Současná ochrana informačních a kybernetických systémů

(Current Protection of Information and Cybernetic Systems)

Radek Dvořáček

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Radek Dvořáček**
Osobní číslo:	**L16125**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**prezenční**

Téma práce: **Současná ochrana informačních a kybernetických systémů**

Zásady pro vypracování:

1. **Na základě informačních zdrojů světa vyjádřete technické a praktické možnosti řešení zadaného tématu.**
2. **Zpracujte modelovou představu k řešení zadaného tématu.**
3. **Modelováním řešeného problému vyjádřete výsledky řešení daného systémového procesu.**
4. **Zpracujte návrhy a řešení zadaného úkolu a přínos pro rozvoj perspektivní oblasti kybernetické bezpečnosti.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

[1] HROMADA, Martin et al. Kybernetická bezpečnost: teorie a praxe. Praha: Powerprint, 2015. 250 s. ISBN 978-80-87994-72-6.

[2] HRŮZA, Petr. Kybernetická bezpečnost. Brno: Univerzita obrany, 2012. 90 s. ISBN 978-80-7231-914-5.

[3] PORADA, Viktor. Kriminalistika: technické, forenzní a kybernetické aspekty. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016. 1024 s. ISBN 978-80-7380-589-0.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **prof. Ing. Jiří Dvořák, DrSc.**
Ústav krizového řízení

Datum zadání bakalářské práce: **30. listopadu 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

V Uherském Hradišti dne 30. listopadu 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení
L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 15.5.2019

Jméno a příjmení studenta: Radek Dvořáček

.....
podpis studenta

ABSTRAKT

Tato bakalářská práce se zaměřuje na současnou ochranu informačních a kybernetických systémů. Práce je rozdělena na dvě části, a to teoretickou a praktickou. V teoretické části jsou popsány a definovány pojmy týkající se kybernetické bezpečnosti a zabývá se teorií informačních a kybernetických systémů. Praktická část zpracovává konkrétní bezpečnostní opatření, které se při ochraně informačních a kybernetických systému používají. V závěru je provedeno modelování kybernetické bezpečnosti konkrétní organizace.

Klíčová slova: kybernetická bezpečnost, kyberprostor, ochrana, kybernetický systém

ABSTRACT

This bachelor thesis focuses on the current protection of information and cybernetic systems. The thesis is divided into two parts, theoretical and practical. The theoretical part describes and defines terms related to cyber security and deals with the theory of information and cybernetic systems. The practical part deals with specific security measures that are used in the protection of information and cybernetic systems. In the conclusion, the modeling of cyber security of a particular organization is performed.

Keywords: Cyber Security, Cyberspace, Protection, Cybernetic System

Poděkování

Rád bych poděkoval svojí rodině za podporu při mém studiu a prof. Ing. Jiřímu Dvořákovi, DrSc., vedoucímu této bakalářské za odborné vedení a za pomoc a rady při zpracování této práce.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Kyberkriminalita, kyberterorismus a kybernetická válka, jsou v současnosti velmi diskutovaná témata, která souvisejí s masivním rozvojem informačních, komunikačních a kybernetických systémů ve společnosti. Společnost začíná být čím dál více závislá na těchto systémech, a je proto důležité tyto systémy odpovídajícím způsobem chránit. Právě kyberkriminalita je velkou hrozbou pro firmy a společnosti, jelikož většina z nich již dnes využívá informační a kybernetické systémy při své práci. Útoky na informační a kybernetické systémy mohou být pro určité společnosti i likvidační, což znamená že je nutné se těmto útokům věnovat a co možná nejúčinněji se proti nim bránit, což je však velmi složité, jelikož různých typů možných hrozeb je velké množství. S vzrůstajícím počtem věcí a systémů připojených do kyberprostoru, roste riziko jejich zneužití či napadení. Současným fenoménem začíná být připojování různých přístrojů do tzv. internetu věcí, s čímž riziko zneužití a napadení v kyberprostoru roste.

Jelikož se s informačními či kybernetickými systémy dostávám do styku prakticky každý den je pro mě téma ochrany těchto systémů velmi aktuální. Tuto bakalářskou práci jsem proto zaměřil na možné útoky, které mohou být proti informačním a kybernetickým systémům vedeny a na způsoby ochrany a prevence před těmito útoky.

Cílem praktické časti je vytvořit model kybernetické bezpečnosti za pomoci konkrétních bezpečnostních opaření, které jsou v současné době využívány k ochraně informačních a kybernetických systémů. S tímto rovněž konkrétní aplikace softwarové ochrany a v současné době velmi diskutované téma, kterým je bezpečnost mobilních zařízení. Závěrem budou uvedeny návrhy pro rozvoj kybernetické bezpečnosti.

I. TEORETICKÁ ČÁST

1 TEORETICKÁ VÝCHODISKA SYSTÉMŮ

Teorie systémů vznikla jako odpověď na praktické problémy související s růstem složitosti technických a ekonomických projektů. Systém je charakterizován s ohledem na praktické použití jednotlivých vědeckých disciplín. S využitím teorie systémů je možné se setkat už od filosofie, přes fyziku a technické aplikace až k informatice. Z tohoto důvodu je možné nalézt různé definice pojmu systém. Podle těchto definicí je systém: [1]

- Organizovaná množina myšlenek, principů, doktrín, seskupená za účelem vysvětlení vnitřního uspořádání nebo činnosti celku
- Soustava zvolených principů pro řešení určitých celospolečenských problémů (sociální systémy)
- Množina komponent (prvků), která interaguje, aby splnila nějaký cíl
- Pravidelně se ovlivňující nebo vzájemně závislá skupina položek, která je chápána jako celek

1.1 Atributy systémů

Každý systém je spojení různorodých příčin a následků, které na sebe vzájemně působí. Z tohoto důvodu se u systémů používá zjednodušující model, který zahrnuje jen vybranou část těchto projevů. Proto se obvykle předpokládá, že části, které nebyly do systémového modelu zahrnuty neovlivní vývoj modelovaného procesu do té míry, že se závěry stanou nepoužitelnými. Základními atributy systému jsou: [1]

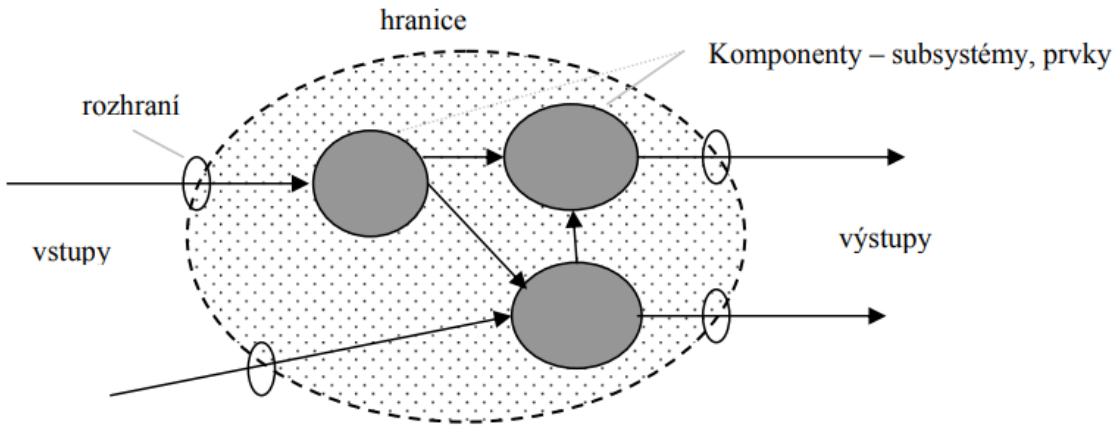
- **Struktura** – je definovaná množinou všech prvků a vazeb (vztahů, relací) mezi prvky, resp. dalšími různými podsystémy daného systému. Systém je možné graficky zobrazit jako reprezentaci fyzické konfigurace reálných objektů, nebo jejich skupin s příslušnými vazbami nebo propojením.
- **Chování** – je projevem dynamiky systému. Dynamika je schopnost vyvolat změnu v systému, zejména jeho stavu. Chování prvků ve vzájemných interakcích, které vyplívají ze struktury systému, určuje chování celého systému.
- **Stav systému** – je souhrn hodnot jeho atributů, vlastností, které lze rozpoznat v daném časovém okamžiku za přesně definovaných podmínek.
- **Stabilita** – je schopnost systému udržovat si při změně vstupů a stavů svých prvků nezměněné chování i přes působení procesů probíhajících uvnitř systému. Stabilitu

je možné chápat jako vlastnost zaručující, že i po určité malé změně podmínek nastane v systému při nezměněných vstupech pohyb jen málo odlišný od původního.

1.2 Popis systému

Systém je velice komplexní záležitost a je proto důležité popsat jednotlivé komponenty, které se v systému nacházejí, a které ho tím pádem tvoří: [1]

- **Prvky systému -** jsou obecně elementární, dále neoddělitelné části systému, které představují jeho rozkladové části, tedy taková část systému, která tvoří na dané rozlišovací úrovni neoddělitelný celek, jehož strukturu není možné rozlišit.
- **Subsystémy -** jsou podmnožina prvků systému, kterou je obvykle možné hodnotit jako samostatný systém se specifickou charakteristikou. Proces rozkladu systému na subsystémy je vhodný pro analýzu a vede k většímu počtu rozhraní (mezi subsystémy).
- **Okolí systému (prostředí) -** je entita, která se zdrojem podnětů působících na systém a která přijímá reakce systému na tyto podněty:
    - Všechny prvky, které neleží v systému, ale za jeho hranicí
    - Přes vstupy ovlivňují systém nebo přes výstupy jsou systémy ovlivňován
    - Jejich změny stavu, chování nebo vlastností ovlivňují systém nebo jsou ovlivňovány jím
- **Hranice systému**
    - Obvykle uzavírá systém nebo odděluje dva či více systémů
    - Logická hranice – podsystém
    - Prostorová hranice – fyzická, nějak prostorově související
    - Propojují se prostřednictvím výstupu jednoho a vstupu jiného
- **Vstup systému -** je množina vazeb či proměnných, jejichž prostřednictvím se uskutečňuje působení okolí na systém.
- **Výstup systému -** je množina vazeb či proměnných, jejichž prostřednictvím se uskutečňuje působení systému na jeho okolí.



Obrázek 1 Schéma systému [1]

1.3 Typy systémů

Rozlišujeme několik typů systémů, které mají různé vlastnosti a specifika. Každý z těchto typů se využívá k jiným aplikacím. Rozlišují se následující typy systémů: [1]

- **Uzavřené** – uzavřený systém je zcela izolován, nemá se svým okolím žádné vazby, trpí entropií nebo poruchami.
- **Otevřené** – u otevřeného systému dochází k energetické a informační výměně s okolím, zpracovávají neočekávané vstupní hodnoty, jsou adaptivní, reagují takovým způsobem, aby pokračovala jejich existence.
- **Deterministické** – deterministické systémy operují a řídí se předurčenou množinou pravidel a zákonitostí, jejich následné chování je jednoznačně určeno aktuálním stavem, charakteristikami systému a vstupními veličinami.
- **Nedeterministické** – nedeterministické systémy jsou řízeny náhodnými událostmi, jejich chování je dáno více pravděpodobností než jistotou množinou pravidel, ovlivňující chování systému je neznámá, nebo příliš složitá a rozsáhlá.
- **Dynamické** – dynamický systém si pamatuje vnitřní stav a řídí se diferenciální rovnic.
- **Statické** – statický systém je tokový systém, jehož výstup závisí pouze na vlastnosti vstupu a řídí se lineární rovnicí.
- **Diskrétní** – diskrétní systémy jsou systémy, které obsahují diskrétní prvky. Diskrétní prvek je prvek s diskrétním chováním, což znamená, že časová množina tohoto prvku je dána konečným nebo spočetným souborem časových okamžiků.

- **Spojité** – systém se nazývá spojitým systémem, jestliže všechny jeho prvky mají spojité chování. Prvek označíme spojitým, jestliže je jeho časová množina interval.
- **Kombinované** – kombinované systémy jsou kombinací systémů spojitých a diskrétních, což znamená že obsahují prvky z obou těchto systémů.

1.4 Informační systém

Definice informačního systému zní následovně: *„Informační systém zkráceně IS je takový typ systému, který se skládá z počítačového hardwaru a počítačového softwaru. Tento systém zpracovává a poskytuje uživateli informace v podobě dat. Informační systém zajišťuje přehlednější organizaci dat. Hlavním úkolem informačních systémů je postarat se o správné uložení, správu a zpracování uložených dat.“* [2]

2 VÝCHODISKA TEORIE INFORMACE

Definice informace je následující: *„Informace je přesná a včasná data, které mají svojí specifikaci a jsou organizována za účelem prezentace v takovém kontextu, který dává smysl a význam. Jejich cílem je zvýšení porozumění a snížení nejistoty. Informace mají svoji důležitost, jelikož dokáží ovlivnit chování, rozhodování nebo výsledky. Pouhé části informací jsou ovšem bezcenné, jelikož po jejich obdržení zůstávají věci nezměněny.“* [3]

V současnosti každá organizace, bez ohledu na svou velikost a odvětví, ve kterém působí, zpracovává nějaká data a informace. Informace se v organizacích mohou nacházet jak v papírové, tak i čím dál častěji v elektronické formě. Tyto informace a data mohou být uložena na nejrůznějších nosičích informací například: [4]

- HDD, SSD discích počítačů, serverů, NAS/SAN, v cloudu
- Přenosných mediích Jako jsou optické disky (CD, DVD, BR) pásky, USB flash disky, paměťové karty (SD, micro SD, CompactFlash, MemoryStick)
- Interní (ne)volailní paměti

2.1 Typy dat a informací

Na nosičích informací uvedených výše se nacházejí data a informace vytvořené. Zpracované a uložené pomocí systému, programu či aplikace nejčastěji v podobě nějakého souboru, například v adresářové struktuře či v databázi. Bez ohledu na použitý formát, kódování a způsob uložení se zpravidla jedná o informace týkající se jedné z těchto oblastí: [4]

- **Řízení lidských zdrojů:**
  - osobní údaje o zaměstnancích (osobní číslo, kontaktní informace, pracovní zařazení, výše mzdy, výsledky hodnocení)
  - seznam, popis a obsazenost pracovních pozic
  - motivační systém (bonusy, zaměstnanecké výhody, systém hodnocení)
- **Marketing:**
  - informace o klientech
  - informace o dodavatelích
  - detaily o proběhlých, stávajících nebo budoucích obchodech
  - informace o nových produktech a službách
  - informace o připravovaných marketingových kampaních
  - výsledky průzkumu trhu a nejrůznější analýzy

- **Management:**
  - strategické plány
  - taktické plány
  - operativní plány
  - pracovní postupy
  - projektová dokumentace
  - bezpečnostní politika, standardy a směrnice
- **Finanční řízení:**
  - účetní doklady
  - výkazy
- **ICT:**
  - síťová infrastruktura (nastavení, dokumentace, hesla)
  - systémy (nastavení, dokumentace, hesla)
  - aplikace (nastavení, dokumentace, hesla)
  - databáze (nastavení, dokumentace, hesla)
  - zdrojové kódy (nastavení, dokumentace, hesla)
- **Facility:**
  - plány budov
  - umístění kamer, čidel, či spínačů
  - počet členů bezpečnostní služby a jejich úkoly

Tento výčet není samozřejmě kompletní, ale výše uvedená data a informace jsou z těch, které by mohli být pro případného útočníka velmi užitečné a zajímavé. Ztráta těchto informací by byla pro organizaci velice nepříjemná. [4]

2.2 Životní cyklus informací

Informace, se kterými organizace pracuje, musí být po celou dobu jejich životního cyklu chráněny způsobem, odpovídajícím povaze těchto informací. Informace musí být chráněny jak v úložišti, tak během přenosu, ale hlavně při jejich používání, neboť hrozí, že by mohlo dojít k narušení jejich důvěrnosti, integrity a též dostupnosti. Každá informace by měla být klasifikována, aby bylo jasné, kdo má k této informaci přístup a jaký přístup má. [4]

2.2.1 Jednotlivé cykly informací

Data at rest – což znamená data v úložišti. K datům v úložišti by měl být řízen přístup, čímž by mělo být dosaženo toho, že se k těmto datům dostane pouze pověřená osoba a bude s nimi nakládat pouze způsobem, který odpovídá prověření této osoby. Informace v úložišti by měly být šifrovány i zálohovány, vzhledem k tomu, že je možné fyzicky ukrást médium, na kterém se informace nacházejí, případně se může útočník pokusit data zničit s čímž pomůže právě záloha. Nesmí se opomenout také na likvidaci informací, protože je žádoucí, aby nemohly být zlikvidované informace znovu použity. [4]

Data in motion – což znamená data v pohybu (při přenosu). Data během přenosu mohou být útočníkem odposlechnuta, pozměněna nebo zahozena. Jako ochrana při přenosu se používá šifrování, dále číslování jednotlivých zpráv (z důvodu ověření, že dorazily ve správném pořadí) a jako ochranu před nežádoucí modifikací se používá podepisování dat. [4]

Data in use – což znamená data při používání. Největší hrozbou pro data při používání je samotný uživatel, který tyto data pořizuje. K práci s daty potřebuje uživatel potřebná oprávnění, ovšem tato oprávnění jsou eliminována, pokud se k datům přistupuje pomocí aplikace. Vzhledem k tomu, že uživatel má během vykonávání práce k datům legitimní přístup je nutné, aby byly jeho aktivity v systému auditovány, čímž je možné odhalit případné nekalé jednání tohoto uživatele. [4]

Obrázek 2 Životní cyklus informace [4]

2.3 Informační bezpečnost

Informace mají v dnešní době vysokou cenu a je nutné je odpovídajícím způsobem chránit. Informace je možné pomocí informačních technologií uchovávat, přenášet, vyhodnocovat a prezentovat. Dle Čandíka musí být informace chráněny tak: [5]

- aby k nim měly přístup pouze oprávněné osoby
- aby se zpracovávaly nefalšované informace
- aby se dalo zjistit, kdo je vytvořil, změnil nebo odstranil
- aby nebyly nekontrolovaným způsobem vyzrazeny
- aby byly dostupné tehdy, když jsou potřebné.

3 TEORETICKÁ VÝCHODISKA KYBERNETIKY

Definice kybernetiky je následující: *„Kybernetika je věda zabývající se obecnými principy řízení a přenosu informací ve strojích, živých organismech a společenstvích. K popisu používá zejména matematický aparát. Za zakladatele je považován americký matematik Norbert Wiener, který v roce 1948 vydal knihu Kybernetika aneb Řízení a sdělování u organismů a strojů.“* [6]

Kybernetika je obvykle pojímána šířeji jako věda o obecných principech vzniku, přenosu, zpracování a uchovávání informace ve složitých živých a neživých systémech a o jejich řízení: [7]

- Kybernetika v sobě zahrnuje více vědních disciplín, např.: metodika přenosu a zpracování informací - informatika
- Využití poznatků z biologie, medicíny a modelování k realizaci technických zařízení obdobných vlastností jaké mají biologické objekty - bionika
- Studium kooperativních (spolupůsobících) jevů, kdy společnou akcí jednotlivých podsystémů vzniknou jevy nové kvality, které by nevznikly prostou sumací vlastností podsystémů - synergetika
- Studium biologických systémů - biokybernetika

3.1 Kyberprostor

Pojem kyberprostor je pro tuhle práci velmi důležitý, a proto bude v této kapitole podrobně popsán, jelikož jak je možné se dozvědět níže s definicemi kyberprostoru to není tak jednoduché, jak by se mohlo na první pohled zdát.

Pojem kyberprostor nemá úplně jasnou definici. Poprvé se pojem kyberprostor (cyberspace) objevil v roce 1982 v povídce Burning Chrome od amerického spisovatele Williama Gibsona, jednoho z nejznámějších autorů tzv. kyberpunku. Pojem kyberprostor zde byl definován jako imaginární prostor tvořený počítačově zpracovanými daty. V souvislosti s počítačovými sítěmi byl poprvé pojem kyberprostor definován Johnem Perry Barlowem, který jej definoval jako symbolický prostor komunikace, kde komplexnost tohoto prostoru záleží na vyspělosti technologie. Další, kdo definoval kyberprostor byl antropolog David Hakken, který jej charakterizoval jako sociální arénu, do které vstupují všichni sociální aktéři, kteří používají ke vzájemné sociální interakci pokročilé technologie. V roce 2001 byl ve slovníku Computer Science and Communications Dictionary definován kyberpro-

stor jako nehmotný svět informací, který vzniká vzájemným propojením informačních a komunikačních systémů. V roce 2006 popisuje Sofia Tzimopoulová kyberprostor jako imaginární místo, na které se nevztahují omezení fyzického světa, což umožňuje mimo jiné vznik nových identit. Uživatel vlastně opouští své tělo a pobývá v prostředí kyberprostoru bez něj. [8]

Jelikož bývá pojem kyberprostor vykládán různými způsoby, není možné v současnosti najít jednu stoprocentně platnou definici, kterou by bylo možné bez výjimek používat, jelikož žádná z definic neobsahuje vše. Většina definic se shoduje v tom, že kyberprostor je nefyzickým místem, kde se nacházíme během komunikace zprostředkovanou moderními technologiemi. [8]

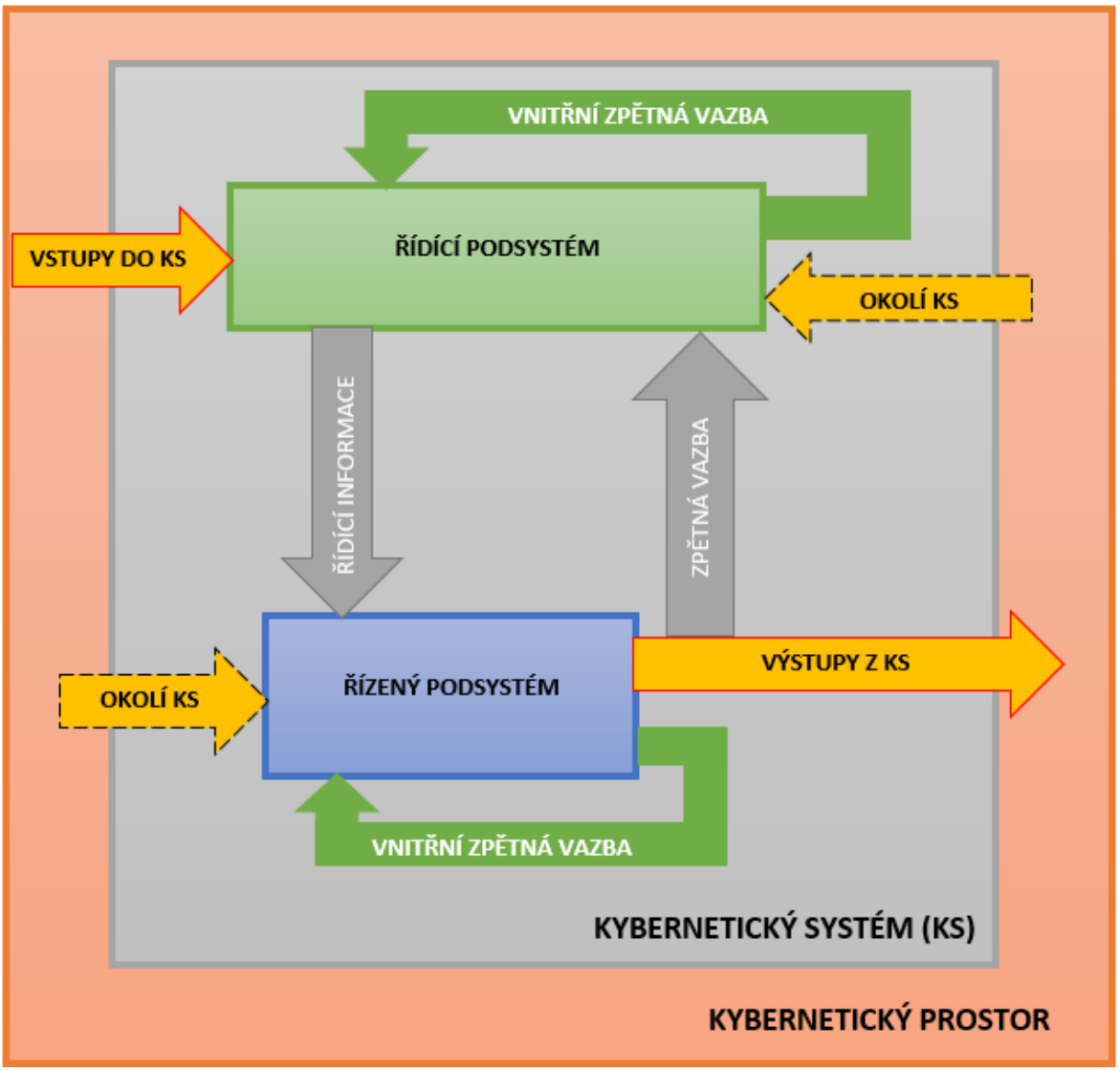
3.2 Kybernetický systém

Jedná se o dynamický systém, jehož existence závisí na výměně informací mezi jednotlivými prvky systému a mezi systémem a jeho okolím prostřednictvím vstupů a výstupů. Kybernetický systém přijímá vstupní signály, následně zpracovává informace, které jsou v těchto signálech obsaženy, a nakonec vytvoří výstupní signály. Pro kybernetický systém je velmi důležitá zpětná vazba. [9]

Kybernetický systém se skládá z řídících prvku, řízených prvků, řídících příkazů a informací. Řídící prvek zabezpečuje tok informací nezbytných pro činnost systému, tyto informace předává řízenému prvku a působení řídících příkazů na řízený prvek jsou následně pomocí zpětné vazby předávány zpět řízenému prvku. Tyto informace jsou zpracovány na nové řídící informace a celý tento cyklus se opět opakuje. [9]

U kybernetického systému je možné rozeznávat tři stavy: [9]

- Konstantní
- Předem určený rovnovážný stav
- Proměnný rovnovážný stav



Obrázek 3 Kybernetický systém [10]

4 KYBERNETICKÁ BEZPEČNOST

Pojem kybernetická bezpečnost se skládá ze dvou dalších pojmů, a to kyber a bezpečnost. Takže pod pojmem bezpečnost rozumíme ochranu něčeho před zničením, poškozením a zcizením. Pro tuto práci je ale důležitější pojem kyber. V anglickém výkladovém slovníku, z angličtiny pojem kyber pochází, je možné najít, že slovo kyber (angl. cyber) se používá jako přídavné jméno nebo předpona související s počítači či počítačovými sítěmi. [4]

V oblasti kybernetické bezpečnosti se řeší narušení základních atributů bezpečnosti, přesněji jde o ohrožení dostupnosti počítačů a počítačových sítí, důvěrnosti a integrity dat a informací, které jsou v těchto počítačích a počítačových sítích uložena, zpracovávány nebo přes ně přenášena. [4]

S rozvojem informačních technologií se dramaticky změnila situace při nakládání s informacemi a daty, kdy mohou být tyto data uložená v elektronické podobě lehce kopírována, měněna či mazána bez toho, aniž by bylo nutné být přímo na místě, kde jsou uložena. Vzhledem k těmto skutečnostem se z ochrany informací stala vědní disciplína a dnes již bezpečnost informací představuje poměrně rozsáhlý obor. Při ochraně informací není podstatné v jaké formě se informace nachází, ale podstatná je hodnota těchto chráněných informací, případně velikost škody související s případným odcizením či zneužitím těchto informací. [11]

4.1 Zákon o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Cílem Zákona je stanovit minimální požadavky na standardní zabezpečení kritické informační infrastruktury, kritické komunikační infrastruktury, významných informačních systémů a významných sítí a zajistit dohledovým pracovištím přehled o situaci v kybernetické bezpečnosti, a to tak, aby zásahy do soukromé sféry povinných subjektů byly co nejmenší. Zákon je ve sbírce zákonů uveden pod číslem 181/2014 Sb. a nabyl účinnosti dne 1. ledna 2015. [12]

4.1.1 Narušení kybernetické bezpečnosti dle zákona

Kybernetická bezpečnostní událost je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací. [12]

Kybernetický bezpečnostní incident je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události. [12]

4.2 Bezpečnost dat a informací

Jak již bylo výše popsáno v kybernetické bezpečnosti se řeší narušení základních atributů bezpečnosti, přesněji jde o ohrožení dostupnosti počítačů a počítačových sítí, důvěrnosti a integrity dat a informací, které jsou v těchto počítačích a počítačových sítích uložena, zpracovávány nebo přes ně přenášena. Vzhledem k důležitosti těchto pojmů, budou níže tyto pojmy popsány.

4.2.1 Důvěrnost

Pod pojmem důvěrnost rozumíme zajištění přístupu k informaci pouze těm, kteří jsou k tomu oprávněni. Narušení důvěrnosti znamená nežádoucí zpřístupnění určitých informací třetí osobě. Ochrana důvěrnosti dat může zahrnovat také různá zvláštní školení pro ty, kteří budou s těmito informacemi pracovat. [4]

Informace se klasifikují dle určitého klasifikačního schématu. Toto klasifikační schéma by mělo být v prvé řadě srozumitelné, aby mu zaměstnanci rozuměli a neměli tak problém s klasifikací informací. U klasifikační schématu je rovněž důležitý počet klasifikačních stupňů, kterých nesmí být ani příliš mnoho, ani příliš málo. Příliš mnoho stupňů by znamenalo jak vyšší obtížnost zařazování informací, tak i vyšší nákladnost. Příliš málo stupňů by zase mohlo znamenat podceňování hodnoty informací. V praxi se využívají dvě klasifikační schémata, jedno ve státním sektoru a druhé v komerční sféře. [4]

Ve státní sféře se používá následující schéma: [13]

- Přísně tajné
- Tajné
- Důvěrné
- Vyhrazené

V komerční sféře se nejčastěji používá následující schéma: [4]

- Důvěrné
- Soukromé

- Citlivé
- Veřejné

4.2.2 Integrita

Integrita dat a informací znamená zajištění jejich správnosti a úplnosti. Narušení integrity spočívá v nežádoucí modifikaci tzn. změně. Problémem integrity dat je, že když dojde k narušení integrity těchto dat je problematické toto narušení odhalit, což znamená že většinou dojde k zjištění tohoto problému až po dlouhé době. Z tohoto důvodu je možné, že se původní hodnotu nepodaří zjistit, či jen velmi obtížně. [4]

4.2.3 Dostupnost

Dostupnost znamená zajištění, že informace je v okamžiku potřeby přístupná pro konkrétní oprávněné uživatele. Pokud se stane, že je informace zničená znamená to, že je narušena její dostupnost. Dostupnost dat je velmi důležitá, jelikož při nedostupnosti dat není možné vykonávat žádnou činnost s nimi související. Z tohoto důvodu je žádoucí, aby byla dostupnost dat co možná nejvyšší. V souvislosti s dostupností dat se používají dva pojmy: [4]

- **RTO (doba nedostupnosti)** – vyjadřuje, jak dlouho po výpadku musí být systém funkční
- **RPO (ztráta dat)** – vyjadřuje kolik práce, či jaké množství dat může být ztraceno

5 KYBERNETICKÁ KRIMINALITA

Vzhledem k anonymitě v kyberprostoru je možné očekávat kriminální činnost. Vzhledem k velice rychlému vývoji v oblasti informačních technologií se dostala ochrana informačních systémů a počítačových dat před útoky v kyberprostoru do trestněprávních předpisů všech vyspělých zemí. [14]

Pojem kybernetická kriminalita je odvozován od pojmu kybernetický prostor zkráceně kyberprostor, který byl popsán v první kapitole této práce. Kybernetická kriminalita, dříve také označována jako informační kriminalita, je definována v Policii ČR jako trestná činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí. Samotná oblast informačních a komunikačních technologií je buď předmětem útoku, nebo je páchána trestná činnost za výrazného využití informačních a komunikačních technologií jakožto významného prostředku k jejímu páchání. [14]

Kybernetická kriminalita se v České republice začala postihovat v roce 2002 dle zákona č. 140/1961 Sb., trestního zákona, ve znění pozdějších předpisů. Právní úprava související s kybernetickou kriminalitou je nyní obsažena v Trestním zákoníku. Vzhledem k Úmluvě Rady Evropy o počítačové kriminalitě ze dne 23. Listopadu 2001 se postihování kybernetické kriminality v České republice značně rozšířilo. [14]

5.1 Kybernetický útok

Kybernetický útok je typ útoku odehrávající se v kyberprostoru. Kybernetický útok bývá označován jako operace využívající informační technologie a počítačové sítě za účelem přerušení, zhoršení kvality, potlačení nebo zničení informací v počítačích případně v počítačových sítích. Jelikož kybernetický prostor nemá jasně stanovené hranice, je nutné tyto útoky řešit z mezinárodního pohledu. [11]

V současné době se stávají kybernetické útoky stále častějšími a organizovanějšími a mají za následek větší škody. Tyto útoky jsou vedeny převážně na řídící prvky technologie, což může mít za následek nejen ohrožení této technologie případně počítačové sítě, ale může vážně ohrozit také životy lidí anebo výrobu. [11]

Vzhledem k tomu, že jsou kybernetické útoky vedeny v kyberprostoru, je obtížné pachatele vystopovat, což pachatelům přináší větší zisky s menším rizikem. Ministerstva, vládní

agentury, ale i soukromé společnosti na celém světě čelí každý den stovkám až tisícům kybernetických útoků za den. [11]

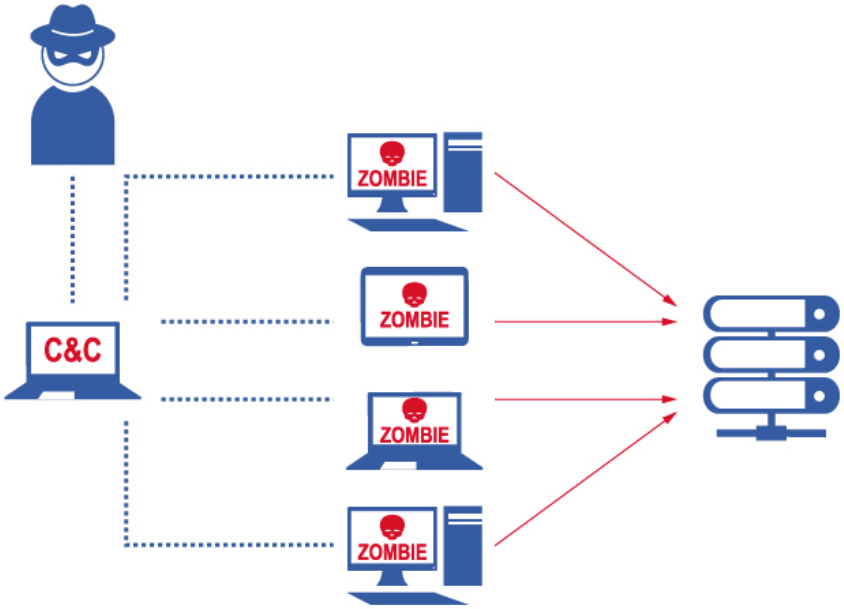
5.2 Typy kybernetických útoků

Různých typů kybernetických útoků je velká spousta, z toho důvodu jsou zde vypsány pouze ty nejdůležitější. Problémem kybernetických útoků je, že útočníci vymýšlejí stále nové způsoby, jak na uživatele případně organizace zaútočit, ať už s cílem uškodit, poškodit, či ukrást data. To znamená, že uvést všechny typy útoků ani není možné, jelikož i právě v tuto dobu může být vymýšlen nový typ útoku.

5.2.1 Botnet

Botnet je síť softwarově propojených botů, což jsou programy, které umí plnit příkazy útočníka zadávané z jiného počítačového systému. Botnety jsou v současnosti využívány převážně k ilegální činnosti za pomoci malwaru. [15]

Cílem Botnetu není poškození uživatele zařízení, ale finanční zisk. Útok pomocí botnetů probíhá tak, že útočník si pronajme od tvůrce botnetu jeho síť a pomocí této sítě pak provádí různé kybernetické útoky či jinou nekalou činnost v kyberprostoru. Toto řešení je pro útočníka výhodné v tom, že vystupuje zcela anonymně, jelikož útok nevede ze svého zařízení. [16]



Obrázek 4 Schéma Botnetu [16]

5.2.2 Malware

Malware je škodlivý software, který slouží k různým nekalým činnostem v kyberprostoru, například: k narušení standardní činnosti počítačového systému, zisku informací či dat, k získání přístupu do počítačového systému. Pod souhrnným názvem malware se skrývají různé počítačové viry, jako jsou například: adware, spyware, červi, trojské koně, rootkity, keyloggery. [15]

5.2.3 Ransomware

Ransomware je druh škodlivého kódu, který se projevuje tak, že uživateli zablokuje přístup k jeho souborům, či části systému. Soubory, ke kterým ransomware zablokuje přístup, zpravidla zašifruje a za jejich dešifrování si útočník žádá nemalý obnos peněz, který chce vyplatit v kryptoměně, nejčastěji v Bitcoinech. Rizikem při vyplácení výkupného je, že útočník data nedešifruje. Nejznámějším ransomwarovým programem je program WanaCry. [17]

Dle mého názoru, je ransomware v současnosti jednou z největších hrozeb, jelikož hrozí bezprostřední ztráta dat a je těžké se proti tomuto typu útoku bránit. Mezi odborníky je ransomware označován jako hrozba budoucnosti. Nejlepší ochranou před ransomwarem je zálohování dat, jelikož i po napadení počítače ransomwarem, jsou data v bezpečí v cloudu.

Obrázek 5 WannaCry [18]

5.2.4 Spam

Pojem spam se v ICT využívá zejména pro označení nevyžádané komunikace. Spam je možné chápat ve dvou rovinách. Může se jednat o hromadné šíření či rozesílání nevyžádaného sdělení, nejčastěji jde o nějaké reklamy, což probíhá prostřednictvím elektronické pošty. Nebo jde o všechny doručené nevyžádané zprávy, což zahrnuje zprávy obsahující viry, červi, trojské koně apod. Spam je v současnosti hodně rozšířený a asi každý kdo vlastní nějakou e-mailovou adresu se s ním setkal. [15]

5.2.5 Phishing

Phishing je podvodné jednání, při němž se využívají informační a komunikační technologie. Cílem phishingu je získání uživatelových citlivých údajů, může se jednat o přihlašovací údaje k různým internetovým službám, různá hesla, čísla platebních karet, PIN kódy apod. [19]

Při phishingu se často využívá sociálního inženýrství, kdy se útočník snaží napodobit různé žádosti, převážně z bank a vylákat tak z uživatele potřebné údaje. Tyto žádosti jsou nejčastěji šířeny pomocí elektronické komunikace, nejčastěji e-mailů, i když v dnešní době se phishing rozšiřuje i do dalších komunikačních služeb či aplikací. [19]

5.2.6 Hacking

Hackingem se nejčastěji rozumí proniknutí do cizího počítačového systému, prolomením či obejitím bezpečnostních opatření, které učinil uživatel tohoto systému. Útočník většinou nemá z tohoto jednání žádný užitek. Nejčastěji mu jde jen o to, aby si dokázal určitou intelektuální či individuální převahu. Objevují se však i útočníci, kteří uživatelům přímo škodí. [11]

Útočníkům tzv. hackerům jde nejčastěji o poznání, jakým způsobem informační technologie, aplikace či technický prostředek funguje. Tyto informace pak zpřístupňují ostatním uživatelům. Hackeři mývají vynikají znalosti o fungování informačních a komunikačních systémů, díky čemuž jsou i skvělými programátory. [15]

5.2.7 Cracking

Cracking znamená proniknutí do cizího systému prolomením či obejitím jeho ochranných prvků, jehož cílem je způsobit uživateli škodu, získat informace, případně získat nějaké finanční prostředky. Cracking se používá i k obcházení ochranných prvků, které chrání před ilegálním kopírování různé aplikace, programy či hudební a filmové produkty, to znamená porušování autorských práv a duševního vlastnictví. [15]

5.2.8 Sniffing

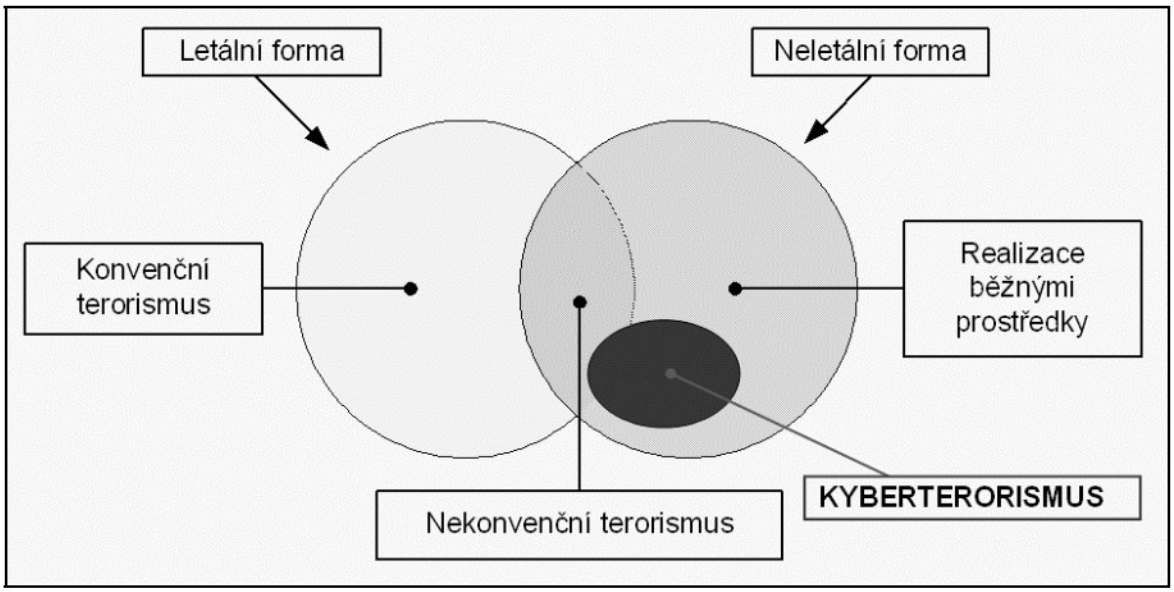
Při sniffingu dochází k odposlechu přenášených dat. Využívá se k tomu tzv. sniffing paket. Sniffing umožňuje jednotlivcům zachytit data v průběhu přenášení po síti. Sniffing převážně využívají síťoví profesionálové k diagnostice sítě a problémů týkajících se sítě. Sniffing však může být využit i k nekalému jednání což znamená, že útočník odposlouchává síťovou komunikaci, čímž získává cenná data o uživateli, která může využít ke svému obohacení. Pokud útočník zachytí data při přenosu může je použít i k získání přístupu do systému. [20]

5.2.9 DoS a DDoS útoky

Při DoS útocích jde o znepřístupnění služby a je realizován tak, že se napadaný počítačový systém zahltí pomocí opakovaných požadavků na úkony, které má systém realizovat. DoS útok se v systému projeví hlavně jeho zpomalením, nebo jeho úplnou nedostupností. DoS útoky jsou nejčastěji realizovány proti nějakým internetovým službám či webovým stránkám. Rozdíl mezi DoS útokem a DDoS útokem je v tom, že při DoS útoku je útok veden z jednoho zdroje (počítače), kdežto DDoS útok je veden z více zdrojů (počítačů). Z tohoto vyplývá, že DDoS útoky jsou mnohem nebezpečnější a je mnohem obtížnější se proti nim bránit. [15]

5.2.10 Kyberterorismus

Kyberterorismus je název pro teroristické aktivity, které jsou uskutečňovány pomocí informačních a komunikačních technologií a odehrávají se v kyberprostoru. Jde vlastně o teroristické aktivity zaměřené proti informačním a kybernetickým systémům. Jedná se o jednu z aktuálních globálních hrozeb, která se prudce rozšiřuje do celého světa. Cílem kyberterorismu je povětšinou ovlivnění veřejného mínění. [21]

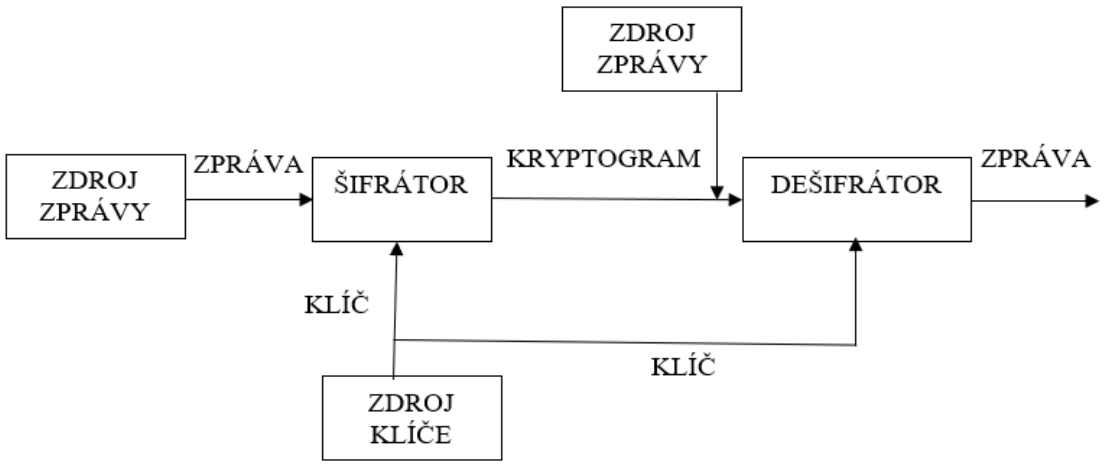


Obrázek 6 Zobrazení forem terorismu [22]

6 KRYPTOGRAFIE

Kryptografie pomocí matematických metod chrání informaci před jejím přečtením nebo modifikací. Kryptografie se využívá převážné při přenosu informací po síti, jelikož v této době je informace nejzranitelnější. Nejúčinnějším řešením ochrany informací při přenosu by bylo nepřenášet informace elektronickou cestou, což se však neshoduje s filozofií informační společnosti, tudíž se o této variantě ani neuvažuje. Dalším opatřením by mohlo být pouze fyzické přenášení informací, což by však bylo velmi nákladné a časově náročné. Z těchto důvodů je dnes kryptografie jedinou rozumnou možností ochrany dat při přenosu. [8]

Kryptografický systém se skládá z šifrovacího a dešifrovacího zařízení, šifrovacího a dešifrovacího klíče a zprávy v otevřeném textu a kryptogramu. Při kryptografii dochází k šifrování textu zprávy od odesílatele do tzv. kryptogramu, což probíhá v šifrátoru pomocí určitého klíče. Následně se zpráva v podobě kryptogramu přenáší k příjemci, přičemž může být napadena útočníkem, který však bez odpovídajícího klíče nemůže zprávu rozluštit. K dešifrování probíhá v tzv. dešifrátoru, což probíhá u příjemce za pomoci dešifrovacího klíče. [8]



Obrázek 7 Schéma kryptografie [8]

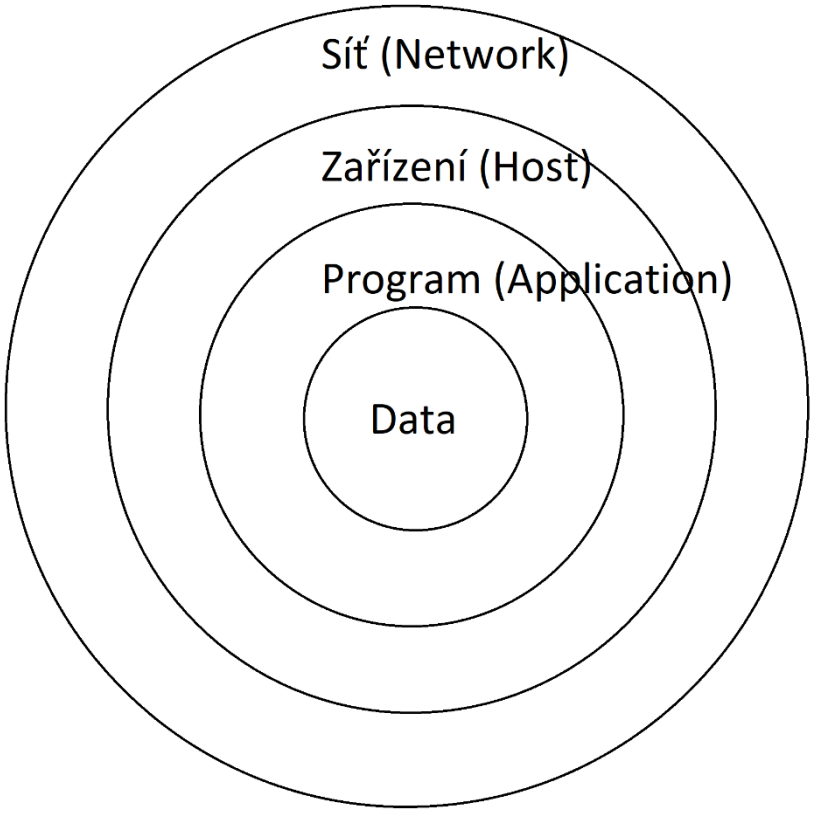
II. PRAKTICKÁ ČÁST

7 POUŽÍVÁNÁ BEZPEČNOSTNÍ OPATŘENÍ

Bezpečnostní opatření mohou být jak informační, tak i technické povahy. Bezpečnostní opatření uvedená v kapitole by měla implementovat každá organizace bez ohledu na velikost a odvětví ve kterém působí. Úkolem těchto opatření je snížit riziko na akceptovatelnou úroveň. Rozeznáváme několik typů opatření, patří mezi ně např.: organizační, technická, systémová, aplikační, databázová, komunikační a kryptografická. [4]

Aby bylo dosaženo alespoň minimální optimální ochrany dat, je nutné implementovat a prosazovat tzv. security-in-depth přístup, jenž spočívá v zavedení preventivních, odstrašujících, zdržujících, detekčních, reaktivních a obnovujících opatření, a to je nutné udělat ve všech vrstvách informačního systému organizace. [4]

Vícevrstvá struktura je nejčastěji chápána tak, že pokud jedno z provedených opatření selže, tak alespoň další opatření v řadě budou účinná. Pro takovýto přístup se používají názvy jako obrana v hloubce (defence in depth) a vícevrstvá bezpečnost (layered security). Zobrazení vícevrstvé struktury na následujícím obrázku je to, které je nejčastěji používáno, avšak toto konkrétní zobrazení nezachycuje dvě z podstatných částí informačních systémů, a to jsou prostory ve kterých se informační systémy nachází, a to vůbec nejdůležitější lidi, kteří se systémem pracují. [4]



Obrázek 8 Přístup k datům u vícevrstvé bezpečnosti [37]

7.1 Identifikace

Identifikace je pro bezpečnost organizace důležitým bezpečnostním prvkem. Každému subjektu v informačním systému je přidělen jednoznačný identifikátor, díky němuž je poté možné zjistit, činnost tohoto subjektu v systému a jeho odpovědnost. Takovýto identifikátor by měl být používám výhradně daným subjektem a za žádných okolností by neměl být sdílen. Subjektem v tomto případě rozumíme většinou nějakého lidského operátora případně nějakou komponentu. Identifikátory využívající se k identifikaci jsou nazývány zkratkou ID, která je mezinárodně uznávaná. Je několik typů ID, které se v současné době využívají a budou uvedeny v následujících odstavcích. [4]

7.1.1 Systémem generované ID

Takové to ID, jak už název napovídá, generuje samotný systém, díky čemuž je nepredikovatelné a nedá se z něj zjistit komu toto ID patří. Na tato ID je obtížné vést útoky, jelikož není možné vědět, zda se takové ID v systému vůbec nachází a rovněž není možné vést útok na konkrétní subjekt. Problémem systémem generovaného ID je jeho obtížné zapamatování pro uživatele. [4]

7.1.2 Uživatelem vytvořené ID

Uživatelem vytvořené ID je výhodné v tom, že si jej bude uživatel snadněji pamatovat, avšak je problematické z několika důvodů. Aby bylo ID bezpečné je nutné uživateli nařídit jaká má být minimální délka a jaké znaky má obsahovat. U uživatelsky vytvořeného ID je asi nejdůležitější to, co se objeví na obrazovce při vytváření ID, pokud již bylo použito. Taková to situace by mohla napomoci útočníkovi k získání seznamu již existujících účtů. [4]

7.1.3 E-mail jako ID

Využití e-mailu jako ID je pro uživatele tou nejpříjemnější variantou, jelikož si stačí pamatovat pouze heslo. Problémem však může být právě to heslo, protože hrozí, že uživatel použije k přístupu do systému stejné heslo, jaké využívá k přihlašování do svého e-mailu. Dalším problém je to, že útočník může útok cílit přímo proti konkrétnímu uživatel, jelikož získat jeho e-mail není v dnešní době vůbec složité. [4]

7.2 Autentizace

Autentizací se rozumí proces, který určuje, kdo jste a jaké máte oprávnění pro přístup do informačního systému, subjekt prakticky prokazuje, zda je tím, za koho se vydává. V informačních systémech bývají implementovány systémy řízení oprávněného přístupu, které zajišťují kontrolu a audit autentizačních procesů. [23]

Autentizace bývá zpravidla založena na některém z následujících způsobů, které jsou vázány na uživatele. Autentizace je založena na tom že uživatel: [4]

- **Něco ví** – nejčastěji uživatelské jméno a heslo případně ID
- **Něco má** – například USB flash disk nesoucí identifikační informace
- **Něco je** – tento způsob je založen na biometrických charakteristikách

7.2.1 Dvoufaktorová autentizace

Výše uvedené metody je možné ke zvýšení bezpečnosti kombinovat. Tato kombinace metod se nazývá dvoufaktorová autentizace a odborníci v oblasti bezpečnosti poukazují na nezbytnost využití této dvoufaktorové autentizace. Doporučuje se využívat dvoufaktorového ověření už i u základních informačních systémů. Využitím dvoufaktorového ověření je eliminována zranitelnost informačních systémů, které využívají autentizaci typu jméno a heslo. [23]

7.2.2 Autentizace založená na sdíleném tajemství

Jedná se o nejpoužívanější autentizační metodu a označuje se také jako sdílené tajemství mezi uživatelem a serverem. K autentizaci se využívá uživatelské jméno a heslo. Heslo je řetězec znaků, kterým uživatel potvrzuje svoji identitu. Autentizace v tomto případě probíhá tak, že uživatel zadá uživatelské jméno a heslo, načež server tyto údaje ověří ve svojí databázi, a pokud se tyto údaje shodují, povolí přístup do systému. Výhodou této metody je, že na počítači, pomocí kterého se uživatel do systému přihlašuje, nemusí být instalována žádná softwarová nebo hardwarová komponenta. Nevýhodou této metody je, že si uživatel musí pamatovat přihlašovací heslo a jelikož se uživatel většinou potřebuje přihlašovat do více systémů k nimž potřebuje odlišná hesla je pravděpodobné, že si hesla začne zapisovat případně bude jedno heslo jen lehce modifikovat, díky čemuž může útočník další hesla lehce odhalit. [4]

Možností útoků na tuto metodu autentizace je více a o prolomení hesla se uživatel systému nemusí ani dozvědět, což znamená velké riziko. Možnosti útoků na autentizační metodu založenou na sdíleném tajemství:

- **Sociální inženýrství –** Sociální inženýrství spočívá v tom, že útočník útočí na nejslabší článek v zabezpečení systému, což je v tomto případě člověk. Největší slabinou člověka je, že není stroj, ale jedná například na základě svých emocí, znalostí či zkušeností. Díky tomuto může člověk důvěřovat klamným informacím, které byly zaslány například e-mailem a na základě sdělených instrukcí také jednat. O svém omylu, který si tímto jednáním způsobil se zpravidla dozví až je mu způsobena nějaká škoda. [24]
- **Zcizení hesla** – Heslo může být velice jednoduše zcizeno, pokud si je uživatel někam zapíše. Pokud možno je nejlepší si hesla zapamatovat, čímž eliminujeme riziko odcizení hesla. Ne vždy je však možné si heslo zapamatovat, například administrátorská hesla jsou velice složitá a je velmi obtížné si takové heslo zapamatovat. V tomto případě je vhodné takové to zapsané heslo vložit například do uzamykatelného trezoru. Pozornost by se též měla věnovat uložení hesel v systému, ta by nikdy neměla být uložena v otevřeném tvaru. [4]
- **Odpozorování a odposlechnutí hesla –** Aby nemohlo dojít k odpozorování hesla je nutné učinit potřebná opatření. Tato opatření mohou zahrnovat kontrolu okolního prostoru, jestli se tu náhodou nenacházejí osoby, které tu nemají co dělat či jestli se v prostoru nenacházejí nastražené kamery. Dále by se na obrazovce místo znaků měli objevovat puntíky či hvězdičky v nejlepším případě nic, čímž je útočníkovi zabráněno zjistit počet zadávaných znaků. Jednou z nejlepších metod ochrany je zadání určitých znaků hesla podle pořadí umístění, čímž je útočníkovi zabráněno v odpozorování hesla, jelikož zná pouze nějaké znaky a nezná jejich pořadí. Odposlechnutí hesla je možné na základě rozdílných zvuků, které vydávají jednotlivé klávesy. Zabránit odposlechnutí hesla je možné zadáváním pomocí virtuální klávesnice. [4]
- **Zjištění hesla pomocí Softwaru –** Zjištění hesla pomocí softwaru je možné je možné pomocí tzv. keyloggerů, což jsou specializované programy vytvořené právě pro získání hesla. Tyto programy jsou obtížně odhalitelné a obvykle se dokáží důkladně maskovat. Ochranou před tímto způsobem zjištění hesla může být využití

virtuální klávesnice, avšak existují typy keyloggerů, které jsou schopné snímat obrazovku včetně pozice kurzoru díky čemuž heslo snadno zjistí. [4]

- **Zjištění hesla pomocí Hardwaru –** Tento způsob zjištění hesla spočívá v instalaci, nějakého specifického hardwarového zařízení, které je schopné zjistit heslo. Takové to zařízení může být umístěno například do klávesnice případně na kabel vedoucí ke klávesnici, nebo do samotné bedny počítače. Ochrana před tímto způsobem zjištění hesla spočívá v kontrole hardwaru počítače a připojených zařízení. [4]
- **Odchycení hesla při bezdrátové komunikaci –** Heslo je možné zachytit při přenosu po síti, která již není pod správou té určité organizace. Jako opatření se využívá šifrování komunikace. Heslo je možné zachytit také při použití bezdrátové klávesnice. Nejnebezpečnější je využití bezdrátové klávesnice využívající k přenosu dat rádiové frekvence. Bezpečnější je použití klávesnice s technologií Bluetooth, která narozdíl od radiofrekvenční technologie využívá šifrovaný přenos dat. [4]
- **Uhádnutí nebo prolomení hesla –** Ochrana před uhádnutím hesla je jednoduchá, a to používat složitá hesla kombinující různé znaky. Nejhorším typem hesla je jednoduché slovo, které má nějaký vztah k určité osobě. Prolomení hesla, které obsahuje jedno slovo je možné za pomoci speciálních programů využívajících slovník. [4]

7.2.3 Autentizace pomocí biometriky

Biometrika je jeden z nejlepších způsobů využívaných k autentizaci. K identifikaci osoby využívá biometrika jejích jedinečných tělesných znaků. Biometrika je zároveň velmi výhodnou metodou i z pohledu nákladů, jelikož žádné pozdější náklady na tento systém nejsou. Další nespornou výhodou biometriky je, že si uživatel systému nemusí pamatovat žádná složitá hesla či další přihlašovací údaje. Biometrické charakteristické znaky zůstávají většinou po celou dobu života neměnné, díky čemuž je není možné ukrást či zapomenout. I když při určitých vážných zraněních by se mohli biometrické znaky poškodit, například popálením rukou se mohou znehodnotit otisky prstů. V současné době se začíná využívat biometriky čím dál tím více a různé čtečky či senzory se nacházejí už i na noteboocích či mobilních telefonech. [25]

Nejpoužívanější metody autentizace pomocí biometriky:

- **Otisk prstu –** Autentizace na základě otisku prstu je jednou z nejznámějších a nejpoužívanějších metod biometrické autentizace. Snímání otisku se provádí dvěma

způsoby, a to přiložením prstu na snímač, nebo přejetím prstu po snímači. První z těchto dvou způsobů je nákladnější, jelikož dokáže získávat více dat, například tok v krevním řečišti, a zároveň je přesnější a spolehlivější. [4]

Metody zachycení otisků prstů: [25]

- **Otisk získaný pomocí inkoustu a papíru** – jedná se o klasickou metodu využívající se ve forenzní sféře. Při zabezpečení systémů se s touto metodou nesetkáváme, avšak při řešení případných trestných činů se této metody využívá.
- **Statické snímání** – Jedná se o nejběžnější metodu, spočívající v přiložení prstu na snímač bez jakéhokoliv pohybu s ním. Je to uživatelsky velmi intuitivní metoda. Nevýhodou může být nehygieničnost spočívající v zašpinění senzoru, nebo zničení snímače přílišným tlakem. Na senzoru rovněž mohou zůstat latentní otisky.
- **Snímání šablonováním** – Tato metoda spočívá v přejíždění prstem po snímači, čímž se otisk šablonově snímá. Výhodou je že snímač se nezašpiní a nezůstávají tu žádné latentní otisky. Nevýhodou může být horší intuitivnost, kdy se uživatel musí naučit určitý postup a rovněž může z pohledu uživatele docházet k pocitu, že tento způsob je pomalejší.

- **Geometrie ruky –** při snímání geometrie ruky obvykle měříme délku, šířku a tloušťku, jak ruky, tak i jednotlivých prstů. Tento způsob se obvykle využívá k zabezpečení významných objektů, jelikož je bezpečnější a přesnější než například otisk prstu, a také je pořízení takového zařízení mnohonásobně dražší. Velkou výhodou je že získání geometrie ruky je velmi náročné. [4]
- **Geometrie tváře –** V současnosti stále využívanější metoda, založená na identifikaci osob podle tváře. K identifikace se využívá tvar obličeje a poloha opticky významných míst nacházejících se na tváři. V počítači bývá obraz uložen jako matice jasových úrovní. [25]

  Rozlišují se dva systémy snímání a identifikace, a to jsou 2D a 3D systémy. 2D systém je sice levnějším řešením, avšak ne moc spolehlivým, jelikož jde oklamat i pouhou fotografií. U 3D systému se na rozdíl od 2D systému měří i hloubka, což znamená že pouze fotografií oklamat nelze. Ke zvýšení přesnosti snímání se u 3D

systému využívají infračervené kamery, díky nimž je možné tento způsob autentifikace využívat i při sníženém osvětlení, či ve tmě. [4]

- **Oční duhovka –** Oční duhovka je pro každého člověka jedinečná, a to dokonce i u jednovaječných dvojčat. Jedná se o jednu z nejspolehlivějších a nejpřesnějších biometrických metod, která založená na snímání vzorkování duhovky oka. Pro snímání duhovky je důležitá velmi kvalitní kamera a infračervené osvětlení. Aby bylo zabráněno použití fotografie sledují snímače změnu pohybu oka, změnu zornice a mrkání. [25]
- **Akustická charakteristika hlasu –** Při rozpoznávání hlasu se porovnává předem nahraný hlas s hlasem osoby, která se autentizuje. Nevýhodou této metody může být špatné rozpoznávání v rušném prostředí. Dalším problémem může být použití různých mikrofonů s různou úrovní citlivosti, což má za následek zhoršené rozpoznávání hlasu. V posledních letech však tato metoda hodně pokročila a stává se tak stále spolehlivější. [4]
- **Biometrie ušního boltce –** Snímání ušního boltce je zatím nepříliš používaná metoda, která je však velmi přesná. Existují tři metody biometrické identifikace podle ušního boltce což jsou: podle morfometrických vztahů, podle otisku struktur ušního boltce a podle termogramu ušního boltce. Pro komerční využití je nejlépe použitelná první metoda, kdy se používá optické snímací zařízení, které snímá ušní boltec z určité vzdálenosti. Druhý způsob by byl uživatelsky velmi nepohodlný. [25]
- **Způsob psaní na klávesnici –** Tato metoda je založena na dynamice psaní a je vhodné ji využít při vícefaktorové autentizaci. Výhodou této metody je**,** že není nutné instalovat žádný speciální hardware a po uživateli nejsou požadovány žádné úkony navíc. Další výhodou je, že uživatel může být autentizován i v průběhu práce. Nevýhodou může být, že styl psaní určitého uživatele se může v průběhu času měnit. [4]
- **Rukou psaný podpis –** Tato metoda využívá kombinace anatomických a behaviorálních vlastností člověka, které se projevují při podepisování. Při této metodě se snímá dynamika podpisu. Tyto nasnímané pohyby se poté porovnávají s těmi uloženými v databázi. Nevýhodou může být možné napodobení podpisu jiným člověkem. [25]
- **Krevní řečiště –** Snímání krevního řečiště probíhá za pomoci Led osvětlení, které prosvítí prst a eliminuje světlo poblíž IR spektra, následně je pořízen snímek krev-

ního řečiště pomocí CMOS snímače. Výhodou této metody je, že nevadí, pokud je prst znečištěn či zraněn. Další výhodou je obtížné, ba prakticky nemožné získání těchto údajů případným útočníkem, jelikož se snímá něco, co se nachází pod kůží. Jedná se o velmi spolehlivé řešení, jehož míra odmítnutí je 0,01 % a přijmutí dokonce 0,0001 %. Nevýhodou může být delší doba pořízení snímků, což je asi 20 sekund. [25]

7.2.4 Autentizace založená na vlastnictví předmětu

Tento typ autentizace spočívá ve vlastnění nějakého autentizačního předmětu, tyto předměty jsou nazývány autentizačními tokeny. Velkou výhodou těchto autentizačních tokenů je, že jsou obtížně kopírovatelné. Přístup přes autentizační tokeny bývá většinou ještě chráněn nějakým heslem či PIN kódem, což zvyšuje bezpečnost použití této autentizační metody. Nevýhodou této autentizační metody je, že když uživatel ztratí token je nemožné se do systému přihlásit a další nevýhodou je, že pokud dojde k odcizení tokenu spolu s přihlašovacím heslem, může se útočník vydávat za někoho jiného. [4]

V současnosti využívané autentizační tokeny:

- **SMART karta –** většinou plastová karta vybavená čipem s integrovaným obvodem, magnetickým proužkem, či bezdrátovým čipem, která slouží k identifikaci či autentizaci konkrétní osoby. SMART karta bývá obvykle chráněná také PIN kódem. Pro použití SMART karet je nutné, aby byl počítač či notebook vybaven speciální čtečkou těchto karet. [26]
- **USB token –** Funguje na stejném principu jako čipová karta, však mezi jeho nespornou výhodu patří, že USB port má v dnešní době prakticky každý počítač a není tak nutné pořízení speciální čtečky. Na rozdíl od SMART karty nemůže být vybaven fotografií k identifikace konkrétní osoby. [4]
- **Mobilní telefon –** Mobilní telefon je možné využívat k autentizaci například zavoláním na konkrétní číslo, případně může přijímat tzv. One Time Password zasílaných prostřednictvím SMS. Dále je možné mobilní telefon vybavit speciální aplikací sloužící k autentizaci. [4]

V dnešní době bývají moderní mobilní telefony vybaveny i tzv. NFC čipy, které je rovněž možné použít k autentifikaci. Velkou výhodou autentifikace pomocí mobilního telefonu je, že jej má uživatel neustále při sobě.

7.3 Autorizace

Autorizace následuje hned za autentizací. Díky autorizaci může správce systému omezit či jinak modifikovat oprávnění pro určité role nebo funkce, které vykonávají zaměstnanci v té konkrétní organizaci. U autorizace je důležitá pravidelná kontrola uživatelů, kteří mají přístup do oblastí, které jsou jim vyhrazené. [23]

Nastavování práv je založeno na předem definovaných skupinách, jelikož by časově náročné nastavovat práva každému zaměstnanci zvlášť. U autorizace rozlišujeme dva způsoby řízení přístupu, a to diskrétní řízení přístupu a nediskrétní řízení přístupu. U diskrétního způsobu řízení rozhoduje o přístupu k souboru jeho vlastník, kdežto u nediskrétního způsobu je přístup řízen pomocí rolí jednotlivých uživatelů. [4]

7.4 Auditing a monitoring

Cílem auditingu je zpětně vytvářet rekonstrukci činnosti uživatele, administrátora, či části systému. Při auditingu se vytváří log či protokol ze kterého se právě tato rekonstrukce vytváří. Informace obsažené v auditním protokolu bývají většinou velmi cenné, a proto je nutné, aby k nim byl řízený přístup. O tom, jaké informace budou logovány a jak dlouho budou uschovány, rozhoduje provozovatel daného systému. [4]

Při monitoringu se sleduje aktuální situace, či stav systému. Zvýšení určitých sledovaných hodnot, jako je například zatížení CPU či množství dostupné paměti, může vést k nedostupnosti systému, což je pro organizaci nežádoucí. Tento typ monitoringu je nazýván jako provozní monitoring. Kromě provozního monitoringu se rozlišuje také monitoring bezpečností. Funkce bezpečnostního monitoringu spočívá v odhalování pokusů o překonání bezpečnostních opatření. [4]

7.5 HIDS a NIDS

HIDS je anglická zkratka pro host-based intrusion detection system, do češtiny přeloženo jako systém detekce narušení hostitele. Jedná se o systém, který monitoruje počítač, na kterém je instalován a detekuje vniknutí nebo zneužití, což oznámí určenému orgánu/uživateli. HIDS lze považovat za agenta, který monitoruje a analyzuje, zda někdo nebo něco, ať už zevnitř nebo zvnějšku, obcházel bezpečnostní politiku systému. [27]

NIDS je anglická zkratka pro network-based intrusion detection system, do češtiny přeloženo jako síťový systém detekce narušení. NIDS je často samostatné hardwarové zařízení, které obsahuje možnosti detekce sítě. Obvykle se bude skládat z hardwarových senzorů umístěných na různých místech sítě. Může se také skládat ze softwaru instalovaného na různých počítačích připojených po síti. NIDS analyzuje datové pakety jak příchozí, tak odchozí a nabízí detekci v reálném čase. [27]

7.6 Hashování

Hashování je bezpečnostní opatření při němž se řetězec libovolné délky transformuje na bytový řetězec s pevnou délkou. Toto opatření se používá převážně ke kódování malých množství dat převážně hesel. Při přihlašování se uživatelské heslo zakóduje pomocí hashovací funkce a následně se hashovací funkce porovnává s hodnotou uloženou v databázi, díky tomuto je pro útočníka obtížné zjistit heslo, pokud se neoprávněně dostane do databáze. [28]

Pomocí hashovací funkce je možné také zjistit, zda nebyla pozměněna integrita souborů, které se na počítači nacházejí. Speciální programy pro kontrolu identity dokáží pomocí hashovací funkce porovnávat současné hodnoty a hodnoty, které byly vypočteny hned po instalaci. Díky tomuto je možné například zjistit záměnu systémové knihovny za knihovnu útočníkovu. [4]

7.7 Šifrování

Pod šifrováním se rozumí proces převodu dat do takového formátu, který nemůže neoprávněná osoba snadno přečíst. K šifrování se používají dvě metody, a to symetrické a asymetrické šifrování: [23]

- **Symetrické šifrování –** při tomto typu šifrování využívají obě strany, tzn. odesílatel i příjemce, stejný šifrovací klíč. Tento typ je bezpečnější, avšak distribuce klíčů je obtížná, a to zejména ve velkých organizacích, při velkých objemech těchto klíčů.
- **Asymetrické šifrování –** při tomto typu šifrování se využívají dva typy klíčů, a to veřejný klíč pro šifrování a privátní klíč pro dešifrování. Výhodou je snadnější distribuce klíčů, jelikož každý má svůj klíč.

Šifrování se využívá k zajištění důvěrnosti a integrity dat během celého jejich životního cyklu. Aby bylo šifrování co nejbezpečnější, je nutné využívat spolehlivý kryptografický algoritmus. Právě při implementaci kryptografického algoritmu dochází k nejvíce chybám, které snižují bezpečnost zašifrovaných souborů. [23]

7.8 Zálohování a archivace

Zálohování, tedy spíše záloha je kopie určitých dat, která je pořízena v takové podobě, v jaké se nachází v daném časovém okamžiku. Pro optimální ochranu dat je vhodné zálohy uschovávat mimo fyzický dosah dat, které byly zálohovány. Zálohování je v současné době velmi důležité, jelikož po zničení, nebo odcizení dat je možné dále pokračovat v práci na zálohovaných datech. Náklady na zálohování jsou velmi malé v porovnání s možnými ztrátami. [29]

Archivace souvisí právě se zálohováním. Při archivaci se vytvářejí archivy ze záloh, díky čemuž je možné obnovovat systém ke konkrétnímu časovému okamžiku. Archivy jsou využívány k dlouhodobému uchovávání dat, u něhož se nepředpokládá rychlé obnovení těchto dat. V souvislosti se zavedením archivace je nutné vypracovat také skartační plán, jelikož není možné uchovávat všechna data od počátku vzniku organizace. K archivaci se využívají média, která mají dlouhou životnost. [4]

8 APLIKACE SOFTWAROVÉ OCHRANY INFORMAČNÍCH A KYBERNETICKÝCH SYSTÉMŮ

Uživatelé informačních systémů a komunikačních systémů se před možnými hrozbami plynoucími z používání těchto zařízení mohou bránit pomocí různých druhů softwaru, který je k tomu určený. Tento software bývá primárně určen k předcházení útoků, které se týkají programového vybavení počítače. Nejznámějším softwarem, který se k tomuto účelu využívá je antivirový program. Níže jsou popsány možné softwarové řešení včetně již zmiňovaného antivirového programu.

8.1 Antivirové programy

Antivirové programy se využívají k identifikaci virů a jejich následnému odstranění. K identifikaci virů využívají antivirové programy tzv. virové databáze. Antivirové programy fungují tak, že skenují programy v počítači a porovnávají různé zjištěné hodnoty se svojí virovou databází. Vzhledem k tomuto je velmi důležité, aby byla virová databáze pravidelně aktualizovaná. Antivirové programy, nebo spíše antivirové systémy, sledují všechny nejpodstatnější vstupní nebo výstupní místa z počítačového systému, jelikož právě těmito místy by mohl virus do systému proniknout. [30]

V dnešní době je na trhu velké množství produktů, které slibují antivirovou ochranu, ale ne všechny jsou tak spolehlivé, jak slibují. Mezi nejznámější antivirové programy patří například: Kaspersky, ESET, AVG, Avira, Norton, Avast!, McAfee. Za dlouhodobě nejlépe hodnocený antivirový program je považován antivirový program od společnosti Kaspersky, který se často umisťuje na prvních příčkách v hodnocení antivirových ochran.

8.2 Antispam

Antispamová ochrana spočívá ve filtrování nežádoucích zpráv tzv. spamu tak, aby tím nebyl konečný uživatel obtěžován. Antispamové programy fungují na principu vytváření seznamů důvěryhodných a spamových adres. Tyto adresy dokáží antispamové programy rozeznávat samy, ale je možné určité adresy zařadit do seznamu manuálně. [31]

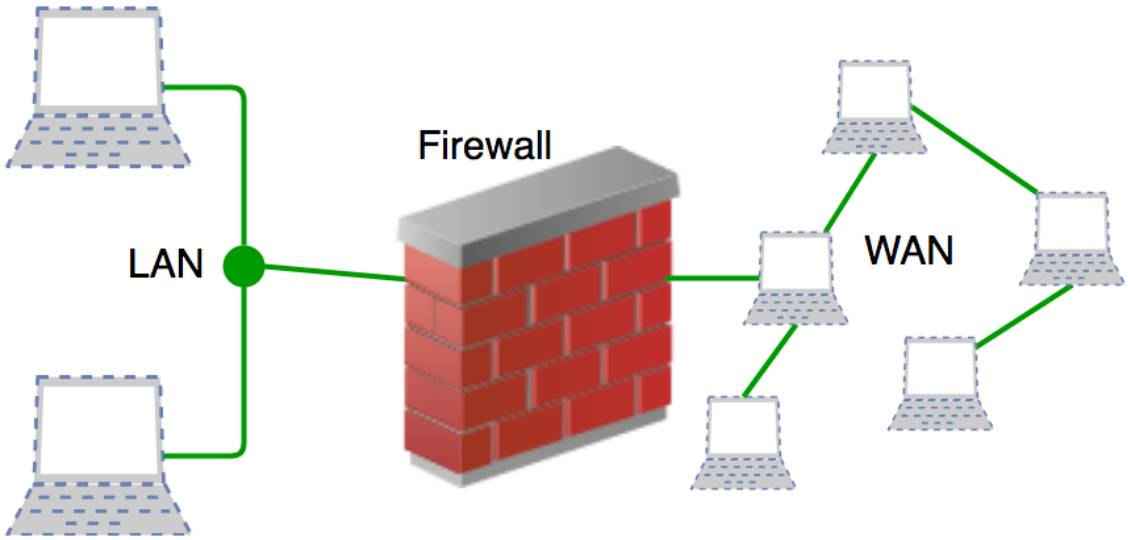
8.3 Antispyware

Antispyware slouží ke zjištění a odstranění špionážního softwaru. Tento špionážní software je nebezpečný v tom, že shromažďuje osobní a jiné důležité informace bez toho, aniž by

sdělil uživateli, co dělá. Problémem u těchto programů je narušení soukromí uživatele, protože tyto programy zaznamenávají každý krok, který je na internetu či v počítači proveden. Největším nebezpečím však je, že špionážní programy dokáží zjistit přihlašovací údaje na různé služby.

8.4 Firewall

Firewall odděluje provoz mezi dvěma sítěmi, a to mezi vnitřní či domácí sítí a internetem. Firewall má definovaná pravidla, podle kterých propouští data jedním nebo druhým směrem, čímž brání neoprávněným průnikům do sítě a také se stará o to, aby nebyly odesílány data ze sítě bez vědomí uživatele. Firewall by měl být instalován na každé zařízení, které přistupuje k internetu, jelikož je to nejefektivnější a nejdůležitější první krok k ochraně počítačových systémů. Není však možné se spoléhat pouze na firewall, ale je dobré jej kombinovat i s nějakým antivirovým programem, jelikož někteří útočníci dokáží proniknout i přes firewall. [32]



Obrázek 9 Schéma firewall [33]

9 BEZPEČNOST MOBILNÍCH ZAŘÍZENÍ

S příchodem chytrých telefonů tzv. smartphonů se rozšířil prostor pro hackery a kyberzločince. Výhodou mobilních zařízení je to, že nepotřebují pevné připojená do komunikační struktury a je možné je používat ve volném prostoru. Velkým problém mobilních zařízení spočívá v tom, že uživatelé si velmi často neuvědomují, jak citlivá a osobní data se v jejich zařízení nacházejí. Vzhledem k tomu, že se mobilní zařízení využívají jak při práci, tak i při provádění plateb, je nutné mít takové zařízení odpovídajícím způsobem zabezpečeno. [8]

9.1 Možné hrozby při používání mobilních zařízení

V současné době se útočníci čím dál více zaměřují na mobilní zařízení, jelikož mobilní zařízení často nejsou tak dobře chráněna, jak počítače, které bývají chráněny lépe, vzhledem k tomu, že se na trhu objevují delší dobu a o útocích na ně, je více informací. Hrozeb ohrožujících mobilní zařízení je stále více a více a je nutné je znát, aby bylo možné se proti nim účinně bránit. Hrozby začínají být stále sofistikovanější a je stále složitější takové hrozby odhalit a bránit se proti nim. [34]

Současné hrozby ohrožující mobilní zařízení: [34]

- **Mobilní spear hishing –** mobilní spear phishing se na rozdíl od klasického e-mailového phishingu, který je založen na rozesílání velkého množství e-mailů a následného čekání na oběť, zaměřuje na konkrétní osoby. Toto mu nejčastěji umožňují sociální sítě a veřejné profily na nich. Právě díky sociálním sítím mohou útočníci přesně cílit své útoky, které tím získávají na věrohodnosti. Tyto útoky jsou založené na zasílání zpráv pomocí komunikačních aplikací či sociálních sítí. Velkým problémem těchto útoků je, že běžné phishingové ochrany jsou proti tomuto typu útoku neúčinné. Společnosti vyvíjející operační systémy do mobilních zařízení sice vytváří různá bezpečnostní opatření, avšak nejslabším článkem zůstává i nadále lidský faktor a zůstává jen na uživateli, jestli takové podvodné jednání odhalí.

- **Hrozby týkající se SMS zpráv** – jednou z hrozeb týkající se mobilních zpráv je tzv. SMS forwarding, což znamené přesměrování příchozích zpráv, například od platebních služeb. Díky těmto zprávám mohou útočníci vniknout do uživatelských účtů.

Další z hrozeb týkající se mobilních zpráv, může být škodlivá aplikace, která automaticky odesílá tzv. premium SMS, které jsou zpoplatněné vysokými poplatky. Uživatel se o takovém napadení mobilního zařízení zpravidla dozví až po delší době, což znamená vysokou finanční ztrátu.

- **Útoky na mobilní bankovnictví –** útoky na mobilní bankovnictví probíhají pomocí škodlivých aplikací, či nějakého malwaru. Tento malware odcizuje čísla platebních karet, osobní údaje či přímo přihlašovací údaje k bankovním aplikacím. Tento typ útoku je pro útočníka velmi výhodný, jelikož po napadení zařízení jde o rychlý a velký zisk.

Obrázek 10 Vybrané vektory a dopady útoků na mobilní zařízení [34]

9.2 Možnosti ochrany mobilních zařízení

U mobilních zařízení se rozlišují tři hlavní možnosti jejich ochrany: [35]

- **Základní vlastnosti platforem (operačních systémů)** – výrobci operačních systémů přináší neustálé aktualizace reagující na aktuální hrozby. Opatření obsažená přímo v operačním systému však nejsou stoprocentní a před nejmodernějšími hrozbami ochránit nedokáže.
- **Řešení typu EMM/MDM –** jedná se o nástroje centrální správy používané převážně ve větších organizacích. Toto řešení nabízí řadu bezpečnostních funkcí jako například omezení přístupu uživatele a aplikací k HW (kamera, GPS, USB rozhraní a další) i ke službám, dále šifrování přenášených a uložených dat, a nakonec je možné pomocí tohoto řešení celé zařízení vymazat, pokud náhodou dojde ke ztrátě či odcizení.
- **Řešení typu MTD –** jedná se o nejmodernější bezpečnostní nástroj. Řešení typu MTD dokáže identifikovat podezřelé nebo škodlivé aplikace díky tomu, že provádí jejich emulaci ve virtuálním prostředí, čímž dokáže zabránit možným škodám způsobeným těmito aplikacemi. Další hrozbou, kterou dokáže MTD odhalit, je podezřelé nebo škodlivé síťové chování. Připojení k těmto podezřelým sítím MTD okamžitě deaktivuje, čímž ochrání soubory uložené v mobilním zařízení. V neposlední řadě dokáže MTD odhalit bezpečnostní trhliny v operačním systému a zaměřuje se na možné hrozby pramenící z tohoto problému.

10 MODELOVÁNÍ

V této kapitole bylo provedeno modelování kybernetické bezpečnosti u společnosti VZP. Modelování vychází z volně dostupného dokumentu „Standardy IS VZP – NIS“. Tento dokument obsahuje charakteristiky, metody, postupy a podmínky, týkající se bezpečnosti informačních a kybernetických systémů.

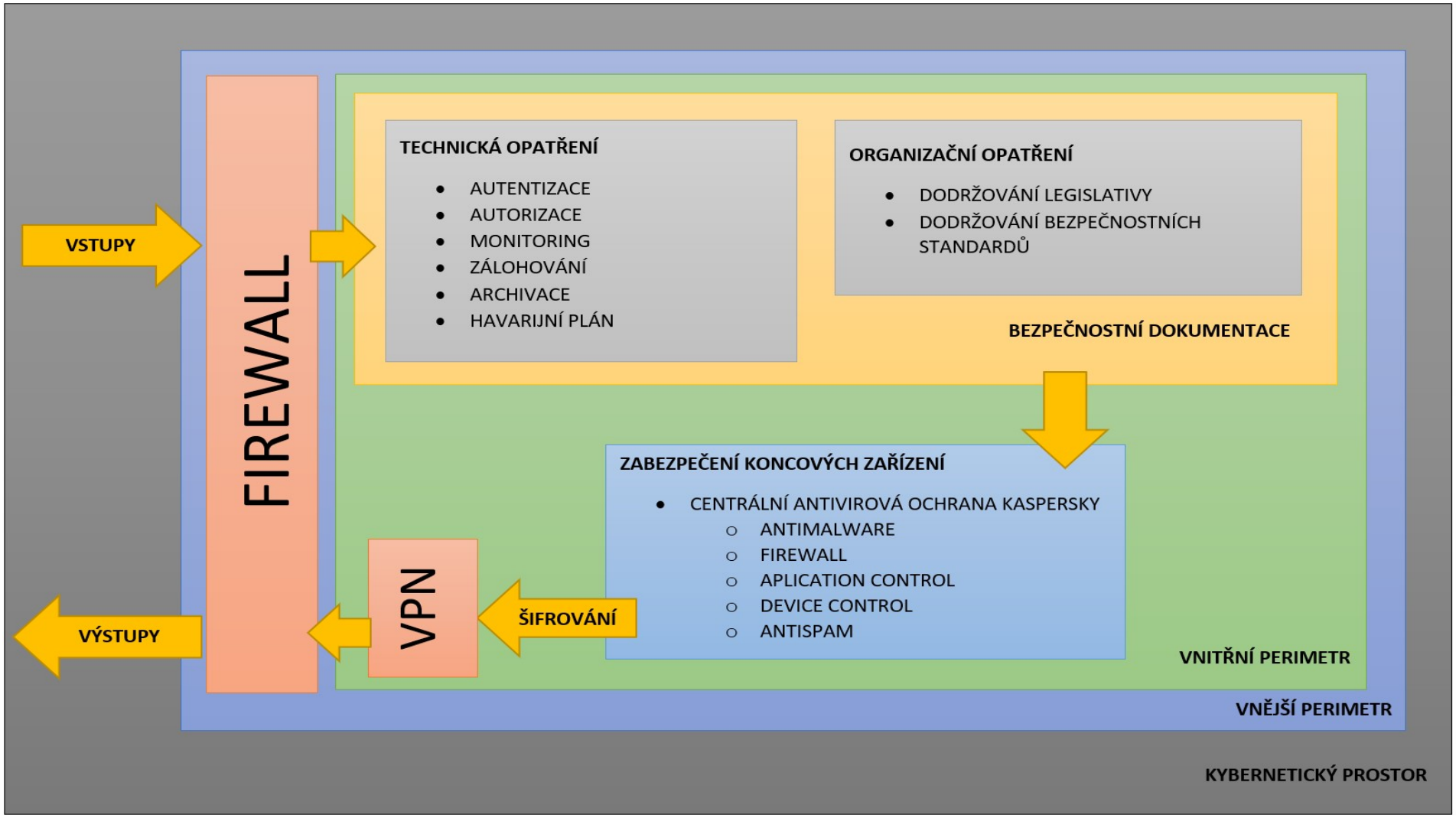
10.1 Společnost VZP

Společnost Všeobecná zdravotní pojišťovna zkráceně VZP je lídrem českého systému veřejného zdravotního pojištění. Byla zřízena dnem 1. ledna 1992, a to zákonem č. 551/1991 Sb. S téměř 6 miliony klientů je VZP největší zdravotní pojišťovnou v České republice. Hlavním úkolem každé zdravotní pojišťovny, a tedy i VZP, je v souladu se legislativními normami vybírat pojistné na zdravotní pojištění na straně jedné a na straně druhé hradit zdravotní služby. [36]

10.2 Vyjádření výsledků modelování

Smyslem modelování je nahrazení zkoumaného systému jeho modelem, který dává ucelený pohled na zkoumaný systém. Výsledkem modelování je tedy model, v tomto případě je to model kybernetické bezpečnosti u konkrétní společnosti.

Tento model se zaměřuje primárně na kybernetickou bezpečnost dané společnosti a zobrazuje klíčové prvky sloužící jako ochrana před kybernetickými útoky. Údaje byly získány z dokumentu „Standardy IS VZP – NIS“, jehož část je součástí přílohy této práce.



Obrázek 11 Model kybernetické bezpečnosti [10]

10.3 Popis modelu

Zajištění kybernetické bezpečnosti spočívá v eliminování hrozeb, které se do systému dostanou z kyberprostoru. Vnější perimetr slouží k oddělení externích sítí od sítě interní. Ve vnějším perimetr se nachází firewall, který dokáže eliminovat možné hrozby přicházející z cizích sítí. Ve vnitřním perimetru se kybernetická bezpečnost řídí podle bezpečnostní dokumentace, která určuje, jaká opatření jsou v systému použity. Mezi technická opatření, která jsou využita ve společnosti patří: autentizace, autorizace, monitoring, zálohování, archivace a havarijní plán. Mezi organizační opatření patří: dodržování legislativy a dodržování bezpečnostních standardů. Koncová zařízení jsou zabezpečena pomocí antivirového programu od firmy Kaspersky, konkrétně jde o program Kaspersky Endpoint Security, který je v tomto konkrétním případě centrálně řízený. Tento produkt zahrnuje antimalware, firewall, aplication control, device control a antispam. Výstupy jsou šifrovány a odesílány přes VPN server, aby nedošlo k jejich napadení při odesílání.

11 NÁVRHY PRO ROZVOJ KYBERNETICKÉ BEZPEČNOSTI

I když i v současnosti je nutné věnovat se kybernetické bezpečnosti, bude v budoucnu nutné zaměřit se na kybernetickou bezpečnost mnohem více. Technologie začínají do života zasahovat čím dál více a s internetem věcí a rozvojem průmyslu 4.0 to bude ještě masivnější.

V současnosti je pro informační a kybernetické systémy největším nebezpečím lidský faktor. Lidé nejsou neomylní a také bývají trochu leniví, z čehož mohou potencionální útočníci těžit. S lidským faktorem to je však složité a nikdy jej nelze zcela eliminovat, i když v budoucnu by dle mého názoru bylo nejlepší vliv lidského faktoru na kybernetické systémy snížit. Dalším možným řešením tohoto problému by mohla být větší osvěta o kybernetické bezpečnosti, aby si lidé uvědomili, jaká hrozí nebezpečí a jak je možné se proti těmto nebezpečím bránit. Rovněž by bylo vhodné, aby organizace více kontrolovali své zaměstnance při pohybu v kyberprostoru. Organizace by však rovněž měli svým zaměstnancům poskytovat zařízení, která splňují všechny bezpečnostní standardy.

Další kapitolou je softwarová ochrana, která se pořád vyvíjí a tím reaguje na stále nové hrozby. V budoucnu se dle mého bude muset softwarová ochrana vyvíjet mnohem rychleji, vzhledem ke vzrůstající tendenci kybernetických útoků.

Ochrana mobilních zařízení už je v současné době hodně řešeným tématem. V budoucnu se však dle mého začne kybernetická bezpečnost u mobilních zařízení řešit mnohem více. Lidé si dnes ještě plně neuvědomují, jaká rizika jim z používání mobilních zařízení plynou. Bezpečnost u mobilních zařízení úzce souvisí s již zmiňovaným lidským faktorem tím pádem by mělo dojít k větší osvětě uživatelů využívajících tato zařízení. V budoucnu by se měly firmy vyrábějící tato mobilní zařízení zaměřit více na technické možnosti zabezpečení, jelikož v současnosti nejsou všechny tyto technické metody plně dostačující a vznikají zde tzv. bezpečností díry.

Momentálně se zatím příliš neřeší bezpečnost ostatních zařízení připojených do tzv. internetu věcí, jelikož zatím nejsou příliš vyvinuté technologie, které by tyto zařízení podporovaly. V budoucnu se však bude muset pozornost odborníků na kybernetickou bezpečnost zaměřit právě tímto směrem, jelikož počet zařízení připojených do sítě bude dle mého rychle přibývat. Přibývat budou i taková zařízení, o kterých by si běžní lidé nikdy nemysleli, že půjdou do sítě připojit.

ZÁVĚR

Tato bakalářská práce se zabývala současnou ochranou informačních a kybernetických systémů. Cílem práce bylo vytvořit model kybernetické bezpečnosti pro kybernetický systém určité společnosti.

V teoretické části této práce byly vypsány a popsány pojmy, které přímo souvisí s ochranou informačních a kybernetických systémů. Z teoretické části rovněž vyplývá že kybernetická bezpečnost je v současnosti velmi důležitým tématem a je potřeba se jí zabývat. Teoretická část se zabývá teorií informačních a kybernetických systémů a dává pochopit, co to vlastně ty informační a kybernetické systémy jsou. Z tohoto důvodu jsou zde uvedena teoretická východiska systémů, která dávají pochopit co to systém je a jaké typy systémů je možné rozlišit. Dále se teoretická část práce zabývala informacemi a východisky jejich teorie, ať už se jedná o definici informace, typy informací a životní cyklus informace. Teoretická východiska kybernetiky dávají pochopit, co to kybernetika je a jaký je její smysl. V této části byla uvedena definice kybernetiky a definován kyberprostor, což je pro tuto práci velice důležité. Následovala kybernetická bezpečnost, která vychází právě z teorie kybernetiky a řeší převážně bezpečnost dat a informací. Předposlední část se zabývá kybernetickou kriminalitou, jejími aspekty a jejím vymezením v zákoně. Následuje definice kybernetického útoku a typy kybernetických útoků, se kterými je možné se v současné době setkat. Na konci teoretické časti byl definován pojem kryptografie, jenž je jedním z klíčových pojmů při ochraně informačních a kybernetických systémů.

Praktická část této práce byla rozdělena na pět částí. V první kapitole praktické časti jsou popsány konkrétní bezpečnostní opatření, které se při ochraně informačních a kybernetických systému používají. Velká pozornost byla věnována především metodám autentizace, která je jedním z nejdůležitějších prvků při ochraně informačních a kybernetických systémů. V další kapitole jsou uvedeny konkrétní aplikace softwarové ochrany, z nichž za nejdůležitější je považován firewall. V další kapitole je rozebráno v současnosti velmi aktuální téma, kterým je bezpečnost mobilních zařízení. V předposlední kapitole je provedeno modelování kybernetické bezpečnosti. Modelování kybernetické bezpečnosti bylo provedeno na základě dokumentu „Standardy IS VZP – NIS“, jehož část je součástí přílohy této práce. V poslední kapitole jsou uvedeny návrhy pro rozvoj kybernetické bezpečnosti. Zpracování této práce mi zvýšilo znalosti v oboru kybernetické bezpečnosti a rozšířilo povědomí o metodách ochrany informačních a kybernetických systémů.

SEZNAM POUŽITÉ LITERATURY

[1] HRONEK, Jiří. Informační systémy. *Přírodovědecká fakulta, Univerzita Palackého: Katedra informatiky* [online]. Olomouc, 2007 [cit. 2019-05-11]. Dostupné z: https://phoenix.inf.upol.cz/esf/ucebni/infoSys.pdf

[2] Informační systém. *IT-Slovník* [online]. IT-Slovnik.cz team, 2018 [cit. 2019-05-11]. Dostupné z: https://it-slovnik.cz/pojem/informacni-system/?utm_source=cp&utm_medium=link&utm_campaign=cp

[3] Informace. *IT-Slovník* [online]. IT-Slovnik.cz team, 2018 [cit. 2019-05-11]. Dostupné z: https://it-slovnik.cz/pojem/informace/?utm_source=cp&utm_medium=link&utm_campaign=cp

[4] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

[5] ČANDÍK, Marek. *Informační bezpečnost* [online]. Praha, 2011 [cit. 2019-05-11]. Dostupné z: https://moodle.unob.cz/pluginfile.php/15173/mod_resource/content/2/Informační%20bezpečnost.pdf. Policejní akademie ČR.

[6] Kybernetika. *IT-Slovník* [online]. IT-Slovnik.cz team, 2018 [cit. 2019-05-11]. Dostupné z: https://it-slovnik.cz/pojem/kybernetika/?utm_source=cp&utm_medium=link&utm_campaign=cp

[7] Biokybernetika - systém. *Univerzita Palackého* [online]. Olomouc, b.r. [cit. 2019-05-11]. Dostupné z: www.biofyzika.upol.cz/userfiles/file/biokybernetika_1_system.doc

[8] HRŮZA, Petr. *Kybernetická bezpečnost II*. Brno: Univerzita obrany, 2013. ISBN 978-80-7231-931-2.

[9] Systém kybernetický. *Univerzita Komenského v Bratislavě: Katedra aplikované informatiky* [online]. Bratislava: Univerzita Komenského v Bratislavě, 2019 [cit. 2019-05-11]. Dostupné z:

http://dai.fmph.uniba.sk/~filit/fvs/system_kyberneticky.html

[10] *Vlastní tvorba*.

[11] HRŮZA, Petr. *Kybernetická bezpečnost*. Brno: Univerzita obrany, 2012. ISBN 978-80-7231-914-5.

[12] ČESKÁ REPUBLIKA. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Sbírka zákonů. Praha: ČESKO, 2014, roč. 2014, částka 75, číslo 181.

[13] ČESKÁ REPUBLIKA. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů*. Praha: ČESKO, 2005, roč. 2005, částka 143, číslo 412.

[14] HROMADA, Martin, Petr HRŮZA, Josef KADERKA, Oldřich LUŇÁČEK, Miroslav NEČAS, Bohumil PTÁČEK, Leopold SKORUŠA a Richard SLOŽIL. *Kybernetická bezpečnost: teorie a praxe*. Praha: Powerprint, 2015. ISBN 978-80-87994-72-6.

[15] KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

[16] Botnet. *Internetem bezpečně* [online]. Karlovy Vary: Internetem bezpečně, 2018 [cit. 2019-05-11]. Dostupné z: Zdroj: https://www.internetembezpecne.cz/internetem-bezpecne/malware/botnet/

[17] Ransomware. *Internetem bezpečně* [online]. Karlovy Vary, 2018 [cit. 2019-05-11]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/ransomware/

[18] WannaCry. *Avast* [online]. Praha: Avast, 2019 [cit. 2019-05-11]. Dostupné z: https://www.avast.com/cs-cz/c-wannacry

[19] Phishing. *Internetem bezpečně* [online]. Karlovy Vary: Internetem bezpečně, 2018 [cit. 2019-05-11]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/podvodne-praktiky/phishing/

[20] Sniffing. *Computer Hope* [online]. Computer Hope, 2019 [cit. 2019-05-11]. Dostupné

z: https://www.computerhope.com/jargon/s/sniffing.htm

[21] Kybernetický terorismus, kyberterorismus. *Ministerstvo vnitra České republiky* [online]. Praha: Ministerstvo vnitra České republiky, 2019 [cit. 2019-05-11]. Dostupné z: https://www.mvcr.cz/clanek/kyberneticky-terorismus-kyberterorismus.aspx

[22] VÁCLAV, Jírovský. *Zobrazení forem terorismu*. Praha. (prezentace na konferenci – nepublikováno). ICTfórum/PERSONALIS 2006, 2006.

[23] KODL, Jindřich a Vladimír SMEJKAL. *BEZPEČNOST ICT A OCHRANA DAT*. Moravská vysoká škola Olomouc, o. p. s., 2018. Dostupné také z: https://mvso.cz/wp-content/uploads/2018/02/Bezpečnost-ICT-a-ochrana-dat-studijní-text.pdf

[24] Sociální inženýrství. *Národní centrum kybernetické bezpečnosti* [online]. Praha: Národní centrum kybernetické bezpečnosti, 2019 [cit. 2019-05-11]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2486-socialni-inzenyrstvi/

[25] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi: Studijní text*. VŠB TU Ostrava, 2008. Dostupné také z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf

[26] JURÁK, Karel a Zuzana NEJEZCHLEBOVÁ. Karty chytré až biometrické – Terminologie. *DPS* [online]. Liberec: CADware s.r.o., 2017 [cit. 2019-05-11]. Dostupné z: https://www.dps-az.cz/zajimavosti/id:52927/karty-chytre-az-biometricke-terminologie

[27] Host-Based Intrusion Detection System (HIDS). *Techopedia* [online]. Techopedia Inc., 2019 [cit. 2019-05-11]. Dostupné z: https://www.techopedia.com/definition/12826/host-based-intrusion-detection-system-hids

[28] Bezpečnost a zabezpečení: Kódování a hashování. *VŠB-TU: Katedra informatiky* [online]. Ostrava: Technická univerzita Ostrava, 2019 [cit. 2019-05-11]. Dostupné z: http://www.cs.vsb.cz/behalek/vyuka/pcsharp/text/ch09s01.html

[29] Zálohování dat. *SŠ-COPT* [online]. Kroměříž: Střední škola – Centrum odborné přípravy technické Kroměříž, 2019 [cit. 2019-05-11]. Dostupné z:

https://coptkm.cz/portal/reposit.php?action=0&id=21551&revision=-1&instance=5

[30] Antivirový software. *SŠ-COPT* [online]. Kroměříž: Střední škola – Centrum odborné přípravy technické Kroměříž, 2019 [cit. 2019-05-11]. Dostupné z: https://coptkm.cz/portal/reposit.php?action=0&id=40910&revision=-1&instance=1

[31] Antispamová ochrana. *Help.ESET* [online]. ESET, 2019 [cit. 2019-05-11]. Dostupné z: https://help.eset.com/eis/11/cs-CZ/idh_config_smon_main.html

[32] Firewally. *Antivirové centrum* [online]. Nový Jičín: AMENIT s. r. o., 2019 [cit. 2019-05-11]. Dostupné z: https://www.antivirovecentrum.cz/firewally.aspx

[33] Introduction to Firewall. *GeeksforGeeks* [online]. Uttar Pradesh: Geeksforgeeks, 2019 [cit. 2019-05-11]. Dostupné z: https://www.geeksforgeeks.org/introduction-to-firewall/

[34] KUPKA, Michael. Trendy v bezpečnosti mobilních zařízení. *SystemOnLine* [online]. Brno: CCB, spol. s r. o., 2019 [cit. 2019-05-11]. Dostupné z: https://www.systemonline.cz/sprava-it/trendy-v-bezpecnosti-mobilnich-zarizeni.htm

[35] SVOBODA, Ivan. Mobilní zařízení a různé typy útoků a rizik. *Computerworld* [online]. Praha: IDG Czech Republic, a. s., 2019 [cit. 2019-05-11]. Dostupné z: https://computerworld.cz/securityworld/mobilni-zarizeni-a-ruzne-typy-utoku-a-rizik-54001

[36] O nás. *Všeobecná zdravotní pojišťovna České republiky* [online]. Praha: Všeobecná zdravotní pojišťovna České republiky, 2019 [cit. 2019-05-11]. Dostupné z: https://www.vzp.cz/o-nas

[37] VZP ČR, ÚICT. *Standardy IS VZP – NIS*. Praha, 2017. Dostupné také z: https://smlouvy.gov.cz/smlouva/soubor/8939387/Standardy_NIS.pdf

[38] ALBERTS, Christopher a Audrey DOROFEE. *Managing Information Security Risks: The OCTAVE Approach*. 1. vydání. Boston: Addison Wesley Longman Publishing, 2002. ISBN 0-321-11886-3.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

2D	Dvourozměrný.
3D	Trojrozměrný.
BR	Blu-ray.
CD	Compact Disc.
CMOS	Complementary Metal–Oxide–Semiconductor.
CPU	Central Procesing Unit.
ČR	Česká republika.
DDoS	Distributed Denial-of-service Attack.
DoS	Denial-of-service Attack.
DVD	Digital Versatile Disc.
EMM	Enterprise Mobility Management.
HDD	Hard Disk Drive.
HIDS	Host Intrusion Detection System.
ICT	Information and Communication Technologies.
ID	Identity Documentation.
IT	Informační technologie.
KB	Kybernetická bezpečnost.
MDM	Mobile Device Management.
MTD	Mobile Threat Defence.
NAS	Network Attached Storage.
NIDS	Network Intrusion Detection System.
PIN	Personal Identification Number.
RPO	Recovery Point Objective.
RTO	Recovery Time Objective

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: STANDARDY IS VZP - NIS

1. Úvod

STANDARDY IS VZP - NIS

- **Představují -** soubor pravidel určených pro vytváření, rozvoj a využívaní IS VZP ČR.
- **Obsahují -** charakteristiky, metody, postupy a podmínky, zejména pokud jde o bezpečnost a integrovatelnost s jinými informačními komponenty a systémy.
- **Jsou určeny -** pro všechny dodavatele řešení/služeb/komponent jako pravidla dodávek IS/IT a k vývoji aplikací a jejich releasů.
- **Všichni dodavatelé komponent IS do VZP** jsou povinni po akceptaci standardu ho respektovat ve znění, v jakém ho přijali.
- **Od standardu se lze odchýlit pouze na základě výjimky** udělené vlastníkem standardu VZP ČR.
- **Při vydání nové verze standardu dodavatelé jsou vyzváni k přistoupení k nové verzi standardu** pro další dodávky. Pokud není poskytované řešení kompatibilní s novou verzí standardu, požádají VZP o výjimku.
- **Jejich účelem je** nasazení a následné provozování řešení/komponent v rutinním prostředí VZP s požadovanými garancemi, s požadovanými provozními parametry, s požadovanou odbornou aplikační a provozní podporou provozu IT při optimalizaci řešení IT.

Logická infrastruktura

Provoz datového centra je z pohledu toku dat směrem od uživatele k vlastním datům rozdělen do jednotlivých funkčních modulů neboli zón. Rozhodujícím hlediskem pro sledování toku dat je „kdo inicializuje komunikaci".

Zóny představují zpravidla několik L3/L2 segmentů, která mají podobná bezpečnostní pravidla. Zóny jsou IP adresací příslušné k lokalitě DC. Výjimku tvoří zóna DC-DB, ta je L2 geograficky rozprostřena mezi lokalitami DC1 a DC2.

Rozdělení DC zón:

- **Síť VZP ČR (VZP NET)**

Zóna označuje síť VZP, která není součástí DC – tj. infrastrukturní část LAN/WAN včetně části koncových uživatelů.

- **Demilitarizovaná zóna (DC-DMZ)**

Zóna je dostupná z obou stran jak pro VZP, tak pro DC. Slouží k zabezpečení a poskytování služeb. Typicky Management, DNS, MS AD DC nebo LDAP, ACS. Do této zóny patří vrstva správy a administrace a vrstva infrastrukturních serverů.

- **Prezentační vrstva (DC-VIP)**

Jedná se o vrstvu, v které jsou umístěné servery zajišťující komunikaci s uživateli. Patří sem i virtuální IP adresy, které reprezentují jednotlivé aplikace pro přístup jak z VZP NET, tak z ostatních aplikací DC.

- **Aplikační vrstva (DC-APP)**

Zde jsou umístěny aplikační servery zajišťující business logiku jednotlivých aplikací.

- **Databázová vrstva DC (DC-DB)**

Umístění DB serverů. L2 vrstva rozprostřená geograficky mezi lokalitami DC1 a DC2. V databázové vrstvě je možné vytvářet clustery se společnou IP adresou mezi jednotlivými lokalitami.

- **Servisní zóna (DC-SERVIS)**

Zóna slouží jako prostředník pro výměnu dat mezi ostatními zónami a mezi prostředími produkce a test.

Zóny DC-APP a DC-DB nejsou přímo dostupné z VZP NET a obráceně. Komunikace musí být zprostřed-kována přes některou ze zón DC-DMZ, DC-VIP, DC-SERVIS .

Komunikační matice zobrazuje podporované komunikace mezi jednotlivými zónami.

	Komunikace do zóny →					
Komunikace ze zóny ↓	VZP NET	DC-DMZ	DC-VIP	DC-APP	DC-DB	DC-SERVIS
VZP NET	ANO	ANO	ANO	ϴ	ϴ	ANO
DC-DMZ	ANO	ANO	ANO	ANO	ANO	ANO
DC-VIP	ϴ	ϴ	ϴ	ANO	ϴ	ϴ
DC-APP	ϴ	ANO	ANO	ϴ	ANO	ANO
DC-DB	ϴ	ANO	ϴ	možné	možné	ANO
DC-SERVIS	ANO	ANO	ϴ	ANO	ANO	ANO

3.2.6. Perimetr

Perimetr je zabezpečená oblast podnikové sítě, která leží mezi internetem a vnitřní sítí VZP ČR.

Perimetr je rozdělen pomocí bezpečnostních bran (firewallů) do několika oddělených bezpečnostních zón:

- vnější perimetr – bezpečnostní oddělení externích sítí (Internetu) od sítě VZP

- vnitřní perimetr – bezpečnostní oddělení veřejně vystavených služeb VZP od vnitřní (uživatelské) sítě VZP

Součástí řešení je i VPN přístup do VZP ČR. VPN slouží pro vzdálený přístup zaměstnanců a externích kontraktorů do sítě VZP ČR z Internetu.

3.2.7. Síťové služby

Síť VZP ČR poskytuje pro koncová zařízení, aplikace a uživatele následující služby:

- Časová synchronizace (NTP)
- Kvalita služby (QoS)
- DNS, DHCP, IPAM (DDI)
- Loadbalancing

3.2.8. Sjednocená komunikace

Sjednocená komunikace je ve VZP ČR tvořena následujícími součástmi:

- **Hlasová komunikace**
  - IP Telefonie
  - Integrované nadstavbové funkcionality
  - Spolupracující systémy
    - Call Centrum Atlantis
    - Cisco Paging
- **Elektronická komunikace**
  - Instant messaging - Cisco Jabber
  - Webová konference – Cisco WebEx

3.3. OS

V době instalace musí mít všechny implementované verze OS zajištěnu podporu ještě minimálně dalších 5 let.

3.3.1. OS pro aplikace třídy A

- Red Hat Enterpise Linux, Oracle Linux, CentOS (verze 7 a vyšší)
- MS Windows Server 2012R2 EN, 2016 EN

3.3.2. OS pro aplikace třídy B

Red Hat Enterprise Linux, Oracle Linux, CentOS (verze 7 a vyšší)

MS Windows Server 2012R2 EN, 2016 EN

3.3.3. Prostředí pro virtualizaci

Hostitelský systém je hypervizor nebo operační systém s hypervizorem , který umožní provoz Virtuálních serverů. Podporované platformy jsou a ve VZP mohou být nasazeny technologie, VMWare vSphere 5.5 Enterprise a vyšší a MS Hyper-V 2012R2 a vyšší.

Podpora řezů dat	Datový model musí být navržen tak, aby pro účely testování bylo možno oddělit testovací derivát – vzorek dat z produkčních dat. Součástí dodávek je nástroj pro vytváření takových derivátů. Toto musí být zohledněno i v dokumentaci.
Zakázané vazby	Data v relačních databázích nesmí být provazována technologicky přes významové klíče, povolena je relační vazba pouze přes nezávislé technologické klíče záznamů. Nejsou dovoleny přímé datové vazby mezi datovými doménami.

3.6. Koncová zařízení

- Koncová pracovní zařízení počítače a notebooky
  - Instalován OS Windows 7/10 enterprise x64/x32
  - Nastavení OS systému a uživatelského prostředí řízeno centrálně doménovou politikou.
  - Uživatel nemá na koncové zařízení administrátorské práva
  - Vzdálený přístup je zajištěn Remote Desktop, Support Assistant
  - Aktualizace OS v 6 měsíčním cyklu

- Programové vybavení koncových pracovních zařízení
  - MS Office 2010/16 Profesionál plus
  - Google Chrome, nastavení řízené centrální doménovou politikou
  - IE aktuální verze 11, nastavení řízené centrální doménovou politikou
  - 7ZIP
  - Cisco AnyConnect Secure Mobility Client (Notebooky)
  - Adobe Reader 11/DC

- Centrální distribuce programového vybavení na pracovní stanice
  - Distribuce SW je použitím SCCM

- Zabezpečení koncových pracovních zařízení
  - Endpoint Protection , Antivirová ochrana Kaspersky Endpoint Securit (centrálně řízený)
    - AntiMalware, IDS/IPS,
    - Firewall,
    - Application control,
    - Device control,
    - Antispam

- Jednotná adresářová struktura
  - Root:
    APPL
    Archiv
    Data
    Nezalohovano
    Program Files
    Temp
    TMP
    Users
    Windows

- Pro Root, Program Files, Windows má běžný uživatel práva pouze pro čtení

- Ostatní programové vybavení
  - JAVA 1.6.045 ,1.7.51 , 1.8. 111
  - NET Framework ver. 4.0 a vyšší

- Tisková koncová zařízení
  - Tisková a multifunkční zařízení připojená přes tiskový server, výjimečně lokální připojení
  - Follow me printing se zabezpečeným tiskem.
  - Ověřování pomocí bezkontaktních karet
  - (embeded čtečka v MFDnebo externí terminál, možnost ověření PINem).
  - Scan to me (možnost naskenovat z jakékoli MFD a obdržet sken v personální složce nebo emailem).

- Ostatní koncová zřízení
  - Mobilní telefony s OS : Android 5.0 a vyšší, Windows 10 mobile

3.7. Elektronická pošta

- Elektronická pošta ve VZP ČR je realizována prostřednictvím Microsoft Exchange 2010. Příjem elektronické pošty z Internetu zajišťují dedikované SMTP brány v perimetru, před předáním zpráv do interního poštovního systému je provedena jejich antivirová a antispamová kontrola. Odesílání pošty mimo lokální poštovní doménu probíhá pomocí SMTP protokolu s využitím poštovních bran.
- Klientský přístup k poštovnímu systému je zajištěn pomocí MS Outlook verze 2010 nebo 2016, případně prostřednictvím internetového prohlížeče (Outlook Web App). Poštovní systém podporuje kromě SMTP i protokoly POP3 a IMAP.

Poštovní systém je využíván pro strategické řízení firmy, a proto je implementován jako vysoce dostupný.

3.8. Active Directory

VZP ČR využívá pro ověřování uživatelů a pracovních stanic Microsoft Active Directory (dále AD). Služby AD jsou realizovány na serverech s MS Windows Server 2012 R2. V AD má každý uživatel i každá pracovní stanice svůj účet. Účty uživatelů jsou spravovány prostřednictvím Identity Managementu na základě údajů uložených v personálním systému. AD zajišťuje pomocí skupinových politik i nastavení pracovních stanic v souladu s platnými bezpečnostními standardy.

3.9. PKI

VZP ČR využívá systém interních certifikačních autorit (PKI) založený na Microsoft Windows Server 2008 R2. Vystavované certifikáty slouží pro identifikaci pracovních stanic a serverů v interní síti VZP ČR a dále pro podpis a šifrování elektronické pošty a pro vzdálený VPN přístup uživatelů do VZP ČR.

4. Bezpečnostní standardy

4.1. Dodržování legislativních požadavků

V rámci dodávky je požadováno striktní dodržování zejména:

- Zákon o ochraně osobních údajů (zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, v platném znění.)
- Autorský zákon (zákon č. 121/2000 Sb., o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů, v platném znění.)
- Zákon o Kybernetické bezpečnosti (zákon č. 181/2014 Sb. v platném znění)
- NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679

4.2. Dodržování obecných standardů a doporučení

V rámci dodávky/vývoje je doporučeno dodržování obecně platných standardů, zejména:

- RFC
- CIS (Center for Internet Security Benchmark)
- OWASP
- ISO/IEC 2700x *(ISMS)*
- ISO/IEC 12207 *(Systems and software engineering – Software life cycle processes)*
- ISO/IEC 15504 *(Software Process Improvement and Capability Determination (SPICE))*

Výjimky nebo odchylky od uvedených standardů musejí být předem schváleny VZP.

4.3. Minimalizování běžících služeb

Na serverech jsou nainstalovány a běží pouze takové služby, které jsou nezbytné pro korektní běh aplikací nebo správy systému. Ostatní služby musí zůstat vypnuté.

4.4. Nevyhovující služby nebo protokoly

Služby nebo protokoly, které nevyhovují bezpečnostním požadavkům pro přenos či zpracování definované kategorie citlivosti informace nesmí být pro přenos nebo zpracování informace použity.

Nevyhovuje zejména:

- použití nešifrovaných protokolů pro vzdálenou administraci (TELNET, http, atd ...)
- použití nešifrovaných protokolů pro přenos dat (FTP, http, atd ...)
- použití slabých a již nevyhovujících metod šifrování (SSL2, SSL3, SHA1, atd...) (viz. minimální požadavky na šifrování)
- použití služeb se známou zranitelností, která není výrobcem opravena nebo je neopravitelná
- použití služeb bez podpory výrobce (Out Of life)

4.5. Minimální požadavky na šifrovací algoritmy

Obecně kryptografické algoritmy musí vždy splňovat požadavky ZoKB (181/2014) a vyhlášky 316/2014.

Použití konkrétního algoritmu podléhá schválení VZP. Jsou preferovány následující algoritmy:

Advanced Encryption Standard (AES) s využitím délky klíčů 256 bitů, SHA-2, SHA-256

4.6. Mechanismus obrany proti hádání přístupu do systému

Ve všech systémech nebo aplikacích musí být implementována kontrola proti pokusům o uhádnutí uživatelských jmen a hesel (např. prostřednictvím omezeného počtu pokusů o přihlášení a definované doby omezení přístupu do systému či aplikace). V případě několika neoprávněných přístupů musí dojít k automatickému uzamčení postiženého účtu. (Nevztahuje se na systémové účty, které to neumožňují. Např. administrátor u win, nebo je tato funkce z provozních důvodů nežádoucí. U těchto účtů musí být nastaveno velmi silné heslo.) Opětovné odemknutí je v kompetenci Administrátora systému nebo aplikace. Navržený mechanismus musí být navržen tak, aby nedošlo k hromadnému zamykání a tím odepření služby.

4.7. Důvěrnost

4.7.1. Klasifikační schéma informačních/datových aktiv

Pro účely klasifikace informací VZP ČR je stanoveno následující klasifikační schéma informací:

1. **chráněné** informace – informace, jejichž ochrana vyplývá ze zákona, nebo informace vyžadující zvýšenou úroveň ochrany na základě obchodních nebo vnitřních požadavků z hlediska dostupnosti, důvěrnosti nebo integrity,
2. **interní** informace – informace související s běžným provozem VZP ČR a jednotlivých organizačních celků, které nejsou určeny ke zveřejnění a nesmějí být volně přístupné externím subjektům,
3. **veřejné** informace – informace, které nevyžadují žádný zvláštní stupeň ochrany ve vztahu k zachování důvěrnosti, dostupnosti a integrity. Tyto informace mohou být volně zveřejněny i mimo VZP ČR.

4.7.2. Bezpečnost umístění informačních/datových aktiv/souborů

- Úložiště datových aktiv musí umožnit řízení přístupových oprávnění pro jednotlivé uživatele a na jednotlivá aktiva.
- Řízení přístupových oprávnění musí být integrovatelné/napojitelné s/na Active Directory VZP.
- Úložiště musí umožnit auditing operací s jednotlivými aktivy – logování přístupů a operací (File Auditing)
- Úložiště musí logovat neúspěšné pokusy o přístup.
- Úložiště musí podporovat napojení logů na SIEM a Centrální úložiště logů (*viz. Nepopíratelnost - Požadavky na auditing*)
- Úložiště musí umožnit napojení na systémy ochrany proti malware. Nebo jinak zabránit uložení a šíření škodlivého kódu a zajistit možnost pravidelné antivirové kontroly.
- U diskových polí je doporučené/preferované napojení pomocí ICAP nebo RPC.

4.7.3. Bezpečnost přenosu dat

- Pokud jsou chráněné informace přenášeny po síti, musí být během přenosu šifrována. Nebo musí být zajištěno šifrování komunikační linky bez ohledu na přenášená data. Toto neplatí pro komunikace v rámci datového sálu VZP ČR.
- Pokud jsou chráněné informace uloženy na nosičích, ať již pro potřeby přenášení informací či z důvodu zálohy, musí být zašifrována.

- V rámci dokumentace a testování nesmí být použita osobní nebo citlivá data. Taková data musí být anonymizována.
- Anonymizací se rozumí taková úprava, po které nelze údaje vztáhnout k určenému nebo určitelnému subjektu údajů.
- Jakýkoliv privátní klíč uživatele musí být chráněn heslem.
- Privátní klíče musí být spolehlivě zálohovány pro případ jejich ztráty nebo poškození.
- Musí být definovány postupy pro obnovení klíče a postupy instalace nového klíče v případě nedůvěry ve starý aktuální klíč.
- Přenos dat pomocí nosičů (uložení data na nosič) musí být logován a log archivován. Logy musí být předávány do SIEM a Centrálního úložiště logů (*viz. Nepopíratelnost - Požadavky na auditing*).

4.7.4. Popis umístění dat a jejich životní cyklus

- **Data at rest – Data v klidu**
  - K datům v úložišti musí být řízen přístup a musí být zajištěno, že se k nim dostane pouze oprávněná osoba a bude jí umožněno s nimi nakládat jen způsobem, který odpovídá její úrovni prověření.
  - Pokud hrozí, že úložiště může být fyzicky ukradeno, musí být chráněné informace na úložišti šifrovány.
  - Pro případ zničení dat musí být data zálohována a archivována. Média se zálohou musí být umístěna v geograficky vzdálené lokalitě, nebo tak, aby nehrozilo současné zničení medií a zdrojových dat.
  - Zálohovaná data se musí podepisovat nebo vytvářet kontrolní součty.
  - Musí být nastaven proces pro bezpečnou likvidaci již nepotřebných informací, tak aby je nešlo snadno obnovit.

Operace (vytvoření, modifikace, smazání a v případě citlivých dat i čtení) s uloženými daty musí být logovány a log archivován. Logy musí být předávány do SIEM a Centrálního úložiště logů (*viz. Nepopíratelnost - Požadavky na auditing*).

- **Data in motion – Data v pohybu**
  - Během přenosu z/do úložiště musí být data chráněna proti odposlechu (Viz. Bezpečnost přenosu dat.)
  - Je doporučeno jednotlivé zprávy číslovat, aby bylo zřejmé, že dorazily ve správném pořadí nebo že se někdo nepokusil o tzv. replay attack.
  - Jako ochranu před nežádoucí modifikací je možné data podepsat a tím podvrženou nebo pozměněnou zprávu snadno odhalit.
  - Přenos dat z/do úložiště musí být logován a log archivován. Logy musí být předávány do SIEM a Centrálního úložiště logů (viz. Nepopíratelnost - Požadavky na auditing).

- **Data in use – Data v použití**
  - Přístup k datům musí být řízen na základě přidělených oprávnění.
  - Aktivity uživatele v systému musí být auditovány/logovány. Logy musí být předávány do SIEM a Centrálního úložiště logů (viz. Nepopíratelnost - Požadavky na auditing).
  - V případě přístupu k osobním údajům musí logy odpovídat požadavkům zákona č. 101/2000 a „NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679“

5. Provozní standardy

5.1. Monitoring

5.1.1. Rozsah monitoringu

Služba dohledu provozu informačního systému je centralizovaná a je zajišťována dohledovým centrem s dvousměnným provozem v pracovních dnech od 6:00 do 22:00 hod. (v režimu 5x16). V těchto časových úsecích jsou drženy pohotovosti řešitelských skupin pro síťovou infrastrukturu, operační systémy Unix, operační systémy Windows, Oracle infrastrukturu (databáze a middleware), provoz aplikací, Exchange, a pro dohledové nástroje.

Z hlediska teorie spolehlivosti IT systémů a služeb jsou sledovány a vyhodnocovány:

- chybovost, resp. dostupnost systémů a služeb (Availability) a jejich vytížení (Utilization),
- výkonnost služeb (Performance).

Z technicko-provozního hlediska je monitoring provozován ve dvou hlavních úrovních – infrastrukturní a aplikační.

- Infrastrukturní monitoring pokrývá všechny prvky produkční IT infrastruktury ZIS od síťových prvků přes servery, databáze až po middleware. Je vyhodnocována dostupnost, resp. chybovost, jakož i vytíženost sledovaných prvků.
- Aplikační monitoring je zaměřen na sledování klíčových služeb produkčních aplikací. Probíhá aktivně pravidelným spouštěním aplikačních úloh, simulujícím uživatelské akce. Zároveň jsou pasivně vyhodnocovány vybrané úlohy reálných uživatelů. Je vyhodnocována dostupnost úloh a služeb, a současně jsou zaznamenávány a vyhodnocovány odezvy takto měřených transakcí, tedy výkonost aplikací. Výstupy pasivního monitoringu jsou využitelné pro sledování vytíženosti sledovaných oblastí.

5.1.2. Používané dohledové nástroje pro On premise řešení

Centrální systém dohledu provozu informačního systému je vybudován na platformě **HP Operations Manager** (HP OM). Do dohledového centra HP OM (centrální konzole) jsou soustřeďovány všechny důležité zprávy z ostatních monitorovacích nástrojů.

- **HP OM** – agent na úrovni OS, centrální konzole
- **HP OM Performance Manager (PM)** – sledování vytíženosti systémů
- **Oracle Enterprise Manager Cloud Control (OEM)** – agent, integrace vybraných událostí do HP OM
- **Microsoft System Center 2012 Operations Manager (SCOM)** – agent na úrovni OS, integrace vybraných událostí do HP OM
- **Nagios** – bezagentní, s integrací vybraných zpráv do HP OM
- **HP Business Service Management (HP BSM)** – integrace do HP OM
  - **Business Process Monitor (BPM)** – aktivní aplikační monitoring
  - **Real User Monitoru (RUM)** – pasivní aplikační monitoring
- **HP Network Node Manager i (HP NNMi)** – aktivní SNMP poll, pasivní SNMP trap, je integrován s HP OM
- **HP SiteScope** – bezagentní, integrace do HP OM a HP BSM

Není-li možné nasadit monitoring pomocí zavedených nástrojů, poskytne dodavatel v rámci dodávky aplikace monitorovací nástroj (například skript), jehož výstup lze integrovat do HP OM.

- datum a čas ve formátu '%Y.%m.%d %H:%M:%S'
- severity události podle výsledku operace: Critical, Major, Minor, Warning, Normal
  - Critical při fatální chybě, např. nemožnosti spustit operaci, kdy je nutný zásah v co nejkratší době;
  - Major při neúspěšném celkovém výsledku operace, např. neúspěchu posledního z pokusů o přenos, kdy je nutný zásah, např. manuální zpracování;
  - Minor při neúspěchu běhu operace, který bude opakován nebo jiné dílčí chybě, která nemusí znamenat neúspěch celé akce, a kdy je žádoucí kontrola průběhu
  - Warning při zjištění problémů u operace s úspěšným výsledkem nebo jiná upozornění, která vyžadují příležitostné prověření
  - Normal při úspěšném dokončení operace bez výhrad
- proces, ke kterému se vztahuje událost, nepovinné
- objekt, který je zdrojem zprávy (např. program, název certifikátu, apod.), nepovinné
- text zprávy, obsahující popis události a případné chyby

5.2. Zálohování a archivace

Všechna DC jsou zálohována jedním společným zálohovacím subsystémem (dále jen ZS).

5.2.1. Zálohovací systém

ZS je tvořen těmito komponentami:

- Řídící SW „Data Protector".
- Cluster dvou serverů v oddělených lokalitách, na nichž je řídící SW provozován.
- HW pro ukládání zálohovaných dat, umístěný rovněž ve dvou různých lokalitách (DC), dostupný pomocí LAN a SAN infrastruktury. Jsou používány robotické páskové knihovny, které mohou být v případě potřeby doplněny o jiný HW (např. typu B2D), připojitelný pod řídící zálohovací software

Zálohování probíhá tak, aby byla respektována bezpečnostní zásada „3-2-1" (tj. „důležitá data musí existovat 3x, ve 2 různých datových formátech, 1 kopie ve druhé lokalitě") dle příslušné třídy aplikace.

5.2.2. Požadavky na aplikační celky z pohledu jejich zálohování:

Aplikace musí být navržena tak, aby:

- SW a HW komponenty aplikačních celků byly zálohovatelné technologiemi, které má VZP ČR v době nasazení aplikace a během jejího provozování k dispozici, v souladu s bezpečnostními standardy VZP ČR. Zálohovatelné musí být všechny SW komponenty a datové objekty potřebné pro činnost aplikace, a to s ohledem na předpokládané datové objemy, případné odstávky, propustnost potřebné infrastruktury a dobu potřebnou pro provedení záloh. Součástí dodávky aplikace musí být i analýza vývoje předpokládaných zálohovaných datových objemů.
- Umožňovala a podporovala datové odklady na jiná úložiště nebo zálohovací média. Musí tedy umět připravit data určená k odkladu/archivaci (např. umístit je do dohodnuté lokace, vhodně je pojmenovat, ...) a vést o nich potřebnou evidenci po provedení odkladu. Musí