolnosti. Řeší například napadení **AD** (Active Directory), adresáře, který zajišťuje autentizaci a autorizaci uživatelům sítě.

Tyto tři úrovně tvoří základní kostru **SOCu**. Další jednotlivé činnosti se pak granulárně rozpadají na další.

5.4.1 SIEM

Srdcem celého pracoviště **SOC** je zařízení typu **SIEM** (Security Information and Event Management) nebo také **management bezpečnostních informací a událostí**. **SIEM** poskytuje celkový přehled o aktivitách v síti, díky tomu, že tento software má k dispozici veliké úložiště logů. Tyto logy pocházejí ze systému kolektorů, které je sbírají ze všech zařízení a **SIEM** je koreluje a řídí. Díky **SIEMu** mohou operátoři a analytici rychle reagovat na kybernetické útoky a ostatní hrozby.

Co všechno **SIEM** řídí a může řídit záleží na **vyhlášce 82/2018,** která pojednává *„o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)“*. [11] Jelikož skupina ČEZ je v rámci bezpečnosti správcem kritické informační infrastruktury, musí se touto vyhláškou řídit.

Zároveň pro ni platí i **zákon 181/2014**, který ukládá plnění toho, jak se má informační infrastruktura ochraňovat. Tento zákon o kybernetické bezpečnosti *„upravuje práva a povinnosti osob, jakož i pravomoc a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zpracovává příslušné předpisy Evropské unie a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů“* [12].

To jediné, v čem zákon dává prostor, je volba intenzity bezpečnostních opatření. Každá firma si tak může vybrat, jak moc do detailu bude bezpečnost řídit, jaké nástroje bude pro kybernetickou bezpečnost využívat, či jak personalizované bezpečnostní řešení bude.

Zákon 181/2014 také určuje, že každá systémová operace se musí řádně logovat a systém tyto logy musí někam ukládat, aby vznikla přesná dokumentace o chodu

kybernetického bezpečnostního systému. Tyto logy také musí být pravidelně prohlíženy, aby byl člověkem zaznamenán chod sítě a dalo se tak zjistit, zda se nějaké síťové prvky nechovají nevhodně. Pokud se totiž tyto prvky chovají nevhodně, bývá to známkou toho, že jsou buď poničeny, nebo přímo napadeny.

Tyto logy má pak na starosti právě **SIEM**, na který jsou napojené další technologie, jako třeba **IPS** či **IDR,** a i další zařízení skenující technické zranitelnosti. Tato zařízení jsou nasazena na celý rozsah serveru, porovnávají skutečný chod sítě s bezpečnostní politikou jejich výrobců a výsledky posílají přímo do **SIEMu**. Ten tyto výsledky mezi sebou porovnává a ve formě zprávy je posílá operátorům. Operátor zprávu přečte, vyhodnotí možné kritické zranitelnosti a předává dál na provoz. A pokud se cokoliv v síti začne chovat nestandardně, je nasazen analytik, který provede úvodní analýzu a v případě potřeby přikročí k forenznímu řešení, kdy jde do hloubky a řeší konkrétní novou zranitelnost či nákazu.

5.4.2 Nadstavba SOAR

Nad **SIEMem** je navíc ještě napojená nadstavba, která se nazývá **SOAR**. **SOAR** (Security Orchestration, Automation and Response), čili **bezpečnostní orchestrace, automatizace a reakce**, umožňuje veškeré operace zautomatizovat, dle takzvaných playbooků.

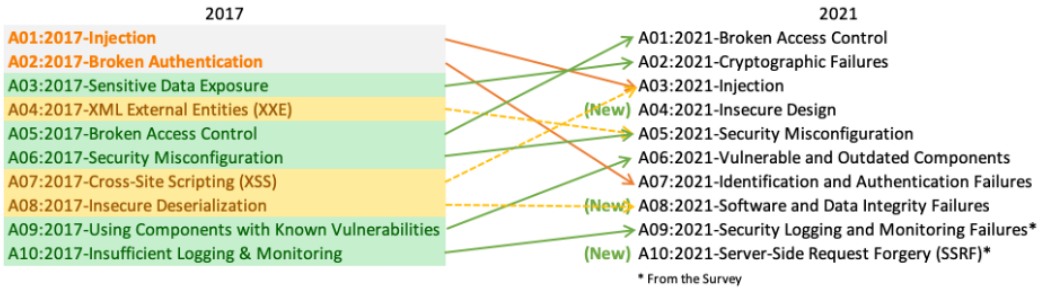
Playbooky jsou dokumenty vytvořeny **SOC** týmem, které fungují jako řešení rutinních incidentů. Jedná se o podrobné návody pro řešení kybernetických útoků a hrozeb. Jejich úkolem je poskytnout strukturovaný přístup k řešení těchto událostí, a právě na jejich základě dokáže **SOAR** svoje operace automatizovat. [14]

Kdykoliv **SIEM** odhalí nějakou chybu či konkrétní **vektor útoku**, **SOAR** dokáže ovládat další prvky, aby problém bez pomoci operátora opravil. **SOAR** se dokáže i sám učit pomocí technologie machinelearningu a může být napojen i na další zdroje o zranitelnostech, jakými jsou například **MITRE ATT&CK** či **OWASP**.

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) je místo, kde kybernetická komunita z celého poskytuje všem ostatním znalosti o kybernetických útocích i s návody na jejich odvrácení. Jedná se o volně dostupnou globální databázi, která má za úkol zlepšit kybernetickou bezpečnost po celém světě. [15]

Další obdobnou databází je **OWASP**. Ta obsahuje primárně ty nejčastější a nejzákeřnější útoky, které se ovšem většinou týkají aplikační vrstvy. Udržuje i přehled

o deseti nejčastějších druhů kybernetických útoků, takzvaný **Top Ten OWASP,** který je každých pár let obnovován. Nejnovější obnova proběhla roku 2021 a momentálně tam patří takové typy útoků, jakými jsou například injektování či cross-site scripting.



Obrázek 8: Porovnání vývoje OWASP Top Ten mezi roky 2017 a 2021; Zdroj: [16]

Na základě těchto databází jsou pak nastavená pravidla v **SIEMu**, který koreluje logy reálného systému s těmi v databázích a na základě takových korelací vyhodnotit, zda jsou odchylky od řádného provozu známkou chyby, false positive, či útoku.

5.4.3 Anti-DDoS

Na systém je napojena také ochrana proti útokům **DDoS**. Ta se nazývá **Anti-DDoS** a dokáže samo vyhodnotit, zda příchozí provoz je **DDoS** útok, definovat falešné odesílatele požadavků a zahazovat je, aby se jimi síť nezatěžovala. Operátor díky tomuto nástroji vidí nebezpečně se zvedající aktivitu na stránce, odklonit ho, a sám ho za běžného provozu internetových stránek eliminovat.

Nejdůležitější je v případě **DDoS** útoku detekovat, odkud proudí, poté už se dá odříznout od sítě a nenapáchá žádné škody. Boj proti tomuto typu útoků ovšem může být problematický a pro bezpečnostního operátora náročná práce. Lepší a výkonnější **DDoS** totiž umí dynamicky měnit adresu počátku útoku a vyhnout se tak systému **Anti-DDoS**, který pak tyto změny musí neustále sledovat. Jelikož kvalitnější **DDoS** útok může trvat i půl dne, boj proti němu může být vyčerpávající. Samotný systém **Anti-DDoS** je navíc také výkonově omezen a hrozí tak, že by také mohl přestat stíhat.

Z těchto důvodů se někdy používá i daleko jednodušší, i když překvapivější metoda obrany. Pokud se totiž zjistí, že nějaký stroj začíná selhávat, nejjednodušším řešením je prostě ho vypnout. Tato akce nemá u většiny služeb dlouhodobý dopad a krátkým přerušením chodu stroje žádné ztráty nenastanou. Proto je obvykle tato možnost zvažována jako první a po vypnutí stroje se počká, dokud útočníkovi nevyprší na **DDoS** službě zakoupený čas.

U některých kritických služeb je ovšem nepřípustné, aby se třeba jen na chvíli přerušil jejich provoz, proto se bezpečnostní tým musí snažit udržet je co nejdéle v řádném

chodu. Například jedna ze sesterských firem ČEZ Distribuce, ČEZ Prodej, má přes webové stránky rozběhnutý systém fakturací a tam se bezpečnostní tým musí vždy pomocí systému **Anti-DDoS** snažit odklonit nebezpečný příchozí provoz, aby chod webu zůstal neporušený.

Systém **Anti-DDoS** už je dnes zcela běžně instalován i jako součást lepších firewallů a firmy si můžou zařídit buď vlastní řešení tohoto systému, nebo si ho objednat u nějakého operátora, kteří nabízejí velké rozsáhlé řešení typu box, ve kterém je obsaženo vše, co daná firma pro obranu proti **DDoS** útokům potřebuje. ČEZ Distribuce má právě takové řešení u operátora NETSCOUT, a to box jménem Arbor.

5.5 Dokumentace

Velice důležitou součástí bezpečnostního systému je také řádná dokumentace, která je pečlivě vytvářena, hlídána a upravována. Bezpečnostní dokumentace vychází ze zákona a je udržována dle mezinárodní normy **ISO 27001**. Ta „poskytuje rámec pro **systémy řízení bezpečnosti informací**, který umožňuje zachování důvěrnosti, integrity a dostupnosti informací, jakož i dodržování právních předpisů“ [18] a podle ní je řízena kvalita informačních bezpečnostních systému.

5.5.1 Systémy ISMS

Tyto **systémy řízení bezpečnosti informací** – Information Security Management Systems, dále jen **ISMS**, stanovují způsob zavádění, monitorování a provozování bezpečnosti informací a dat. Díky standardům uloženými **ISMS** je ve firmě vše zdokumentováno, včetně auditní stopy, tak, aby žádná změna v systému neproběhla bez povšimnutí. Dokumentace je kompletní, obsahuje jak řídící pokyny, tak i informace o jednotlivých technických prostředcích, a i o celém prostředí.

5.5.2 Konfigurační databáze CMDB

Veškeré informace o nastavení a stavu systému by měly být **CMDB**, tedy v konfigurační databázi. Pracovníci starající se o provoz sem shromažďují všechny informace o tom, jak se síť chová, jak by měla být správně nastavená, a jak je nastavená aktuálně.

Kdykoliv pak operátoři či analytici najdou nějaký nesoulad, nahlédnou do **CMDB** a porovnají aktuální nastavení s tím v databázi. Díky tomu se zjistí, zda se jedná jen o false positive, tedy například jen chybné nastavení, nebo zda nastavení někdo změnil schválně, což už může být známka kybernetického útoku.

5.6 Zabezpečení zevnitř

Celkové zabezpečení zvenku je ve společnosti ČEZ vedené i zevnitř. Pro řádnou bezpečnost je nutné mít stálé informace o všech zaměstnancích s přístupem k výpočetní technice. Každý zaměstnanec má založený účet, pomocí kterého přistupují do kybernetického prostředí, ve kterém pracují. Tento účet je nutno evidovat, stejně jako znát důvod vzniku účtu a přiřadit danému uživateli odpovídající sadu práv a rolí. To vše má na starost **systém řízení identit**.

5.6.1 Řízení identit

Každý proces řídící uživatelské účty a s nimi spojené identity je zautomatizován. To je zařízeno díky systémům **IDM** (identity management), které dokážou automaticky řídit přístupová práva.

Vedle systémů **IDM** se o uživatelské účty starají i jiná zařízení, a to systémy **PIM** a **PAM**. Tyto dva nástroje se starají o odlišné aspekty řízení identit. Systém **PIM** (Privileged Identity Management) čili **řízení privilegovaných identit** se stará převážně o monitorování a pasivní ochranu uživatelských účtů. Naproti tomu systém **PAM** (Privileged Access Management – **řízení privilegovaných přístupů**) s přístupovými právy pracuje aktivně a dokáže je uživatelům odebírat a přidávat.

Všechny tyto systémy pracují ve vzájemné shodě a celý systém přidělovaný práv je tak plně automatizovaný. Pokud tak třeba nějaký zaměstnanec z firmy odejde, proběhne celý proces následovně. Všechny odchody ze společnosti začínají u HR (lidské zdroje), které do systému zadá ukončení pracovního poměru. To se automaticky propíše do **IDM**, které tuto zprávu odešle do **AD** (Active Directory), adresářové služby, kde se příslušný účet vypne a znepřístupní se mu všechna práva.

Bývalému zaměstnanci se také odebere veškerá firemní výpočetní technika, jako notebook a telefon. Tato zařízení jsou proskenována a zavře se i uživatelův komunikační účet. Po těchto krocích nastává perioda čekání, během které se kontroluje, zda odcházející zaměstnanec nenapáchal na zařízeních nějaké škody. Pokud nějaké známky narušení skutečně vyjdou najevo, začne se podrobně prohledávat zaměstnancova historie, aby se našly náznaky, s kým v předešlé době komunikoval, jaká data posílal ven z firmy, a podobně.

5.6.2 Klasifikace dokumentů

Nejčastější událost, která při odchodu nespokojeného zaměstnance z firmy nastává, je jeho snaha stáhnout si firemní dokumenty, které mohou být citlivé. Proto je ve firmě

zavedený systém **DLP** (Data Loss Prevention), čili **ochrana před únikem informací**, který tomu brání a hlídá všechno od úrovně stahování až po úroveň odesílání. Díky tomuto systému se důležité dokumenty nedají odesílat vůbec a notebooky jsou zajištěné tak, že až na výjimky se k nim nedá ani připojit flash disk. Při každém pokusu o neoprávněné použití je navíc nahlášen přestupek.

Pro tento dohled v **DLP** je nutno ovšem provést klasifikaci firemních dokumentů a informací. Každý dokument, mail, či komunikační prvek má tak svou úroveň zabezpečení. Dělí se na prvky **veřejné**, **interní**, **citlivé** a **mimořádně citlivé**.

- **Veřejné** prvky bývají dokumenty, u kterých nehrozí, že by se při jejich uniknutí ven způsobila nějaká škoda na firemních aktivech. Proto se tyto prvky dají sdílet volně dle libosti a jejich odesílání není nijak omezené.
- Prvky **interní** už poskytují nějaké bližší informace o firmě, a proto se dají sdílet pouze mezi zaměstnanci a případně s externisty dle jejich smlouvy.
- **Citlivé** prvky se pak týkají konkrétní části firmy a mohou obsahovat nějaké firemní tajemství. Ty proto mezi sebou mohou sdílet pouze zaměstnanci, kteří k nim mají povolený přístup, například pracující na společném projektu.
- Prvky s nejvyšším možným zabezpečením se označují jako **mimořádně citlivé.** Ty už obsahují data, která jsou klasifikována jako vysoce citlivá a kritická. Proto se nedají odesílat ani stahovat, a jejich uniknutí by firmě mohlo způsobit škody.

Jakékoliv přístupové výjimky jsou navíc evidované a všechna aktivita je logovaná. I lidé, co k daným dokumentům mají oprávněný přístup, mají veškerou jejich aktivitu evidovanou v systému pro případné narušení. Významné dokumenty jsou navíc opatřeny neviditelnými značkami. Ty si i mimo jiné pamatují všechny uživatele, kteří s nimi manipulovali, a tak se v případě uniknutí dá vystopovat, který zaměstnanec dokument vypustil ven.

5.6.3 Školení zaměstnanců

Důležitou součástí vnitřního zabezpečení firmy je postarat se o to, aby byl každý zaměstnanec v rámci bezpečnosti (i té kybernetické) řádně proškolen, jelikož **vektor kybernetického útoku** nemusí být prováděn přes výpočetní techniku, ale pomocí **spamů** či **sociotechniky** může být veden přímo na zaměstnance. Dle Ing. Luďka Tichého je *„během 22leté praxe bezpečáka tisíckrát potvrzeno, že 86 % všech kybernetických útoků na firmy*

pochází buď zevnitř, nebo za spolupráce vnitřního účastníka, ať už jen z nedbalosti, nebo protože je komprimovaný“.

Položka zvyšování bezpečnostního povědomí je ze zákona povinná. Každý zaměstnanec musí projít řadou školení, které se navíc periodicky opakují. Na školení je zavedený speciální systém, který kontroluje, zda všichni zaměstnanci podstoupili každé povinné školení a za jak dlouho ho budou muset opakovat.

Účinnost školení a povědomí zaměstnanců o bezpečnosti se testuje šestkrát do roka. Provádí se to pomocí falešných **spamů**, které jsou zaměstnancům záměrně posílány a díky těm se kontroluje, jak budou na takové podvodné zprávy reagovat. O odesílání těchto falešných **spamů** se stará dedikovaný **anti-spam systém**.

Testování a kontrola zaměstnaneckých bezpečnostních znalostí je velmi důležitá, jelikož i přes všechna školení se pravidelně vyskytuje zhruba 3,5 % uživatelů, kterých na falešné podvodné **spamy** naletí a pošlou jim například svoje přihlašovací údaje. Takový zaměstnanec musí neprodleně podstoupit další školení zaměřená na kybernetickou bezpečnost, která budou následována opětovným testováním.

IT zaměstnanci, kteří se starají o kritické bezpečnostní systémy, musí podstoupit ještě vyšší formy školení, která jsou potřeba k administraci certifikací. Důležitost těchto školení je tak vysoká, že dokud daný zaměstnanec toto školení nepostoupí, nebo mu na něm vyprší lhůta, zamkne se mu přístup do informačního systému, dokud si požadovaná školení nedoplní a nepodstoupí je.

Vytvoření efektivního školení může být ale obtížný úkol a největší důraz je kladen na obyčejný selský rozum. Jelikož většina **spamů** i metod **sociotechniky** je založená na obyčejných lidských slabostech, jakými jsou chamtivost nebo snaha být vychytralý, je důležité naučit zaměstnance nad každým příchozím e-mailem či zprávou přemýšlet, a aby se sami zeptali sebe, proč právě jim někdo něco nabízí nebo je žádá o pomoc. Podle Ing. Tichého je ovšem tento boj nekonečný, protože *„Souboj proti lidské hlouposti se nedá vyhrát, můžete se jen snažit zlepšit si skóre“*.

Spolu se školeními se pro zvyšování podvědomí o kybernetické bezpečnosti vydávají i firemní články o bezpečnostních tématech jako následky phishingu či hrozby sociotechniky. Všechna školení jsou navíc samozřejmě řádně zdokumentovaná pro audit.

5.7 Krizové řešení

Manažer kybernetické bezpečnosti se také musí zamyslet nad tím, co se stane v případě, že dojde k nějaké katastrofě. Katastrofou v tomto případě může být kompletní nakažení systému, zašifrování ransomwarem a podobně. Už ze zákona o krizovém řešení je dané, že firma musí mít připravené krizové plány, tedy **disaster recovery**. Celý provoz v ČEZu je tedy zálohovaný, aby se v případě nákazy dal poškozený systém nahradit nepoškozeným. Zálohuje se kompletně od fyzické vrstvy až po vrstvu aplikační a zálohy také obsahují návody o tom, jak je správně obnovit. Je zavedený také proces **BCM** (Business Continuity Management) tedy **řízení kontinuity činností**, podle kterého jsou zálohovány i procesy a je zajištěna jejich kontinuita, takže i v případě krize může firma stále na nějaké snížené úrovni fungovat.

Jsou od sebe vzájemně oddělené zálohy systémů, aplikací a dat. Jsou takhle rozdělené pro případ, že by útočník nakazil pouze jednu z těchto tří složek. Pokud by tak nakazil data, stačí jen obnovit ty, a nemusí se nahrávat záloha celého systému, což by zabralo mnohem více času a úsilí, jelikož různé druhy obnovy trvají různě dlouho. Pokud například útočník provede na nějaké webové stránce defacement, stačí jen přehrát onu webovou stránku, což trvá jen chvíli. Pokud ovšem napadne celý systém, může obnova trvat klidně celý den a některé věci mohou být už neobnovitelné a musí se sestavit od základů znovu.

Největší problém ale nastane, pokud se útočníkovi povede nakazit uložené zálohy. Jedním z oblíbených **vektorů útoků** je napadnout zálohy a vzápětí narušit něco, co přiměje bezpečnostní tým je použít. V tu chvíli se ovšem napadené zálohy spustí a s nimi i poškozený systém bez záloh, který napáchá obrovské škody. Proto je dobré zálohy pravidelně kontrolovat, skenovat je antivirem a ukládat různé části záloh na různých místech, aby nemohly být nakaženy najednou, vždy zůstaly nějaké části záloh neporušené a v případě nákazy stačilo odpojit pouze ty narušené.

Moderním trendem je použití takzvaných živých záloh, které se neustále aktualizují a vždy díky tomu poskytují nejaktuálnější verzi celého systému. Jejich velkou slabinou je ovšem případ, kdy útočník napadne systém malwarem, který bude ihned uložen do zálohy. Proto je při zavedení těchto záloh použit systém, kdy se záloha uloží jen v případě zaznamenání změnových přírůstků, které už byly proskenovány antiviry, a po uložení se záloha ihned odpojí.

6 Navrhované metody prevence útoků

Prostor pro zlepšení kybernetické bezpečnosti je prakticky nekonečný. Už z principu může být útočník vždy o krok napřed a úlohou bezpečnostního manažera je neustále vymýšlet možnosti **vektorů útoků** a snažit se jim předcházet. V oblasti bezpečnosti se technologie vyvíjí neuvěřitelně rychlým tempem a zařízení, kterých se dá použít, je obzvlášť v oblasti detekce čím dál tím víc. Aby se předešlo novým hrozbám, které mohou útočníci sledovat, musí být bezpečnostní manažer vždy na pozoru, sledovat nejnovější trendy v bezpečnostních technologiích a zvažovat jejich zavedení ve firemním systému.

6.1 Navrhované nástroje

Technologie se nejrychleji posouvá v oblasti jednotlivých nástrojů, které slouží pro kybernetickou ochranu systému. Obzvlášť v oblasti detekce jednotlivých kybernetických útoku je vyvíjená celá řada aplikací a programů, které dokážou třeba i podrobně rozebrat IP protokol útoku a na základě toho jednat.

Vzhledem k tomu, že doba jednoduchých **antivirů** postupně odchází, jelikož jejich samostatné použití ani zdaleka neslouží k plné kvalitní ochraně firemních aktiv, musí se firmy porozhlédnout po alternativách a nových nástrojích, aby s útočníky udržely krok.

6.1.1 EDR

Jedním z nástrojů, který by se dalo využít, je takzvaný **EDR** (Endpoint Detection and Response), čili **detekce a reakce koncových bodů**. Jedná se o software, který používá všemožné analýzy a umělou inteligenci pro ochranu koncových uživatelů a zařízení v síti. Kontinuálně sbírá data ze všech těchto síťových zařízení, analyzuje je a snaží se najít jakoukoliv stopu po kybernetickém útoku. V případě nalezení takové stopy na něj dokáže automaticky zareagovat a předejít tak ztrátám nebo je alespoň minimalizovat. Umí také účinně odhalovat útoky, které dokážou obejít antiviry a další tradiční systémy detekce. [26]

Dle studií se zhruba 90 % všech úspěšných kybernetických systému zrodí na koncových zařízeních v síti, tedy zařízeních poskytující datovou komunikaci s okolím. Proti těmto útokům jsou běžně instalovány **firewally** a **antiviry**, ty sice dokážou síť ubránit pouze proti známým útokům, ovšem proti sociotechnickým metodám, jako je **phishing**, jsou mnohem méně účinné. Systém **EDR** byl proto vytvořen, aby zalepil tuto bezpečnostní trhlinu a dokáže automaticky, často bez lidské pomoci, identifikovat a odstranit potenciální hrozby dřív, než dokážou napáchat škody. [26]

EDR je schopný vyhledat tyto skryté hrozby díky své struktuře. Tento systém neustále z koncových zařízení sbírá data o jejich spuštěných procesech, výkonu, změnách v nastavení, síťovému připojení i o jejich stahovaných a odesílaných souborech a tyto záznamy ukládá ve své centrální databázi. Tyto záznamy pak pomocí analýz a strojového učení rozebírá a hledá známky podezřelé aktivity. Tuto aktivitu provádí systém **EDR** tím způsobem, že koreluje získaná data s online databázemi útoků, které jsou pravidelně aktualizovány a poskytují tak nejnovější informace o typech útoků, jejich taktikách a typech zařízení, které napadají. Jedna z databází, která může být pro tento účel využita, je již zmíněný **MITRE ATT&CK**. Díky strojovému učení se navíc tento nástroj dokáže sám naučit rozpoznávat příznaky kybernetických útoků a odhalovat tak i neznámé hrozby. [26]

Detekce útoku ovšem není to jediné, co systém **EDR** svede. Díky předem stanoveným pravidlům či své umělé inteligenci může automaticky provádět spoustu akcí, včetně podání hlášení bezpečnostnímu týmu, odpojení napadeného zařízení nebo odhlášení uživatele ze sítě. Umí také zamezit spuštění podezřelých souborů a softwaru a dokáže také automaticky spustit **antiviry**, aby nalezly stejný druh **malwaru** na jiných zařízeních. [26]

EDR také bývá kompatibilní s ostatními prvky kybernetické bezpečnosti. Mnoho EDR řešení se dá napojit na zařízení **SIEM**, díky kterému může získávat ze širší škály zařízení a dostat tak přístup nejen ke koncovým bodům, ale i k aplikacím, databázím, síťového hardwaru a mnoha jiným. Může být také kompatibilní se systémy **SOAR**, aby do automatizovaného řešení kybernetických problémů dokázal zapojit i ostatní zařízení v síti. Jelikož jsou v bezpečnostním systému ČEZ Distribuce oba tyto prvky zavedeny, mohl by být systém **EDR** využívat svých plných kapacit a být užitečným přínosem v odhalování a eliminování neznámých hrozeb.

6.1.2 XDR

Dalším nástrojem, který by se dal zavést, je systém **XDR** (Extended detection and response) čili **rozšířená detekce a odezva**. Podobně jako **EDR** se jedná o nástroj používaný k detekci kybernetických hrozeb, který k vyhledávání podezřelých aktivit využívá analýzy a umělou inteligenci. Na rozdíl od **EDR** ovšem neskenuje pouze koncová síťová zařízení, nýbrž dokáže prohledávat e-maily, aplikace, cloudové nástroje a podobné. Díky tomu dokáže tyto prvky vzájemně koordinovat a ovládat tak, aby dosáhl maximální prevence, dokázal hrozby odhalit a vzápětí na ně i reagovat. [26] [27]

XDR pomáhá v boji proti pokročilým typům útoků, jakými jsou například **DDoS** útoky či **ransomware**. Díky široké škále prvků a nástroje, se kterými komunikuje, dokáže tento systém korelovat bezpečnostní hlášení z celé sítě a díky tomu nemusí být každé z nich řešené zvlášť. To značně urychluje odezvu bezpečnostního týmu a dovoluje jim soustředit se na opravdovou hrozbu jako celek. Spousta řešení **XDR** také zahrnuje plnou integraci se **SIEMem** a **SOARem**, takže vše může být stále ovládáno centrálně a poskytne pracovišti **SOC** plnou efektivitu. [27]

XDR je schopné provádět všechny tyto úkony díky tomu, že spojuje dohromady mnoho nástrojů a sbírá dohromady záznamy ze všech prvků bezpečnostního systému, jakými jsou individuální nástroje jako antiviry či firewally, konkrétní bezpečnostní řešení jako **EDR** anebo i celostní zařízení jako **SIEM** či **SOAR**. Z těchto všech spojení sbírá data o fungování celého systému a ukládá je v centrální cloudové databázi. Podobně jako **EDR** pak tyto data analyzuje pomocí online databází a na nalezenou hrozbu dokáže reagovat všemi možnými způsoby od vytvoření hlášení pro bezpečnostní tým po spuštění relevantních **SOAR** playbooků. [27]

6.2 Provádění analýzy rizik

Při rozhodování zavedení nového nástroje se ve společnosti ČEZ Distribuce vždy skutečně provádí **analýza rizik**. Přesně podle teoretických postupů se nejprve identifikují a nacení firemní aktiva. Toto je jeden z nejdůležitějších kroků a musí se stanovit důležitost aktiv, jelikož z toho nakonec vychází závěr celé analýzy. Dále se k nim přiřadí příslušné hrozby, zranitelnosti a vypočítá se míra rizika.

Součástí rizikové analýzy je navíc i **BIA** (Business Impact Analysis), tedy **dopadová analýza**, která zavedení nástroje zkoumá z finančního pohledu. Během této menší analýzy jsou běžně pokládány dvě otázky: o kolik peněz firma přijde, když aktiva ztratí a o kolik peněz přijde, když budou tato aktiva napadena. Řeší se zde tedy finanční následky hrozeb a finální výsledky se označují jako **dopad peněz**.

S vypočítanou mírou rizika a dopadem peněz se pak společnost rozhoduje, kolik je do daného nástroje ochotna investovat a zda se investice do tohoto nástroje vůbec vyplatí. Bere se zde v potaz poměr investovaných peněz k míře ochrany a bezpečnostní manažer se snaží užitek z vydaných peněz na nový bezpečnostní prvek maximalizovat.

V informačních technologiích platí ovšem kontinuální dynamický vývoj, během kterého se stále objevují nové technologie a ty zavedené se stávají zastaralými. Proto už ve

firmě ČEZ prakticky neexistuje, aby jakýkoliv projekt měl pevně daný začátek a konec a už v průběhu projektu se počítá s dalšími změnami. To má za důsledek to, že celá infrastruktura systému je stavěna otevřeně, aby se v budoucnu daly jednoduše provést další změny a zavést nové nástroje.

Analýza rizik se také neprovádí pouze u nových nástrojů, ale znovu se přepočítává i u změn stávajících systémů, aby se ověřilo, zda se jejich údržba stále vyplatí. Při každé změně, vyvolané například novou kybernetickou hrozbou, se tedy vypočítává nová menší analýza, která se porovná s tou starou.

Vedle **analýzy rizik** provádí architekti ještě procesní a systémové analýzy, které nahlíží na systém jako celek a používají se v případě velkých strukturálních změn.

6.3 Zavádění nových nástrojů

Pro všechny budoucí změny jsou rozjety různé projekty, během kterých se do sítě či do perimetru dostávají nové aplikace a nástroje. Všechno, co se má dostat do produkce, je testováno ve speciálně vytvořeném testovacím prostředí, které věrně napodobuje reálné prostředí a na kterém se bezpečně dají vyzkoušet všechny nové funkce. Toto testování probíhá pomocí penetračních testů, které splňují standardy **OWASP**, a pomocí takzvaného **hardeningu**.

6.3.1 Hardening

Hardening, nebo také česky kalení, je proces, během kterého se testuje nastavení technické vrstvy použitého hardwaru od aktivních prvků až po servery. Provádí se to skenováním, takzvaným **vulnerability scannerem** (skenerem slabin), kterým se porovnává, zda jsou všechny konfigurace a nastavení v pořádku a zda řádně fungují. Během tohoto procesu se eliminují zranitelná místa a celý systém se tak zesiluje.

6.3.2 Penetrační testy

Nad technickou vrstvou se na aplikační vrstvě provádí **penetrační testy**, primárně u webových aplikací či aplikací klient-server. Během **penetračních testů** je nový nástroj vystavený kontrolovaným simulovaným útokům na testovacím prostředí, pomocí kterých se zjistí, zda tento nový nástroj nápor vydrží. Pokud nástroj vyhovuje standardům OWASP, obstál v penetračním testování a nemá žádné další slabiny, vytvoří se dokumentace skutečného provedení projektu, naplní se konfigurační **databáze CMDB** a nový nástroj se spustí do provozu.

Závěr

Cílem této bakalářské práce bylo podrobně popsat teoretické metody používané v boji proti kybernetickým útokům a porovnat je s jejich skutečným fungováním v praxi. Celá praktická část byla provedena u společnosti ČEZ Distribuce, a.s., díky které jsem byl schopný přiblížit reálné fungování bezpečnostních systému ve velké firmě. Vyšlo najevo, že kybernetická bezpečnost je široký obor a aby se byl podnik schopen v moderním kyberprostoru úspěšně bránit, musí už předem počítat s celou řadu vektorů útoků zevnitř i z vnější. Musí také držet krok s dobou a sledovat nejnovější technologie a zvažovat návrhy zapojení nových nástrojů do systému.

Ovšem boj proti kybernetickým útočníkům je nekonečný a je ale sice dobré mít nainstalované nejnovější technologie, mnohem důležitější ovšem je přistupovat ke kybernetické bezpečnosti celostně, s rozumem, a nepodcenit žádnou část přípravy. Ty nejzákeřnější útoky, které napáchají nejvíce škod, jsou běžně ty nejjednodušší a může za ně třeba jen chybné nastavení systému nebo pracovník, který odpověděl na podvodný e-mail. A vzhledem ke statistice a počtu útoků, které jsou vedeny přes zaměstnance, největší ohled musí být brán na neporazitelný lidský faktor, který je všudypřítomný a se kterým musí manažer vždy počítat.

Seznam zdrojů

Použitá literatura

[1] MITNICK, Kevin D. a William L. SIMON. Umění klamu: nejslavnější hacker na světě. Gliwice: Helion, c2003. ISBN 83-7361-210-6.

[2] HUB, Miloslav. Bezpečnost a ochrana informací v prostředí internetu. Pardubice: Univerzita Pardubice, 2013. ISBN 978-80-7395-701-8.

[3] SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

[4] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7.

[5] KIZZA, Joseph Migga. Guide to computer network security. Fourth edition. Cham, Switzerland: Springer-Verlag, 2017. Computer communications and networks. ISBN 978-3-319-55605-5.

Elektronické zdroje

[6] NÁRODNÍ KNIHOVNA ČESKÉ REPUBLIKY. Informační tok. Online. Dostupné z: https://aleph.nkp.cz/publ/ktd/00000/04/000000471.htm. [cit. 2024-04-06].

[7] IBM. What is an intrusion prevention system (IPS)? Online. Dostupné z: https://www.ibm.com/topics/intrusion-prevention-system. [cit. 2024-04-02].

[8] IBM. What is an intrusion detection system (IDS)? Online. Dostupné z: https://www.ibm.com/topics/intrusion-detection-system. [cit. 2024-04-02].

[9] SUBROSA. Understanding the Importance of IDR Security in Cybersecurity: A Comprehensive Guide. Online. Dostupné z: https://www.subrosacyber.com/blog/idr-security. [cit. 2024-04-02].

[10] CYBER DEFENSE MAGAZINE. Understanding Identity Detection and Response. Online. Dostupné z: https://www.cyberdefensemagazine.com/understanding-identity-detection-and-response/. [cit. 2024-04-02].

[11] NÁRODNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI. Nová vyhláška o kybernetické bezpečnosti. Online. 2018. Dostupné z: https://www.govcert.cz/cs/nova-vkb/. [cit. 2024-04-06].

[12] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Legislativa kybernetické bezpečnosti. Online. 2014. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/. [cit. 2024-04-06].

[13] MICROSOFT. Co je SIEM? Online. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-siem. [cit. 2024-04-06].

[14] D3 SECURITY. What is a SOAR Playbook? Online. 2022. Dostupné z: https://d3security.com/blog/soar-playbooks-faq/. [cit. 2024-04-06].

[15] MITRE ATT&CK. Online. 2022. Dostupné z: https://attack.mitre.org. [cit. 2024-04-06].

[16] OWASP. OWASP TOP TEN. Online. 2021. Dostupné z: https://owasp.org/www-project-top-ten/. [cit. 2024-04-06].

[17] CERTIFIKACE MANAŽERSKÝCH SYSTÉMŮ. PDCA cyklus. Online. Dostupné z: https://www.cems-cz.com/clanok/231-pdca-cyklus. [cit. 2024-04-06].

[18] NQA GLOBÁLNÍ CERTIFIKAČNÍ ORGÁN. ISO 27001. Online. Dostupné z: https://www.nqa.com/cs-cz/certification/standards/iso-27001-2022. [cit. 2024-04-07].

[19] AXIANS. Jak probíhá kybernetický útok? Online. Dostupné z: https://www.axians.cz/novinky/jak-probiha-kyberneticky-utok/. [cit. 2024-04-16].

[20] ESET SOFTWARE. DDoS útok. Online. Dostupné z: https://www.eset.com/cz/ddos-utok/. [cit. 2024-04-17].

[21] NOVINKY.CZ. Hackeři zkusili zaútočit na systém přihlášek na střední školy. Online. 2024. Dostupné z: https://www.novinky.cz/clanek/domaci-hackeri-zkusili-zautocit-na-system-prihlasek-na-stredni-skoly-40459572. [cit. 2024-04-17].

[22] LUPA.CZ. Na české weby míří DDoS útoky, výpadky aplikací řeší třeba České dráhy. Online. 2022. Dostupné z: https://www.lupa.cz/aktuality/na-ceske-weby-miri-ddos-utoky-vypadky-aplikaci-resi-treba-ceske-drahy/. [cit. 2024-04-17].

[23] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. Insider Threat Mitigation. Online. Dostupné z: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation. [cit. 2024-04-18].

[24] ESET SOFTWARE. Phishing. Online. Dostupné z: https://www.eset.com/cz/phishing/. [cit. 2024-04-20].

[25] DIGITÁLNÍ PEVNOST. Bot. Online. Dostupné z: https://www.digitalnipevnost.cz/viki/bot. [cit. 2024-04-20].

[26] IBM. What is EDR? Online. Dostupné z: https://www.ibm.com/topics/edr. [cit. 2024-04-26].

[27] IBM. What is XDR? Online. Dostupné z: https://www.ibm.com/topics/xdr. [cit. 2024-04-26].

[28] ESET. Ransomware. Online. Dostupné z: https://www.eset.com/cz/ransomware/. [cit. 2024-04-26].

[29] NOVINKY.CZ. Kybernetických nájezdů na nemocnice dramaticky přibylo. Online. 2022. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-kybernetickych-najezdu-na-nemocnice-dramaticky-pribylo-40402868. [cit. 2024-04-26].