Kybernetická bezpečnost v kontextu internetu věcí

Bc. Michael Kozubek

Diplomová práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Michael Kozubek**
Osobní číslo:	**L21274**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Kybernetická bezpečnost v kontextu internetu věcí**

Zásady pro vypracování

1. Proveďte rešerši současného stavu kybernetické bezpečnosti v kontextu internetu věcí.
2. Analýzujte současný stav řešené problematiky ve vybrané oblasti.
3. Vypracujte systémový model útoku na vybraný prvek internetu věcí.
4. Návrhněte opatření ke zlepšení stavu kybernetické bezpečnosti v dané oblasti.

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

Seznam doporučené literatury:

1. EVANS, Lester. *Cybersecurity: What You Need to Know About Computer and Cyber Security, Social Engineering, the Internet of Things + An Essential Guide to Ethical Hackings for Beginners.* Bravex Publications, 2019. ISBN 978-1647481742.
2. GUPTA, Aditya. *The Iot Hacker´s Handbook: A Practical Guide to Hacking the Internet of Things.* Apress, Berkeley, CA, 2019. ISBN 978-1-4842-42995.
3. SERPANOS, Dimitrios a Marilyn WOLF. *Internet-of-Things (IOT) Systems: Architectures, Algorithms, Methodologies.* Springer International Publishing, 2018. ISBN 978-3-319-69714-7.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **1. prosince 2022**
Termín odevzdání diplomové práce: **28. dubna 2023**

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2022

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji diplomovou 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 Univerzita Tomáše Bati 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 – diplomovou 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 diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové 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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 28. dubna 2023

Jméno a příjmení studenta: Bc. Michael Kozubek

.....
podpis studenta

ABSTRAKT

Diplomová práce řeší problematiku kybernetické bezpečnosti internetu věcí. V teoretické části je provedena rešerše současného stavu kybernetické bezpečnosti a legislativy v ČR a ve světě. Vysvětluje problematiku informační a kybernetické bezpečnosti a teorii internetu věcí. V praktické části se zabývá identifikací rizik vybraného prvku internetu věcí, a to chytré kamery. Analyzuje rizika, jejich identifikace zpracovává za pomocí Ishikawa diagramu a hodnotí rizika metodou PHN. Vypracovává systémový model kybernetické bezpečnosti za pomocí penetračního testování chytré kamery, a na zjištěné zranitelnosti a rizika navrhuje ošetření rizik pro zlepšení stavu vybrané oblasti.

Klíčová slova: internet věcí, IP kamery, kybernetická bezpečnost, Penetrační testování (počítačová bezpečnost)

ABSTRACT

The diploma thesis deals with cyber security issues of the Internet of Things. In the theoretical part, research is carried out on the current state of cyber security and legislation in the Czech Republic and in the world. It explains the issues of information and cyber security and the theory of the Internet of Things. In the practical part, it deals with identifying the risks of a selected element of the Internet of Things, namely a smart camera. Analyzes risks, processes their identification using the Ishikawa diagram and evaluates risks using the "PHN" method. It develops a system model of cyber security with the help of penetration testing of a smart camera and, based on the detected vulnerabilities and risks, proposes risk treatment to improve the state of the selected area.

Keywords: cyber security, Internet of thinks, IP cameras, penetration tests (computer security)

Rád bych poděkoval své rodině za podporu při studiu, zejména mé ženě Evě, za trpělivost a oporu při studiu. V neposlední řadě bych rád poděkoval mému vedoucímu práce, panu Ing. Petru Svobodovi, Ph.D. za rady a vedení při vypracovávání této diplomové práce.

Motto: *Per aspera ad astra (lat.).*

Seneca

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

OBSAH

ÚVOD

V dnešním světě je digitální existence stejně důležitá jako fyzická. Toto je potvrzeno faktem, že každý člověk, organizace, firma nebo stát má kromě fyzické podoby i svůj digitální obraz, ve formě různých odvětví propojených do internetu. Internet jako takový, propojuje všechny tyto lidi, organizace, firmy a státy. V současné době jsou však ve velkém připojovány i běžné věci, jako jsou naše auta, lednice, lampy, celé domácnosti, města a průmysl. Vznikl a rozvíjí se pojem internetu věcí. Dnes se každé zařízení může stát počítačem a každý počítač se může stát obětí kybernetického útoku. Z toho tedy plyne, že vše může být dnes tzv. "hacknuto". Česká republika má ve své legislativní úpravě zákony a vyhlášky, které spolu s mezinárodními směrnicemi tvoři právní podklad kybernetické bezpečnosti. V době vypracování této diplomové práce je již zpracováván nový kybernetický zákon. Ten jako národní implementace směrnice Evropské unie NIS2, bude nadále zvyšovat nároky na zajištění kybernetické bezpečnosti u vybraných odvětví, ve kterých jsou tyto prvky internetu věcí. Oblast internetu věcí se rozvíjí velmi dynamicky. Ještě před několika lety nebylo u těchto prvků internetu věcí zamýšleno s tak komplexním ošetřením před kybernetickými útoky, jako dnes. V současné době je na výrobce vyvíjen velký tlak na cenu a dostupnost. To vede k otázce, zda je prvek internetu věcí zároveň dostatečně zabezpečen proti hrozbě kybernetických útoků současnosti. Jedním z těchto prvku internetu věcí, je v dnešní době stále oblíbenější rozřešení použití IP kamer a není výjimkou jejich instalace svépomocí v malých firmách, provozovnách a domácnostech. Tato praxe však klade požadavky na zajištění zmíněné kybernetické bezpečnosti. Tyto dostupnější levné kamerové systémy, které tyto subjekty často volí, a kde je kladen požadavek na nízkou cenu, jsou spojeny s přirozenou nedůvěrou k dodržení všech standardů kybernetické bezpečnosti. Proto bylo vybráno zařízení chytré kamery s ohledem na dostupnost a nízkou cenu zařízení, kde je předpoklad, že bude hrozit vyšší míra rizika kybernetického útoku. Zjištěné informace z návrhové části diplomové práce mohou sloužit jako návod pro zvýšení kybernetické bezpečnosti u těchto zařízení.

CÍLE PRÁCE A POUŽITÉ METODY

Tato kapitola popisuje hlavní a dílčí cíle práce, použité metody, které byly použity k jejímu naplnění a omezení práce.

Cíle práce

Hlavním cílem při zpracování této diplomové práce bylo zvýšit úroveň kybernetické bezpečnosti chytré kamery, jakožto vybraného prvku internetu věcí, při modelové instalaci u rodinného domu.

K dosažení tohoto hlavního cíle byly vypracovány dílčí cíle. Ty mají přispět k lepšímu porozumění problematiky kybernetické bezpečnosti internetu věcí. Byla provedena rešerše současného stavu kybernetické bezpečnosti internetu věcí a stavu současné legislativy v dané oblasti. Dále byla zpracovaná analýza kybernetických útoků na prvky internetu věcí. Byla provedena identifikace a hodnocení možných hrozeb kybernetického útoku na chytré kamery. A byl sestaven systémový model možného kybernetického útoku na chytrou kameru, provedením penetračního testu na tuto kameru.

Použité metody

K dosažení výše uvedených cílů byly v diplomové práci použity tyto metody:

- **Literární rešerše** – Ta se zaměřila na dvě části, a to na národní a mezinárodní část norem, zákonů, směrnic a důležitých dokumentů.
- **Popis** – Tato metoda popisuje informační a kybernetickou bezpečnost a všechny její součásti. Popsány byly také teoretické znalosti potřebné pro vstup do problematiky internetu věcí.
- **Definice –** V praktické části byl definován prvek internetu věcí, a to chytrá kamera. Byl definován objekt chytré kamery jako systém, jeho vlastnosti, souvislosti a vztahy.
- **Komparace** – Popisuje jednotlivé rozdíly ve složitosti systému chytrých kamer.
- **Analýza** – Byly analyzovány kybernetické útoky, internetové zdroje a publikace věnující se etickému hackingu.
- **Indukce** – Ta byla použita pro sestavení penetračního testu na zařízení chytré kamery.

- **Dedukce** – Touto metodou byl předpoklad nalezení zranitelností, s ohledem na typ zařízení chytré kamery, u které se předpokládal nižší požadavek na kybernetickou bezpečnost.
- **Syntéza** – V závěrečné kapitole byly ošetřeny nejvýznamnější hrozby v modelovém nasazení chytré kamery.

Omezení práce

V praktické části se práce zaměřuje na IoT zařízení chytrou kameru, z hodnocených rizik budou v návrhové části pro modelové zapojení kamery ošetřeny jen nejvýznamnější rizika, a to z důvodu rozsáhlé oblasti kybernetické bezpečnosti IoT. Provedený penetrační test nebude zahrnovat přímou fázi útoku na zařízení, ale bude jen výčtem zjištěných zranitelností. Také nebude tato práce obsahovat penetrační test na aplikaci mobilního telefonu, a to z důvodu dodržení legislativy.

I. TEORETICKÁ ČÁST

1 LITERÁRNÍ REŠERŠE SOUČASNÉHO STAVU KYBERNETICKÉ BEZPEČNOSTI V KONTEXTU INTERNETU VĚCÍ

V této první části je zpracována rešerše současného stavu řešení problematiky kybernetické bezpečnosti internetu věcí. Protože činnost státu jako garanta bezpečnosti ČR, podle článku 2. ústavního *zákona č. 110/1998 Sb., o bezpečnosti České republiky,* musí se stát věnovat ochraně informační infrastruktury, kdy narušení této funkce státu by mělo závažný dopad na bezpečnost státu a zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu. Tato kapitola se zaměřuje na obecné legislativní dokumenty České republiky (dále jen ČR) v kontextu internetu věcí (z anglického Internet of Things, nebo také IoT). A na světové a evropské normy, které se prolínají s normami a legislativou v ČR, jakožto nedílnou součástí Evropského společenství (Česko, 1998).

1.1 Kybernetické bezpečnost v České republice a internet věcí

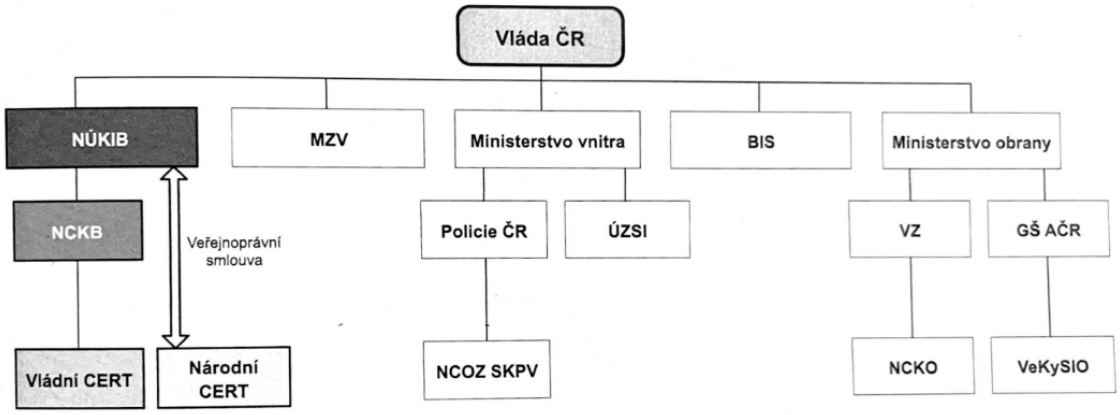
Česká republika jako jedna z prvních zemí v Evropské unii, měla ve své legislativě zákon o kybernetické bezpečnosti od roku 2014 (Česko, 2014). V této kapitole bude shrnut a s ním druhý důležitý dokument, a to vyhláška o kybernetické bezpečnosti a jejich vliv na bezpečnostní prostředí. Dále zde bude věnována pozornost na zákony, které se dotýkají oblasti kybernetické bezpečnosti. Závěr kapitoly se zaměřuje na aktuální Národní strategii kybernetické bezpečnosti ČR na období 2021 až 2025, Akční plán k této strategii a Zprávu o stavu kybernetické bezpečnosti za rok 2021.

Zákon o kybernetické bezpečnosti

Jak bylo uvedeno, problematiku kybernetické bezpečnosti v ČR řeší *zákon č.181/2014 sb., o kybernetické bezpečnosti a o změně souvisejících zákonů* (dále jen zákon o kybernetické bezpečnosti). Tento právní předpis, který stanovuje povinnosti pro subjekty v oblasti kybernetické bezpečnosti, se dělí na organizační opatření, technické opatření a bezpečnostní dokumentace. Zákon může stanovit povinnosti pro poskytovatele kritické infrastruktury, jako jsou energetické sítě, důležité dopravní systémy nebo zdravotnické zařízení, aby zajistili odpovídající úroveň ochrany svých systému před kybernetickými hrozbami. Zákon také stanovuje povinnosti pro organizace, jako jsou velké banky či společnosti, aby zajistily ochranu informaci (Česko, 2014).

Zákon se několikrát novelizoval, zejména novelizace z 1. srpna 2017 kdy nabyla účinnost tato novelizace zákona č.205/2017 Sb., jako reakce na evropskou směrnici NIS a kdy byl

zřízen Národní úřad pro kybernetickou a informační bezpečnost (dále jen NÚKIB). (Sedlák a Konečný, 2021). NÚKIB se zařadil přímo do struktury ČR jako samostatný úřad. Neboť do té doby se jednalo o podřízený úřad pod Národním bezpečnostním úřadem. Schéma zakotvení do struktur\y ČR je vyobrazeno na obrázku č. 1.



Obrázek 1 – Ukotvení NÚKIB v struktuře úřadů ČR. (Sedlák, Konečný, 2021)

Hlavním cílem vzniku zákona bylo vytvořit právní postavení státní instituce, jakožto vymahatele státní moci. Smyslem zákona je tedy stanovení základních bezpečnostních opatření níže uvedených subjektů, zlepšení detekce a hlášení kybernetických incidentů a zavedení opatření k reakci na bezpečnostní incidenty (Sedlák a Konečný, 2021).

V současné době podléhají tomuto zákonu tyto subjekty v ČR (NÚKIB, 2023):

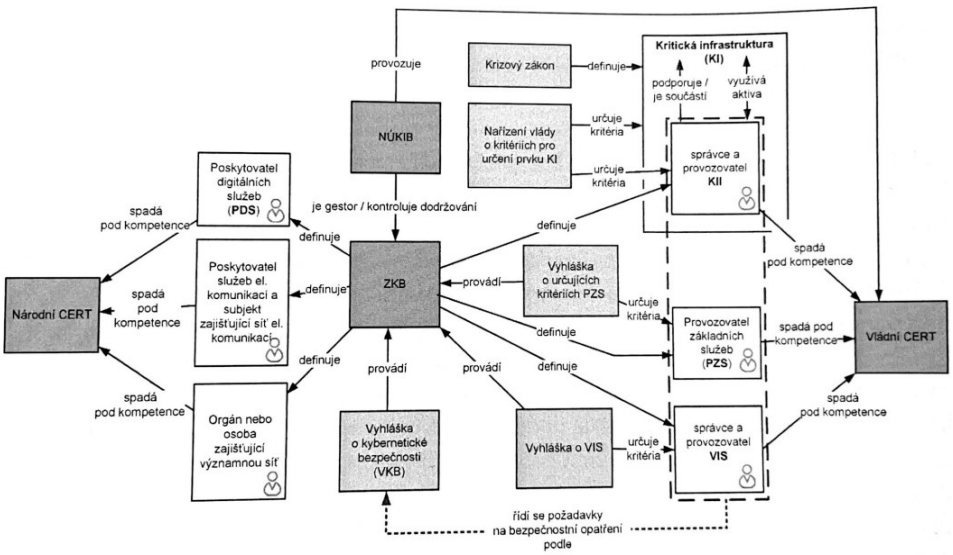
- **Poskytovatelé služeb elektronických komunikací a subjekty zajišťující síť elektronických komunikací.** Jako jsou poskytovatelé telekomunikačních služeb, radiové, optické, družicové služby a další. Dále orgán či osoba zajišťující významnou síť.
- **Kritická informační infrastruktura** (dále jen KII). Mezi ní patří systémy, jejichž poškození, či narušení služeb může mít za následek přímou škodu na majetku nebo zdraví, hospodářská ztráta, ušlý zisk. Ne všechny systémy zde patří, jejich výběr je určen procesem schvalování a stanovují se průřezová kritéria. Jako příklad je limit 250 mrtvých nebo 2500 zraněných, hospodářské ztráty větší než 0,5 % HDP a omezení služeb, či zásah do života více než 125 000 osob.

- **Významné informační systémy** (dále jen VIS). Tyto systémy nejsou zařazeny mezi kritickou informační infrastrukturu, ale jejich narušení by mělo za následek ohrožení, či omezení výkonu orgánu veřejné moci.
- **Poskytovatelé základních služeb**. Služby, jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností, a to v odvětvích jako: OBJ

    1. Doprava
    2. Bankovnictví
    3. Infrastruktura finančních trhů
    4. Zdravotnictví
    5. Vodní hospodářství
    6. Digitální infrastruktura
    7. Chemický průmysl

- **Poskytovatelé základních služeb**. Těmto službám podle zákona o kybernetické bezpečnosti rozumíme on-line tržiště, internetové vyhledávače a poskytovatele Cloud Computingu.

Na obrázku 2. jsou vyobrazeny vazby zákona o kybernetické bezpečnosti na povinné subjekty a jiné předpisy.



Obrázek 2 – Provázanost zákon o kybernetické bezpečnosti (Sedlák a Konečný, 2021)

V současné době také začíná NÚKIB vypracovávat nový zákon o kybernetické bezpečnosti, který bude harmonizovat požadavky nové směrnice Evropského parlamentu a Rady EU, směrnice NIS2.

„Zákon neřeší bezpečnost informačních systému podléhajících stupeň utajení. Tyto systémy řeší zákon č. 412/2005 Sb. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti.“ (Kozubek, 2018).

Vyhláška o kybernetické bezpečnosti

Tato *vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidace dat (vyhláška o kybernetické bezpečnosti)* obsahuje zejména požadavky na organizační a technická opatření, které musí povinné subjekty podle ZKB implementovat. Toto obsahuje zejména (Česko, 2018):

- Obsah a strukturu bezpečnostní dokumentace subjektu.
- Obsah a rozsah bezpečnostních opatření subjektu.
- Typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů.
- Náležitosti a způsob hlášení kybernetického bezpečnostního incidentu.
- Náležitosti oznámení o provedení reaktivního opatření a jeho výsledku u subjektu.
- Vzor oznámení kontaktních údajů a jeho formu.
- Způsob likvidace dat, provozních údajů, informací a jejich kopií.

Vyhláška se kontextu IoT dotýká definicí aktiv, řízení provozu a komunikací, řízením kontinuity činností a z technických opatření je to řízení uživatele, kryptografické požadavky, bezpečnost průmyslových a řídících systému.

Krizový zákon

Zákon č.240/200 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) stanovuje pravomoci a působnosti veřejných institucí a práva a povinnosti právnických a fyzických osob při řešení krizových situací. Ve vztahu na kybernetickou bezpečnost řeší ochranu kritické infrastruktury a ve vztahu na *Nařízení vlády č.432/2010 Sb., o kritériích pro určení prvků kritické infrastruktury*, definuje kritéria v odvětví Komunikačních a

informačních systémů, oblast kybernetické bezpečnost. Při splnění se jedná o kritickou informační infrastrukturu (Sedlák, Konečný, 2021).

Národní strategie kybernetické bezpečnosti České republiky na období let 2021–2025

Strategie jako taková je prostředek státu, který zajišťuje kybernetickou bezpečnost státu. Aktuální znění zpracovává NÚKIB a přináší tři nové vize (Národní strategie kybernetické bezpečnosti České republiky na období let 2021–2025, 2020):

- **Sebevědomě v kyberprostoru** – Je kladen důraz na zajišťování kybernetické bezpečnosti v ČR. Hlavní body jsou společný přístup ke kybernetické bezpečnosti, bezpečná infrastruktura, účinná strategická komunikace, sebevědomá reakce a budoucí výzvy.
- **Silná a spolehlivá spojenectví** – Zde je směřován směr na mezinárodní spolupráci, posílení jednotné bezpečnosti a obranyschopnosti. Nacházení efektivní mezinárodní spolupráce, prohlubování těchto spojenectví, mezinárodní právní rámec a předávání schopností a expertíz.
- **Odolná společnost 4.0** – Lze toto definovat jako společnost, která naplno využívá výhody moderních technologií s minimalizací kybernetických rizik, jako je digitální společnost a státní správa. Vzdělávání společnosti s dodržování digitální hygieny, jakožto souboru zásad a návyků, které uživatele těchto služeb chrání při jejich využitím a uživatelé aktivně přistupují při vlastní ochraně v digitálním prostředí.

Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025

K úspěšnému naplnění a dosažení hlavních cílů Národní strategie kybernetické bezpečnosti České republiky na období 2021 až 2025 je zapotřebí postupovat dle stanoveného časového rámce. Akční plán vymezuje odpovědné subjekty, zodpovědné za plnění stanovených úkolů. Ty jsou za toto plnění právně odpovědné. Zároveň je definována role a působnost těchto subjektů veřejné správy ČR (Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025, 2021).

Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021

Tato každoročně vydávaná zpráva o stavu kybernetické bezpečnosti je shrnutím událostí a vývoje kybernetických útoků, které má ve své gesci NÚKIB. V úvodním slovu ředitele je zmíněna skutečnost, že za tento rok byla kybernetická bezpečnost poznamenána

celosvětovou pandemii a jejímu vlivu na zvýšenou potřebu komunikace přes internet v rámci práce z domova a distančního vzdělávání. Mezi nejvážnější hrozby za rok 2021 byly zaznamenány hrozby typu ransomware a phishing. Významu těchto útoku se bude tato práce věnovat v následujících kapitolách. Nejčastějším cílem útoků byly prvky kritické infomační infrastruktury. Nejvýznamnějších faktorem (přes 70 %) byl podíl incidentu na nedostupnost těchto KII (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021, 2022).

1.2 Evropské a mezinárodní normy řešení kybernetické bezpečnosti v kontextu internetu věcí

V rámci Evropské unie se jedná o tři základní milníky, které za poslední roky formovaly evropské pojetí kybernetické bezpečnosti. A to je *Nařízení Evropského parlamentu a Rady (EU) 216/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zapracováním osobních údajů a volnému pohybu těchto údajů a o zrušení směrnice 95/46/ES* (Obecněji nazvané **GDPR**) (EU, 2016a), dále *Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o ochraně fyzických osob v souvislosti se zajištěním společné úrovně bezpečnosti sítí a informačních systému v Unii* (Obecněji nazývané **Směrnice NIS**) (EU, 2016b)a *Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA, o certifikaci kybernetické bezpečnosti informačních a komunikačních technologii a o zrušení nařízení (EU) č. 526/2013* (Obecněji **Akt o kybernetické bezpečnosti**) (EU, 2019). V těchto dokumentech je uvedeno několik ukazatelů, které formulují myšlenku, že při rozvíjejícím se kyberprostoru nebylo na některé věci pamatováno. Vyjmenovávají hlavní problematické oblasti, a to jednotlivé síťové infrastruktury, normy přenosu a jejich zabezpečení. Aplikace na internetu nebyly původně také nijak zabezpečeny. S příchodem IoT se také nepočítalo a už vůbec ne jeho rozšíření do průmyslového prostředí, zvaného Industrial Internet of Thinks (Sedlák a Konečný, 2021).

Koncem roku 2020 byl na evropské úrovni vydán takzvaný Balíček opatření v oblasti kybernetické bezpečnosti. Především byla představena nová **Strategie kybernetické bezpečnosti EU na období 2020 až 2025**. Ta má za úkol posílit kolektivní bezpečnost Evropy proti kybernetickým hrozbám, a to formováním digitální budoucnosti Evropy, plánu na podporu oživení Evropy a strategie bezpečnosti EU, aby se dalo těžit z výhod spolehlivých digitálních služeb a nástrojů. Tvoří ji tyto pilíře (Sedlák a Konečný, 2021).

- Bezpečnost prostředí, které obstojí i v budoucnu, například Ochrana a KB kritické energetické infrastruktury, ochrana KII.
- Potírání vyvíjejících se hrozeb, například přístup EU k hybridním hrozbám.
- Ochrana Evropanů před terorismem a organizovanou trestnou činností
- Silný evropský bezpečnostní ekosystém.

Směrnice NIS

Tato Evropská direktiva cílí na informační a komunikační technologie (dále jen ICT) států EU. Tato směrnice nemá direktivní účinek a státy EU ji zapracovaly do svých právních úprav. V ČR již plnil některé funkce zákon o kybernetické bezpečnosti, a proto byl pouze novelizován zákonem č. 205/2017. Tím došlo k harmonizaci legislativy a novelizace kybernetického zákona. Tato novelizace dala vzniknout vládnímu a národnímu CSIRT teamů a mimo jiné rozšířila seznam subjektů s povinnosti k plnění ZKB o provozovatele základních služeb a poskytovatele digitálních služeb (EU, 2016 a).

Směrnice NIS2

Koncem roku 2022 došlo k publikaci připravované nové směrnice o kybernetické bezpečnosti – *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (***směrnice NIS 2***)*. Dne 16. ledna 2023 vešla v platnost a začala běžet lhůta 21 měsíců k tomu, aby členské státy Evropské unie zapracovaly tuto novelizaci do svých zákonů a legislativy. Protože změn v směrnici NIS2 je relativně hodně, začal od ledna 2023 NÚKIB jakožto garant legislativního rámce v ČR, pracovat na novém zákonu o kybernetické bezpečnosti. Hotovou a harmonizovanou legislativu by státy EU měly mít k 16. říjnu 2024. Nejpodstatnější jsou změny v rozsahu povinností subjektů, které budou spadat do okruhu pro tento nový zákon o KB. Jako příklad jsou energetické společnosti, nemocnice, výzkumné organizace, samospráva státu na úrovní obcí s rozšířenou působností, vysoké školy, výrobní podniky a další. U výrobních podniků nespadají všechny subjekty v odvětví. Rozhodující bude velikost, kdy se toto týká velkých a středních podniků, a navíc strategického hlediska zájmu státu. NÚKIB již nebude určovat subjekty podléhající nové úpravě ZKB. Toto budou mít na starosti přímo konkrétní subjekty podle procesu

určování, zda do vybrané skupiny patří nebo ne. Celkově je odhad subjektů, kterých se změny budou týkat asi 6000 (EU, 2022). Směrnice nově definuje tzv. *Important Entities* (důležité entity), které budou plně muset plnit požadavky NIS2 a ZKB. Pod tyto budou zařazeny (Sedlák a Konečný, 2021).

- Poštovní a kurýrní služby
- Odpadové hospodářství
- Výroba, produkce a distribuce chemikálii
- Výroba a zpravování a distribuce potravin
- Výroba zdravotnických zařízení
- Výroba počítačů a elektroniky
- Výroba strojů
- Výroba vozidel, přívěsů a vybavení k dopravě
- Poskytování digitálních služeb (online tržiště, internetové vyhledávače a nově i poskytovatele sociálních sítí)

V případě pochybení ze strany subjektu, nedodržení zákona a nedostatečné kybernetické bezpečnosti, se zpřísňují sankce podle směrnice NIS2.

Agentura ENISA a její normy pro IoT

Agentura ENISA (European Union Network and Information Security Agency) je od roku 2004 agenturou zřízenou Evropskou unii k zabezpečování kybernetické bezpečnosti pro EU. Původně vznikla k přípravě Evropské směrnice NIS. Dnes zastává roli spolupráce mezi státy EU ve věci poskytování doporučení, tvorbu národních politik, koordinace vzdělání informovanosti, školení mezi státy EU a soukromými subjekty. Nedílnou součástí je i celoevropský tým CSIRT a standardizace a certifikace.

Pro IoT vydává agentura ENISA několik doporučení jako například ***Baseline Security Recommendation for IoT in the context of Critical Information Infrastructures.*** Zde uvádí základní postupy a doporučení pro zařízení IoT. (ENISA, 2017)

Řada norem ISMS (Information Security Management System) – normy Systému řízení bezpečnosti informací a IoT

Tato sada norem má pomoci organizacím a subjektům všech velikostí se zavedením a provozováním řízení bezpečností informací. Definuje požadavky na řízení bezpečnosti informací, které požaduje po firmě či subjektu, aby s veškerými informacemi nakládala tak aby nedošlo k jejich ztrátě, zneužití, či narušení důvěry (SYSTÉM A ROZSAH ISMS, 2021).

Pro IoT jsou to zejména normy ***ISO/IEC CD 27400 – Cybersecurity – IoT security and privacy – Guidelines, ISO/IEC CD 27402 – Cybersecurity – IoT security and privacy – Device baselines requirements a ISO/IEC CD 27403 Information technology – Security techniques – Guidelines for IoT – domotics security and privacy*** (Sedlák a Konečný, 2021, s. 26).

Normy NIST

Institut NIST - National Institute of Standards and Technology, v překladu Národní institut standardů a technologie USA, je americký institut, který vydává normy a obecně slouží k podpoře subjektu při implementaci a nasazení pro kybernetickou bezpečnost (Sedlák a Konečný, 2021 s. 27)

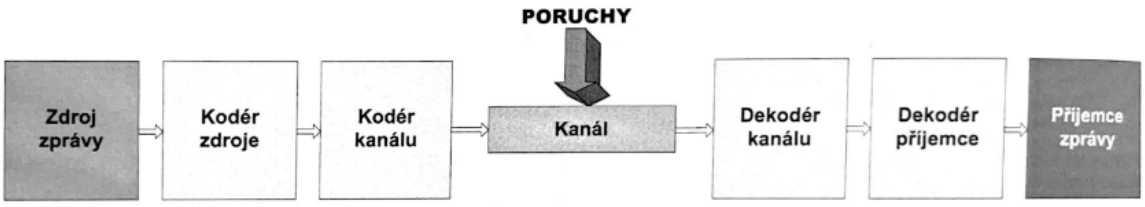
Z norem NIST, zabývajících se IoT, uvádíme tyto: ***NISTIR 8200 Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT),*** a normu pro domácí použití IoT: ***NISTIR 8267 Security Review Of Consumer Home IoT Products.***

2 INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOSTI

V současné době je pojem kybernetické bezpečnosti spojován nejčastěji s internetovou kriminalitou. To však z pojetí oblasti je jen pomyslná špička ledovce. Kybernetickou bezpečnost můžeme chápat dvěma pohledy. Prvním, který vychází z normy ČSN ISO/IEC 27032), že kybernetická bezpečnost je pevnou součástí informační bezpečnosti a navzájem se prolínají. A druhým je pohled na celé topografické vnímáni toho, že informační bezpečnost je omezena na jeden subjekt, ale kybernetická bezpečnost se potkává i mimo perimetr subjektu a prolíná se s globálním kyberprostorem internetu. (Sedlák a Konečný, 2021 s. 57). Tak či onak je potřeba komplexního pohledu na problematiku kybernetické bezpečnosti. V této kapitole si vysvětlíme teorii potřebnou pro základní předpoklady ke zvládnutí vybrané problematiky této práce od obecné teorie o informacích, přes základní pojmy či teorii kybernetické a informační bezpečnosti a její plnění v ČR.

2.1 Teorie informací a postupná digitalizace

Za otce teorie informací je považován americký vědec, matematik a visionář Claude Elwood Shannon (1916–2001). Jedná se o vědu, která se zabývá přenosem informací a jeho matematickým popisem. Mimo jiné se zabývá měřením, přenosem, kódováním, ukládáním a následném zpracování informací. Informace se podle Shannonova schématu, na obrázku č. 3, se šíří přes prostor k příjemci za pomocí jednotlivých kroků této modifikace. Tyto jednotlivé kroky, původně analogové se koncem 20. století začaly postupně digitalizovat, až k dnešní technologii plně digitálního přenosu (Sedlák a Konečný, 2021 s. 16).



Obrázek 3 – Shannonovo schéma (Sedlák a Konečný, 2021 s. 16)

Vynálezem tranzistoru roku 1947 se rozběhla revoluce v průmyslu, dnes označovaná jako třetí průmyslová revoluce. Začalo se s digitalizací signálů, což lze v obecné rovině chápat jako konverzi analogového signálu na digitální. Tento digitalizovaný signál je ukládán ve

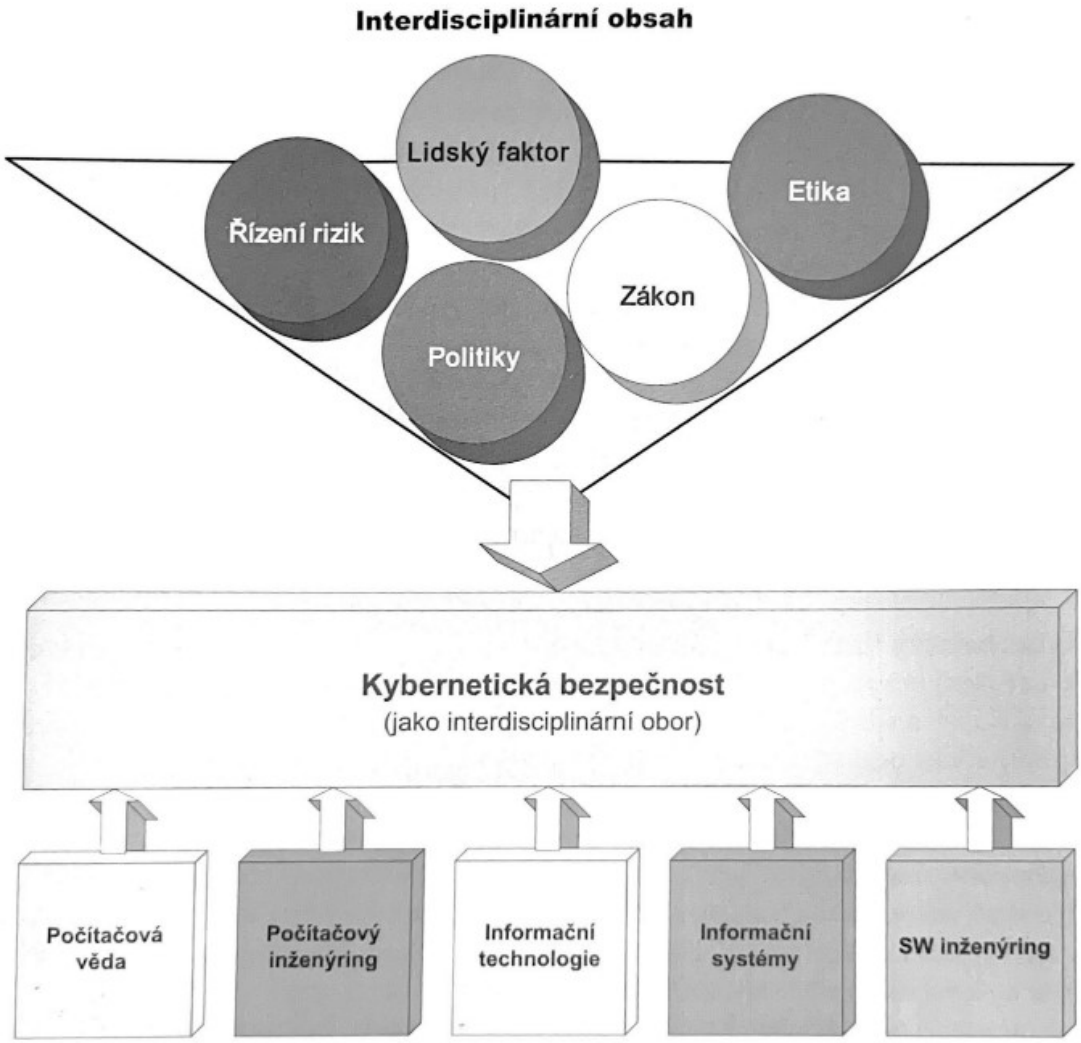
formě bitů a kolem roku 2010 bylo celosvětově ukládáno již jen 5 % komerčních dat pouze v analogové formě ((Sedlák a Konečný, 2021 s. 17)).

2.2 Kybernetický prostor

Kybernetika jako věda se popisuje podle Wienera (Wiener, 1960), jako studium komunikace lidí, zvířat a strojů. Určují ji sociálně – ekonomické faktory jako dělba práce a ekonomické podmínky, dále technické faktory jako rozvoj komunikačních a informačních technologii, postupy a přírodovědné faktory, kterými jsou například objevy ve vědě a rozvoj vzdělání. Kybernetika je dnes na vzestupu a chápeme ji jako společensko-sociální a technologický obor, který je nedílnou součástí života lidí a pojmy jako kybernetický prostor, kybernetická bezpečnost a kybernetický systém jsou dnes každodenní součásti života jednotlivců, organizací a subjektů ve světě. Zákon o kybernetické bezpečnosti definuje kyberprostor jako: *Virtuální oblast, kde pracují, případně spolu prostřednictvím elektronických prostředků komunikují informační systémy, jednotlivé počítače a počítačové sítě. V kybernetickém prostoru jsou zpracovávány a vyměňovány informace a ukládána, sdílená či přenášená data v elektronické podobě* (Česko, 2014).

2.3 Kybernetická bezpečnost

Tento pojem vysvětluje výkladový slovník kybernetické bezpečnosti (Jirásek, Novák a Požár, 2013), jako komplexní souhrn právních, organizačních, technických a vzdělávacích prostředků, které směruji k dosažení ochrany v kybernetickém prostoru. Digitalizací a posunem ve vnímání světa, vznikl nový prostor propojený do internetu, který však v začátcích nebyl svázaný pravidly a ani tak nebyl v historii zamýšlen. Tím pádem se s tímto rozvíjejícím kybernetickým prostorem rozvíjí i kybernetické útoky a kybernetická kriminalita a na ní reagující kybernetická obrana v nekončící smyčce. To, že se jedná o mezidisciplinární, mezioborovou záležitost je znázorněno na obrázku č. 4.



Obrázek 4 – Znázornění kybernetické bezpečnosti (Sedlák a Konečný, 2021 s. 14)

Kybernetickou bezpečnost můžeme chápat jako složení vědních oborů, mezi které patří: počítačová věda, počítačový inženýring, informační technologie, informační systémy a SW inženýring. Na ty působí faktory složené ze zákonů, legislativy, bezpečnostních politik subjektů, etických zásad i lidského faktoru jako takového. (Sedlák a Konečný, 2021 s. 14)

Základní pojmy kybernetické bezpečnosti v kontextu internetu věcí

Pro potřeby práce jsou zde objasněny některé pojmy z oblasti kybernetické bezpečnosti v kontextu kybernetické bezpečnosti internetu věcí. Ty, jsou základem ke zvládnutí řešené problematiky.

- **Kybernetická kriminalita** – Souhrn trestné činnosti podle práva, která za pomoci technického a programového vybavení jednoho, či více počítačů, propojených do

počítačové sítě, má za cíl páchání trestné činnosti, či jako nástroj trestné činnosti. Obecně lze říct, že cílem je únik informací, narušení integrity dat a systémů, potlačení služby a negativní použití (Sedlák a Konečný, 2021 s. 13).

- **Kybernetický útok** – Útok vedený na infrastrukturu informačních a komunikačních technologií za účelem způsobit cílovému subjektu poškození, nebo získat důležité či jinak citlivé informace ve vztahu k útočníkovi, z motivu politického nebo vojenského (Sedlák a Konečný, 2021 s. 13).
- **Kybernetická obrana** – Reakce na kybernetický útok a zmírňování jeho následků, či vytvoření odolnosti proti těmto útokům (Sedlák a Konečný, 2021 s. 13).
- **Kyberterorismus** – Jako kybernetická kriminalita se jedná o trestnou činnost. Zde se však jedná o primární cíl vyvolání strachu a neadekvátní reakce napadeného subjektu. Hlavní motivací zde je politický či extremistický důvod (Jirásek, Novák a Požár, 2013).
- **Hacker –** Osoba, která využívá svých schopnosti a dovedností k tomu, aby v informačních systémech odhalovala slabá místa, a hledá nápravu ve formě bezpečnostních opatření (Sedlák a Konečný, 2021 s. 13).
- **Cracker** – Osoba, která na rozdíl od Hackera využívá své schopnosti k pronikání do systému za účelem vlastního obohacení, nebo porušováním bezpečnostních opatření (Sedlák a Konečný, 2021 s. 13).
- **Malware –** Jedná se obecně o typ škodlivého software ve formě virů, počítačových červů, ransomware až po SW cryptominers, sloužící pro krádeže kybernetických peněz (Jirásek, Novák a Požár, 2013).
- **Web Applicaton Attacs (útoky z webových aplikaci) -** Útoky využívají napadání SQL databázi a vkládání nebezpečného kódu do aplikací, a to skrze selhání identifikace a autorizace (Sedlák a Konečný, 2021 s. 13).
- **DDoS – (odepření služby serveru) –** Jedná se o distribuované odmítnutí služby zahlcením serveru požadavky, zejména z botnet sítě (Jirásek, Novák a Požár, 2013).
- **Identity Theft – (krádež identity) –** Zisk identity důležité osoby či osoby s velkým majetkem a vlivem za účelem zisku či získání výhod (Sedlák a Konečný, 2021 s. 13).

- **Botnet –** Je síť infikovaných počítačů, IoT zařízení, takzvaných zombie, s pomocí kterých útočník může využitím sdruženého výkonu provádět náročné útoky jako například DDoS útoky (Jirásek, Novák a Požár, 2013).
- **Physical Manipulation, Damage, Theft and Loss –** Pod tímto pojmem lze rozumět fyzický útok na zařízení, jako poškození, krádež, či ztrátu, a to zejména překonáním fyzického zabezpečení, nebo jeho neexistencí (Sedlák a Konečný, 2021 s. 13).
- **Information Leakage –** Útok s přístupem k datům a informacím o oběti útoku, který nemá dostatečně ošetřeno Řízení přístupu k informacím – například porušením politiky „need to know“ (Sedlák a Konečný, 2021 s. 13).
- **Ransomware –** Útoky s cílem zašifrovat informační systémy a počítače obětí, zejména státní sektor, nemocnice, případně jiná kritická infrastruktura s cílem žádat o výkupné za odšifrování (Jirásek, Novák a Požár, 2013).
- **Sniffer** – Program umožňující odposlouchávání protokolů, které jsou přijímány a odesílány počítačem a který slouží k zachycení přístupových jmen a hesel, dat a údajů (Jirásek, Novák a Požár, 2013).
- **Skript** – Soubor, který obsahuje instrukce v programovacím jazyce používaném systémy a programy (Jirásek, Novák a Požár, 2013).
- **Port** – Používá se komunikaci protokolů TCP či UDP a dalších. Definuje jednotlivé služby, které jsou spuštěny v síťovém rozhraní počítače (Jirásek, Novák a Požár, 2013).

2.4 Informační bezpečnost

Ve dnešní době je již zcela standardem použití triády CIA neboli důvěryhodnost, celistvost a dostupnost (podle anglických slov Confidentiality, Integrity, Availability) a to zejména při práci s informacemi v prostředí informačních a komunikačních technologii. Jak je uvedeno v předchozí kapitole, informační bezpečnost dnes zapadá plně do mezí interdisciplinárního oboru kybernetické bezpečnosti. Informační bezpečnost je vnímána jako přímo návazná na ochranu informací, ať už klasifikaci informací nebo celým životním cyklem informace. Kromě pojetí informace, je kladen důraz právě na celistvost pojmu kybernetické bezpečnosti. Proto jsou zde dnes zařazena data a prvky ICT (Kolouch a Bašta, 2019).

Základní rozdíl vnímaní informace a dat je, že informace jsou údaje, které jsou zpracovány pro příjemce. Každá informace je tedy určitá zpracovaná část dat. Pouze data sama o sobě nemohou byt informacemi (Kolouch a Bašta, 2019)

Triáda CIA

Jeden ze základních způsobů, jak je možno přistupovat k plnění kybernetické bezpečnosti dat, informací ale i celých informačních systému a jejích součástí je použití zmíněné triády CIA (Doporučení k používání protokolu TLP ke sdílení chráněných informací, 2022). Jednotlivé části triády jsou:

- **Důvěryhodnost**

  Základní myšlenkou je, že subjekt poté, co je autentizován, neboli je ověřena jeho identita, je autorizován pro daný typ dat, informací a přístupu k nim. Například klasifikace protokolu TLP podle zpracování a doporučení od NÚKIB, který má sloužit právě ke sdílení informací v organizacích. K určení míry důvěrnosti a nakládání v rámci organizace i mimo ni. Koncem minulého roku došlo ke zveřejnění aktualizovaného systému, který oproti předchozímu se liší ve změně označení „WHITE“, kde se nově používá „CLEAR“. Dále byla doplněna pátá kategorie: „AMBER+STRICT“ Od 1. 1. 2023 je vyžadováno použití tohoto aktualizovaného systému. V následující tabulce číslo 1 je vysvětlen význam těchto skupin.

Tabulka 1 – Význam protokolu TLP (NÚKIB, 2022)

Barva	Podmínky použití
TLP:RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
TLP:AMBER+STRICT	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je

	důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:AMBER	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
TLP:CLEAR	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Jak sám NÚKIB uvádí, tento systém je doporučen používat u organizací a subjektu, které se spolu předem domluvily na tom, že budou tento systém používat. Navíc pokud organizace spadá pod *zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů,* je povinna plnit nakládání s informacemi podle znění tohoto zákona (Doporučení k používání protokolu TLP ke sdílení chráněných informací, 2022).

- **Integrita**

  Integritou v systému triády CIA je myšlena integrity jako taková. Integrita dat a integrita systému. Ve všech případech se jedná o určitou míru nemožnosti toho, aby bylo do informací, dat nebo systému zasáhnuto osobou, která k tomu není autorizována (Kolouch a Bašta, 2019).

- **Dostupnost**

  Dostupnosti se v kontextu triády CIA hovoří jako o garanci toho, aby byl pro subjekty, kterým poskytuje dvě předchozí vlastnosti důvěryhodnost a integritu dostupný, neboli garantuje přístup podle potřeby subjektu (Kolouch a Bašta, 2019).

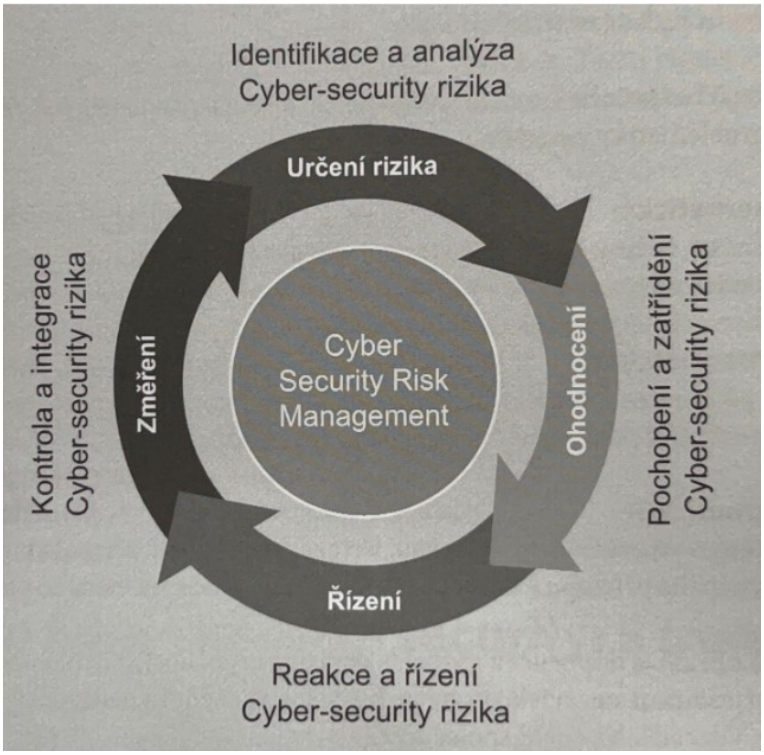
2.5 Řízení kybernetických rizik útoku

Stejně jako je obecné pojetí rizika v oblasti řízení rizik, kde se jedná o určitou událost, která je mírou nežádoucí a za pravděpodobnosti jejího vzniku, tak v oblasti řízení kybernetických rizik se jedná o zranitelnost aktiva. Tedy souhrn okolností, kdy útočník využije hrozbu. Aktivum je rozuměno jako informační, fyzické nebo cokoliv co má pro danou organizaci nebo subjekt hodnotu (význam), a v případě ztráty či poškození by byla negativně ovlivněna činnost organizace/subjektu. Kybernetickou hrozbou se tak stává i potencionálně nechtěný incident, který může mít za následek poškození organizace nebo systému jako takového.

Sedlák (Sedlák a Konečný, 2021, s. 55) definují 5 principů, které by se měly uplatňovat v organizacích ve vrcholovém managementu pro pochopení závaznosti celé problematiky kybernetické bezpečnosti:

- **Pochopení kybernetické bezpečnosti** – V globálním pohledu, nikoliv jen konkrétní problém, který nastane například při provádění ročního auditu.
- **Pochopení právních důsledků kybernetických rizik** – Vztah daného subjektu a třetích stran.
- **Odpovídající přístup ke znalostem kybernetické bezpečnosti** – Zde je myšlen vztah vedení společnosti ke spolupráci s manažerem kybernetické bezpečnosti neboli rolí CISO - Chief Information Security Officer , v překladu vedoucí pracovník v oblasti bezpečnostních informací.
- **Nastavení rámce řízení kybernetických rizik** – Rozumí se míra nasazení finančních a lidských zdrojů, které budou adekvátní a udržitelné pro organizaci/subjekt.
- **Zahrnutí kybernetické bezpečnosti do řízení společnosti** – Při plánování o budoucím rozvoji.

Řízení kybernetických rizik může být tedy chápáno jako koloběh nekončících činností, při kterých nelze určit míru, kdy je společnost nebo subjekt plně chráněn, protože z principu věci toto ani není možné. (Sedlák a Konečný, 2021).



Obrázek 5 – Řízení kybernetických rizik (Sedlák a Konečný, 2021, s. 56)

Cyklus řízení kybernetických rizik začíná u identifikace a analýzy, neboli souhrnně určení kybernetického rizika. Toto riziko je potřeba ohodnotit. Tím dojde k určení míry ohrožení a pochopení daného rizika. Při výstupu těchto dat je možno provést reakci a řízení, neboli na návrh opatření, jejichž cílem je minimalizace rizik. Tyto opatření poté prochází kontrolou a přezkoumáváním pro stanovení kontextu, zda je opatření účinné a opět začíná nový koloběh. Jeho znázornění je uvedeno na obrázku č. 5.

2.6 Motivace a důvody kybernetických útoků

V této kapitole je uvedeno, jaké jsou motivace, které vedou k provádění kybernetických útoku z pohledu útočníka. Jak se rozlišují a jak se dotýkají kybernetické kriminality.

Motivace

Motivací z pohledu útočníka může být několik. Pokud se například jedná o začínajícího hackera neboli nováčka, je nosnou motivací provádění kybernetických útoků jeho snaha se prosadit, osvojit si dovednosti a překonat výzvy. Osobou hackera je z pohledu samotného hackera obyčejný uživatel, který ale má zkušenosti, dovednosti a nadání k tomu, aby pronikl

za hranice běžného uživatele. Pokud však těchto útoků zneužije pro konání kybernetické kriminality, stává se Crackerem (Jirovský, 2007).

Z kontextu věci vzešla kategorizace hackerů na takzvané „Hats“, neboli pomyslné klobouky, které ve starých filmech nosili kladní (bíle) a záporní (černé) protagonisté filmů. Tato kategorizace se dále dělí na skupiny (AO kaspersky Lab, © 2023):

- **White hats** – Někdy také nazývaný jako etický hacker neboli dobrý hacker. Jak bylo zmíněno, využívá svých znalosti k prověřování systému formou například penetračních testů. Za svou funkci je placen přímo od subjektu/organizace, které takovéto hackery najímá, či nabízí odměny za sdílení bezpečnostních děr v jejich systému, za účelem jejich odstranění. Hlavní zásadou je, že o jejich působení subjekt, či organizace má informaci a udělil jim povolení. Cílem etického hackingu je zlepšit celkovou bezpečnost a ochranu před případnými útoky (Evans, 2019).
- **Black hats** – Opak white hats – jedná se o zmíněné crackery, kteří napadají systémy. Jejich počínání je za hranicí etiky, či přesahuje do legislativy pro kvalifikaci kybernetického zločinu. Mohou své znalosti využívat pro své obohacení, ale i nabízet své služby jiným za úplatu – na objednávku (Evans, 2019).
- **Grey hats** – Jejich počínání není pevně spojeno s předchozími dvěma skupinami. Šedý hacker je buď bývalý hacker jedné ze zmíněných barev, který změnil strany, nebo jeho jednání může být někdy hodnoceno jako špatné i dobré. Jako příklad hacker, který objeví bezpečnostní díru a výsledky svého zjištění oznámí organizaci, kterou napadl. Někdy ale výsledky takříkajíc daruje široké komunitě hackerů, i těch špatných. Anebo si své zjištění nechá pro sebe a o dané bezpečnostní díře ví jen on (Evans, 2019).

V obecném kontextu má tedy motivace k provedení kybernetického útoku několik směrů. Od osobního směru, který zahrnuje například pomstu, třeba bývalého zaměstnance, nebo problematické vztahy na pracovišti či nedostatek uznání. Přes finanční motivaci, jako je krádež například digitální měny – kryptoměny, či prodej informací a dat třetí osobě. Také je motivací publicita, a to zveřejněním citlivých informací, kyberterorismus, ale také zviditelnění samotného hackera.

V dnešní době se na popředí dostává motivace, která již přesahuje osobu jednoho hackera a jedné organizace, kdy se začíná se hovořit o takzvaném státním

kyberterorismu, kde aktéry jsou celé státy. Kyberterorismus se pak stává nástrojem k vyvolání neadekvátní reakce nebo strachu, nejčastěji je identifikován jako politický, nacionalistický, či extremistický. Další dnes aktuální motivací je kybernetická špionáž, která se zaměřuje na získávání citlivých, strategických a důležitých informací od jednotlivých organizací či celých státu. Důvody jsou opět politické, ekonomické či vojenské (Sedlák a Konečný, 2021).

Kybernetická válka

S rostoucím nebezpečím mezistátních kybernetických útoků je dnes kyberprostor chápán jako další doména, ve které platí logika útočných a obranných operací. Od roku 2019 je kyberprostor zařazen summitem NATO ve Varšavě jak pátá doména, po zemi, vzduchu, vodě a vesmíru. Definuje kyberprostor z hlediska kybernetické války jako doménu, kde za použití elektroniky a elektromagnetického spektra je skladováno, modifikováno a vyměňováno množství dat skrze systémy a fyzickou infrastrukturu (Sedlák a Konečný, 2021, s. 120).

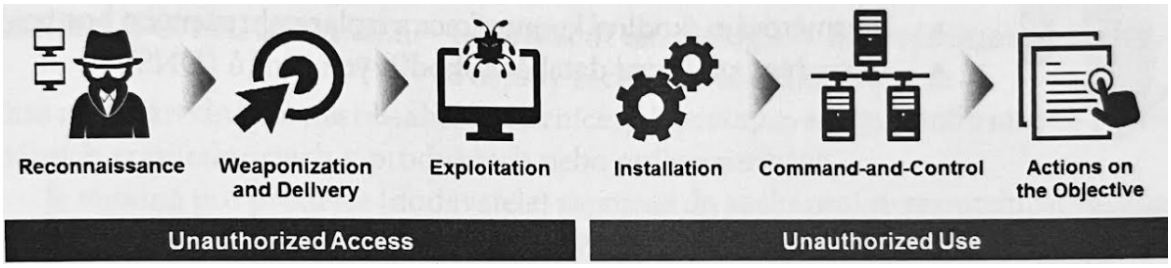
Kyberprostor je dnes tedy chápán jako součást fyzického světa, se všemi aspekty jako jsou ostatní domény. Proto i vlády a státy zřizují jednotky kybernetických sil, například v ČR to je Velitelství informačních a kybernetických sil Armády České republiky. To bylo zřízené roku 2019 a je nástrojem přispívajícím k bezpečnosti ČR. Spolupracuje s koaličními partnery v rámci NATO i s civilními subjekty (Velitelství informačních a kybernetických sil, 2021).

2.7 Životní cyklus kybernetického útoku

Kybernetický útok lze popsat jako sérii po sobě jdoucích událostí, jež vedou k vzniku ohrožení subjektu, a lze jej dělit na dvě fáze:

- **Neautorizovaný přístup**
- **Zneužití**

Neautorizovaný přístup se dělí na rekognoskaci sítě, kdy dochází k průzkumu sítě a mapování jednotlivých služeb a aplikací. Dále se stanovuje strategie, jak bude proveden útok a následně je provedena aktivace škodlivého kódu pro napadení sítě.



Obrázek 6 – Fáze kybernetického útoku (Sedlák a Konečný, 2021, s. 113)

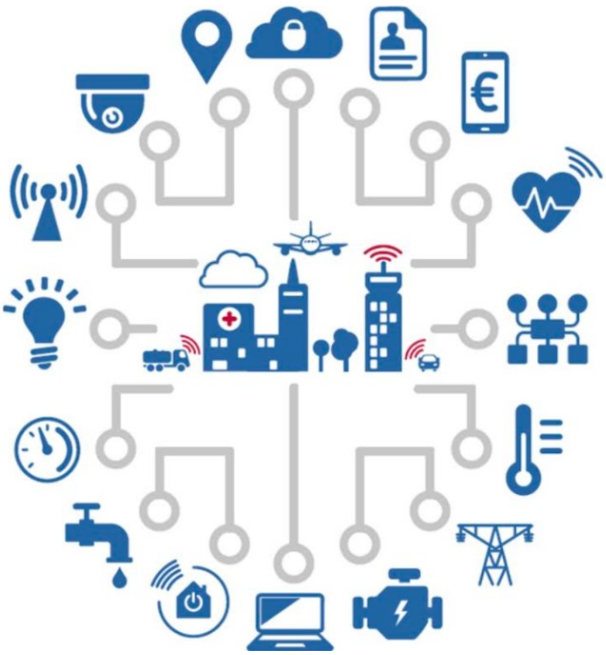
Zneužití je dále děleno na tři fáze, a to na přizpůsobení toho, jak bude prostředí připraveno pro útočníka, například se otevřou porty a nastaví vzdálená komunikace. Tím se definuje způsob, jakým bude útočník komunikovat se škodlivým kódem v systému, nakonec je proveden cílený útok, jehož výsledkem může být, cokoliv od krádeže dat až po úplně zničení fyzického zařízení. Fáze kybernetického útoku jsou uvedeny na obrázku č. 6 (Sedlák a Konečný, 2021, s. 113).

3 TEORIE INTERNETU VĚCÍ

V této kapitole se zaměříme na teoretické popsání základu internetu věcí, co se vlastně rozumí pojmem internetu věcí, jak funguje komunikace a jak byla a je zamýšlena architektura propojení prvků IoT.

3.1 Co to je internet věcí

Pojem internet věcí poprvé použil Kevin Ashon v roce 1999 a to jako široce rozšířený ekosystém, kde zařízení, automobily, domácí spotřebiče a další ne počítače, spolu zajišťují sběr, předávání, a zpracování dat skrze síť internet a kde je každý prvek jednoznačně identifikován (ENISA, 2017). Ashton tehdy použil RFID čip neboli radiofrekvenční čip, kterým jednoznačně identifikoval zboží a tím se dalo přesně pracovat s daty o zboží, které se tak stalo chytrým prvkem. V následujících letech začal pozvolný ale exponenciálně rostoucí trend chytrých zařízení, které se spojují do internetu, a vzniká internet věcí.



Obrázek 7 – Internet věcí (ENISA, 2017, s. 18)

Na obrázku číslo 7 je vyobrazen diagram, který vystihuje, do jaké oblasti internet věcí dnes může zasahovat. Mezi oblasti, které dne spojeny s internetem věcí můžeme zařadit:

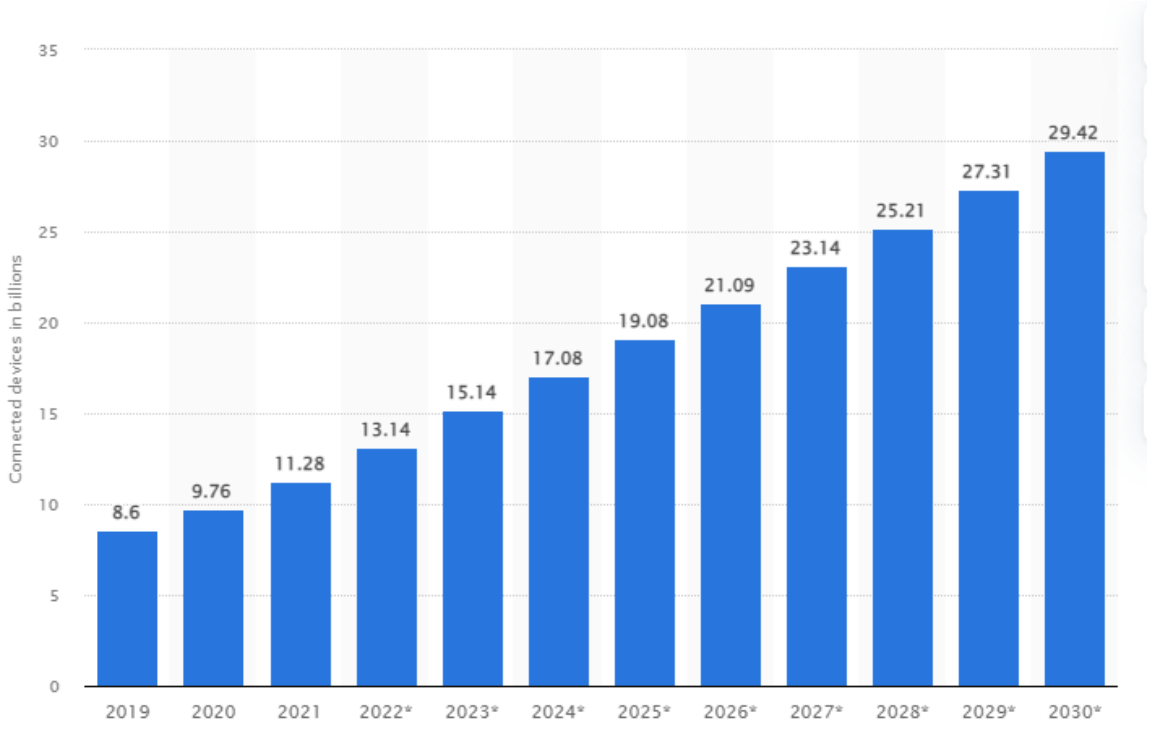
- **Chytrá domácnost** – Smart home – Neboli dnes jedna z rychle se rozvíjejících oblasti internetu věcí, zejména ve spotřební zboží. Mezi které si můžeme vybavit řízení vytápění, rekuperace a chlazení domu, senzorické zabezpečení domu,

inteligentní kamerový systém, chytré osvětlení, chytré spotřebiče jako televize, lednička, pračka, kávovar, to vše je řízené za pomocí dálkového ovládání například přes aplikaci v mobilním internetu, či hlasem za pomocí hlasového asistenta.

- **Chytré město** – Smart city – Ať už se jedná o chytré budovy nebo celé chytré město, jsou pomocí senzoru a snímačů získávaná data pro řízení infrastruktury města, jako elektřiny, vody, dopravy, bezpečnosti, kde uveďme třeba opět chytrý kamerový systém. (Serpanos a Wolf, 2018)
- **Chytrá energetika** – Smart energy – Využitím prvků IoT je možno dnes řídit energetickou rozvodnou soustavu, pomocí chytrých prvků automatizovat a snímat energetické vytížení a aktivně a automatizovaně přepínat mezi zdroji energie pro zachování energetické vyváženosti a stability kritické infrastruktury (Serpanos a Wolf, 2018).
- **Chytré zdraví** – Smart health, eHealth – Jedná se o dnes nejčastěji používané zdravotní snímače, jako chytré kardiostimulátory, měřiče glukózy pro diabetiky, inhalátory, chytré hodinky s měřením tělesných funkcí, tepu, i celého elektrokardiogramu – EKG. Tyto zdravotní pomůcky odesílají data o zdravotním stavu do aplikace, nejčastěji v mobilním telefonu a umožňují uživateli a zdravotníkům kontrolovat důležité funkce organismu člověka (Serpanos a Wolf, 2018).
- **Chytrá doprava** – Mezi kterou dnes řadíme chytrá letiště, železniční dopravu, nákladní dopravu, ale i obyčejné řízení vytíženosti automobilové dopravy ve velkých městech. To za pomocí čidel může upravovat jednotlivé křižovatky pro průjezdnost a plynulost dopravy. K tomu i komunikovat zároveň s aplikacemi jednotlivých řidičů, a tak navrhovat například efektivní průjezdy kritickými uzly (Serpanos a Wolf, 2018).
- **Chytrý průmysl** – Jedná se o jednu z nejvíce se rozvíjejících oblastí nasazení IoT, o této konkrétní problematice se budeme více zajímat v následující kapitole.

Celkově tedy lze na výše uvedených příkladech rozpoznat, do jakých oblastí dnes proniká takzvaný internet věcí. Velikost jeho exponenciálního růstu jde sledovat i na počtu zařízení, která jsou evidována a připojena do internetu. Stav nasazení IoT ke dnešnímu dni a jakých

predikcí nasazení se do budoucna očekává v oblasti IoT je uveden v následujícím obrázku č. 8.



Obrázek 8 – Množství připojených IoT celosvětové v miliardách (Vailshery, © 2022)

Výše uvedený obrázek jasně dokresluje počet připojených zařízení při vydání statistiky za rok 2021 s výhledem do roku 2030 kdy podle webu statista.com bude registrovaných téměř 30 miliard zařízení (Vailshery, © 2022).

3.2 Průmyslový internet věcí

Dalším očekávaným odvětvím kde se bude masivně implementovat IoT je průmysl. S tímto se také pojí vlastní označení a to IIoT, neboli Industrial Internet of Things. Uváděné výhody použití prvků IIoT v oblasti průmyslu jsou (Serpanos a Wolf, 2018):

- **Viditelnost jednotlivých zařízení** – Výhoda pro řízení procesu, jako jsou velíny a kontrolní místa ve výrobě.
- **Podpora „Edge computing“** – Pro případy, kdy je výhodné mít takzvanou nízkou Latenci, neboli kdy potřebujeme velmi rychle komunikovat s nejnižším spojením, je použití IIoT. To zpracovává výpočetní signály a mezi řídícím prvkem a jeho klientem probíhá jen nejnutnější komunikace.

- **Vzdálený přístup na vyžádání** – Použitím chytrých prvků IIoT je možné, aby technik přistupoval bezpečně na velké vzdálenosti k jednotlivým zařízením, jako příklad jsou větrné elektrárny, které jsou tak řízeny vzdáleně.
- **Předvídavá údržba** – Prvky IIoT jsou schopny měřit v reálném čase parametry ukazující potřebu servisního zásahu.
- **Segmentace** – Jednotlivé procesy a skupiny mohou být sdružovány pro lepší obsluhu, jednoduchost, a hlavně bezpečnost pro předpoklady autorizace a autentizace techniků a správců systémů.

Tyto všechny parametry a mnoho dalších má pro průmysl jednoznačné výhody jako snížení nákladu, zvýšení výkonnosti, snížení údržby a zefektivnění procesu (Serpanos a Wolf, 2018).

Digitalizace výrobního procesu

Použitím prvků IIoT se plně shoduje i koncept digitalizace výrobního procesu podniků. Tato digitální transformace má čtyři stádia vývoje výroby (Sedlák a Konečný, 2010):

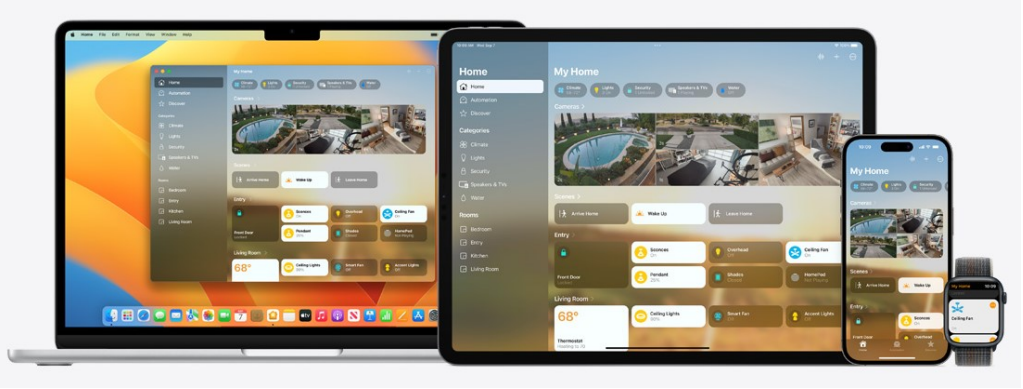
- V první fázi se provádí sběr dat v logistice a výroby a vytvoření digitálního obrazu podniku, a to za pomocí IoT prvků a mobilních zařízení.
- Druhá fáze, se zabývá společnou integrací a logickým spojováním procesu do celku k horizontální integrace procesu v podniku.
- Ve třetí fázi se opět sbírají data, která se analyzují se snahou o optimalizaci procesu a tvorbu reportů, které jsou určující pro management.
- V poslední finální fázi optimalizace procesu probíhají autonomně a zařízení se optimalizují na základě dat samy. To vše za účelem zvýšení produkce, minimalizace chyb a snížení nákladů.

3.3 Chytrá domácnost

Chytrá domácnost, jak bylo řečeno, je dnes po průmyslu nejvíce se rozvíjejícím odvětvím. Velké společnosti i menší výrobci spotřební elektroniky začínají s produkcí spotřební elektroniky s možností připojení do internetu. Tím je umožněno uživatelům domů a bytů automatizovat jednotlivé funkce v domácnostech, jako jsou osvětlení, vytápění, zabezpečení a další. Většina systému dnes umožnuje vzdálenou správu těchto systémů. Uživatel je tak

schopen upravovat například vytápění domácnosti přes internet, i když je stovky kilometru od domova. Základem chytré domácnosti je použití senzorů různých typu a druhů měření. Vlhkoměry, teploměry, snímače světla a vlhkosti jsou dnes již běžnou součástí řízení automatizací v těchto domácnostech (Spivey, 2015). Mezi největší a nejrozšířenější systémy chytré domácnosti patří:

- **Apple Home app** – Společnost Apple nabízí své řešení v rámci zařízení Apple. Hlavní výhodou je integrace do všech zařízení Apple, jako je IPhone, IPad, Apple Watch, Apple TV a jednoduchost připojení (obrázek č. 9). Další hlavní výhodou je vysoký požadavek na bezpečnost dat. Každé zařízení, které uživatel chce připojit, musí být certifikováno pro Apple a musí obsahovat šifrování přenosu dat. Z čeho plyne zároveň nevýhoda řešení od Apple, a to je vyšší cena a menší počet zařízení, které Home app podporují (Home app, © 2023).



Obrázek 9 – Apple Home app (Home app, © 2023).

- **Google Home** – Společnost Google nabízí své řešení za pomocí hlavní části chytré domácnosti, a to hlasového asistenta Google Assistant a zařízeních Google Nest. Stejně jako Apple je multiplatformní a umožnuje širokou úkonů škálu připojených zařízení. Hlavní výhodou je jedno z nejlepších vyhledávání a odpovědí hlasového asistenta na otázky díky vyhledávači Google a množství cenově dostupných zařízení, podporujících Google Home (Google Home, © 2023).

- **Amazon Alexa** – Řešení od společnosti Amazon je celosvětově nejrozšířenější. Nabízí také nejvíce kompatibilních zařízení, která lze do ekosystému Amazon Alexa připojit. Jedná se tedy o poměrně otevřený ekosystém s tisíci různými výrobci zařízení, které spolupracují s tímto řešením (Alexa Smart Home, © 1996-2023).

- **Home Assistant** – Je zástupce nekomerčního nejpoužívanější řešení chytré domácnosti. Jedná se o softwarové řešení chytré domácnosti. Je zdarma, na principu licence open-source, jedná se o otevřenou komunitu vývoje aplikace. Nabízí možnost otevřené integrace prakticky všech možných zařízení. Jelikož se jedná o SW, je nutné tuto platformu instalovat na HW třetích stran, jako například mikropočítač typu Rasberry Pi. Výhoda platformy je otevřenost systému a možnost programování vlastních zařízení, nevýhoda je vyšší požadavek na technické znalosti uživatele(Home Assistant, © 2023).

3.4 Komunikace v kontextu internetu věcí

Zařízení IoT můžeme obecně rozdělit podle komunikace na drátové a bezdrátové spojení. Určení typu je závislé od druhu použití. Komunikují na různých protokolech, které mají ale jedno společné, a to je schopnost přijímat i vysílat informace skrze různé sítě a za pomocí různých parametru přenosu (ENISA, 2017).
Bezdrátová komunikace je přímo spojená s použitím různorodých protokolů přenosu, například zde můžeme zařadit (ENISA, 2017):

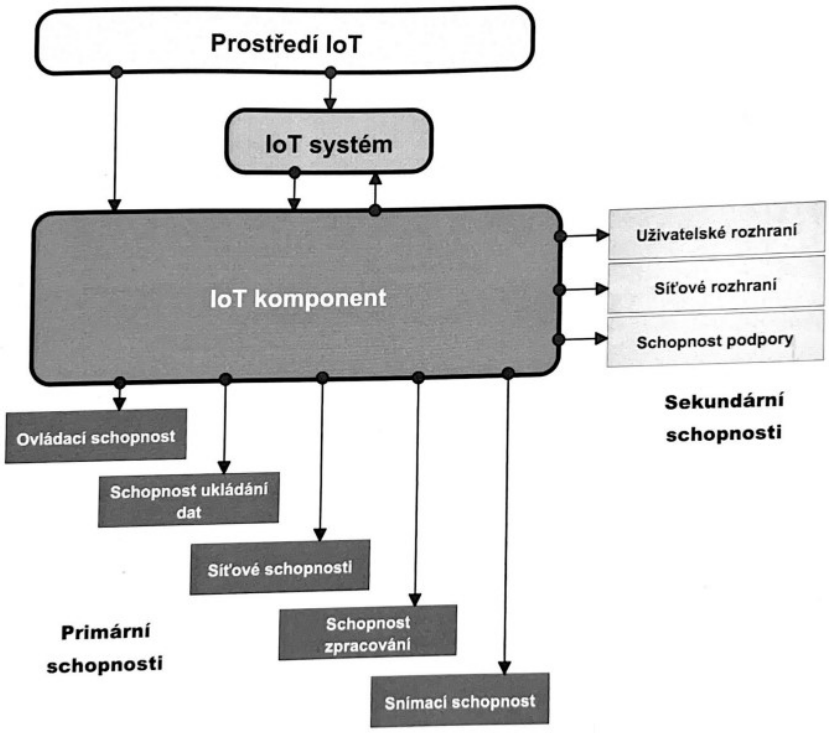
- Rádiové komunikace krátkého dosahu jako ZigBee protokol, Bluetooth a Bluetooth Low Energy (BLE), Wi-fi, Near Field Communication (NFC) nebo Radio Frequency Identificator (RFID).
- Rádiové komunikace na delší a dlouhou vzdálenost kde můžeme uvést technologie LoRaWan, SigFox ale hlavně mobilní přenos jako LTE-M a dnes se rozvíjející sítě 5G.

Drátová komunikace po metalickém vedení je vytvořena klasickým protokolem spojení jako je Ethernet, USB, SPI, MIPI a další.

Tím že zařízení mohou, jak vysílat, tak přijímat není někdy potřeba jejich neustálé konektivity do prostředí internetu, za určitých podmínek jsou schopny pracovat i izolovaně ve vlastním ekosystému, tímto se integrací slova internet ve IoT myslí jako metaforické přirovnání ekosystému IoT k prostředí internetu, neboť jedním z oněch parametru je i použití IP protokolu (ENISA, 2017).

3.5 Architektura internetu věcí

Prvky IoT jsou fyzické či virtuální objekty schopné se identifikovat a integrovat do jednotlivých komunikačních sítí. Zároveň jsou schopny s daty nejen pracovat při sběru a zpracování, ale i vyhodnocovat je a tvořit rozhodování v procesech (ENISA, 2017).
Schopnosti IoT prvku jsou znázorněny na obrázku číslo 10.

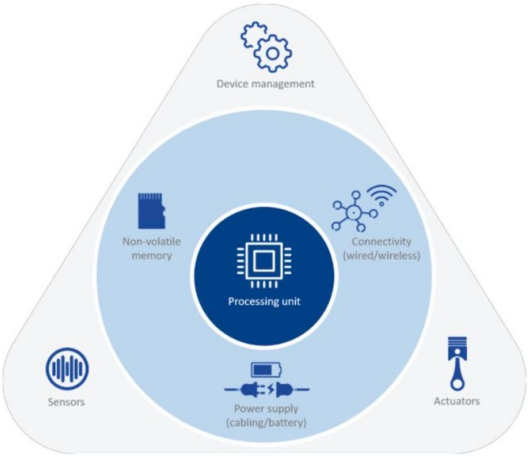


Obrázek 10 – Schopnosti IoT komponent (Sedlák a Konečný, 2021, s.135)

Rozdělení z hlediska architektury IoT je (ENISA, 2017):

- **Řídící – Inteligentní prvky** – Mohou ukládat, zpracovávat, analyzovat a sdílet data, zpracováním ohromným množstvím dat se dále mohou rozvíjet procesy za pomoci například strojového učení. Mezi tyto prvky si uveďme Cloudové služby, Chytré brány, a domácí asistenty.
- **Sběrné prvky – Senzory a snímače** – Jedná se o nejzákladnější prvky IoT, jejich základní účel je sběr a monitoring dat a jejich přenos. Díky integraci a provedení rámci miniaturizace dnes mohou být nasazeny prakticky kdekoliv, ať už pro snímání teploty, tlaku, světla, či stavu věcí, dějů a fyzikálních veličin. Data mohou přenášet stovky kilometrů daleko.

- **Výkonné prvky – Spouštěče, spínače** – Jedná se opět o nejzákladnější prvky IoT. Jsou přesný opakem senzoru a snímačů, mají tedy za účel vykonávat, nehledě na vzdálenosti, činnosti či procesy, které inteligentní prvky vyhodnotily od snímačů a například spínat či rozepínat stavy různých systému.
- **Komplexní systémy – jednotlivé chytré IoT** – Ty jsou dnes nejrozšířenějšími IoT prvky, skládají se z výše uvedených třech skupin a mohou být připojeny přímo k internetu, či ke cloudové službě či aplikaci v mobilním telefonu. Mohou sami vykonávat činnosti. Jedná se chytré spotřebiče, zdravotní pomůcky, chytré termostaty, chytrá osvětlení, chytré kamery a další.



Obrázek 11 – Architektura Komplexních systému IoT (ENISA, 2017, s. 21)

Na obrázku číslo 11 je uvedena architektura těchto složených systému. Ta se zakládá z vnitřní procesorové jednotky, s níž je spojena paměť zařízení, její komunikační část a část napájení. Ve vnější části nákresu jsou zobrazeny sběrné a výkonné prvky a management zařízení.

4 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

V teoretické části bylo nastíněno, jak je kybernetická bezpečnost multioborovou disciplínou. Jak je složité její pojetí z hlediska definice, čeho všeho se týká a že je dnes již plně uznanou doménou, jako je vzduch, voda, země a vesmír. A že tak jak se ve fyzickém světě definuje subjekt, nebo organizace, tak je její digitální obraz i v kyberprostoru. Bylo řečeno, co taková existence nabízí za výhody, ale také jak je zranitelná kybernetickými útoky a obecně kybernetickou kriminalitou. A v poslední kapitole teoretické části je definice teoretického základu, jak dnes lze rozumět pojmu internet věcí a jak je, stejné jako kybernetická bezpečnost, rozsáhlou a exponenciálně se zvěčňující oblastí současného světa.

II. PRAKTICKÁ ČÁST

5 ANALÝZA RIZIK INTERNETU VĚCÍ

První kapitola praktické části je zaměřena na analyzování kybernetických útoku na prvky internetu věcí. A to seznámením s vybranou oblastí internetu věcí včetně vypracování analýzy kybernetických útoku v této oblastí pro přehled o problematice při tvorbě hodnocení rizika IoT prvku. V této kapitole je také vypracován diagram příčin a následků pro znázornění rizika kybernetického útoku. Následně je provedeno hodnocení rizik kybernetických útoku na prvky internetu věcí metodou PNH.

5.1 Vybraná oblast internetu věcí

Tato práce se věnuje vybrané části internetu věcí. Proto pro další práci bude v této kapitole přiblíženo odvětví vybraného prvku IoT.

Chytré kamerové systémy současnosti

Chytré kamery, také označované jako IP kamery podle zkratky Internet Protokol, si v současné době můžeme představit jako zařízení, které se instaluje do interiéru nebo exteriéru a má za úkol zprostředkovat vizuální záznam oblasti. To, čím se ale liší od klasického CCTV (Closed-Circuis Television) kamerového systému je zejména připojení do internetu včetně možnosti jejich vzdálené správy a monitoringu například pomocí aplikací chytrých telefonů. Mezi jedny z nejjednodušších mohou být takzvané dětské chůvičky. Příklad dětské chůvičky je uvedený na obrázku číslo 12. Zařízení, které přenáší obraz spícího dítěte pro kontrolu spánku, či jednouché systémy například k monitoringu domácích mazlíčků, dětí a podobně. Tyto systémy už navíc mohou obsahovat přidané funkce jako obousměrnou komunikaci, funkce vysílání zvuků, či připojení přes aplikaci v mobilním telefonu a další. Jedná se o základní produkty s určením pro použití v domácnostech bez větších nároků například na mechanickou odolnost.

Obrázek 12 – Dětská video-chůvička (Phillips, © 2004–2023)

Mezi pokročilejší systémy patři chytré kamery, jejíž použití je od rozsáhlejšího domácího systému přes monitoring komerčních prostor až po průmyslové využití přímo ve výrobě pro sledování technologických procesů nebo zajišťování bezpečnosti. Tyto systémy se liší zejména provedením a požadavky na mechanické zpracování, jako je odolnost proti vodě a prachu IPXX. Domácí komerční kamery slouží k ochraně nemovitosti a kontrole dění v domácnosti. Mají již možnost ukládání záznamu např. na vnitřní paměťové médium a další chytré funkce, které se dále ještě rozšiřují v případě průmyslových kamer.

Chytré funkce IP kamer můžeme shrnout na:

- **Rozlišení obrazovky** – Chytré kamery mají obyčejně větší rozlišení obrazu, u současných kamer je to od 720 p (HD – 1280x720 pixelů), přes 1080 p (Full HD – 1920x1080 pixelů) až po 4 K (Ultra HD – 3840x2160 pixelů) rozlišení. Čím větší detail obrazu je snímán, tím lepší je schopnost použití dalších chytrých funkcí jako detekce objektů a osob.
- **Detekce objektu a osob** – Chytré kamery jsou schopny detekovat objekty v určité chráněné části objektu. Mohou detekovat například dav, při sportovních utkáních a rozpoznat agresivní chování subjektu, či ležící osobu (Lau et al., 2019). Dále rozpoznávat obličeje a státní poznávací značky aut a tím řešit automatickou evidenci vstupu osob a vozidel. Termo kamery, snímající obraz v tepelném spektru, jsou schopny plnit funkci v protipožárním systému a mnoho dalšího. Příklad nastavení prostoru pro detekci pohybu je na obrázku č. 14.

- **Noční vidění** – Většina IP kamer současnosti je již dnes schopna poskytnou kvalitní obraz, i při snížených světelných a povětrnostních podmínkách.
- **Zvuková signalizace** – IP kamery mohou být vybaveny záznamem zvuku a možností reproduktoru, pro obousměrnou komunikaci. Také mají automatické přehrání alarmu, nebo mluveného slova při narušení prostor.
- **Ukládání dat** – Zmíněná kvalita obrazu u IP kamer dnes klade nároky na ukládání zaznamenaných dat. Dnes nejběžnější používané způsoby jsou **lokání úložiště** v konkrétním zařízení – IP kameře. Ty mohou být build-in neboli pevně zabudované do zařízení ve formě vnitřní paměti, nebo formou externího záznamového média, do takové kamery vložené. Jako příklad můžeme uvést paměťové karty. Dále je možnost data ze záznamu IP kamer ukládat na **lokání síťové úložiště**, jako je NAS (Network Attached Storage) nebo NVR (Network Video Recorder). Tím je jednodušší přístup pro obsluhu k záznamům, jejich zálohu, prohlížení a stahování. To vše je dnes standardně připojeno přes internet také do aplikace v mobilním telefonu uživatele. Poslední možnost je ukládání na **Cloudové úložiště.** To nabízí výhodu zálohování dat, jejich přístup, ale klade požadavky na internetové připojení a často bývá zpoplatněno.

Konkrétním popisem výběrného prvku IoT, IP kamery, pro zpracování systémového modulu kybernetického útoku se bude práce věnovat v kapitole 6.

5.2 Analyzování útoku na prvky internetu věcí

Z teoretické části je patrné že rozšíření oblastí, kde jsou dnes implementovány prvky IoT, nabízí lákavý zájem k provedení kybernetických útoku. Hrozí zde velké materiální a finanční škody s velkým dosahem z pohledu útočníka. Za uplynulé roky bylo již zaznamenáno několik masivních útoků, které vedly k tlaku, ať už na legislativní či technické opatření na rozvoj v kybernetické bezpečnosti prvků IoT. V této kapitole je uvedeno několik příkladu různorodých útoků velkého i malého významu.

Mirai

Název Mirai vychází japonského označení pro budoucnost. Jednalo se o malware, který cílil na zařízení pracující na prostředí LINUX, a to zejména na zařízení IoT jako IP kamery, síťové prvky, routery a další. Ty prohledával v internetu na veřejných adresách, které byly přímo takto propojeny. Po nalezení těchto zařízení se spustil útok, kdy za pomocí od výrobce

nastavených přístupových údajů umožnil, že se útočníci dostali do firmware těchto zařízení a došlo tím k infekci těchto IoT. Takto infikovaná zařízení se staly součástí botnetové sítě, která pak prováděla následně další útoky jako DDoS. Jedním s největších útoků byl například útok 19. září 2016 na francouzskou skupinu OVH Group, poskytovatele služby Cloud computing. Nebo 21. října 2016 na Dyn, providera DNS serverů jako je Netflix, Twitter, PayPal a další. Ten den byl zaznamenán do té doby největší útok infikovanými zařízeními IoT, přes 100 000 zařízení, a to při rychlosti ve špičce téměř 1,2 TB za sekundu. (ENISA, 2017)

Verkada

Tento útok cílil na společnost Verkada, které poskytuje služby chytrých kamerových systémů a jejich cloudové řešení ukládání dat. Útok z března 2021 je přisuzován švýcarskému hackerovi Tillie Kotmannovi. Ten se zmocnil administrátorských oprávnění z nezabezpečených kamerových systému za pomocí absence některých bezpečnostních postupů společnosti Verkada. Tím získal přístup k více než 150 000 kamerovým zařízením, které byly umístěny na nemocnicích, školách, úřadech a dalších. V následném vyšetřování bylo zjištěno, že přes 100 zaměstnanců mělo přístup k těmto kamerovým systémům, bez vědomí zákazníků. Tím porušovali jedno ze základních pravidel informační bezpečnosti a to pravidla - „*Need to Know*“ neboli znát jen to co mají znát (150,000 Verkada security cameras hacked—to make a point, © 2023).

TrendNet

V roce 2012 přiznala problém americká společnost TrendNet, výrobce domácích kamer. Tyto malé domácí kamery americký výrobce prezentuje jako zařízení pro monitoring spících dětí, pacientů v nemocnicích, úřadů, bank a dalších. Všechny kamery byly registrovány na webovou službu společnosti TrendNet. Tu se podařilo hackerům napadnout a prolomit hesla uživatelů. Tím získali přístup k datům a záznamům obrazu přes 700 IP kamer. Následně tyto citlivá soukromá videa útočníci sdíleli na internetu (Kerr, © 2023).

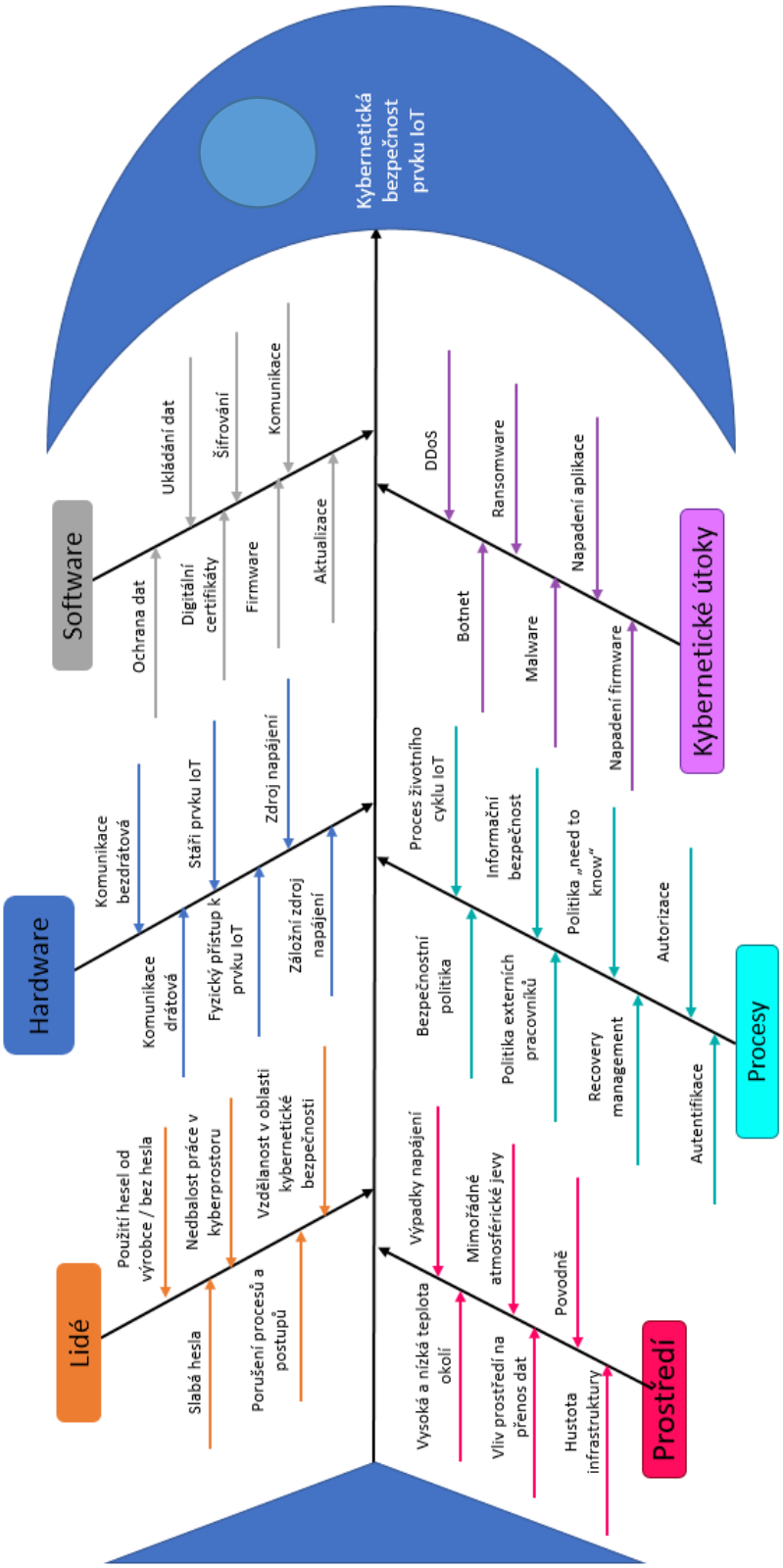
Výše zmíněné kybernetické útoky také ukazují motivace útočníků. Od individuálního hackera, který se s vidinou slávy dostávají do náhodně vybraných společností, až přes organizované útoky na objednávku jako DDoS. To vše naznačuje, jak mohou být vybrané prvky IoT – Chytré kamery zranitelné a zároveň jak jednotlivé kybernetické útoky na různé prvky se opakuji v řádu let a formy útoku zůstávají podobné.

5.3 Ishikawa diagram

Pro znázornění problematiky kybernetické bezpečnosti vybraného prvků IoT je v této kapitole použit Ischikawa diagram, známý také jako diagram příčin a následků. Jedná se o metodu pro analýzu a řešení problému v různých oblastech a s různou problematikou, jako je i kybernetická bezpečnost (Ishikawův diagram, © 2011-2023). Za pomocí tohoto diagramu mohou být identifikovány rizika, tyto děleny na faktory, které mohou vést k problémům v kybernetické bezpečnosti a také pomohou najít řešení těchto problémů. Takto zjištěná rizika budou v následující kapitole podrobena metodou hodnocení rizik PNH.

Jako první úkol při použití Ishikawa diagramu je identifikace problému. V případě této práce se jedná o kybernetickou bezpečnost prvku IoT – IP kamery. Následně musí být identifikovány faktory, které mají vliv na tento definovaný problém. Diagram je znázorněn na obrázku číslo 13. Jednotlivé faktory byly identifikovány jako: Lidé, Hardware, Software, Prostředí, Procesy a Kybernetické útoky.

Zpracování Ishikawa diagramu zde pomohlo pro rozšíření o další metody hodnocení rizik. Pomohlo identifikovat rizika, která mohou ze zmíněných faktorů této metody přispět k přehledu příčin bezpečnostních incidentů. Ty mohou mít za následek ovlivnění kybernetické bezpečnosti prvku IoT.



Obrázek 13 – Ishikawa diagram (zdroj: vlastní)

5.4 Identifikace rizik

Rizika, která budou identifikována, vycházejí z rešerše současného stavu kybernetických útoků, Ishikawa diagramu a dále byly sestaveny a diskutovány v rámci pracovního kolektivu autora práce. Ten byl složen z třinácti systémových administrátorů, pracujících v IT oddělení ve složkách Armády České republiky, se zaměřením na ochranu informací a informačních systémů. S ohledem na ochranu osobních údajů jejich jména nebudou zveřejněna.

Lidé – Jeden z faktorů, který může vést k selhání kybernetické bezpečnosti IoT prvku chytré kamery je zásah člověka, a to až už vědomý, či nevědomý. Jednotlivé dělení této větve je:

- **Použití slabých hesel –** Jedno z nejzákladnějších a zároveň největších rizik v kybernetické bezpečnosti. Použitím slabých hesel útočník může prolomit zabezpečení za pomocí uhádnutí jednoduchých kombinací, či za použití takzvaného hrubého útoku za pomocí automatizovaného SW zkoušením kombinací a permutací hesel. Tímto způsobem může dojít k získání neoprávněného přístupu do prvku IoT.
- **Použití hesel od výrobce –** Tyto hesla jsou v zařízení, nebo v systému zadány od výrobce. Výrobce prvku IoT předpokládá její změnu při prvním použití. Ze zkušenosti z minulosti, kdy útoky cílily právě na tuto zranitelnost, se dá předpokládat, že útočník bude stále mířit na tuto zranitelnost, jako selhaní lidského faktoru.
- **Nedbalost práce v kyberprostoru** – Uživatele nedodržují základní pravidla práce v kyberprostoru, nevěnují pozornost podvodným emailům a klikají na podezřelé odkazy. Nekontrolují si, na jakých stránkách zadávají svá data, a tedy na možnost podvržených stránek. Svým jednáním se vystavují možnosti kybernetického útoku na ně, či zařízení, kterým se pak k prvku IoT mohou útočníci připojit a útok dále šířit.
- **Vzdělanost v oblasti kybernetické bezpečnosti** – Vzdělanost v oblasti kybernetické bezpečnosti se týká nejen znalosti možnosti kybernetického útoku, ale hlavně znalosti prevence před takovými to útoky, znalost legislativy v oblasti kybernetické bezpečnosti a znalost bezpečnostních postupů a politik organizace, či samotného subjektu.

- **Porušení procesů a postupů** – Tyká se nerespektování zavedených postupu a procesu při práci s prvky IoT, práci s informačními systémy či obecními postupy a procesy práce u organizace či subjektu, které mohou mít za následek vznik jiného rizika, které ohrožuje kybernetickou bezpečnost prvku IoT.

Hardware – Faktory, které mohou ovlivňovat hardwarovou stránku IoT zařízení byly identifikovány jako:

- **Komunikace bezdrátová** – Použitím bezdrátové technologie se komunikace mezi jednotlivými prvky IoT vystavují řadě rizik, které s tímto typem přenosu souvisí. Principem bezdrátové sítě je zajistit přenos dat v různorodém prostředí, proto je nutno pokrýt prostor silným signálem. To však může vést k vystavení hranice signálu mimo zamýšlený pokrývaný objekt. Tím se k možnému útočníkovi může dostávat signál mimo kontrolovanou oblast. Touto hrozbou je zachycení komunikace, která od některých prvků může být nešifrovaná. Dále hrozí rušení signálu, nebo jeho zachycení a úprava, jako například útok „Wi-Fi Hijack“.
- **Komunikace drátová** – Stejně jako u komunikace bezdrátové zde hrozí odposlech dat. Ten v případě použití drátové spoje může být útočníkem realizován například u vodiče typu UTP (Unshielded Twisted Pair – nestíněný kroucený párový kabel), jako připojení se na dva páry kabelu v průběhu vedení tohoto kabelu narušením jeho izolace a tím zachytávání přenosu signálu po tomto vedení. Opět vniká riziko úniku dat, jejich manipulace, snižování výkonu, a odposlech dat.
- **Stáří prvku IoT** – Stáří prvků nese několik hrozeb, které mohou být potenciálně velmi nebezpečné. V obecné rovině stáři prvků muže mít vliv na spolehlivost a náchylnost k poruchám. Některé starší prvky IoT mohou používat zastaralý software a firmware, který již výrobce tohoto prvku IoT neaktualizuje a neposkytuje na něj bezpečnostní záplaty systému ani podporu. Také prvek nemusí vůbec obsahovat použití pokročilých možnosti ochrany přenášených dat jako je například šifrování.
- **Fyzický přístup k IoT** – Fyzický přístup k zařízení, které není zabezpečeno opatřeními, může vést k vniku několika nebezpečí prvku. V první řade, jde o věc kriminální povahy, a to krádež vlastního prvku IoT. Dále přístupem potencionálního útočníka k prvku IoT se vystavíme riziku manipulace s tímto prvkem, s jeho potenciálními nezabezpečenými vstupy, jako konektory a dalšími, což může sloužit jako vstupní brána útoku, jako je malware, nebo může nahrát do zařízení vlastní

upravenou verzi firmware a získat kontrolu nad zařízením. Přístupem k zařízení se útočník může seznámit s konkrétním hardware prvku IoT, s jeho součástkami jako je procesor, paměť, základní deska, což může usnadnit případný útok.

- **Zdroje napájení** – Každý prvek IoT obsahuje napájecí část, která jde obecně rozdělit na bateriový zdroj nebo zdroj napájení z elektrické sítě, často i kombinace obou. Z této potřeby napájení prvku IoT tím vyvstávají další rizika. V případě baterie může dojít k jejímu vybití, nebo nesprávné funkci vlivem například teplot. V případě napájení ze sítě může dojít k přerušení napájení. Útočník také může vědomě napadat napájecí zdroj zařízení IoT. Útočník může například vyslat do zařízení vysoké napětí a tím může dojít k poškození zařízení.
- **Záložní zdroje napájení** – V případě použít záložních zdrojů je potřeba provádět pravidelnou kontrolu a testovací přechod na záložní způsob napájení. V případě absence této kontroly může dojít k degradaci bateriových záložních zdrojů, nebo selhání přechodu na záložní zdroje.

Software – Tyto faktory, které ovlivňují software prvku IoT jsou:

- **Aktualizace** – Obecně lze říct, že pokud systém nemá možnost se aktualizovat, vystavuje se riziku vzniku kybernetického útoku na případné chyby. Pokud aktualizace software neprobíhají v co nejkratší době od jejích zveřejnění, vystavuje se prvek riziku, že útočník použije této zveřejněné hrozby na systémy, které nejsou včas ošetřeny touto aktualizací. Také ale provedení aktualizací sebou nese hrozby, a to v případě, kdy prováděním aktualizace dojde k výpadkům spojení, restartem prvku IoT. Prvek IoT může být po dobu aktualizace mimo provoz a tím vznikne hrozba, jakou například může být nefunkčnost bezpečnostních kamer po dobu jejich aktualizace.
- **Komunikace** – Komunikace klade vysoké nároky na bezpečnost v případě kybernetické bezpečnosti prvků IoT. Pokud není dostatečně chráněná informační bezpečnost při přenosu dat, může docházet k vzniku kybernetických útoků, jako je zachytávání komunikace (útoky „man-in-the-middle“ nebo packet sniffing) a zisk citlivých dat, jako například hesla.
- **Firmware** – Firmware jakožto základní kód v zařízeních, který má za úkol základní funkce daného zařízení IoT jako je komunikace SW s HW, zavádění složitějšího

operačního systému a další, a jsou tedy na něj kladeny velké požadavky na kybernetickou bezpečnost. V případě nedostatečné ochrany může útočník přímo ukrást data ve firmware obsažené, nebo zaútočit na firmware a tím jej například infikovat malware, za účelem získáni kontroly na IoT zařízením, zejména při snaze takové zařízení poté připojit do botnet sítě.

- **Šifrování –** Šifrování je dnes považováno za standartní v případě komunikací prvků IoT, ne vždy ale zařízení používá kvalitní šifrování přenosů dat. Tím se vystavuje riziku prolomení šifry a tím kompromitace dat. Šifrování se vyvíjí a zejména starší šifry nemusí být při dnešním výpočetním výkonu dostatečně účinné proti snaze útočníka ji prolomit.

- **Digitální certifikáty –** Digitální certifikáty jsou dnes využívány pro jednoznačnou autentizaci zařízení IoT a také pro komunikaci mezi zařízeními. V případě jejich absence, či nesprávného nakládání s digitálními licencemi může vzniknout hrozba. V první řadě se jedná o nepoužívání digitálních certifikátů, zejména u zařízení, u kterých je kladen důraz na nízkou cenu. Tato zařízení jsou nechráněna a útočník může podvrhem získat přístup například do kontrolního prvku IoT, vydáváním se za periferní zařízení IoT. V případě špatného nakládání s certifikáty, jako je jejich vytváření, distribuce, ověřování, ukládání a po uplynutí platnosti jejich zneplatnění, může útočník takový certifikát odcizit či kompromitovat.

- **Ochrana dat –** Ochrana dat vychází ze správného zabezpečení práce s daty a jejich životním cyklem. Ať už se jedná o jejich vytváření, sběr, přenos, zpracovávání, ukládání a likvidace. Nedostatečně zabezpečená datová komunikace může být Vážným problémem a vznikem hrozby úniku těchto dat. Například absencí šifrování dat.

- **Ukládání dat** – Způsobů ukládání dat je u zařízení IoT mnoho. Od lokálního uložení v zařízení, například paměťové karty, lokální uložiště na řídících prvcích až po cloudové uložení dat. Tyto všechny způsoby se však vyznačují jednotným prvkem, a to způsobem ukládání dat. Pokud jsou ukládány v nešifrované podobě, může k datům po překonání přístupu do zařízení se dostat útočník bez většího úsilí.

Prostředí – Tento faktor plyne z prostředí, kde se zařízení může vyskytovat. A kde v tomto prostoru na něj mohou působit hrozby jako:

- **Povodně** – V případě povodní mohou být prvky IoT náchylné na voděodolnost. Poškození způsobené lokálními i rozsáhlými povodněmi může mít vliv na funkci prvku IoT. Dále vlivem těchto povodní může docházet k výpadkům napájení elektrickým proudem.
- **Hustota infrastruktury** – Hustota infrastruktury má významný vliv na přenosové prostředí a komunikaci prvků IoT. Mohou zde vznikat problémy s rušením signálu, například příliš mnoho zařízení komunikujících na jediném radiovém signálu. Tím mohou vznikat útlumy signálu, snížení dosahu, snížení přenosové rychlosti dat a tím vzniká hrozba výpadků a sběru dat z periferních zařízení IoT.
- **Vliv prostředí na přenos dat –** V případě použití prvku ve specifických prostředích mohou vznikat hrozby, které ovlivňují kvalitu přenosu a spolehlivost. Vysoká hustota zastavěných oblastí snižuje šíření signálu, například dosah Wi-Fi, při průchodu zdmi, či podlahou se snižuje. A tím může opět dojit k nespolehlivosti prvků IoT.
- **Mimořádné atmosférické jevy** – Mezi mimořádné atmosférické jevy, které mohou ohrozit kybernetickou bezpečnost IoT zařízení můžeme zařadit elektromagnetické projevy v přírodě, jako například blesky, Ty mohou, v případě úderu, zničit zařízení či jej poškodit například elektromagnetickým naindukovaným napětím. Dalšími jevy mohou být silné větry a extrémy počasí jako sněhové bouře. Ty všechny mohou ovlivnit funkce IoT zařízení, spolehlivost a mohou způsobit fyzické poškození zařízení.
- **Vysoká a nízká teplota okolí** – Každé zařízení, i zařízení IoT má výrobcem definované pracovní hodnoty rozmezí teplot, ve kterých zařízení pracuje dle parametru zadaných výrobcem. V případě extrémně nízkých teplo jako -30 °C, nebo naopak nad +50 °C může docházet k výpadkům napájení u bateriových zdrojů zařízení IoT, přehřívání elektronických součástek, kondenzace vlhkosti a následně poškození zařízení zkratem.
- **Výpadky napájení** – Vlivem prostředí může obecně nastat výpadek napájení, například připojením na nestabilní zdroj elektrické energie, opět tím hrozí funkce a spolehlivost prvků IoT.

Procesy – Tato kategorie faktoru definuje procesy a postupy organizace či subjektu, který prvky IoT nasazuje:

- **Autentizace** – Autentizace je jedním z předpokladů fungování IoT zařízeních. Autentizace jako proces zjištění uživatele nebo zařízení, je velmi náchylný na hrozby, které z tohoto mohou plynout. V případě překonání hesel a ověření uživatele, jako jsou například metody útoku „hrubou silou“ za pomocí automatizovaného opakování zadání přihlašovacích údajů, může útočník získat kontrolu nad zařízeními a kontrolními prvky či odcizit data. Útoky mohou vést i přímo na uživatele jako je například Phishingový útok, který se snaží uživatele za pomocí různých metod, donutit k zadání informací a hesel, kliknutí na odkaz nebo otevření přílohy emailu. Vše toto má za cíl tím infikovat zařízení oběti a tím získat informace k prolomení autorizace. Dalším způsobem útoku k prolomení autorizace muže být útok „man-in-the-middle“ neboli zachycení přenosu dat, které mohou obsahovat informace u autorizace uživatele nebo zařízení.
- **Autorizace** – Další nedílnou součástí předpokladů úspěšné komunikace mezi uživatelem a zařízením IoT je nastavená autorizace. Ta opravňuje uživatele k provádění operací, ke kterým by měl být autorizován. Absence těchto pravidel může vést k nechtěným únikům dat, jako se tomu stalo v případě kauzy Verkada popsané v kapitole 5.2, kdy běžní zaměstnanci společnosti měli přístup k soukromým kamerovým záznamům klientu této společnosti.
- **Recovery management** – Tento pojem je chápán jako proces obnovy a zotavení zařízení, či systému IoT po neplánované havárii nebo výpadku zařízení IoT. Jeho základní podmínkou je co nejrychlejší obnovení funkcí, které mělo zařízení před vznikem této události, nebo výpadku. Tento proces se skládá z různých opatření k zabezpečení výše zmíněného, obecně lze říct, že se jedná o důležitý proces, který by měla každý subjekt, který nasazuje technologie IoT zvážit, neboť bez něj může hrozit i několikanásobný výskyt hrozeb.
- **Politika „need to know“ –** Tento proces se zaměřuje na pravidla přístupu uživatelů k jednotlivým datům, a to za účelem minimalizace rizika úniku informací neoprávněnými osobami. Uživatel je tedy definován do jednotlivých rolí a jsou mu uděleny oprávnění k přístupu k informacím nebo k jednotlivým prvkům, či systému

IoT. Absence tohoto procesu může vést k riziku kybernetických útoků skrze osoby, které by k citlivým datům za jiných okolností neměly přístup.

- **Politika externích pracovníků** – Tento proces se zaměřuje na přístup externích pracovníků, kteří nejsou vázáni na subjekt či společnost ale kteří se vyskytují v těchto organizacích či subjektech, a to pro výkon požadovaných prací. Externí pracovník mimo organizaci zvyšuje riziko kybernetického útoku. Ať už vědomým či nevědomým porušením pravidel a postupů společnosti.
- **Informační bezpečnost –** Informační bezpečnost je série procesů a nakládaní s daty popsanými v teoretické části práce. Nedodržení nebo neuplatňování těchto pravidel a procesu zvyšuje riziko kybernetických rizik.
- **Bezpečnostní politika –** Obecně lze říct, že každá společnost, či subjekt by měli mít bezpečnostní politiku. Ta definuje pravidla pro veškeré věci, lidi a procesy u této společnosti vedené. Smyslem tohoto procesu je ochrana společnosti, či subjektu před hrozbami, které by mohly nastat při jejich nedodrženích. Jeho absence výrazně zvyšuje rizika.
- **Proces životního cyklu IoT** – Stejně jako informační systémy a ITC zařízení mají životní cyklus, je nezbytné považovat životní cyklus IoT zařízení jako potřebnou věc pro zajištění bezpečnosti a spolehlivosti IoT během celého jeho cyklu. Ten se obvykle skládá z plánování nasazení, návrhu implementace zařízení, jako vývoj, následné nasazení a údržba až po likvidaci zařízení nebo systému IoT. Nedostatečné ošetření splnění podmínek v kterékoliv části tohoto procesu muže mít za následek zvýšení hrozby kybernetického rizika v jednotlivých částech životního procesu.

Kybernetický útok – Do této kategorie faktoru, který může mít vliv na kybernetickou bezpečnost IoT prvků patří podle rešerše kybernetických útoku a shody pracovního týmu autora práce tyto nejvýznamnější útoky:

- **Botnet** – Z historie rozvoje IoT je patrné že spousta IoT prvků byla vytvořena s co nejjednodušší schopnosti připojení do internetu. Z tohoto plynou i jednoduché autentizační procesy, či jejich úplná absence. Tím se zařízení vystavuje riziku, že dojde k jeho napadení škodlivým malware, který zařízení může ovládnout, nahrát vlastní řídící program a tím zařízení připojí do botnet sítě spících zařízení, které poté

na pokyn útočníka mohou provádět další útoky. Ten ovládá jejich funkce a takové zařízení může mimo vědomí majitele sloužit jako „sluha“ útočníka.

- **DDoS** – Útoky DDoS – Distributed Denial of Service, neboli odepření služeb na pokyn útočníka. Zařízení, které byly většinou napadeny botnetovým útokem mohou zároveň provést velké množství úkonu a tím přetížit síť, server nebo službu. Takto přetížené prvky mohou způsobit výpadky v plnění svých služeb. Například v případě, že by takovýmto zahlcením požadavku byl vystaven kamerový systém připojený do internetu, může dojít k jeho nefunkčnosti a tím zvýšení rizik bezpečnosti.
- **Ransomware** – Hlavní hrozbou ransomware v IoT je infikace zařízení vlivem slabého zabezpečení přístupu do tohoto zařízení a tím jeho zašifrování. Zašifrování způsobí, že uživatel nemá přístup k funkcím systému, jeho datům ani k ovládání systému. To může způsobit veliké škody v soukromém i obchodním sektoru a v sektoru kritických informačních systémů. Útočník často může požadovat výkupné za odšifrování zařízení, placené většinou v nedohledatelné kryptoměně.
- **Malware** – Použití škodlivého kódu v útocích na prvky IoT ,může způsobit infikace zařízení a jejich následné začlenění do botnetové sítě, zašifrování dat, nebo únik citlivých dat jako záznamu z kamerového systému, nebo krádeže osobních dat. Útočník může získat i úplnou kontrolu nad zařízením IoT nebo nad ucelenou sítí zařízení IoT a ovládat jej mimo kontrolu uživatele takovéhoto systému. Tím může způsobit značné škody na materiálu i lidských životech. Například napadení čističek odpadních vod může způsobit otravu obyvatelstva.
- **Napadení aplikace** – Tato hrozba cíli na webové aplikace, které slouží k ovládání IoT zařízení, jejich záloze, a dalších funkcích. Za pomocí útoku XSS – Cross-site scripting, mohou vložit škodlivý kód do těchto webových aplikaci a tím způsobit odcizení dat nebo prvků autorizace uživatele. Útoky typu SQL Injection – napadení databází s uloženými daty mohou s těmito databázemi manipulovat a opět odcizit data. Pokud aplikace neobsahuje dostatečné zabezpečení k zajištění kybernetické bezpečnosti, vystavuje se těmto rizikům
- **Napadení firmware** – Nežádoucí přístup k firmware muže způsobit, zejména při nedostatečně ošetřených aktualizacích těchto firmware, napadení ze strany útočníka. Ten cílí na známé chyby, které výrobci vydali jako zjištěné závady a využívá často

třeba i rozdílu času, mezi zveřejněním bezpečnostní hrozby a jejímu ošetření v nově vydané aktualizaci software. Také může napadnout a infikovat servery, které tyto aktualizace firmware rozesílají, a zařízení IoT si tak stáhnou infikovaný firmware v rámci standartní aktualizace, aniž by o tom uživatelé věděli.

Jednotlivé faktory hrozeb definovaných v této kapitole jsou často provázány, a tak hrozí při působení jedné hrozby, její sloučení s hrozbou jinou, a tak zvyšování hrozeb najednou působících na zařízení IoT.

5.5 Hodnocení rizik

V této diplomové práci je k hodnocení rizik použita metoda analýzy hrozeb PNH. Tato polo kvantitativní, jednoduchá bodová metoda se skládá z prvků ***P*** - jako pravděpodobnost vzniku, v našem případě kybernetické nebezpečnosti IoT prvku, ***N*** - jako následky a závažnost této kybernetické bezpečnosti a ***H*** – jako hodnocení, které je názorem hodnotitelů, v našem případě se stejně jako u metody identifikace rizik, jedná o hodnotící tým autora, zmíněný v kapitole 5.4. Součinem těchto tří hodnot nám vyjde riziko, ze kterého si sestavíme Míru akceptovatelnosti kybernetické bezpečnosti. Vzorec pro výpočet této metody je tedy:

$$\mathbf{R = P \times N \times H}$$

Pro výpočet rizika je nejprve potřeba stanovení hodnot pravděpodobnosti vzniku jevu, závažnosti následků a hodnocení (Šefčík, 2009).

Tabulka 2 – Pravděpodobnost vzniku jevu (zdroj: vlastní zpracování Šefčík, 2009)

Pravděpodobnost	Parametr
Nahodilá	1
Nepravděpodobná	2
Pravděpodobná	3
Velmi pravděpodobná	4
Trvalá	5

Pravděpodobnost, která je uvedena v tabulce číslo 2 určuje, s jakou pravděpodobností může vzniknout faktor, který může ovlivnit kybernetickou bezpečnost prvku IoT. Je ve stupnici

od 1 do 5, kdy hodnota 1 udává jev, který může nastat jen velmi nepravděpodobně, až do hodnoty 5, kdy je pravděpodobnost faktoru jevu trvalá v působení.

Tabulka 3 – Následky a jejich závažnost při ohrožení IoT (zdroj: vlastní)

Následky	Parametr
Krátkodobý výpadek prvku IoT bez zásahu obsluhy	1
Krátkodobý výpadek funkce prvku IoT, nutný zásah obsluhy prvku IoT	2
Střednědobý výpadek funkce / poškození prvku IoT s nutným zásahem obsluhy	3
Dlouhodobý výpadek funkce / poškození s nutnou opravou prvku IoT	4
Trvalé poškození prvku IoT	5

V tabulce číslo 3 jsou uvedeny následky, které mohou nastat při působení faktoru a hrozeb na prvek IoT a jejich závažnost a vliv na nutnou opravu IoT. Stupnice je od 1 do 5. První stupeň znamená krátkodobý výpadek, například krátké rušení signálu při přenosu dat. Toto ale nevyžaduje zásah obsluhy ani správce systému s implementovaným prvkem IoT. Ve druhém stupni je již potřeba zásahu, ale jedná se o krátkodobý výpadek. Ve třetím stupni se opět jedná o snadnou opravu, ale časové okno opravy je delší. Například nutnost fyzického zásahu na prvku IoT jako je restart zařízení, s nutností k prvku překonat vzdálenost, jako prvky IoT v dopravě, energetice apod. Čtvrtý stupeň nejen že je dlouhodobý, ale zároveň rozsah opravy je větší. Zařízení je nutno například odeslat do opravy k externí firmě či specializovanému oddělení organizace. Poslední stupeň je největší stupeň poškození s nemožnou opravou prvku IoT a nutno jeho výměny.

Tabulka 4 – Hodnocení vlivu na prvek IoT (Šefčík, 2009)

Vliv na míru nebezpečí a ohrožení	Parametr
Zanedbatelný vliv na míru nebezpečí a ohrožení	**1**
Malý vliv na míru nebezpečí a ohrožení	**2**
Větší, nezanedbatelný vliv na míru ohrožení a nebezpečí	**3**
Velký a významný vliv na míru ohrožení a nebezpečí	**4**
Více významných a nepříznivých vlivů na závažnost a následky ohrožení a nebezpečí	**5**

Závažnost vlivu hrozeb na kybernetickou bezpečnost IoT prvků je uvedena v tabulce číslo 4. Jedná se o hodnocení hodnotitelského týmu a značí, jaký vliv budou mít jednotlivé hrozby na hodnocení rizik. Stupnice je od 1 do 5, kdy první stupeň značí nejmenší vliv na míru ohrožení kybernetické bezpečnosti prvku IoT, až pátý stupeň s největší mírou nebezpečných vlivu, které navíc mohou působit současně.

Celkové hodnocení rizika vychází ze zmíněného vzorce a hodnoty udávají hodnotu rizik a výsledek, který je potřeba při ošetření rizik zapracovat. Jednotlivé hodnoty a jejich rozmezí je uvedeno v tabulce číslo 5

Tabulka 5 – Hodnocení rizika (Šefčík, 2009)

Rizikový stupeň	R	Míra rizika
I.	> 100	Nepřijatelné riziko
II.	51 ÷ 100	Nežádoucí riziko
III.	11 ÷ 50	Mírné riziko
IV.	3 ÷ 10	Akceptovatelné riziko
V.	< 3	Bezvýznamné riziko

Bodové rozpětí vyjadřuje naléhavost a prioritu v přijetí opatření ke snížení kybernetického rizika na prvek IoT (Šefčík, 2009).

- **I. Nepřijatelné riziko** – S katastrofálními důsledky, kdy toto riziko zasahuje do fungování celého systému, musí být okamžitě systém odstaven a dokud nedojde k ošetření rizika, nemůže být systém používán. Organizace, či subjekt musí okamžitě začít pracovat na ošetření rizika.
- **II. Nežádoucí riziko** – Tato úroveň rizika vyžaduje okamžité provedení opatření ke snížení rizika a musí na tuto činnost vyčlenit prostředky.
- **III. Mírné riziko** – I přes nutnost opatření, které bývá zpracováno na určité časové období, jde o nižší riziko. To by mělo obsahovat i další zhodnocení pro stanovení potřeby zlepšení stavu hrozby rizika, zejména pokud se jedná o riziko s velkými následky.
- **IV. Akceptovatelné riziko** – Riziko, které muže být vyhodnoceno jako akceptovatelné. Zároveň se zvažují náklady na případné zlepšení. Pokud je riziko technického charakteru a již nelze ošetřit technickým opatřením, je možné riziko ošetřit například organizačním opatřením, školením obsluhy nebo stanovením postupu a procedur při vzniku.
- **V. Bezvýznamné riziko** – I když není realizováno žádné opatření, stále je zde možnost vzniku rizika, to by se mělo stále připomínat procesně, aby se na něj nezapomnělo.

Hodnocení jednotlivých faktorů rizik kybernetické bezpečnosti IoT

Provedené hodnocení rizik metodou PNH se bude aplikovat na faktory, které byly identifikovány v předcházející kapitole. A to s rozdělením na jednotlivé faktory:

- **Lidé … Tabulka číslo 6.**
- **Hardware … Tabulka číslo 7.**
- **Software … Tabulka číslo 8.**
- **Prostředí … Tabulka číslo 9.**
- **Procesy … Tabulka číslo 10.**
- **Kybernetické útoky … Tabulka číslo 11.**

Jednotlivé faktory jsou zaznamenány do tabulek a je jím určena: pravděpodobnost vzniku nebezpečí ***P,*** následek plynoucí z ohrožení ***N*** a názor hodnotitele ***H.*** Ukazatel míry rizika je

v tabulce na posledním místě. Ten na základě součinu hodnot stanovuje rizikový stupeň, který vyhodnotí rizika a jejich hodnocení. Toto hodnocení je východiskem pro ošetření rizik.

Tabulka 6 – Faktor hrozeb „Lidé“ (Zdroj: vlastní)

LIDÉ						
Identifikace rizika	**Zdroj rizika**	**Vyhodnocení závažnosti rizika**				**Rizikový stupeň**
		P	**N**	**H**	**R**	
Slabá hesla	Uživatel	**3**	**3**	**5**	**45**	**III.**
Použití hesel od výrobce / bez hesla	Uživatel	**3**	**3**	**5**	**45**	**III.**
Nedbalost práce v kyberprostoru	Uživatel	**3**	**3**	**3**	**27**	**III.**
Vzdělanost v oblasti KB	Uživatel	**2**	**2**	**2**	**8**	**IV.**
Porušení procesů a postupů	Uživatel	**5**	**3**	**5**	**75**	**II.**

Z hodnocení faktoru „Lidé“ v tabulce číslo 7 vychází, že nejzávažnější riziko bylo „Porušení procesů a postupů“, výsledný stupeň II. Co z identifikace rizik vychází, je možný vznik kybernetického rizika, a to zejména více významných vlivů by mohlo mít dopad na následky. Zbytek rizik má podobné hodnocení v III. a IV. stupni.

Tabulka 7 – Faktor hrozeb „Hardware“ (Zdroj: vlastní)

HARDWARE						
Identifikace rizika	**Zdroj rizika**	**Vyhodnocení závažnosti rizika**				**Rizikový stupeň**
		P	**N**	**H**	**R**	
Komunikace bezdrátová	Vlastnost přenosu	**3**	**1**	**4**	**12**	**III.**
Komunikace drátová	Vlastnost přenosu	**2**	**1**	**3**	**6**	**IV.**
Stáří prvku IoT	Uživatel	**2**	**3**	**3**	**18**	**III.**
Fyzický přístup k IoT	Uživatel	**4**	**5**	**5**	**100**	**II.**
Zdroj napájení	Fyzikální vlastnost, útočník	**3**	**2**	**4**	**24**	**III.**
Záložní zdroj napájení	Uživatel	**2**	**2**	**2**	**8**	**IV.**

Z hodnocení faktoru „Hardware“ v tabulce číslo 7 vychází riziko „fyzický přístup k zařízení IoT“ na pranici I. a II. rizikového stupně. Toto riziko bylo hodnoceno takto vysoko, neboť pravděpodobnost že nastane, pokud nepovolaná osoba má umožněn nechráněný přístup k prvku IoT, například k chytré IP kameře. Může provést několik různých útok, zničení, odcizení. Následky jsou tedy různé, podle způsobu útoku, ale hrozí zde i trvalé poškození a hraje zde roli více významných vlivů na míru zabezpečení a ohrožení kybernetické ochrany prvku IoT.

Tabulka 8 – Faktor hrozeb „Software“ (Zdroj: vlastní)

SOFTWARE						
Identifikace rizika	**Zdroj rizika**	**Vyhodnocení závažnosti rizika**				**Rizikový stupeň**
		P	**N**	**H**	**R**	
Aktualizace	Uživatel, proces	**3**	**1**	**3**	**9**	**IV.**

Komunikace	Uživatel, útočník	**5**	**1**	**4**	**20**	**III.**
Firmware	Uživatel, útočník	**3**	**3**	**2**	**18**	**III.**
Šifrování	Uživatel, útočník	**4**	**2**	**4**	**32**	**III.**
Digitální certifikáty	Uživatel, útočník	**3**	**3**	**4**	**36**	**III.**
Ochrana dat	Uživatel	**4**	**3**	**3**	**36**	**III.**
Ukládání dat	Uživatel	**4**	**3**	**4**	**48**	**III.**

Z hodnocení faktoru „Software“ v tabulce číslo 8 vychází rizika velmi podobně. Mimo jednoho se všechny hrozby zařadili na III. rizikový stupeň. Každé z těchto rizik může nést následky, které je potřeba ošetřit a v případě reálného útoku, musí tyto hrozby odstranit odborník. Ještě je nutno poukázat na hrozbu „komunikace“, zde byla hodnocena pravděpodobnost jako trvalá. To je zapříčiněno tím, že na jakýkoliv prvek IoT připojený do internetu prakticky ihned začne působit automatizované programy, takzvaní „boti“

Tabulka 9 – Faktor hrozeb „Prostředí“ (Zdroj: vlastní)

PROSTŘEDÍ						
Identifikace rizika	**Zdroj rizika**	**Vyhodnocení závažnosti rizika**				**Rizikový stupeň**
		P	**N**	**H**	**R**	
Vysoká a nízká teplota okolí	Fyzikální vlastnost	**2**	**2**	**2**	**8**	**IV.**
Vliv prostředí na přenos dat	Fyzikální vlastnost	**3**	**1**	**2**	**6**	**IV.**
Výpadky napájení	Fyzikální vlastnost	**1**	**2**	**4**	**8**	**IV.**
Mimořádné atmosférické jevy	Fyzikální vlastnost	**1**	**5**	**4**	**20**	**III.**
Povodně	Fyzikální vlastnost	**1**	**5**	**4**	**20**	**III.**
Hustota infrastruktury	Fyzikální vlastnost	**2**	**1**	**3**	**6**	**IV.**

Z hodnocení faktoru „Prostředí“ v tabulce číslo 9 vychází rizika s relativně malým rizikovým stupněm, zejména hodnotící parametr pravděpodobnosti je zde nízký. To je dáno tím, že se jedná z nahodilé, nepravděpodobné až pravděpodobné fyzikální vlastnosti, zejména počasí. Výrobce většinou toto ošetřuje při výrobě zařízení pro venkovní, či vnitřní použití, riziko vzniká překročením krajních parametrů těchto vlastností.

Tabulka 10 – Faktor hrozeb „Procesy“ (Zdroj: vlastní)

PROCESY						
Identifikace rizika	**Zdroj rizika**	**Vyhodnocení závažnosti rizika**				**Rizikový stupeň**
		P	**N**	**H**	**R**	
Bezpečnostní politika	Uživatel	**5**	**3**	**5**	**75**	**II.**
Politika externích pracovníků	Uživatel	**3**	**3**	**3**	**27**	**III.**
Recovery management	Uživatel	**4**	**3**	**4**	**48**	**III.**
Autentizace	Uživatel	**5**	**4**	**5**	**100**	**II.**
Autorizace	Uživatel	**5**	**3**	**5**	**75**	**II.**
Politika „need to know“	Uživatel	**3**	**3**	**4**	**36**	**III.**
Informační bezpečnost	Uživatel	**5**	**3**	**4**	**60**	**II.**
Proces životního cyklu IoT	Uživatel	**3**	**4**	**3**	**36**	**III.**

Z hodnocení faktoru „Procesy“ v tabulce číslo 10 vychází jako faktor s největším výskytem nejzávažnějších rizik s vysokým číslem R. Zejména hrozba „Autentizace“ je stejně jako hrozba „Fyzický přístup k IoT“ v tabulce 7 na hranici rizikového stupně I. a II. Jedná se o

nejvýraznější riziko opět s vysokou pravděpodobností, dlouhodobými následky a je zde více výrazných vlivů na míru zabezpečení a ohrožení. Další významné hrozby jsou „Bezpečnostní politika“, „Autorizace“ a „Informační bezpečnost“. Všechny spojuje vysoká prakticky neustálá pravděpodobnost vzniku hrozby, s více významnými vlivy na míru zabezpečení a ohrožení KB prvku IoT.

Tabulka 11 – Faktor hrozeb „Kybernetické útoky“ (Zdroj: vlastní)

KYBERNETICKÉ ÚTOKY						
Identifikace rizika	**Zdroj rizika**	**Vyhodnocení závažnosti rizika**				**Rizikový stupeň**
		P	**N**	**H**	**R**	
Botnet	Útočník	**5**	**3**	**3**	**45**	**III.**
DDoS	Útočník	**5**	**2**	**4**	**40**	**III.**
Ransomware	Útočník	**4**	**4**	**4**	**64**	**II.**
Malware	Útočník	**5**	**4**	**4**	**80**	**II.**
Napadení aplikace	Útočník	**4**	**3**	**4**	**48**	**III.**
Napadení firmware	Útočník	**4**	**3**	**3**	**36**	**III.**

Z hodnocení faktoru „Kybernetické útoky“ v tabulce číslo 11 vychází největší rizika z útoku ransomware a z infekce škodlivého kódu malware. Ty totiž mají největší vliv na následky. Uživatel v tom případě musí spoléhat na relativně dlouhou dobu opravy dat. Například v případě ransomware jde o obnovu a instalaci celého systému, v lepším případě ze zálohy dat systému, popřípadě bez uživatelských dat.

5.6 Dílčí závěr analýzy rizik

Kapitola analýzy rizik identifikovala vybranou oblast prvku IoT a to chytré kamery. Za pomocí Ishikawa diagramu byly znázorněny hrozby, rozdělené na jednotlivé faktory. Ty sdružují možná rizika do oblasti: lidského faktoru, hardware prvků IoT, software prvku IoT, prostředí, ve kterém se může vyskytovat prvek IoT, procesy a postupy subjektu/organizace, které prvek IoT nasazuje a možná kybernetická rizika ze strany útočníka. Identifikace rizik jednotlivých faktorů hrozeb, poskytuje náhled, o jak mezioborovou oblast se jedná. Jsou zde

rizika, která v případě výskytu jedné hrozby mohou vést ke krátkodobému výpadku funkcí prvku IoT, nebo také může dojít k úplnému zničení zařízení a vzniku nenávratných škod na zařízení a datech uživatele. Vše záleží na motivaci útočníka a spolupůsobících faktorech hrozeb. Mezi takové rizika se identifikovaly hrozby: „fyzický přístup k prvku IoT“ a „autentizace“ při práci s prvkem IoT. Následující kapitola se bude zabývat vypracováním systémového modelu útoku na vybraný prvek IoT a to na IP chytrou kameru. Model se zaměří na tyto dvě rizika a bude s nimi pracovat. Tyto dvě kapitoly tím poskytnou výstupy pro zpracování opatření ke zlepšení stavu kybernetické bezpečnosti vybraného prvku IP chytré kameře.

6 SYSTÉMOVÝ MODEL ÚTOKU NA PRVEK INTERNETU VĚCÍ

Pro sestavení systémového modelu kybernetického útoku na prvek IoT bude proveden penetrační test, který se používá pro zjištění odolnosti systému proti případným útokům. Výsledkem systémového modulu bude provedení penetračního testu za účelem porozumění fungování systému a schopnosti identifikovat případné zranitelnosti systému pro návrh opatření. Autor práce se staví do role etického hackera a pohlíží na zapojení jako útočník a hledá možné slabiny systému. Se zaměřením na hrozby, které byly v kapitole analýzy rizik hodnoceny jako nejzávažnější, pro potvrzení těchto analýz.

6.1 Popis vybraného zařízení internetu věcí

V této kapitole bude blíže specifikováno vybrané zařízení internetu věcí, a to IP kamera. Výběr IP kamery byl autorem zvolen s ohledem na v současné době rostoucí oblibu instalací kamerových systému svépomocí. Jednotlivé domácnosti, malé provozovny a firmy, s komerčně nabízeným segmentem levných kamerových systému, tyto systémy nasazují a mnohdy si neuvědomují potřebu zabezpečení před možnými kybernetickými útoky, které použitím těchto systému hrozí.

Popis IP kamery

V této prací byla pro sestavení systémového modelu útoku na internetu věcí vybrána IP kamera značky BESDER, model 6024PB-IA20H1 2.0MP, od společnosti Shenzen Besder Technology Co,. Ltd. Jedná se o výrobce bezpečnostních kamer od roku 2012, sídlícím ve městě Shenzen, Čínská lidová republika (Shenzhen Besder Technology Co., © 1999-2023). Společnost se zabývá výrobou a prodejem chytrých kamer, NVR síťových videorekorderů a switchů, zajištujících PoE funkci napájení „Power over Ethernet“, což je technologie napájení přes ethernetový kabel, bez nutnosti přívodu napájení k zařízení. Kamera je zobrazena na obrázku číslo 14.

Obrázek 14 – IP kamera BESDER 6024PB-IA20H1 (Zdroj: vlastní)

Napájecí zdroj, který je dodáván s kamerou, je zobrazen na obrázku číslo 15.

Obrázek 15 – Napájecí zdroj 12V/1A (zdroj: vlastní)

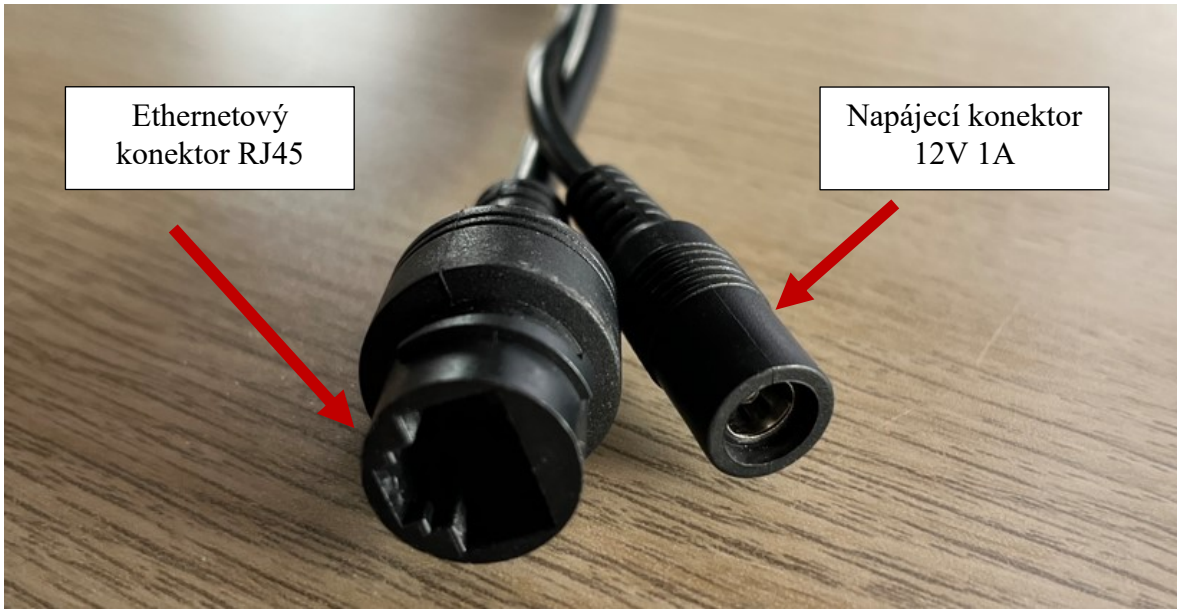
Základní parametry kamery

- Použití: Digitální CCTV, IP kamera.
- Rozměry: 10 x 8 cm.
- Materiál: ABS plast.
- Rozlišení: 2MP – 1920x1080 20fps.

- Ohnisková vzdálenost: 3.6 mm.
- Napájení: DC12V, 1 A – externím síťovým zdrojem.
- Obsahuje 24 IR LED, infračervených diod, pro přísvit do vzdálenosti 5 až 15m s automatickou funkcí přepínáním denního a nočního provozu.
- Záznam obrazu je přenášen formátem komprese dat H.265 (Hight Efficiency Video Coding - HEVC).
- Podporuje vzdálené připojení skrze aplikaci chytrého telefonu, s podporou operačního systému Android a Apple.
- Připojení: Skrze RJ45 konektor s přenosovou rychlostí 10M/100M.
- Pracovní podmínky: Teplotní rozsah -10 až +60 °C, vlhkost vzduchu do 90 %.
- Prostory použití: Venkovní/vnitřní, norma IP65.
- Funkce: Audio mikrofon pro příjem zvuku, detekce pohybu, odesílání zprav skrze email.

6.2 Postup připojení kamery a instalace

IP kamera BESDER se umístí pomocí tří šroubů na požadované místo, které má tato kamera monitorovat. IP kamera má možnost plné rotace ve všech třech osách, takže umožnuje instalaci na strop, i na zeď. K místu zapojení je potřeba přivést běžnou elektrickou zásuvku pro napájení 230 V/50 Hz, či volbu tohoto místa instalace kamery předem technicky připravit. Dále k tomuto místu je potřeba přivést standartní kabel Ethernet – osazený na obou stranách koncovkami RJ45, který umožnuje datový přenos alespoň 100Mbps. Dále bude potřeba stolního či přenosného počítače s operačním systémem Windows. Kamera je kompatibilní se systémy Windows verze 7, 8, 8.1, Vista a 10. V testovaném případě se jedná o Windows 10 s webovým prohlížečem Microsoft Edge verze 111.0.1661.62. Posledním požadavkem pro test je připojení k internetu a pro sledování skrze aplikaci IP kamery je potřeba mobilní telefon s operačním systémem Android verze 5.0 a vyšší, nebo se systémem Apple iOS verze 9.0 a vyšší. Na obrázku číslo 16 je znázorněno připojení konektorů kamery.



Obrázek 16 – Popis připojení kamery (zdroj: vlastní)

Na těle IP kamery se nacházejí informace potřebné pro připojení do kamery. Ty jsou znázorněny na obrázku číslo 17.

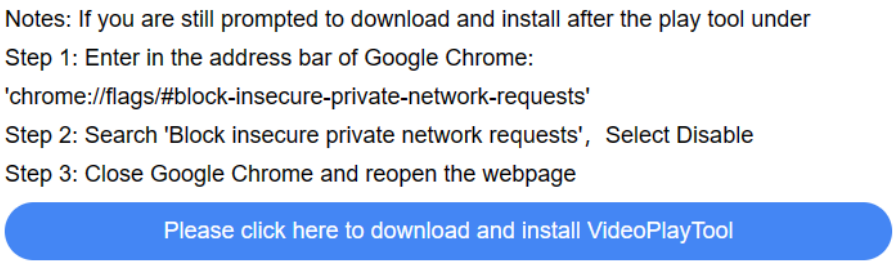
Obrázek 17 – Označení a informace na kameře (zdroj: vlastní)

Z těchto informací lze vyčíst, že je třeba mít zařízení připojeno pro první inicializaci kamery v IP síti s adresním rozsahem 192.168.1.xxx, kde IP kamera má adresu 192.168.1.10. Tuto hodnotu je potřeba zadat do webového prohlížeče, a to ve formátu:

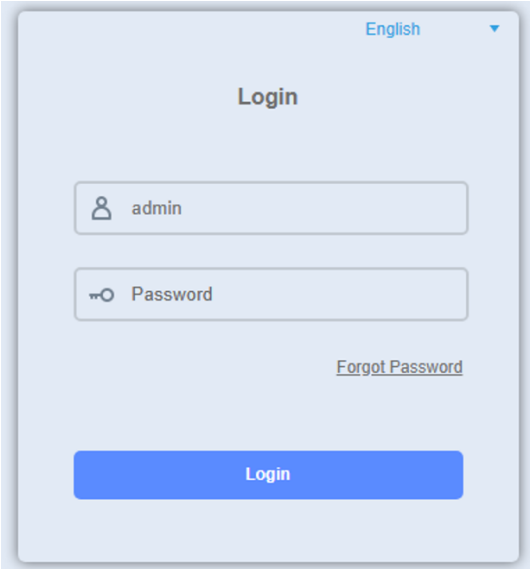
http://192.168.1.10

Následně se zobrazí informace o potřebě instalovat do počítače program **VideoPlayToolSrtup.exe** a po kliknutí na zobrazené tlačítko se provede automatické stažení

a instalace nástroje, k tomu je potřeba mít připojení na internet. Stažení se provede automaticky z internetu (obrázek č. 18).



Obrázek 18 – Žádost o instalaci programu (Zdroj: vlastní)



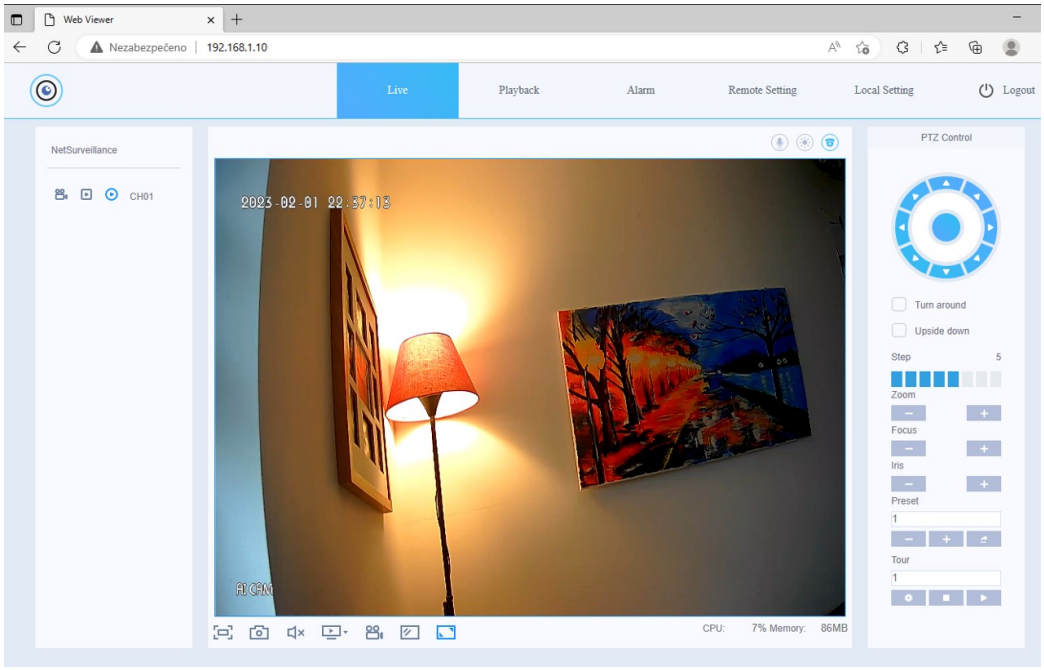
Obrázek 19 – Autorizace uživatele (zdroj: vlastní)

Po instalaci je na IP adrese kamery přístupná přihlašovací obrazovka s výzvou na prvotní autorizaci (obrázek č. 19). Přihlašovací jméno a heslo je opět uvedené na štítku IP kamery (obrázek číslo 17).

Tyto informace jsou:

- **User: admin**
- **Password: null (empty)** …neboli bez hesla, prázdné pole

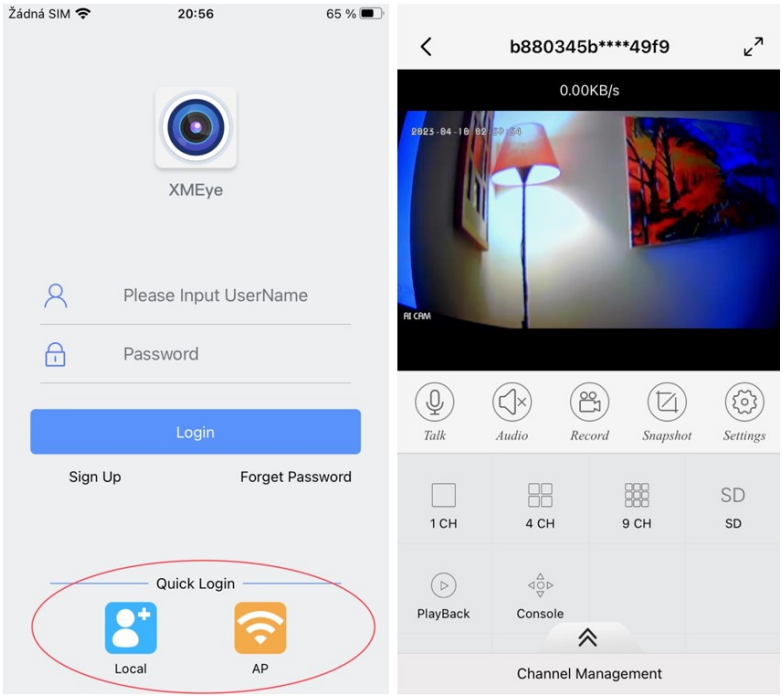
Po přihlášení je již uživatel schopen plně ovládat všechny funkce kamery, je schopen vidět živý obraz z kamery, a nastavovat další funkce kamery. Například způsob ukládání záznamu, inteligentní rozpoznávání osob a oblasti zájmu v záznamu, které je možno odesílat do mobilní aplikace, nebo formou emailu. Toto webové zobrazení je znázorněno na obrázku číslo 20.



Obrázek 20 – Rozhraní testované IP kamery (zdroj: vlastní)

6.3 Připojení mobilní aplikace

Pro připojení ke IP kameře skrze aplikaci mobilního telefonu je potřeba nainstalovat aplikaci XMEYE Pro z obchodu Google Play, v případě OS Android, nebo z App store, v případě OS iOS od Apple.



Obrázek 21 – Připojení a náhled aplikace na mobilním telefonu (zdroj: vlastní)

Na obrázku číslo 21 je zobrazená aplikace na mobilním telefonu. V případě vzdáleného internetového připojení k IP kameře je třeba mít založenou registraci skrze email uživatele u vydavatele aplikace. Druhým způsobem je připojení v místní síti, kdy zařízení najde IP kameru, která se nachází zapojena do stejné sítě jako mobilní telefon. V pravé části obrázku je náhled na ovládací prvky IP kamery a obraz přenosu.

6.4 Popis penetračního testu

Pro sestavení schématu útoku bude proveden základní penetrační test na zařízení IoT. Tento test se bude skládat z prvků etického hackingu. Obsahuje jednotlivé fáze penetračního testu vysvětlené v první části. Dále jsou popsány nástroje, které budou použity v testu. A nakonec vlastní penetrační testování vybrané IP kamery. Tento postup nebude obsahovat test mobilní aplikace a Cloudového uložiště s ohledem na legislativu.

Popis fází testu

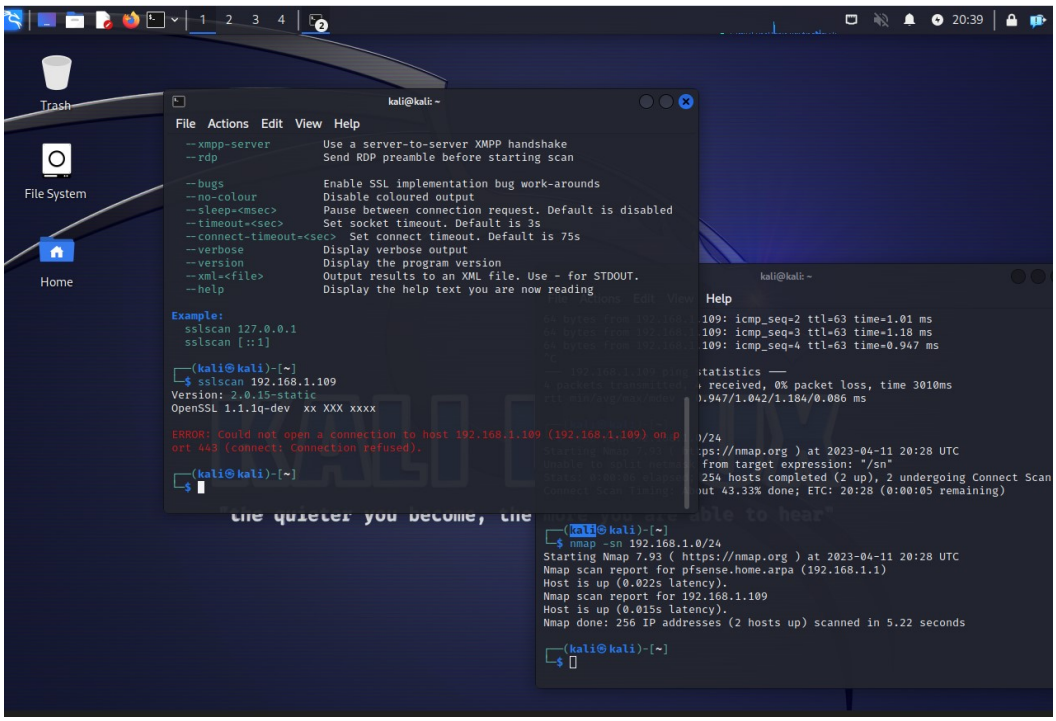
Těmito fázemi jsou popsány možné zranitelnosti a je na nich tak sestaven systémový model možného kybernetického útoku na tuto IP kameru (Gupta, 2019, s. 18).

- **Fáze sběru informací** – V této fázi probíhá sběr všech dostupných informací k získání co největších informací. Vychází se ze znalosti, které o subjektu jsou známy. A to na základě tří jednotlivých kategorii, „Black box“ – o subjektu nevíme vůbec nic, „Grey box“, subjekt nám poskytl jednotlivé kusé informace a „white box“, kdy s námi subjekt plně spolupracuje. Pro práci bude použita kategorie „grey box“. Některé informace jsou nám známy, ale nejsou známy všechny funkce IoT zařízení ani bezpečnostní politika systému.
- **Fáze zranitelnosti** – Fáze se zaměřuje na identifikace zranitelností a zjišťování různých způsobů, jak daný systém zmapovat pro výběr metod a nástrojů k provedení útoku. Jsou použity nástroje jako skenování sítě, skenování verzí SW, zjištění způsobu komunikace a další.
- **Fáze útoku** – Tato fáze na základě předchozího vyhodnocení zranitelnosti používá konkrétní metody a způsoby, jak provést útok. S ohledem na rozsah práce bude tato fáze pouze popsána jako možnosti útoku.
- **Fáze dokumentování** – V poslední fázi testu je provedeno vyhodnocení testu s poukázáním na výsledky testu, identifikuje se slabé místo systému a navrhnou se opatření ke zlepšení stavu bezpečnosti systému.

6.5 Použité nástroje pro penetrační testování

Pro provedení penetračního testu za účelem sestavení schéma útoku budou použity tyto nástroje:

- **Kali Linux** – Jedná se o specializovanou verzi operačního systému LINUX, která je určena primárně pro penetrační testování, etický hacking a provádění bezpečnostních auditů. Vyvinula ji společnost Offensice Security (Offensive Security, © 2023), která ji bezplatně poskytuje pro tyto účely na svých stránkách. Kali Linux je používám zejména pro to, že je v něm již implementována řada nástrojů pro zisk informací, skenování zranitelnosti, forenzní analýzu v IT, testování sítí a další. Prostředí je zobrazeno na obrázku č. 22.



Obrázek 22 – Kali Linux (zdroj: vlastní)

- **Wireshark** – Jedná se o open source (veřejně dostupný, volně šiřitelný, se sdíleným vývojem široké komunity uživatelů) program. Slouží pro analyzování síťového provozu v reálném čase (Wireshark, © 2023). Wireshark dokáže diagnostikovat počítačové sítě, ověřovat jejich funkčnost nebo identifikovat škodlivý provoz a tím zjistit možné narušení bezpečnosti. Umí zachytávat pakety informací a dekódovat protokoly přenosu jako TCP/IP, HTTP, DNS a další.

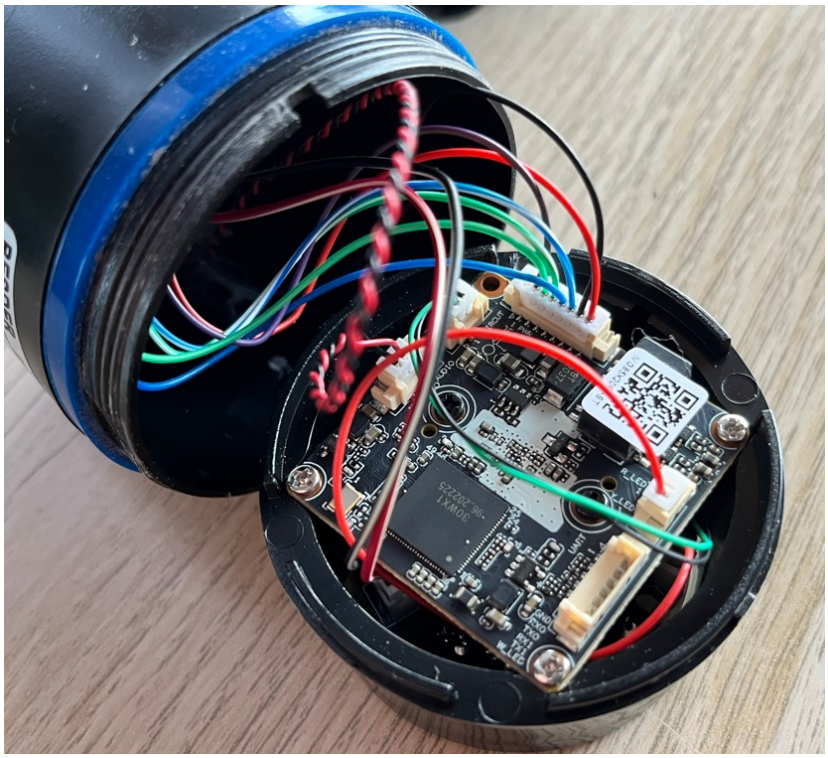
- **Shodan** – Jedná se o internetový vyhledávač pro IoT zařízení připojené k internetu (Shodan, ® 2023). Tento vyhledávač dokáže prohledávat internet a vyhledávat připojené zařízení IoT jako jsou IP kamery, tiskárny, servery a podobně. Vyhledávač může být používán po zaregistrování přes email uživatele zdarma. Pro pokročilé funkce je ale potřeba zakoupit si placenou verzi. Ta v době vypracování této diplomové práce činila $49. Shodan ale nabízí možnost registrace akademického účtu pro školní potřeby. Tento učet je aktivován po emailové žádosti na podporu prohlížeče a potvrzení, že žadatel je student. Tento akademický účet byl využit v rámci zpracovávání této práce.
- **Virtualbox** – Jedná se virtualizační nástroj, který je k dispozici zdarma a umožnuje na jednom počítací spouštět více virtuálních operačních systémů najednou. Ty mohou pracovat zároveň bez nutnosti vlastnit více fyzických počítačů. Program umožňuje nainstalovat širokou škálu operačních systémů jako Windows, Linux, MacOS a další (Virtualbox, © 2023).

6.6 Penetrační test

První část je věnována fázi sběru informací, kde je pozornost zaměřena na fyzické zařízení. Jedná se o IP kameru, která slouží k monitorování objektu zájmu uživatele. Jako taková, je kamera vystavena možnosti fyzického přístupu. Tento fakt je potřeba dále analyzovat s těmito parametry. V jakém místě je kamera umístěna, lze-li k ní například přistoupit nepozorovaně ze směru, který kamera nesnímá, nebo zda je v sérii více kamer, které se navzájem monitorují. Za předpokladu že útočník získal ke kameře fyzický přístup, zjistil toto:

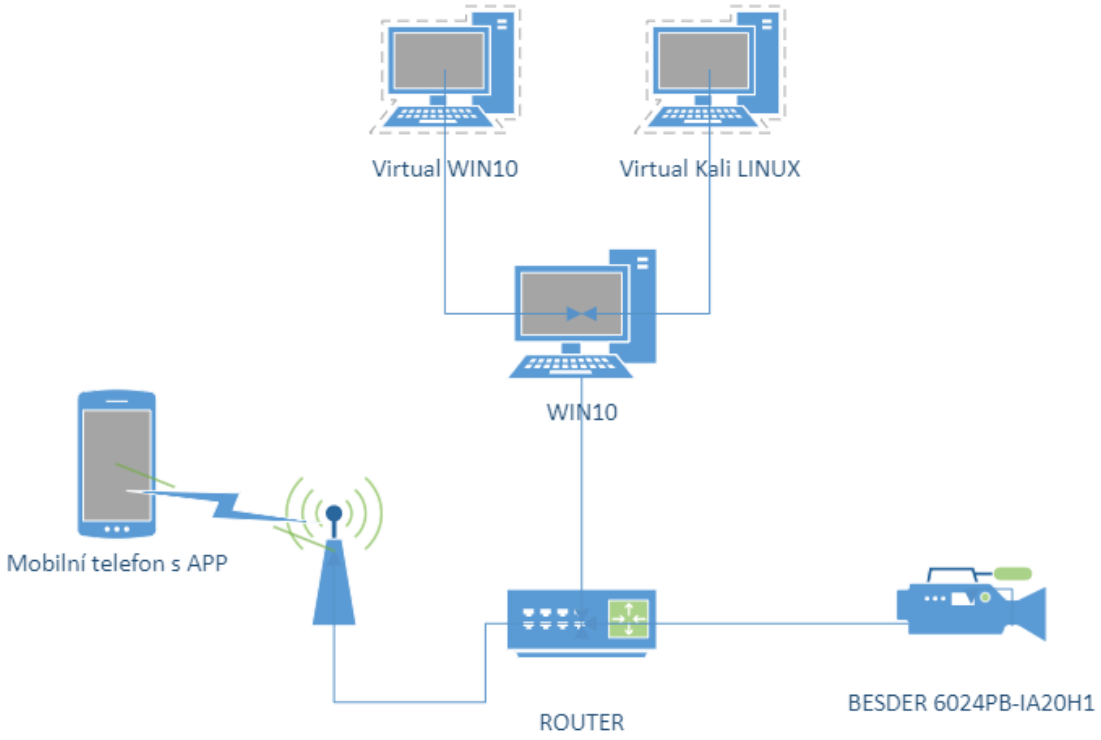
- **Jedná se o IP kameru.**
- **Má připojení pomocí Ethernet kabelu s koncovkou RJ45.**
- **Je napájena pomocí externího zdroje.**
- **Tělo kamery je z plastu a obsahuje informace o kameře, včetně označení modelu a informací o možnostech připojení.**
- **Na zadní straně se nachází mikrofon pro příjem zvuku.**
- **Neobsahuje žádné šrouby na těle kamery**

Už pouhým fyzickým přístupem může útočník provést útok „**Physical Manipulation, Damage, Theft and Loss“,** neboli IP kameru odcizit, poškodit či s ní manipulovat. Také připojením na jednotlivé páry ethernetového kabelu může útočník provádět útoky „**MitM“,** neboli Man in the Middle, kdy bez vědomí příjemce a odesílatele tuto komunikaci zachytává během přenosu. Samotné tělo lze jednoduše rozebrat bez použití nástrojů a to odšroubováním stínící přední části. Toto je zobrazeno na obrázku č. 23. Tím je schopen útočník dostat se ke vnitřním součástkám kamery i bez nástrojů. Uvnitř kamery se nachází základní deska a součástky kamery, ty jsou připojeny kabely. Ze základní desky lze vyčíst podle označení, že se jedná o základní desku společnosti Xiongmai OEM. Ta dodává součástky do více než stovky značek kamerových systémů. Deska je popsána, jde na ni přečíst, který kabel vede ke které součástce. Je zde několik portů, které nejsou připojeny a slouží k propojení s programovacím zařízením výrobce. Toto rozhraní vypadá jako rozhraní RS 232 a mohlo by být použito k připojení programovacího zařízení a k možnému nahrání nového firmware. Ten by již mohl být infikován škodlivým SW. Je zde také vidět označení jednotlivých součástek na základní desce kamery.



Obrázek 23 – Vnitřní zapojení IP Kamery (zdroj: vlastní)

Po fyzickém prozkoumání je pozornost dále věnována způsobům připojení. Zapojení pro penetrační test je znázorněno na obrázku číslo 24.



Obrázek 24 – schéma zapojení pro penetrační test (zdroj: vlastní)

Testovací zapojení se skládá z routeru, který je rozhraním WAN, připojen do sítě internetu. Do lokální sítě je připojena kamera a dále je zapojen testovací počítač s OS Windows 10, na kterém je spuštěn virtualizační nástroj VirtualBox se dvěma virtuálními počítači. Jedná se o druhý OS Windows 10, na kterém běží webová služba pro ovládání kamer a OS Kali Linux, za pomocí kterého jsou provedeny některé části penetračního testu (Mining, 2019).

Pokud využije útočník informace dostupné na štítku kamery je schopen se pokusit o připojení ke kameře skenováním IP adres na ve stejném rozhraní, takzvaný **Sniffing**. Takové skenování je na obrázku č. 25.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.1.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-02 15:42 UTC
Nmap scan report for pfsense.home.arpa (192.168.1.1)
Host is up (0.0024s latency).
Nmap scan report for 192.168.1.109
Host is up (0.0040s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.74 seconds
```

Obrázek 25 – Skenování počítačové sítě pomocí Kali Linux (zdroj: vlastní)

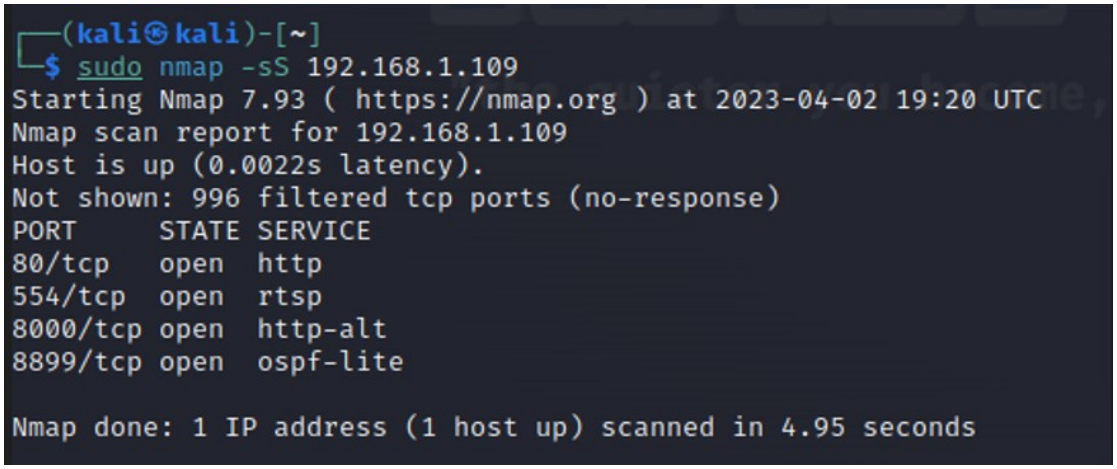
Skenování zvoleného rozsahu získáme po zadání příkazu do příkazové řádky v OS Kali Linux:

- ***nmap –sn 192.168.1.0/24***

Ze zadaného skenování bylo zjištěno, že je v sítí router 192.168.1.1 a zařízení 192.168.1.109. Toto zařízení je pravděpodobně naše kamera. Nyní zjistíme, jaké porty jsou na tomto zařízení otevřené. To zjistíme zadáním příkazu s administrátorským privilegiem „sudo“:

- ***sudo nmap –sS 192.168.1.109***

Výsledek je zobrazen na obrázku číslo č. 26, kde lze vyčíst otevřené porty.



Obrázek 26 – Skenování otevřených portů (zdroj: vlastní)

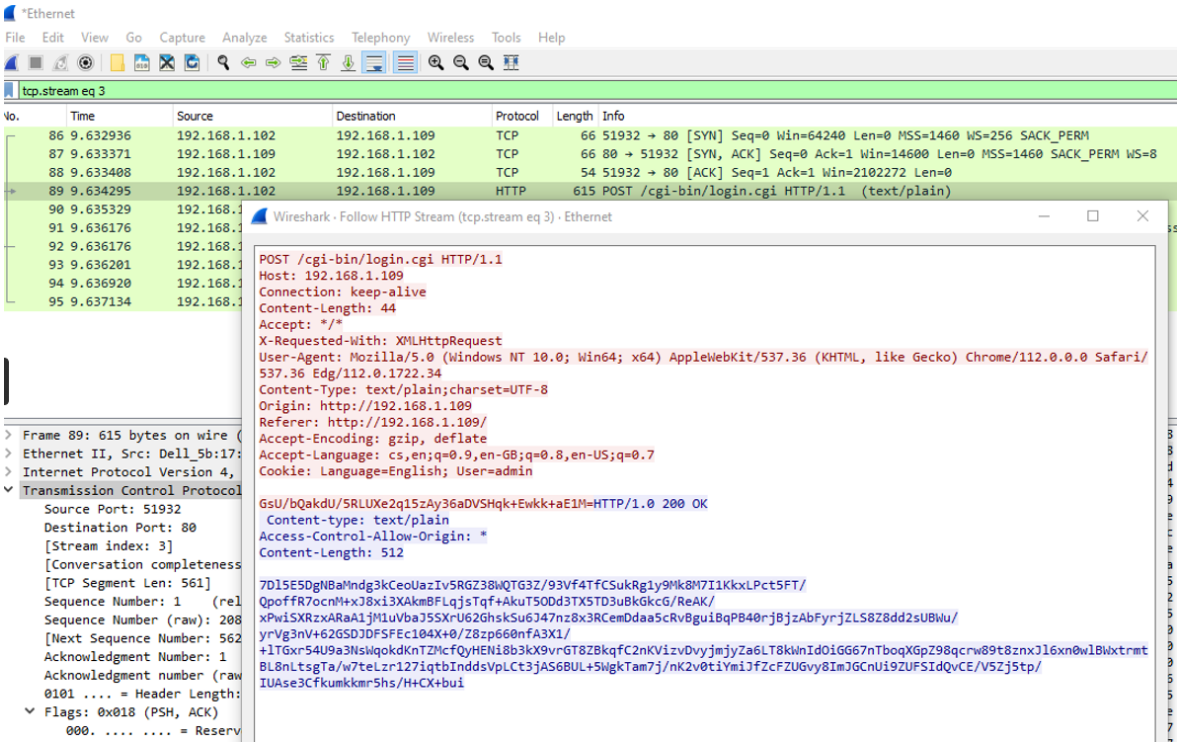
Zde lze hned z prvního zjištěného portu vyčíst jeho číslo 80, kde se jedná o port http protokolu. Protokol http přenáší data v nešifrované podobě a jedná se o webovou stránku. Zde může jít o zranitelnost nešifrovaného protokolu http. Ten neobsahuje šifrování jako v případě protokolu https, který vytváří bezpečnou cestu dat vytvořením certifikátu SSL nebo TLS. Při zadání této adresy a portu se nám zobrazí přihlašovací obrazovka kamery. (obrázek č. 20). Jedná se tedy o zařízení – IP kameru, kde je možno zkusit použít přihlašovací údaje zjištěné z těla kamery v případě, že uživatel nezměnil tato hesla. Pro další analýzu komunikace se více zaměříme na další otevřené porty. A to zadáním hlubšího vyhledávání příkazem:

- ***sudo nmap -V -sS -sV -sC -p- 192.168.1.109***

Výsledek tohoto skenování je uveden v příloze číslo I. a II. této práce. Z tohoto skenování je patrné, co jednotlivé otevřené porty dělají

- **Port 80 -** Jedná se o webový port sloužící pro nastavování kamery přes webové rozhraní.
- **Port 554** – Jedná se o RSTS stream, jde o síťový protokol přenosu dat jako audio a video v reálném čase. Kdy uživatel nemusí stahovat celý záznam, ale lze jej sledovat přímo jako tok dat. Tato IP kamera přes tento port komunikuje metodou komprese dat H264DVR rspd 1.0.
- **Port 8899** – Tento port slouží často pro komunikace kamerových zařízení se síťovými rekordéry NVR. Pří jeho použití přes tento port komunikuje SW nástroj gSOAP, který je „open source“ SW a umožnuje vzdálené volání služeb a komunikaci různých protokolů jako XML-RPC a je široce používán v aplikacích.
- **Port 34567** – Jedná se o port, na kterém běží SW služba „dhanalakshmi“, port 34567 se běžně používá pro vzdálený přístup k bezpečnostním k IP kamerám.

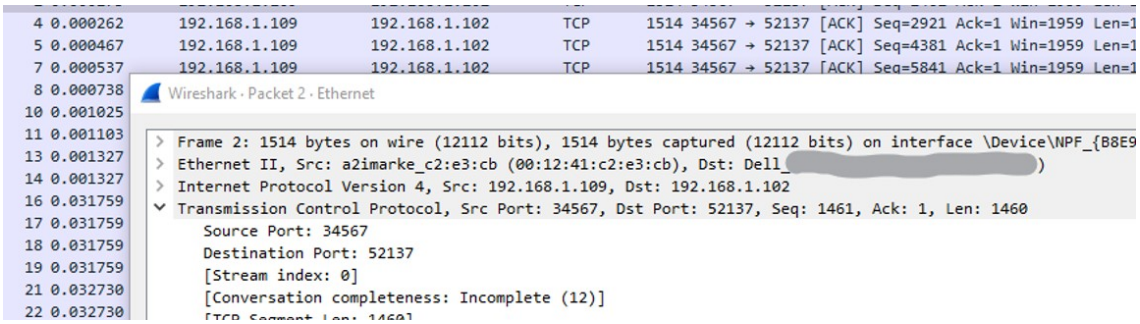
Za pomocí sestavení testovacího zapojení provedeme některé skenování komunikace přes nástroj Wireshark. První komunikace, na kterou je zaměřena pozornost, je komunikace mezi kamerou a webovým prohlížečem při zadávání hesla do aplikace. Toto je zobrazeno na obrázku číslo 27.



Obrázek 27 – Zachycená komunikace při zadávání hesla (zdroj: vlastní)

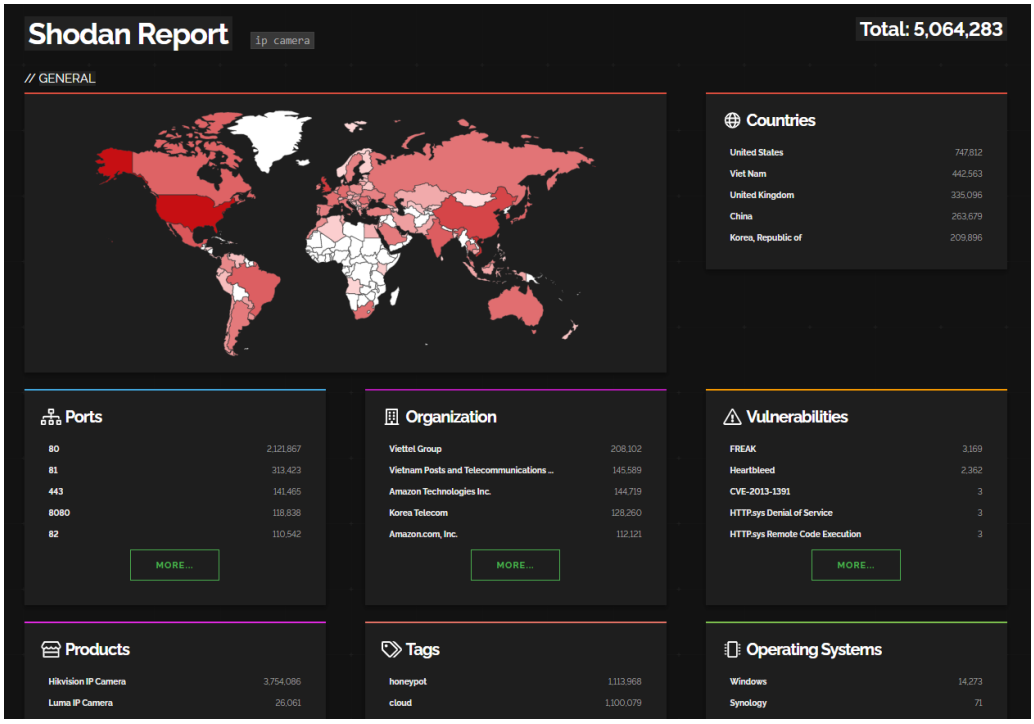
Ze zachycené komunikace je patrné, že pro přenos jména a hesla se používá „Login.cgi“ kdy se jedná o skriptovací program, který oproti databázi prověřuje přihlášení uživatele. Tento skript je možné kompromitovat a pomocí útoku silou získat přístup přes zabezpečení (Vulnerabilities in password-based login, © 2023). Dále na řádku „Cookie“ je parametr jazyku vedený u uživatele „admin“. Tím je možno zjistit jakým uživatelským jménem se učet zrovna přihlašuje.

Druhou částí je komunikace na Portu 34567. Zde slouží pro přenos RTSP přenosu mezi webovou aplikací kamery a IP kamerou, jako cílový port je 52137, což není specifický port. Tento port je volný a různé aplikace jej využívají pro různé účely. Přenos je zobrazen na obrázku číslo 28.



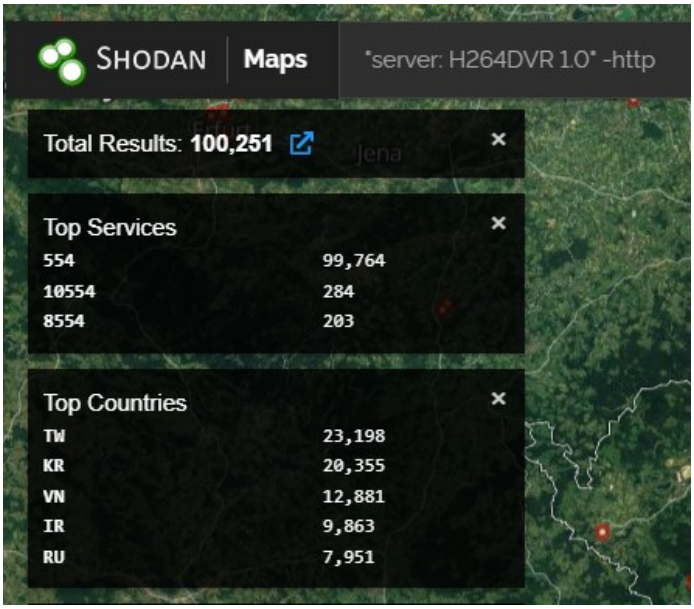
Obrázek 28 – Přenos mezi IP kamerou a ovládacím PC (Zdroj: vlastní)

V předposlední části testu se zjišťují známé skutečnosti o zranitelnostech za pomocí vyhledávače Shodan. Při vyhledání obecného názvu „IP camera“ eviduje vyhledávač Shodan přes 5 milionu zařízení které komunikují do internetu a přes 2 miliony zařízení komunikuje na portu 80, což je webové rozhraní. Jednoznačně je nejvíce připojených kamer společnosti Hikvision a to přes 3,7 milionu. Report z Shodan na IP kamery je na obrázku 29.



Obrázek 29 – Vyhledání IP kamer v Shodan (Zdroj: vlastní)

Port 554, ze zjištění zranitelnosti obsahuje zmínku o RSTP přenosu „H24DVR 1.0“. Tento typ komprese byl zadán do Shodan a výsledkem bylo zjištěno přes 100 000 zařízení, které celosvětově vysílají tímto protokolem. V České republice bylo v době provádění testu zjištěno 158 subjektů. Některé subjekty na otevřených portech vysílají obraz, nezabezpečený heslem ani žádnou další ochranou. Každý, kdo tento parametr zadá, tak vidí zahrady, kanceláře, provozovny, prodejny, parkoviště a jiná soukromá místa. (Obrázek č. 30)



Obrázek 30 – Vyhledání RSTS přenosu na portu 554 (zdroj: vlastní)

U vyhledaných zařízení Shodan, v případě již nalezené zranitelnosti, vypíše přímo zjištěnou zranitelnost, označenou písmeny CVE a číslem zranitelnosti. Tyto zranitelnosti jsou spravovány organizací MITRE a pravidelně doplňovány. Jacob Baines na blogu VulnCheck, věnovaném odhalování těchto zranitelnosti s použitím HW od Xiaongmai, uvádí několik případu velmi závažných až kritických zranitelností. Tyto zranitelnosti jsou z důvodu omezení rozsahu práce pouze vypsány a nebude za jejich pomoci proveden žádný další test (Baines, © 2023):

- CVE-2017-7577: Unauthenticated HTTP request path traversal resulting in arbitrary file and credential disclosure.
- CVE-2018-10088: Unauthenticated and remote HTTP login request stack-based buffer overflow.
- CVE-2020-22253: Port 9530 debug interface that allowed an unauthenticated attacker to open a telnet.
- CVE-2021-41506: Port 9527 debug interface that allows an attacker using default credentials to execute arbitrary operating system commands (technically speaking, the wording of the CVE could include CVE-2020-22253 / port 9530).
- CVE-2022-26259: Unauthenticated and remote RTSP parsing stack buffer overflow.

- CVE-2022-45045: Authenticated and remote command execution via port 34567 upgrade logic.
- CVE-2022-45460: Unauthenticated and remote HTTP request URI parsing stack-based buffer overflow.

6.7 Shrnutí penetračního testu

Vybrané IoT zařízení IP kamera Besder model 6024PB-IA20H1 2.0MP, obsahuje několik kritických zranitelností. Z identifikace rizik bylo identifikováno, že jedna z nejzávažnějších zranitelností je „**Physical Manipulation, Damage, Theft and Loss“**, neboli fyzická manipulace se zařízením, krádež a ztráta. Z testu vyplynulo, že hrozba je reálná a zařízení obsahuje několik zranitelností shrnutých v tabulce č12.

Tabulka 12 – Přehled zjištěných zranitelností penetračního testu (zdroj: vlastní)

Zranitelnost	**Druh útoku, který hrozí**
Napájení adapterem	Physical Manipulation, Damage, Theft and Loss
Nevhodné umístění	Physical Manipulation, Damage, Theft and Loss
Fyzická bezpečnost zařízení	Physical Manipulation, Damage, Theft and Loss
Označení výrobce s daty k připojení	Physical Manipulation, Damage, Theft and Loss, Krádež identity
Jednoduchá možnost demontáže	Sniffing
Základní připojení bez hesla	Krádež identity
Komunikace na portech	Sniffing Krádež identity, Narušení bezpečnosti dat, DDoS, MitM
http protokol	Sniffing Krádež identity, Narušení bezpečnosti dat, MitM
Přihlašovací skript	Krádež identity, Narušení bezpečnosti dat

Nutnost instalace SW z neprověřeného zdroje při prvním připojení	Narušení bezpečnosti dat, botnet, Ransomware, Malware
Známé zranitelnosti CVE	Známé zranitelnosti CVE DDoS, Únik informací, botnet, MitM
Použití slabých hesel	Krádež identity, Únik informací

V části testu komunikace bylo zjištěno, že je přes otevřený port 80 vedena nezabezpečená komunikace pomocí protokolu http. Obsahuje sice další již složitější formy ověřování autorizace uživatele, ale i tyto formy potvrzení přes skriptovací program „Login.cgi“ již jsou dnes zranitelné pomocí útoku hrubou silou. V obou případech se jedná o zranitelnost autorizace. Komunikace webové služby a kamery probíhá přes port 34567. Komunikace je sice zabezpečena šifrováním, ale průzkum známých zranitelnosti již odhalil zranitelnost tohoto portu. Jedná se však o složitější formy útoku, které nejsou zahrnuty do tohoto testu. Hrozí však útoky typu „**výpadky systému**“, **„DDoS“, „Sniffing“, „Krádež identity“, „Narušení bezpečnosti dat“, „Únik informací“** a útoky sítě **„botnet“**. Při práci s vyhledávačem IoT Shodan bylo potvrzeno, že jedna ze základních zranitelností je hrozba autorizace a porušení, nebo neexistence bezpečnostní politiky subjektu. Uživatelé používají standartní hesla výrobce nebo nepoužívají hesla vůbec. Uživatelé také nemají definovány pravidla pro práci se systémy, jejích údržbu, zálohu a obnovu po kybernetických útocích.

7 NÁVRH OPATŘENÍ KE ZLEPŠENÍ STAVU

V předchozích dvou kapitolách praktické části této akademické práce byla identifikována rizika, která můžou působit na prvek IoT, konkrétně na IP kameru. V hodnocení rizik byla identifikována nejvýznamnější rizika a provedeným základním penetračním testem bylo prokázáno, že tyto rizika jsou reálna. Tato kapitola se bude zaměřovat na praktický návrh na zlepšení opatření k zlepšení kybernetické bezpečnosti. A to formou návrhu k ošetření těchto nejvýznamnějších rizik, na nasazení kamer testovaných v této práci na rodinném domě.

7.1 Fyzický přístup k zařízení

Identifikované hrozba fyzického přístupu neoprávněné osoby k zařízení má dle analýzy rizik a provedeného penetračního test několik závažných zranitelností. Identifikované rizika nelze z hlediska ošetření rizik ani přijmout ani zcela eliminovat. Neboť jejich pravděpodobnost a následky, které z hrozby plynou, jsou vysoké. Reálné se tedy jeví jen jejích snaha o snižování. V případě zranitelnosti fyzického přístupu je potřeba zajištění fyzického prostoru, kde je kamera umístěna. Zejména těmito opatřeními:

- **Umístění** – IP kamera by měla být instalována v takové výšce, aby bylo znemožněno na ni dosáhnout bez použití pomůcek (židle, schůdky, žebřík apod.). Na následujícím obrázku č. 31 je zobrazen návrh umístění kamer, které se nachází 3 metry od země.

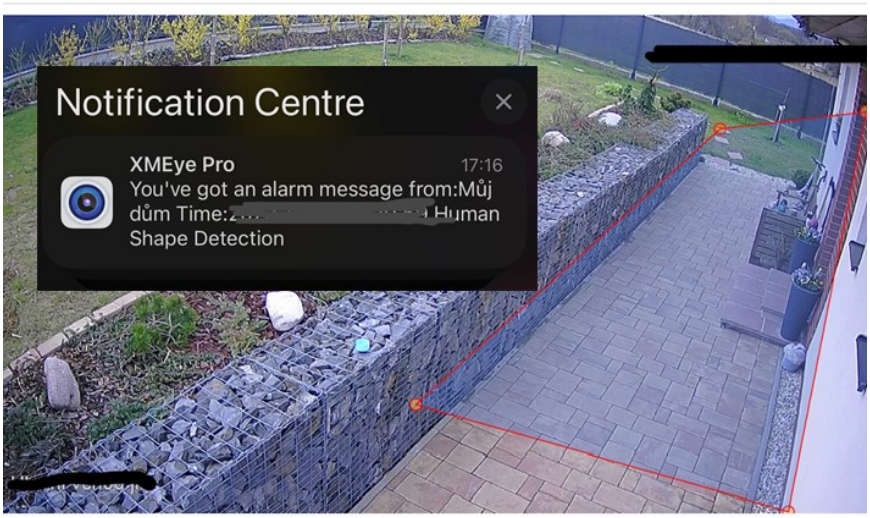
Obrázek 31 – Návrh umístění kamer (Zdroj: vlastní)

V zobrazeném umístění kamer je patrná odpadní roura na odvod vody ze střechy. I přes to, že se jedná o relativně nepravděpodobné, že by se útočník pokusil o přístup ke kamerám, je toto ošetřeno dalším bodem.

- **Prostor** – Pro instalaci bezpečnostních IP kamer je potřeba počítat s prostorem, který tyto kamery budou zaznamenávat. Je potřeba pokrytí zájmového prostoru a zároveň je ideální, pokud jsou kamery umisťovány ve vzájemném krytí. Tím je rozuměno, že každá kamera je snímána jinou, která snímá záznamem její umístění pro detekci manipulace s kamerou. Na obrázku číslo 32 je zobrazen obraz dvou kamer (označeny šipkou), které jsou takto umístěny, lze vidět noční svit z IR přísvitu, a jsou tak navzájem kontrolovány.

Obrázek 32 – Vzájemné umístění kamer (Zdroj: vlastní)

Zároveň je aktivována chytrá funkce kamer, a to monitorování vyhrazených zón. Pokud vstoupí osoba do vymezeného prostoru, je automaticky zasláno upozornění na aplikaci XMEYE uživatele. Toto je zobrazeno na obrázku číslo 33.



Obrázek 33 – Hlídání pohybu osob v zónách (Zdroj: vlastní)

- **Obal** – V případě, že by kamery nemohly být umístěny na nedostupné místo, měli by být zhodnoceny z hlediska jejich konstrukce a umísťován do ochranného obalu. Ty znemožňují přímý kontakt s kamerou. V případě modelového zapojení nebylo potřeba toto realizovat.
- **Vedení dat** – Datové spoje jako je kabel UTP je nutno vést mimo dosah osob, pro znemožnění manipulace s těmito vodiči. Měly by být pravidelně kontrolovány po celé své délce a v místech kde toto nelze by měly být vedeny v ochranných krytech. V případě modelového zapojení jsou vedeny skrytě v prostorech podbití střechy a nejsou přístupné.
- **Vrstvení ochrany** – Kamerové systémy by měly být zapojeny do procesu ochrany objektu. Při umísťování důležitých částí kamerového systému jako je například NVR síťové uložiště je potřeba pro toto místo zabezpečit režim vstupu pro neoprávněné osoby. Umístění kamerového systému bylo tedy umístěno do půdních prostor, ke kterému je přístup pouze skrze uzamykatelné dveře, opatřené bezpečnostním zámkem. Objekt je oplocen 2 metry vysokým skládaným betonovým plotem.
- **Napájení a záloha napájení** – Systém napájení kamer by měl být postaven ideálně na technologii PoE, tím je ke kameře přivedeno napájení skrze kabel typu UTP. Je proto v případě nasazená potřeba volit kamery, které to umožnují. Toto napájení je zobrazeno na obrázku číslo 33. kde je zobrazen PoE switch.

Obrázek 34 – PoE Switch (Zdroj: vlastní)

Ten zabezpečuje napájení kamer z jednoho místa, bez potřeby tažení napájecího kabelu ke kamerám. Centralizací napájení můžeme poté, v případě výpadku proudu celý systém napájet použitím UPS záložního zdroje, pro případ výpadku proudu (obrázek č. 34).

Obrázek 35 – Záložní zdroj UPS (Zdroj: vlastní)

Záloha elektrické energie by měla zajistit napájení při výpadku elektrické energie, pro další důležité systémy pro provoz IP kamer. V našem případě se jedná o optický převodník poskytovatele internetu, router a PoE switche.

7.2 Autorizace a Autentizace

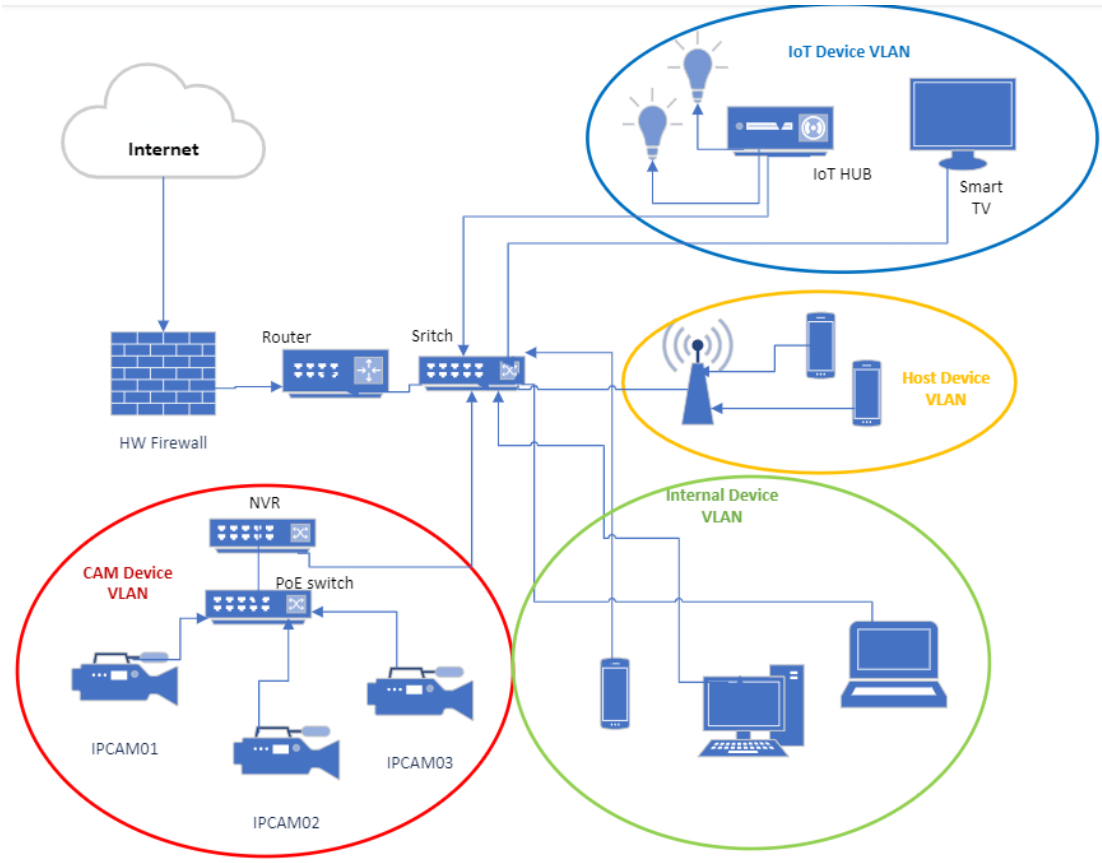
Autorizace a autentizace je v kterémkoliv systému stěžejním prvkem. Pravidla pro tvorbu hesel jsou již uživatelům známá, avšak je často uživatelé nedodržují. Používat rozdílná hesla pro jednotlivé systémy, čímž se eliminuje možnost kompromitace více systému v případně úniku. Heslo by mělo být dlouhé, ideálně 12 a více znaků, s použitím velkých malých písmen, číslic a speciálních znaků. Je tedy potřeba nastavit silná hesla nejen na NVR rekordér, ale i na jednotlivé kamery. Po správné autentizaci je potřeba zajistit i autorizaci uživatelů. V případě použitého SW pro správu IP kamery BESDER je již možnost nastavit více uživatelských účtů a jednotlivá práva k přístupu k datům a nastavením. Je tedy možné nastavit roli uživatele, který bude mít přístup do programu, jen pro možnost monitoringu kamer. Za obvyklé je dnes použití certifikátů PKI (Private Key Infrastructure) ve správě IoT. Ty zajistí, že každý přenos bude zašifrován. V současné době obsahují nové zařízení IoT stále více použitých zabezpečení typu PKI a kryptografických metod. Což může být ukazatelem zodpovědného přístupu výrobce zařízení IoT. V modelovém příkladu nasazení kamer však tyto funkce kamery nepodporují, proto jej zde nebudou realizovány.

7.3 Bezpečnostní politika, postupy a procesy

Za zásadní opatření je dnes nutné nastavení pravidel, které definují IoT zařízení od jeho plánování, výroby, nasazení a likvidací. Zavedení ISMS muže být jedním z nich. Toto je ekonomicky a procesně těžko realizovatelné v případě nasazení v malé firmě nebo rodinném domě. Ale i u malého subjektu lze nastavit pravidla pro bezpečný provoz a procesy, pomocí kterých se bude postupovat v každodenním užití ICT systémů i minimalizovat rizika. Tyto pravidla, které by měla obsahovat například:

- **Řízení přístupu** – Jak již bylo zmíněno u autentifikace a autorizace, je potřeba nastavit mechanismus práv uživatelů, správců systému a rovněž za jakých podmínek a jakým způsobem budou do systému přistupovat.
- **Zero Trust** – Princip nulové důvěryhodnosti neboli přístup k otázce důvěry. Pro modelové nasazení kamer bude toto řešeno právě určením práv uživatele a správce. Dále bude přístup k umístění technologii v půdním prostoru trvale uzamčen a jen správce bude mít klíč.

- **Need to know** – Princip, že každý uživatel má mít jen takové informace, které jsou nezbytné pro výkon jeho práce v systému. A zařízení nemá přístup v síťové struktuře do celého systému. To bude ošetřeno segmentací v dalším bodě.
- **Segmentace –** Systémy by měly být odděleny podle jednotlivých úrovní a druhů z hlediska přístupu. Tím je zajištěna ochrana při napadení jednoho segmentu izolací od ostatních. Jako příklad si při ošetření rizik definujeme možné rozdělení sítí, ve kterých je IoT kamerový systém. Návrh segmentace pro systémový model použitý v předchozí kapitole práce je znázorněn na obrázku číslo 36.



Obrázek 36 – Segmentace sítě za pomocí VLAN (zdroj: vlastní)

Zde jsou jednotlivé rozhraní pojmenovány jako **„Internal Device VLAN“,** neboli důvěryhodné zařízení (servery, počítače, mobilní telefony). Dále jsou v síti **„IoT Device VLAN“**, pod které spadají chytré zařízení. Pomocí **„Host Device VLAN“**, se připojují do sítě nepravidelní uživatelé a hosté, například pro připojení Wi-Fi internet. Poslední rozhraní je **„CAM Device VLAN“**, které obsahuje IP kamery a NVR. Mezi jednotlivými částmi je aktivována zmíněná technologie VLAN neboli

virtuální lokání oddělené sítě. Ty umožnují na stejném zařízení typu switch, provozovat několik navzájem oddělených sítí. Každá z těchto sítí má své vlastní pravidla pro přenosy souboru. Tím je docíleno toho, že útočník připojený přes IP kameru nemůže skenovat celou síť organizace, ale jen úzký okruh zařízení na daném segmentu VLAN.

Procesy aktualizací – Jako jedna ze základního procesu každé organizace, by měla být nastavena přísná politika aktualizací všech systému a firmware. Ovládací systém kamer nabízí automatické aktualizace, které sám provádí v předem nastaveném čase. Je na správci systém toto kontrolovat.

- **Plán zálohování a obnovy** – Zálohování dat je jeden ze základních předpokladů práce s daty. Pravidelné zálohování by mělo probíhat na více než jedno místo pro snížení rizika poškození, nebo ztráty dat.

Obrázek 37 – Vnitřní uložení záložního disku pro kamerové záznamy (Zdroj: vlastní)

V případě použití NVR je možno k němu přímo připojit pevný disk, který bude zálohovat data po dobu až jednoho týdne. Toto je zobrazeno na obrázku č. 37. Zároveň se záznamy ukládají na uživatelský účet na Cloudovém uložišti aplikace XMEYE.

ZÁVĚR

Internet věcí je dnes jedním z nejvíce rozšiřujících se odvětví zařízení připojených do internetu. Jeho správně zabezpečená kybernetická bezpečnost je předpokladem úspěšného použití, bez ohledu na oblast implementace. Diplomová práce řešila kybernetickou bezpečnost vybraného prvku IoT, chytré IP kamery. Cíle práce, zvýšit úroveň kybernetické bezpečnosti vybraného prvku internetu věcí, cenově dostupné chytré kamery, při jejím nasazení v modelové instalaci u rodinného domu, byly splněny. K dosažení tohoto cíle byla v této diplomové práci zpracována literární rešerše současného stavu a rešerše stavu legislativy na národní i mezinárodní úrovni. Za pomocí metody analýzy příčin a následků Ishigawa byly definovány jednotlivé faktory, vedoucí k možnému kybernetickému ohrožení prvku IoT. Mezi tyto faktory se zařadili lidé, hardware, software, prostředí, procesy a kybernetické útoky. Na základě roztřízení do těchto faktorů byly jednotlivé hrozby definovány a hodnoceny pomocí metodou PNH. V diplomové práci byl tedy sestaven systémový model útoku, a to za pomocí provedení penetračního testu vybraného zařízení, IP kamery Besder. Penetrační test odhalil několik závažných zranitelností, které byly ve shodě s provedenou analýzou rizik. Potvrdilo se, že při použití zařízení se základním stupněm zabezpečení a nesprávným nastavením, je IP kamera vystavena riziku kybernetických útoků. Tím se potvrdil i předpoklad testu, definovaný v metodách práce. Mezi nejvýznamnější rizika, která byla výsledkem analýzy a penetračního testu jsou hrozby fyzického přístupu k zařízení, selhaní procesu autorizace a autentizace a porušení procesu, či neexistence bezpečnostní politiky. Výše zmíněným byly naplněny i dílčí cíle této diplomové práce. Přínosem práce je provedená analýza rizik na vybraný prvek, provedení penetračního testu a návrh opatření ke zlepšení současného stavu nasazeného modelu chytrých kamer. V době psaní této diplomové práce je odbornou i laickou veřejností řešen význam výrazného rozvoje umělé inteligence a její vliv na společnost. S tím se pojí i její vliv na odvětví internetu věcí. Je otázkou, jak moc bude umělá inteligence provázána s internetem věcí. Dnes se dá minimálně předpokládat její zapojení do řízení procesů v průmyslu a integrace do asistentů chytrých domácností. Nadále bude potřeba dalších analýz kybernetické bezpečnosti, ke zjištění na kolik bude schopna umělá inteligence řešit výzvy zajištění kybernetické bezpečností internetu věcí.

SEZNAM POUŽITÉ LITERATURY

150,000 Verkada security cameras hacked—to make a point, © 2023. *Malwarebyte* [online]. Malwarebytes [cit. 2023-04-18]. Dostupné z: https://www.malwarebytes.com/blog/news/2021/03/150000-verkada-security-cameras-hacked-to-make-a-point.

Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025 [online], 2021. Brno: NÚKIB [cit. 2023-04-18]. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/akcni_plan_2021-2025.pdf.

Alexa Smart Home [online], © 1996-2023. Amazon [cit. 2023-04-18]. Dostupné z: https://www.amazon.com/alexa-smart-home/b?ie=UTF8&node=21442899011&ref=pe_alxhub_aucc_en_us_IC_HP_1_HUB_SMA.

AO KASPERSKY LAB, 2023. Black hat, White hat, and Gray hat hackers – Definition and Explanation. *Kaspersky* [online]. [cit. 2023-04-18]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/hacker-hat-types.

BAINES, Jakob, © 2023. *Xiongmai IoT Exploitation* [online]. VulnCheck [cit. 2023-04-18]. Dostupné z: https://vulncheck.com/blog/xiongmai-iot-exploitation.

ČESKO, 1998. *Ústavní zákon č. 110/1998 Sb. o bezpečnosti České republiky*. In:. ČR: Sbírka zákonu ČR, ročník 1998, částka 39, číslo 39. Dostupné také z: https://www.zakonyprolidi.cz/cs/1998-110/zneni-20001201.

ČESKO, 2000. *Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon)*. In:. Sbírka zákonů České republiky, částka 73, 240/2000. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-240.

ČESKO, 2014. *Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. In:. Sbírka zákonu ČR, ročník 2014, částka 75, číslo 181. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181.

ČESKO, 2018. *Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti*

a likvidaci dat (vyhláška o kybernetické bezpečnosti). In:. ČR: Sbírka zákonu ČR, ročník 2018, částka 43, 82/2018. Dostupné také z: https://www.zakonyprolidi.cz/cs/2018-82.

Doporučení k používání protokolu TLP ke sdílení chráněných informací, 2022. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno: NÚKIB [cit. 2023-04-18]. Dostupné z: https://nukib.cz/cs/infoservis/doporuceni/1593-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci/.

ENISA, 2017. *Baseline Security Recommendations for IoT: in the context of Critical Information Infrastructures* [online]. European Union Agency for Network and Information Security [cit. 2023-04-18]. ISBN 978-92-9204-236. Dostupné z: doi:10.2824/03228.

EU, 2016a. *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679: o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. In:. Evropský parlament, Rada Evropské unie. Dostupné také z: https://www.zakonyprolidi.cz/pravoeu/dokument?celex=32016R0679.

EU, 2016b. *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/1148 ze dne 6. července 2016: o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii*. In:. Evropský parlament, Rada Evropské unie. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016L1148.

EU, 2019. *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2019/881: o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost"), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti")*. In:. Evropský parlament, Rada Evropské unie. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:32019R0881.

EU, 2022. *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2555ze dne 14. prosince 2022: o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)*. In:. Evropský parlament, Evropská Rada. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32022L2555&from=CS.

EVANS, Lester, 2019. *Cybersecurity: What You Need to Know About Computer and Cyber Security, Social Engineering, The Internet of Things + An Essential Guide to Ethical Hacking for Beginners*. Bravex Publications. ISBN 978-1-4842-4300-8.

Google Home [online], 2023. Google [cit. 2023-04-18]. Dostupné z: https://home.google.com/what-is-google-home/.

GUPTA, Aditya, 2019. *The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things*. Apress, Berkeley, CA. ISBN 978-1-4842-4300-8.

Home app, © 2023. *Apple* [online]. Cupertino: Apple [cit. 2023-04-18]. Dostupné z: https://www.apple.com/home-app/.

Home Assistant [online], © 2023. Home Assistant [cit. 2023-04-18]. Dostupné z: https://www.home-assistant.io/.

Ishikawův diagram, © 2011-2023. *Management mania* [online]. Wilmington: ManagementMania [cit. 2023-04-18]. Dostupné z: https://managementmania.com/cs/ishikawuv-diagram

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2013. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze. ISBN 978-80-7251-397-0.

JIROVSKÝ, Václav, 2007. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada. ISBN 978-80-247-1561-2.

KERR, Dara, © 2023. FTC and TrendNet settle claim over hacked security cameras. *CNET* [online]. CNET, a Red Ventures company. [cit. 2023-04-18]. Dostupné z: https://www.cnet.com/news/privacy/ftc-and-trendnet-settle-claim-over-hacked-security-cameras/

KOLOUCH, Jan a Pavel BAŠTA, 2019. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-80-88168-31-7.

KOZUBEK, Michael, 2018. *Zhodnocení možných rizik kybernetických útoků a jejich hrozba v krizovém řízení*. Zlín. Bakalářská práce. Univerzita Tomáš Bati ve Zlíně. Vedoucí práce Jiří Dvořák.

LAU, Phooi Yee et al., 2019. A real time aggressive human behaviour detection system in cage environment across multiple cameras. *International Journal of Computational Vision and Robotics* [online]. **9**(5) [cit. 2023-04-18]. ISSN 1752-9131. Dostupné z: doi:10.1504/IJCVR.2019.102287.

MINING, Ethem, 2019. *Kali Linux Hacking: A Complete Step by Step Guide to Learn the Fundamentals of Cyber Security, Hacking, and Penetration Testing. Includes Valuable Basic Networking Concepts*. Independently published. ISBN 978-1672429733.

Národní strategie kybernetické bezpečnosti České republiky na období let 2021 – 2025 [online], 2020. Brno: NÚKIB [cit. 2023-04-18]. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/akcni_plan_2021-2025.pdf.

NÚKIB: Povinné osoby [online], 2023. Brno: Nárosní úřad pro kybernetickou a informační bezpečnost [cit. 2023-04-15]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/povinne-osoby/.

Offensive Security [online], © 2023. OffSec Services Limited [cit. 2023-04-18]. Dostupné z: https://www.offsec.com/category/offsec/.

Phillips [online], © 2004 - 2023. Koninklijke Philips N.V. [cit. 2023-04-18]. Dostupné z: https://www.philips.cz/c-p/SCD923_26/p%C5%99ipojen%C3%BD-p%C5%99ipojen%C3%BD-d%C4%9Btsk%C3%BD-monitor.

SEDLÁK, Petr a Martin KONEČNÝ, 2021. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství. ISBN 9781647481742.

SERPANOS, Dimitrios a Marilyn WOLF, 2018. *Internet-of-Things (IoT) Systems: Architectures, Algorithms, Methodologies*. Springer International Publishing. ISBN 978-3-319-69714-7.

Shenzhen Besder Technology Co., © 1999-2023. *Alibaba* [online]. Alibaba.com [cit. 2023-04-18]. Dostupné z: https://besdertech.en.alibaba.com/company_profile.html?spm=a2700.shop_index.88.42.66145909Rmibbl.

Shodan [online], ® 2023. Shodan [cit. 2023-04-18]. Dostupné z: https://www.shodan.io/dashboard

SPIVEY, Dwaight, 2015. *Home Automation For Dummies*. New Jersey: John Wiley. ISBN 978-1-118-94927-6.

ŠEFČÍK, Vladimír, 2009. *Analýza rizik*. Zlín: Univerzita Tomáše Bati ve Zlíně. ISBN 978-807-3186-968.

VAILSHERY, Lionel Sujay, 2022. Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030. *Statista* [online]. Statista [cit. 2023-04-18]. Dostupné z: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

Velitelství informačních a kybernetických sil, 2021. *Armáda České republiky* [online]. Praha: MO ČR [cit. 2023-04-18]. Dostupné z: https://acr.army.cz/struktura/generalni/kyb/velitelstvi-kybernetickych-sil-a-informacnich-operaci-214169/.

Virtualbox [online], © 2023. Oracle [cit. 2023-04-18]. Dostupné z: https://www.virtualbox.org/.

Vulnerabilities in password-based login, © 2023. *PortSwigger* [online]. PortSwigger [cit. 2023-04-18]. Dostupné z: https://portswigger.net/web-security/authentication/password-based.

WIENER, Norbert, 1960. *Kybernetika neboli řízení a sdělování v živých organismech a strojích*. Praha: Státní nakladatelství technické literatury. Řada teoretické literatury.

Wireshark [online], © 2023. Wireshark Foundation [cit. 2023-04-18]. Dostupné z: https://www.wireshark.org/.

Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021 [online], 2022. Brno: NÚKIB [cit. 2023-04-18]. Dostupné z: https://nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kybernetick_bezpenosti_2021.pdf.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

2FA	Two face autentization
5G	Síť mobilních operátorů páté generace
A	Ampér
CCTV	Closed Circuit Television
CIA	Confidentiality Integrity Availability
CISO	Chief Information Security Officer
CSIRT	Computer security Incident Responce Team
ČSN	Česká státní norma
DDoS	Distributed Denial of Service
DNS	Domain Name Service
EU	Evropská unie
GDPR	General Data Protection Restriction
HD	Hight Definition
HDP	Hrubý domácí produkt
http	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
Hz	Hertz
ICT	Information Computer Technology
IEC	International Electrotechnical Commission
IIoT	Industrial Interneto of Things
IoT	Internet of Things
IP	Internet Protocol
IPXX	Ingress Protection
IR	Infra Red

ISMS	Information Security Management
ISO	International Organization for Standartization
IT	Information technology
KB	Kybernetická bazpečnost
KII	Kritická informační infrastruktura
LED	Ligth Emitting Diode
LTE-M	Long Term Evolution - Machines
Mbps	Megabit za sekundu
MIPI	Mobile Industry Processor
MitM	Man in the Middle
MP	Megapixel
NAS	Network-Attached Storage
NATO	North Atlantic Treaty Organization
NFC	Near Field Communication
NIS	Směrnice Evropského Parlamentu a Rady (EU) 2016/1148
NIST	National Institute
NÚKIB	Národní úřad kybernetické a informační bezpečnosti
NVR	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OS	Operační systém
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PNH	Příčina, následky, hodnocení
PoE	Power over Ethernet
RFID	Radio Frequency Identification
RSTS	Real Time Streaming Protocol

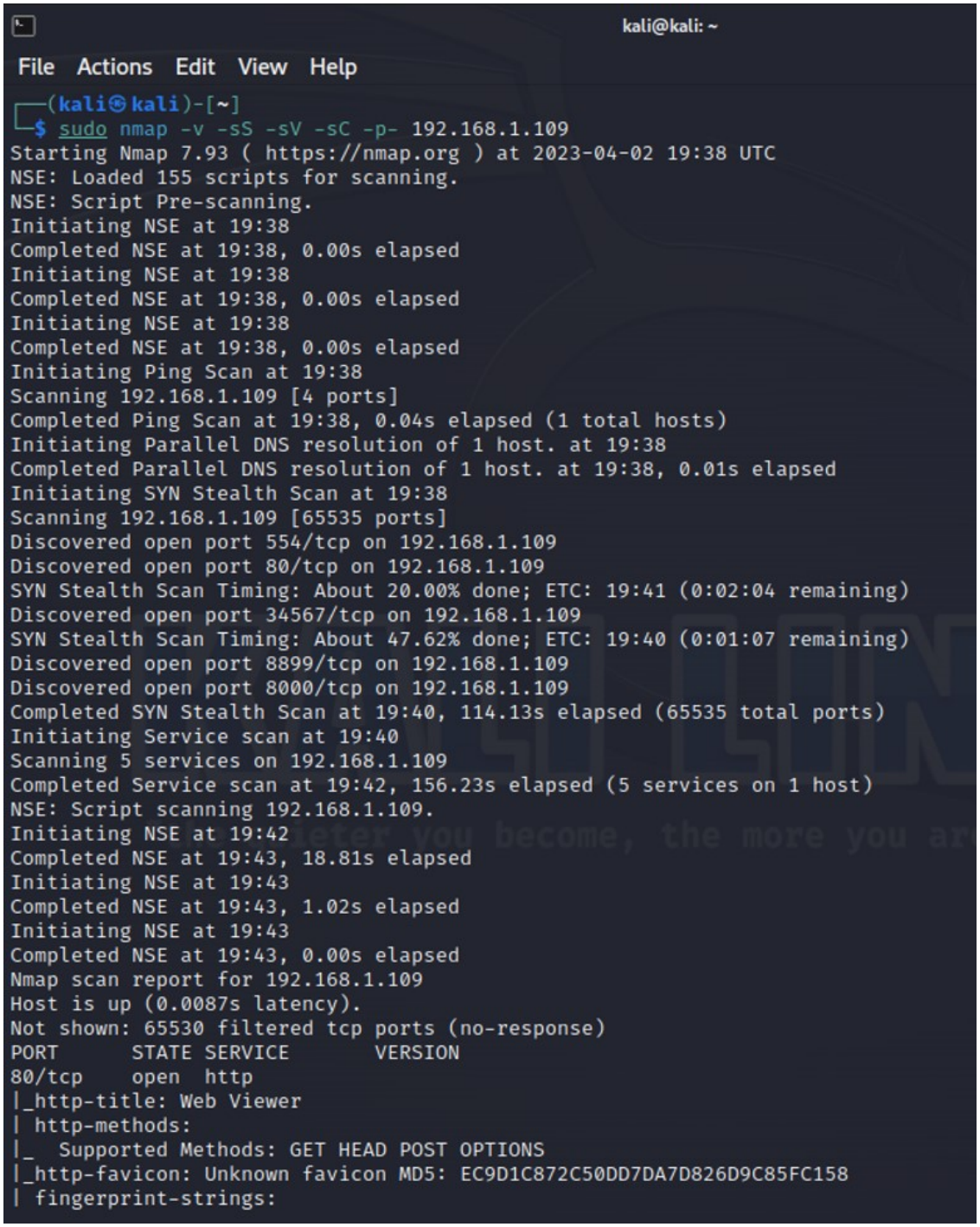
SPI	Serial Peripheral Interface
SQL	Structured Query Language
SW	Software
TB	Terabyte
TCP	Transmission Control Protocol
TLP	Tuning Linux Power Management
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
USA	Spojená státy Americké
USB	Universal Seriál Bus
UTP	Unshielded Twisted Pair
V	Volt
VIS	Významné informační systémy
VLAN	Virtual Local Area Network
XSS	Cross-Site Scripting
ZKB	Zákon o kybernetické bezpečnosti

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

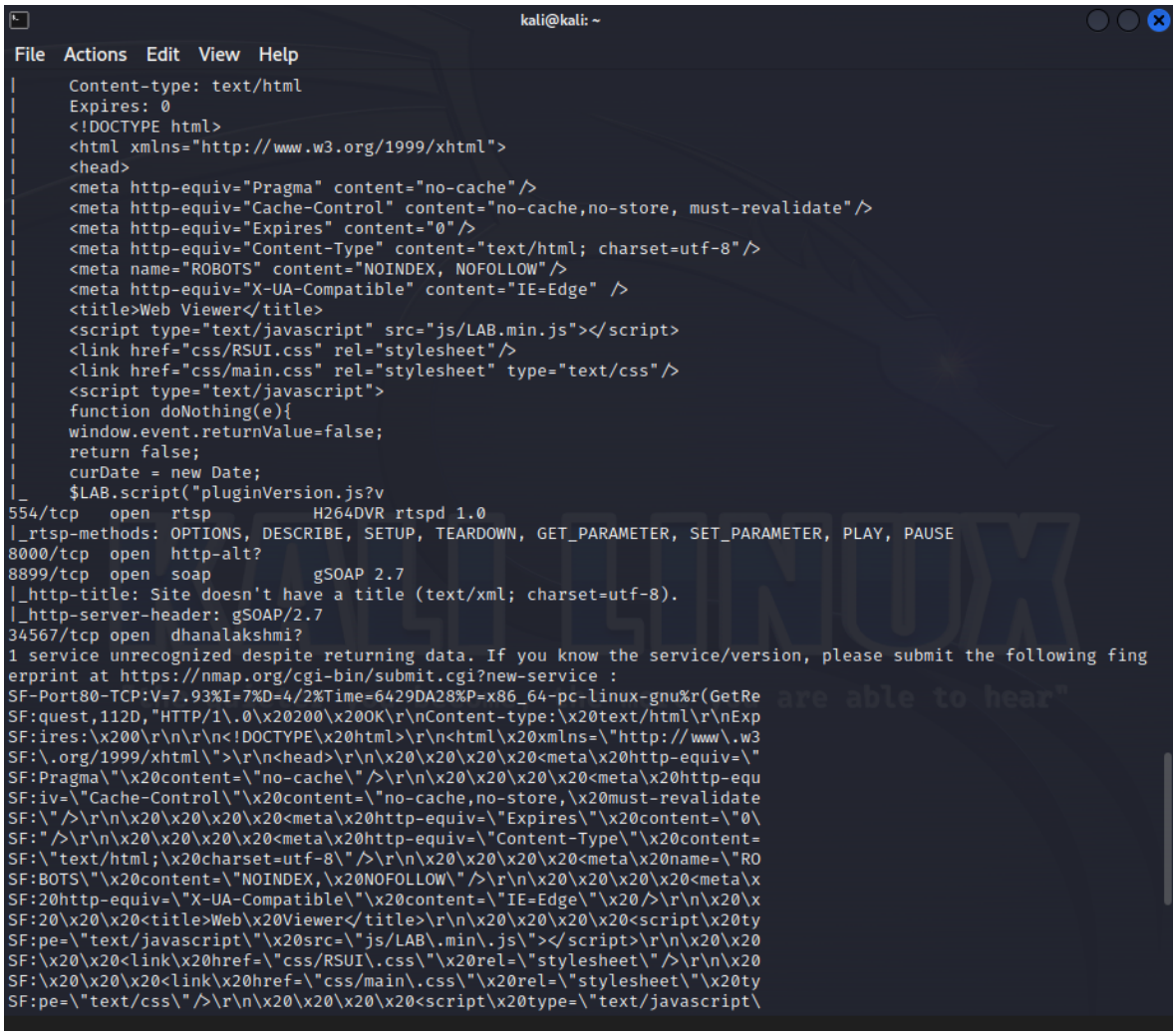
SEZNAM PŘÍLOH

PŘÍLOHA P I: SKENOVÁNÍ PORTŮ 1. ČÁST



Zdroj: vlastní

PŘÍLOHA P II: SKENOVÁNÍ PORTŮ 2. ČÁST



Zdroj: vlastní