Analýza bezpečnostních rizik v systémech pro chytrou domácnost

Nikita Zaykov

Bakalářská práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Nikita Zaykov**
Osobní číslo:	**A21259**
Studijní program:	**B1032A020001 Bezpečnostní technologie, systémy a management**
Forma studia:	**Prezenční**
Téma práce:	**Analýza bezpečnostních rizik v systémech pro chytrou domácnost**
Téma práce anglicky:	**Analysis of Security Risks in Smart Home Systems**

Zásady pro vypracování

1. Proveďte literární rešerši tématu a popište bezpečnostní rizika v systémech Internetu věcí (IoT) chytré domácnosti.
2. Navrhněte způsoby snížení úrovně bezpečnostních rizik.
3. Ověřte vhodnost návrhů v praxi.
4. Proveďte vyhodnocení vhodnosti a úspěšnosti návrhů.

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

Seznam doporučené literatury:

1. ALI, Bako a Ali AWAD. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. Sensors [online]. 2018, 18(3), 817. ISSN 1424-8220. Dostupné z: doi:10.3390/s18030817
2. ARAFAT ALI, Hesham; ALI, Zainab a BADAWY, Mahmoud. Internet of Things (IoT): Definitions, Challenges, and Recent Research Directions. International Journal of Computer Applications. October 2015, roč. 2015, č. 128(1):975-8887, s. 11.
3. ČÍKA, Petr, 2017. *Internet věcí pro inteligentní domácnost: Internet of things for smart home : zkrácená verze habilitační práce*. Brno: Vysoké učení technické v Brně, nakladatelství VUTIUM. ISBN 978-80-214-5559-7.
4. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST [NUKIB]. *Doporučení k ochraně počítačů a chytrých zařízení v domácností*. Online. Dostupné z: https://www.nukib.cz/cs/infoservis/doporuceni/1512-ochrante-svuj-domov-proti-hackerum/. [cit. 2023-11-14].
5. SURESH, P.; J. VIJAY, Daniel; PARTHASARATHY, V. a ASWATHY, R. H. A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. *International Conference on Science Engineering and Management Research (ICSEMR)*. 2015, roč. 2014, č. 10.1109/ICSEMR.2014.7043637, s. 10.
6. STERGIOU, Christos; PSANNIS, Kostas E.; BYUNG-GYU, Kim a GUPTA, Brij. Secure integration of IoT and Cloud Computing. *Future Generation Computer Systems*. 2018, roč. 2016, č. 10.1016/j.future.2016.11.031, s. 25. ISSN 0167-739X.

Vedoucí bakalářské práce: **prof. Mgr. Roman Jašek, Ph.D., DBA**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **8. prosince 2023**
Termín odevzdání bakalářské práce: **28. května 2024**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN
L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 8. prosince 2023

Nikita Zaykov

Analýza bezpečnostních rizik v systémech pro chytrou domácnost

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

Ve Zlíně, dne …….

podpis studenta

ABSTRAKT

Tato bakalářská práce se věnuje analýze bezpečnostních rizik v systémech chytré domácnosti. Důvodem výběru tohoto tématu je rychlý rozvoj technologií v této oblasti a nedostatek návodů, které by uživatelům pomohly bezpečně a spolehlivě používat jejich zařízení. Tato bakalářská práce se skládá ze dvou důležitých částí: identifikace a analýzy hrozeb a rizik a návrhu a praktické implementace bezpečnostních opatření. První část se zabývá bezpečnostními hrozbami pocházejícími zevnitř i zvenčí chytrých domácích systémů. Druhá část bakalářské práce se zaměřuje na vypracování účinných bezpečnostních opatření k minimalizaci rizik a na testování navržených opatření v praxi. K vytvoření bezpečnostních opatření byla použita metoda analýzy rizik FMEA. Ověření vhodnosti opatření bylo provedeno pomocí 3 různých skupin lidí, kteří používali různá zařízení, měli různé zkušenosti s kybernetickou bezpečností a patřili do různých věkových skupin. V závěru práce byla zhodnocena vhodnost a úspěšnost navržených bezpečnostních opatření pro zmírnění rizik pro systémy chytré domácnosti.

Klíčová slova: chytrá domácnost, bezpečnostní rizika, analýza rizik, bezpečnostní opatření

ABSTRACT

This bachelor thesis focuses on the analysis of security risks in smart home systems. The reason for choosing this topic is the rapid development of technologies in this area and the lack of guides to help users use their devices safely and reliably. This bachelor thesis consists of two important parts: the identification and analysis of threats and risks, and the suggestion and practical implementation of security measures. The first part deals with security threats originating from inside and outside smart home systems. The second part of the bachelor thesis focuses on the development of effective security measures to minimize risks and on testing the proposed measures in practice. The FMEA risk analysis method was used to develop the security measures. The validation of the suitability of the measures was performed using 3 different groups of people who used different devices, had different experiences with cyber security and belonged to different age groups. Finally, the thesis evaluated the suitability and success of the proposed security measures to reduce the risks to smart home systems.

Keywords: smart home, security risks, risk analysis, security measures

Zde bych chtěl poděkovat svému vedoucímu práce panu prof. Mgr. Romanu Jaškovi, Ph.D., DBA za velmi cenné rady, které mi pomohly při realizaci mé práce. Také bych chtěl poděkovat svým příbuzným a přátelům, kteří souhlasili s účastí v mém výzkumu.

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

OBSAH

ÚVOD

Každý rok se tempo vývoje technologií i jejich široké využití a implementace jen zrychluje. Lidé používají různá chytrá zařízení, která jim pomáhají automatizovat nebo zjednodušit různé životní procesy. Spolu s pohodlím při používání technologií chytré domácnosti však vznikají nová bezpečnostní rizika, která je třeba pečlivě analyzovat a eliminovat. Lidé často ani nepřemýšlejí o tom, že jejich chytrá zařízení mohou být vystavena různým rizikům, která mohou způsobit uživateli škodu. Motivací pro výběr tohoto tématu pro mě byl nedostatek návodů pro uživatele a rostoucí počet hrozeb spojených s chytrými domácími zařízeními.

Cílem mé bakalářské práce je analyzovat bezpečnostní rizika systémů inteligentních domácností a navrhnout účinná bezpečnostní opatření k jejich zmírnění. Zvláštní pozornost by měla být věnována identifikaci hlavních vnitřních a vnějších bezpečnostních hrozeb, kterým mohou být systémy chytrých domácností vystaveny. Rovněž je mým cílem identifikovat hrozby související se softwarovým i hardwarovým zabezpečením zařízení.

Bakalářská práce bude rozdělena do několika částí, aby bylo možné systematicky dosáhnout mých cílů. V teoretické části budu muset podrobně pochopit, co je to chytrá domácnost a internet věcí. V jakých oblastech je lze využít a jak probíhá komunikace mezi zařízeními. To je nezbytné pro lepší pochopení možných bezpečnostních hrozeb. Pro realizaci teoretické části bude analyzována literatura z této oblasti.

V praktické části budou nejprve identifikovány a kategorizovány hlavní bezpečnostní hrozby pro systémy chytrých domácností. A také bude provedena analýza rizik pomocí metody FMEA, která umožňuje vyhodnotit možná rizika z hlediska pravděpodobnosti výskytu, závažnosti a odhalitelnosti. Na základě výsledků analýzy bude možné identifikovat nejkritičtější hrozby, které vyžadují prioritní řešení. Dalším důležitým úkolem je vyvinout účinná bezpečnostní opatření, která sníží míru rizik pro systémy inteligentních domácností. Následně budou všechna navržená opatření otestována v praxi a bude vyhodnocena jejich vhodnost a úspěšnost.

Především bude tato bakalářská práce užitečná pro běžné uživatele, kteří již mají nebo plánují zakoupit zařízení chytré domácnosti. Bude užitečná i pro zkušené specialisty, kteří se chtějí seznámit s novým pohledem na řešení konkrétních hrozeb. Věřím, že všechny cíle, které jsem si stanovil, jsou reálné a dosažitelné.

I. TEORETICKÁ ČÁST

1 INTERNET VĚCÍ

Pro lepší pochopení fungování chytrých zařízení je nejprve nutné porozumět tomu, co je to internet věcí (IoT). Světoznámá korporace IBM, která vyvíjí a vyrábí software a hardware a poskytuje služby v oblasti informačních technologií, nabízí následující definici internetu věcí. Ve volném překladu definice uvádí, že internet věcí je síť fyzických zařízení, která jsou vybavena senzory, vysílači, softwarem, síťovým připojením a mohou mezi sebou sbírat a vyměňovat data. Internet věcí zahrnuje jak jednoduchá chytrá domácí zařízení, tak nositelná zařízení a sofistikovaná průmyslová zařízení. Jinými slovy, internet věcí je množství zařízení, která mnoho lidí denně používá, jako jsou chytré telefony, chytré hodinky a fitness náramky, chytré ledničky a virtuální asistenti, jako je Siri od Apple nebo ChatGPT od OpenAI. [1]

Široké rozšíření internetu věcí je způsobeno vznikem velmi malých a velmi levných počítačových čipů a také rozšířeným používáním bezdrátových sítí po celém světě. Každoročně přibývá stále více předmětů, které získávají např. připojení přes telefon, a také možnost propojení s dalšími spotřebiči. Zásluhou technologického pokroku a zlevnění výroby si stále více lidí může dovolit kupovat více zařízení, která jsou součástí internetu věcí. Internet věcí se v posledních několika letech stal jednou z nejdůležitějších technologií 21. století. [1]

1.1 Historie internetu věcí

Předchůdcem myšlenky vytvoření internetu věcí byl Nikola Tesla, který již v roce 1926 hovořil na toto téma. Podle jeho názoru se rádio s tím, jak se bude zdokonalovat, postupně promění v "obrovský mozek" a všechny ostatní nástroje a zařízení k němu budou připojeny a stanou se tak kompaktními, že se vejdou do kapsy každého člověka. Nikola Tesla téměř přesně předpověděl princip internetu věcí. "Obrovským mozkem" je v naší době internet, který propojuje všechna zařízení. Mezi kompaktní zařízení patří telefony, tablety a chytré hodinky, které má dnes mnoho lidí. [2]

V 90. letech 20. století se aktivně diskutovalo o sítích umožňujících komunikaci mezi stroji, ale jedním z prvních zařízení připojených k síti byl automat na Coca-Colu. Ten byl instalován v roce 1982 na univerzitě Carnegie Mellon. Tento automat přenášel údaje o počtu lahví, které obsahoval, a také o svém celkovém stavu. [3]

„Vědec Bill Joy zase ve svém projevu na Mezinárodním ekonomickém fóru v Davosu v roce 1999 navrhl myšlenku "šesti sítí" - šesti typů internetu budoucnosti. V ní poměrně přesně

předpověděl vznik bezdrátových mobilních internetových sítí, inteligentních hlasových asistentů a komunikace mezi zařízeními (v jeho typologii se taková komunikace nazývala Device-to-device). Současně se objevily pokusy o vytvoření prvních projektů internetu věcí - například společnost Microsoft v roce 1993 uvedla na trh platformu at Work, která zahrnovala speciální operační systém a protokol pro přenos dat, jehož účelem bylo sjednotit kancelářská zařízení (faxy, kopírovací stroje atd.) společným protokolem a přenést funkce správy a ovládání nad nimi na počítače se systémem Windows. Projekt at Work však nebyl úspěšný a po nějaké době byl ukončen. V roce 1994 přišla s podobným projektem společnost Novell - její platforma NEST (Novell Embedded Systems Technology) umožňovala různým zařízením připojit se ke službám síťového operačního systému NetWare a pro vzájemnou komunikaci používat jeho protokol IPX. NEST zopakoval osud svého předchůdce at Work a zanikl.“ [3]

Rok 2000 byl obdobím rychlého rozvoje internetu věcí. V letech 2000 a 2010 se začaly masově objevovat a spouštět úspěšné projekty internetu věcí v praxi. Vzniklo tak mnoho uživatelských zařízení souvisejících s internetem věcí - od fitness trackerů po chytré lampy a chytré dveře. Kromě toho se začaly rozvíjet rozsáhlé projekty založené na technologiích internetu věcí - chytrá města, chytrá výroba, chytrá doprava, bezpilotní automobily a mnoho dalších. [3]

1.2 Oblasti využití internetu věcí

Mnoho lidí si myslí, že internet věcí byl vytvořen pouze pro pohodlí každodenního života, ale technologie internetu věcí lze použít téměř v jakékoli oblasti, kterou lze automatizovat. Mezi takové oblasti patří například obchodní sféra, energetika, průmysl, zdravotnictví a další. Pro pochopení významu technologií internetu věcí bych chtěl upozornit na některé oblasti použití.

1.2.1 Zdravotnictví

Zdravotnictví je velmi důležité pro všechny lidi na světě, a proto zde nachází uplatnění mnoho technologií internetu věcí. Bylo vytvořeno velké množství "chytrých" zařízení, která monitorují důležité životní funkce pacientů a v případě potřeby předávají tyto ukazatele ošetřujícímu lékaři. V dnešní době již není nutné chodit ke každému pacientovi a ručně měřit krevní tlak, puls, hladinu cukru v krvi a další ukazatele, protože technologie chytré domácnosti všechny tyto věci měří a všechny údaje zobrazují na obrazovce. Dokonce i nemocniční

lůžka jsou vybavena různými senzory. Některé nemocnice mají senzory, které monitorují tlak vyvíjený na matraci a automaticky jej rovnoměrně rozkládají, aby se pacientovi nevytvořily proleženiny. [2]

Pacienti s chronickými onemocněními používají různá chytrá zařízení, která nepřetržitě monitorují životní funkce a předávají údaje ošetřujícímu lékaři. Také technologie internetu věcí umožňují konzultace s lékaři kdekoli. A lékaři nyní mohou na dálku přijímat informace o pacientech a předepisovat léčbu z pohodlí svých ordinací. [2]

Mám několik známých, kteří trpí cukrovkou. Ke sledování hladiny glukózy používají vestavěný senzor, což znamená, že si nemusí každý den píchat do prstu. Tento snímač můžete také připojit k telefonu a dostávat notifikace, když je hladina glukózy v krvi nízká. Všechny naměřené údaje mohou být automaticky odeslány vašemu ošetřujícímu lékaři, což lidem s chronickým onemocněním zkracuje obrovské množství času a zjednodušuje život. Internet věcí pomáhá každým rokem stále většímu počtu lidí s onemocněním cítit se pohodlněji a bezpečněji. Aplikace technologií internetu věcí lze nalézt téměř ve všech oblastech zdravotnictví.

1.2.2 Elektroenergetika

Technologie internetu věcí v energetice přinášejí do správy energetických zdrojů inovace, optimalizaci a efektivitu. Technologie internetu věcí lze v energetice využít mnoha způsoby, například ke sledování stavu zařízení a strojů, shromažďování dat pro zlepšení a optimalizaci infrastruktury a inteligentnímu rozdělování energetických zdrojů. [2]

Elektrické vedení lze monitorovat na dálku. Ke sledování stavu kabelů, např. při namrzání nebo prohýbání kabelů, lze použít drony. Pokud jsou případné problémy zjištěny včas, lze jejich příčiny odstranit i bez přítomnosti člověka. Drony pomáhají zachraňovat životy lidí, kteří dříve museli šplhat desítky metrů nad zem, aby vyřešili problém s promrznutím nebo prověšenými kabely. [2]

Technologie internetu věcí mají v energetice obrovský potenciál. Zaměstnanci již nemusí provádět rozsáhlé audity, aby optimalizovali provoz a distribuci elektřiny, vše lze provést automaticky pomocí technologií internetu věcí. Optimalizovaná distribuce elektřiny pomáhá ušetřit "přebytečnou" elektřinu, která byla odkloněna na nesprávné místo, což šetří spoustu peněz a přírodních zdrojů. O vývoj technologií internetu věcí se zajímá stále více největších světových energetických společností. Mnoho společností do této oblasti investuje peníze,

protože internet věcí pomáhá šetřit přírodu a peníze zákazníků, a tím zvyšuje zisky samotných společností.

1.2.3 Průmysl a průmyslová výroba

Technologie internetu věcí se v průmyslu používají stále častěji. Každým rokem se stále častěji objevují takzvané "chytré továrny", které jsou vzájemně propojeny pomocí internetu věcí. Díky těmto technologiím je možné optimalizovat provoz všech továren, a tím snížit škodlivý dopad na naši planetu omezením přebytků a odpadu. [2]

Díky sběru dat od zaměstnanců je také možné zkvalitnit jejich výkon. To vše je prospěšné nejen pro přírodu a zaměstnance, ale také pro majitele těchto průmyslových závodů, protože snížení odpadu a přebytků ve výrobě zvýší jejich zisky. [4]

V dnešní době se stále více lidí začíná zajímat o životní prostředí, protože výrazně ovlivňuje náš každodenní život. Globální oteplování, znečišťování ovzduší škodlivými látkami z průmyslových závodů, znečišťování řek, jezer a oceánů odpadními vodami může mít vážné následky pro planetu i pro lidi, protože v průmyslové historii lidstva došlo k mnoha případům, kdy úniky nebezpečných látek z výroby vedly dokonce k úmrtí lidí. Citlivé senzory propojené technologiemi internetu věcí pomáhají automaticky monitorovat životní prostředí v blízkosti průmyslových závodů. V případě zjištění nebezpečných úniků nebo překročení povolených limitů dají senzory pracovníkům průmyslových závodů signál k jejich odstranění. Některé země ze zákona nutí průmyslové závody, aby takové senzory instalovaly, protože to pomáhá nejen zpomalit ničení naší planety, ale také zlepšit kvalitu života lidí žijících v blízkosti těchto závodů. [4]

2 INTERNET VĚCÍ A TECHNOLOGIE CHYTRÉ DOMÁCNOSTI

Rostoucí popularita technologií internetu věcí vede k nárůstu výroby a vývoje v této oblasti. Jen v roce 2020 bude k internetu připojeno více než 28 miliard zařízení, tedy přibližně 6 zařízení na 1 osobu. Možnost připojení a ovládání prostřednictvím telefonu začleňuje do svých výrobků každým rokem stále více společností.[5]

Ještě před 20 lety si internetové technologie mohly kvůli vysokým výrobním nákladům dovolit pouze velké společnosti, ale nyní vidíme jejich využití všude kolem nás. V roce 2023 lidi nepřekvapí, že toustovač vám automaticky opeče toasty ve stejnou dobu jako budík a kávovar vám připraví ranní kávu. S tím, jak se výroba zlevňuje, si stále více lidí může dovolit pořídit si takzvanou technologii chytré domácnosti pro osobní potřeby. V současné době se někteří lidé snaží zaplnit technologiemi chytré domácnosti úplně všechno ve své domácnosti a automatizovat vše, na co si vzpomenou. V tomto bloku bych chtěl pochopit, co jsou technologie chytré domácnosti, jak tato zařízení fungují, a také se zamyslet nad perspektivami rozvoje těchto technologií. [4][5]

2.1 Technologie chytré domácnosti

Chytrý domov je moderní technologický systém, který umožňuje automatizaci všech aspektů života v domácnosti. Současná komunikace uvnitř domu je integrována do jednotného systému, který je ovládán umělou inteligencí. Cílem chytrého domova je zajistit pohodlí a bezpečnost pro uživatele. Moderní chytrá domácnost integruje a ovládá všechny systémy v budově, jako je vytápění a osvětlení, bezpečnostní systémy a dokonce i domácí spotřebiče. Díky takto rozsáhlé technologii mohou lidé vytvářet určité scénáře pro automatizaci každodenních úkolů. Například po probuzení může majitel domu nahlas vyslovit větu "Dobré ráno" a systémy inteligentní domácnosti spustí scénář, který otevře závěsy, rozsvítí světla, upraví teplotu v domě a spustí kávovar. Všechny tyto možnosti nabízejí systémy inteligentní domácnosti, které jsou rok od roku dokonalejší a cenově dostupnější. Ve scénářích neexistují prakticky žádná omezení, kromě fantazie samotného člověka. [6]

V současné době dochází k integraci technologií chytré domácnosti s umělou inteligencí, která bude analyzovat lidské chování a na základě získaných dat nabídne nové scénáře automatizace a optimalizace procesů pro maximální pohodlí obyvatel a dokonce vysokou energetickou účinnost. [5]

Většina zařízení chytré domácnosti navíc podporuje ovládání pomocí smartphonů. Lidé na dovolené kdekoli na světě se mohou připojit k bezpečnostním kamerám a sledovat, co se v bytě děje. Pohodlí při používání těchto technologií láká stále více lidí a investorů po celém světě. V tomto bloku bych se rád dozvěděl více o různých systémech a jejich fungování. [5]

2.1.1 Systém řízení osvětlení

Systémy pro řízení osvětlení jsou nejoblíbenějšími a cenově nejpříznivějšími zařízeními chytré domácnosti. Mnoho lidí začíná integrovat technologie chytré domácnosti právě s osvětlením. Chytré domácí osvětlení je automatizovaný systém pro ovládání venkovních a vnitřních svítidel, který se ovládá pomocí telefonu, dálkového ovladače, hlasu, senzoru nebo jiných zařízení. Můžete si zakoupit hotová zařízení, jako jsou chytré LED pásky, lustry nebo žárovky, nebo můžete svá stávající svítidla propojit s chytrými zásuvkami.

Pomocí chytrého osvětlení můžete ovládat úroveň osvětlení, měnit teplotu světla a dokonce i jeho barvu. Veškeré osvětlení lze ovládat z telefonu, takže se nemusíte bát, že byste zapomněli v bytě zhasnout. Potřebné žárovky můžete také naprogramovat tak, aby se automaticky rozsvítily nebo zhasly. Toho se dříve využívalo, když jste byli pryč - světla se večer automaticky rozsvítila, což vytvářelo efekt lidské přítomnosti v domě a odrazovalo potenciální zloděje. Nyní ji lze použít pro pěstování rostlin, které vyžadují jasný časový plán zapínání a vypínání ultrafialových lamp. Můžete také připojit senzory pohybu, které v noci zapnou osvětlení schodiště, abyste nezakopli a nespadli ze schodů. Mnoho lidí umisťuje tento druh osvětlení poblíž vchodových dveří, aby nemuseli sahat rukou na vypínač. Chytré osvětlení také šetří obrovské množství energie díky efektivní optimalizaci. Pokud se venku aktivuje světelný senzor, světla v domě se automaticky vypnou. [7][8]

2.1.2 Systém vytápění

Inteligentní systém vytápění domu zahrnuje mnoho zařízení, jako jsou klimatizace, podlahové vytápění, přívodní a odvodní větrání, ventil vodního topného systému, ovládání kotle pro rodinný dům a další. Všechna tato zařízení lze spojit do jednoho systému nebo je ovládat samostatně.

Dálkově ovládané kotle jsou na trhu již delší dobu, protože mnoho lidí přijíždí do rodinného domu pouze na víkend. Dálkové ovládání kotle umožňuje vypnout vytápění domu v době nepřítomnosti a zapnout s předstihem před příjezdem, aby v domě bylo teplo. I když dům

nemá moderní kotel, lze z běžných elektrických topidel udělat "chytrá" pomocí zásuvek s dálkovým ovládáním a topení se zapne příkazem z vašeho telefonu. [7][9]

Pokud všechna zařízení správně propojíte a zkombinujete, můžete získat ekosystém, který se bude regulovat sám. Například klimatizace nebude ochlazovat místnost, když je zapnuté podlahové vytápění nebo je otevřené okno. To vám také pomůže ušetřit elektrickou energii. Můžete vytvořit scénář tak, aby se při aktivaci čidla otevření okna vypnulo podlahové vytápění, klimatizace a kotel, protože není třeba vytápět venkovní prostor. Tento jednoduchý scénář výrazně zvyšuje energetickou účinnost a snižuje náklady na energii. [7][9]

2.1.3 Bezpečnostní systémy

Bezpečnost je velmi důležitým aspektem našeho života. Místo, kde se cítíme bezpečně, nazýváme domovem, a proto je velmi důležité, abychom si tento pocit udrželi neustále. Technologie chytré domácnosti nabízí mnoho různých zařízení, která pomáhají udržet lidi i majetek v bezpečí. Zabezpečovací systém inteligentní domácnosti je plně automatizovaný ekosystém bezpečnostních a požárních alarmů a také systémů ochrany proti úniku vody a plynu. Součástí bezpečnostních systémů chytré domácnosti jsou také kamerové systémy, systémy kontroly přístupu a systémy dálkového oznamování nouzových situací v bytě, domě a okolí.[7][10]

Únik plynu představuje velmi vážné ohrožení lidského života, protože i bez výbuchu vás může plyn zabít. Dříve se vyskytlo mnoho případů, kdy únik plynu způsobil udušení ve spánku. Zemní plyn nemá žádný zápach, proto se zápach do plynu přidává uměle. Lidé však tento zápach nemusí vždy cítit v noci během spánku, proto byly vytvořeny speciální inteligentní senzory. Tyto senzory jsou schopny v případě zjištění úniku plynu přerušit přívod plynu do postižené oblasti a informovat o závadě plynárenské orgány. Přestože je dnes plyn v bytech vzácný, mnoho rodinných domů stále používá plyn k vytápění a vaření. Tyto senzory vám mohou zachránit život, proto se jedná o mimořádně důležité zařízení chytré domácnosti. [10]

Únik vody může být pro život člověka stejně škodlivý jako pro jeho majetek. Přestože se pravděpodobně ve spánku neutopíte, škody na vašem bytě nebo domě mohou být obrovské. V takové situaci může pomoci detektor úniku vody, který poškozený úsek vodovodu uzavře a informuje vás o tom notifikací na vašem telefonu. Mnoho lidí umisťuje takové senzory do blízkosti míst, kde může dojít k úniku vody, například pod kuchyňský dřez, pod pračky,

myčky a do koupelny. Únik vody může způsobit zkrat v celé budově a může dojít k požáru, proto je velmi důležité mít v bytě detektory úniku vody, které jsou velmi levné. [7] [10]

Důležitou součástí chytré domácnosti jsou také detektory kouře, protože nikdo není v bezpečí před náhodným požárem zásuvky nebo zapomenutým jídlem v troubě. Kouř je velmi nebezpečný, protože když se dostane do dýchacích cest člověka, zcela nahradí kyslík a způsobí udušení. Mnoho lidí při požáru zemře spíše na následky kouře než na oheň. Proto je nesmírně důležité mít v bytě alespoň jeden detektor kouře. Chytré detektory kouře vás mohou nejen informovat pomocí SMS, ale také vypnout elektřinu v domě, omezit přívod plynu, následně zapnout hasicí systém a zavolat hasiče. Detektor úniku vody, detektor úniku plynu a detektor kouře jsou základy, které by měli mít všichni lidé ve svých bytech. Stát se může cokoli a ne vlastní vinou, ale mít tato zařízení v bytě může zachránit nejen váš život, ale i životy vašich sousedů. [10]

Důležitou součástí zabezpečení je ochrana vchodů a oken v bytě nebo domě. Existuje velké množství zařízení, která mohou okna a dveře dodatečně chránit. Nejjednodušší je detektor, který snímá otevírání a zavírání oken a dveří. V obchodě lze zakoupit desítky různých typů takových zařízení a každý si bude moci najít vhodnou cenu. Navzdory různým principům fungování je účel těchto snímačů stejný - snímat jakoukoli manipulaci s okny nebo dveřmi. Synchronizací těchto senzorů s chytrým domácím zabezpečovacím systémem můžete nastavit libovolné scénáře, které pomohou dopadnout pachatele. Někteří lidé dávají přednost aktivaci zvukové sirény při aktivaci těchto čidel, která potenciálního zloděje odradí. Stále však existuje možnost, kdy si zločinec ani neuvědomí, že se bezpečnostní systémy spustily. Po spuštění čidlo vyšle signál na policii, a zatímco se zločinec snaží vykrást váš dům - policie už na něj čeká u východů z budovy. Podle mého názoru je druhá možnost nejlepší, protože siréna ho jen vystraší a on vykradne jiný dům, zatímco "tichý" poplašný systém ho donutí převzít odpovědnost za své zločiny. [8][10]

Ještě nedávno se zdálo, že chytré zámky jsou k vidění pouze ve vědeckofantastických filmech, ale na trhu se postupně prosazují. Vyznačují se vysokou bezpečností, snadným používáním a odolností. Jedná se o elektronické zámky, které se otevírají a zavírají díky bezdrátové interakci s chytrým telefonem majitele, a to prostřednictvím snímače otisků prstů nebo digitálního hesla. Už nemusíte nosit klíče s sebou, když odcházíte z domu, ani se bát, že je ztratíte. Místo fyzického klíče může majitel zadat kód, přiložit prst na skener nebo stisknout tlačítko v aplikaci v telefonu. Další důležitou funkcí chytrých zámků je možnost otevřít dveře na dálku. Právo ovládat zařízení má majitel, ale může si vytvořit virtuální klíč

a udělit přístupová práva dalším členům domácnosti. Některé modely zaznamenávají čas příchodu jednotlivých členů rodiny a vy tak budete vždy vědět, v kolik hodin se dítě vrátilo ze školy a zda je doma. Tyto zámky lze synchronizovat s dalšími zařízeními chytré domácnosti. Lze je například propojit s klimatizačním systémem a při vstupu do bytu se zapne klimatizace. [11]

Není třeba předpokládat, že kamerový systém pro chytré domy se omezuje pouze na sledovací kamery. Součástí systému jsou také pohybové senzory, jejichž úkolem je detekovat osoby v kontrolovaném prostoru a okamžitě zapnout videozáznam. Dalším důležitým zařízením je vzdálený videohovor, který umožňuje pochopit, kdo je za dveřmi, a informovat o návštěvě, pokud jste zrovna nebyli doma. Systém je spojen do jednoho celku pomocí přístupového uzlu. Právě on odesílá upozornění a alarmy do vašeho chytrého telefonu. Jednou z hlavních výhod dohledového systému v inteligentní domácnosti je možnost zajistit kontrolu přístupu pomocí kamer. Nejčastěji se s takovými řešeními setkáváme v průmyslových objektech, kde zařízení rozpoznávají obličeje pracovníků a umožňují jim průchod dál. Navíc nemusíte dávat samostatný klíč každé osobě, které chcete umožnit přístup do domu. Stačí, když do video zvonků přidáte jeho biometrické údaje, a ten pak automaticky pustí osoby ze své databáze. Nemusíte se bát – přístup můžete zakázat na dálku ze svého smartphonu. Díky tomu si nejen zjednodušíte život, ale budete vždy vědět, kdo a kdy vstoupil do vašeho domu. [12][13]

Na rozdíl od běžných kamer, které pouze zaznamenávají dění v okolí, kamerový systém inteligentní domácnosti neustále analyzuje obraz a hledá podezřelé aktivity. Pokud se tedy v zorném poli zařízení nachází nějaká osoba, informace o ní se automaticky odešlou do vašeho smartphonu. Pokud z nějakého důvodu nebudete moci na upozornění reagovat, informace se odešle soukromé bezpečnostní společnosti, se kterou máte uzavřenou smlouvu. I když se budete nacházet mimo místo a obdržíte upozornění, budete mít vždy možnost prohlédnout si záznam z kamerového systému. Díky tomu budete moci rychle prostudovat obraz a pochopit, kdo je na snímku, zda se jedná o známou nebo neznámou osobu, a přijmout opatření. Se standardním kamerovým systémem budete mít pouze možnost prohlédnout si záznamy a zjistit totožnost pachatele pro další zachycení. Inteligentní domácnost zabrání trestnému činu a zachová váš majetek. [12][13]

Standardní kamerový systém není schopen generovat žádné výstrahy ani alarmy, takže kamery ve skutečnosti nijak nezvyšují bezpečnost. Znalí narušitelé jsou si toho dobře vědomi, takže se kamer nebojí, ale pouze si zakrývají tvář. Pokud chcete zajistit opravdovou

ochranu, pak vám jistě pomůže systém inteligentní domácnosti. Kamerový systém v inteligentní domácnosti může být doplněn o celou řadu senzorů. Především se jedná o zařízení, která po zapnutí systému detekují jakýkoli pohyb. Pokud je detekován velký objekt, aktivuje se alarm, který automaticky přivolá policii k vám domů. Nemusíte se obávat, pokud s vámi žije malá kočka nebo pes – systém dokáže jejich pohyb ignorovat, aniž by se aktivoval alarm. Ve srovnání se standardním sledováním poskytuje tento přístup mnohem větší bezpečnost. [12][13]

2.1.4 Systémy chytrých domácích spotřebičů

Ještě před 15 lety byly chytré domácí spotřebiče považovány za fantazii. Nikdo nevěřil, že takové spotřebiče budou nejen existovat, ale že se stanou součástí našeho každodenního života. Každý má doma nějaký druh domácích spotřebičů, jako je lednička, pračka, myčka, mikrovlnná trouba a další. Ale co kdybychom mohli přidat nějaké užitečné funkce, které by se daly ovládat na dálku? V roce 2024 si stále více lidí kupuje domácí spotřebiče s "chytrými" funkcemi, protože to nejen zjednodušuje život, ale také pomáhá zkrátit dobu používání těchto spotřebičů díky automatizaci.

2.1.4.1 Velké spotřebiče pro chytrou domácnost

Lednička a pračka jsou nejoblíbenějšími představitelé kategorie velkých chytrých domácích spotřebičů. Jak může systém inteligentní domácnosti pomoci při ovládání ledničky? Je vhodné automatizovat provoz ledničky podle dočasného scénáře. Například máte chladničku v rodinném domě a jezdíte tam jen o víkendech. Když víte, že zítra přijedete v 11 hodin dopoledne, můžete nastavit časovač, který ji zapne, a po příjezdu jednoduše vložíte potraviny do již fungující ledničky. Tento princip se vám bude hodit i v případě, že často cestujete na služební cesty a v chytré lednici neskladujete potraviny podléhající rychlé zkáze. Přepněte ji do úsporného režimu, abyste ušetřili spotřebu energie a prodloužili životnost svého chytrého domácího spotřebiče. S ledničkou bude samozřejmě fungovat i zapínání a vypínání prostřednictvím chytrého telefonu nebo hlasového asistenta. [14][15]

Pračku lze také učit. Když odcházíte do práce, můžete nastavit časovač, kdy se má spustit praní, abyste po návratu mohli jen vytáhnout čerstvé prádlo. Pokud víte, že byste mohli zapomenout věci v bubnu, upozorní vás na to oznámení, takže se můžete vyhnout problému se zatuchlým zápachem, aniž byste museli kupovat drahé a moderní spotřebiče. A příjemným

bonusem budou aktualizace od výrobce. Například přidání nových režimů, které při koupi pračky nebyly k dispozici. [14]

2.1.4.2 Chytré malé domácí spotřebiče

Malé chytré spotřebiče pro domácnost jsou spotřebiče, které lze snadno přenášet v ruce. Pokud mluvíme o chytrých spotřebičích do kuchyně, jedná se o multifunkční vařiče a kávovary. Nezřídka se však používají také čističky vzduchu a zvlhčovače vzduchu, které pomáhají zlepšit kvalitu života a zdraví každého člena rodiny. Alergický kašel, suchá pokožka a hrdlo, riziko nachlazení a akutních infekcí dýchacích cest a neklidný spánek jsou nejčastějšími důsledky suchého vzduchu. Znečištěný vzduch má obzvláště negativní vliv na děti, starší osoby a alergiky. Před negativními účinky je možné se chránit a kvalitu vzduchu ovlivnit používáním čističek a zvlhčovačů vzduchu. Můžete nastavit scénáře pro jednotlivé místnosti, například dětský pokoj, aby byl vzduch čistý a zvlhčený pro zdraví dětí. [14]

Jaké jsou výhody chytrého multifunkčního vařiče? Nemusíte ztrácet čas stáním u sporáku a pravidelným mícháním polévky, aby se nepřipálila. Vhoďte všechny ingredience do multifunkčního vařiče a nastavte požadovaný režim. Volný čas strávíte se svými blízkými a o uvařené večeři budete informováni. Chcete ušetřit čas na ranní sprchu a zároveň si dát zdravou snídani? Nastavte vaření ovesné nebo jiné kaše na požadovanou dobu. [14]

Vaše rána vám může zpříjemnit chytrý kávovar. Vezměme si příklad překapávacího kávovaru. Filtrovaná káva výrazněji odhalí vaši oblíbenou chuť a lépe vás povzbudí, ale proces přípravy nelze označit za rychlý. Pokud jste v kavárně nebo v kanceláři, není čekání na nápoj problém. Co však dělat doma? Odmítáte pít překapávanou kávu, protože ráno máte málo času? Systém inteligentní domácnosti vám umožní připravit kávu nejen bez vaší účasti. Kávovar zahájí proces přípravy, zatímco vy ještě spíte. Jediné, co musíte udělat, je připravit kávovar večer obvyklým způsobem a nastavit scénář na časovač. Není úžasné probudit se s vůní lahodné kávy? Další motivace k aktivnějšímu přivítání nového dne. [14][15]

K automatizaci běžných procesů však nemusíte kupovat nejnovější domácí spotřebiče. Díky chytrým zásuvkám, čidlům, termostatům, branám, relé a dalším komponentům si můžete nastavit vlastní systém domácí automatizace. Připojte několik zařízení v jednom dálkovém ovladači, propojte všechna zařízení prostřednictvím jedné mobilní aplikace a ovládejte je pomocí hlasového asistenta. Zároveň můžete naučit domácí spotřebiče, které již máte doma, aniž by byla ohrožena jejich kvalita. [14]

2.2 Perspektivy vývoje technologií pro inteligentní domácnosti

Když se na konci 90. let poprvé objevil pojem "chytrá domácnost", byla to ještě velká fantazie. Od té doby uplynulo mnoho let a tato technologie urazila ve svém vývoji dlouhou cestu. V posledních letech jsme svědky doslova boomu tohoto trhu, protože se objevila zařízení doslova pro každou místnost v domě. Tyto systémy již nejsou vyhrazeny jen pro nejdražší domy, ani se neukládají na modernizaci po letech – v některých zemích si lidé dnes kupují domy s ohledem na již existující technologie inteligentní domácnosti. Zde jsou některé z nejvýznamnějších trendů v oblasti chytrých domů, kterých je třeba si právě teď všimnout. [16]

2.2.1 Integrace

Jeden z největších trendů v oblasti chytré domácnosti v roce 2024 souvisí s tím, jak je technologie plně integrovaná. Stala se téměř očekávanou součástí domácnosti při její koupi, nikoliv luxusem, a spolu s rostoucími očekáváními přišlo i povinné připojení k internetu a snadné používání. Pokud jde o integraci, stále více zařízení chytré domácnosti začíná vzájemně komunikovat. Například více místností v domácnosti může být vybaveno reproduktory Google Home, které mohou pracovat ve skupinách namísto jednotlivých zařízení. Systém osvětlení Philips Hue dokáže ovládat osvětlení v celé domácnosti a řídit se specifickými pravidly, která si uživatel vytvoří pro zapínání a vypínání světel podle svého rozvrhu a potřeb. [16]

Když chytrá lednička zjistí, že jí došlo mléko, může ho například přidat do nákupního seznamu uloženého v zařízení Amazon Alexa. Při rozšiřování systému chytré domácnosti je přitom klíčové připojení k internetu. [16]

Také používání se nadále zjednodušuje. Člověk už nemusí být technicky zdatný, aby nastavil mnoho chytrých zařízení. Pokud má člověk chytrý telefon, připojení k Wi-Fi a zásuvku, je většina lidí ochotna připojit mnoho zařízení, čímž se bariéra vstupu do systému inteligentní domácnosti výrazně snižuje. [16]

2.2.2 Umělá inteligence v systému inteligentní domácnosti

S rozvojem technologií a vědeckého pokroku se umělá inteligence stala klíčovým prvkem moderního světa. Proniká do různých oblastí našeho života, včetně domácích spotřebičů, a mění způsob, jakým tato zařízení vnímáme a používáme. Co jsou inteligentní domácí spotřebiče, jak s nimi komunikovat – takové otázky jsou dnes aktuálnější než kdykoli předtím.

Moderní chytré domácí spotřebiče se zabudovanou umělou inteligencí jsou stále běžnější. Hlasoví asistenti zajišťují interaktivní komunikaci se zařízeními a umožňují nám ovládat osvětlení, klimatizaci, a dokonce i objednávat potraviny konkrétně naším hlasem. Chytré bezpečnostní systémy a domácí kamery se zabudovanou umělou inteligencí poskytují spolehlivou ochranu a kontrolu nad našimi domovy. A takové známé domácí spotřebiče se nyní označují jako inteligentní domácí spotřebiče a známé značky již mají v této kategorii dobré nabídky. [16][17]

Několik známých značek nyní aktivně využívá funkci umělé inteligence ve svých domácích spotřebičích. Například značka Samsung začleňuje funkce umělé inteligence do svých televizorů, chladniček a praček. Také značka LG vyrábí zařízení s umělou inteligencí, včetně chytrých chladniček, televizorů a praček. Mají funkce rozpoznávání hlasu, analýzy dat a automatického ovládání. V budoucnu bude stále více domácích spotřebičů vybaveno umělou inteligencí. Zde je několik příkladů, které již existují. [16]

- Chytré ledničky využívají umělou inteligenci k udržování potravin v lepším stavu. Dokážou monitorovat stav potravin, kontrolovat teplotu a vlhkost a posílat oznámení o objednání nových produktů. [16]

- Chytré sporáky a trouby poskytují přesné a automatické řízení vaření. Dokážou rozpoznat typ potravin, řídit teplotu a dobu vaření a poskytovat doporučení pro optimální vaření. [16]

- Chytré kávovary s umělou inteligencí se mohou naučit vaše chuťové preference a upravit parametry přípravy kávy podle vašich preferencí. Mohou mít také funkci automatického objednání kávy, když dojdou zásoby. [16]

- Chytré multifunkční vařiče s umělou inteligencí mohou předvídat dobu vaření různých pokrmů s ohledem na jejich složení a počet ingrediencí. Mohou také poskytovat recepty a tipy na přípravu různých pokrmů. [16]

- Chytré pračky a myčky nádobí mají speciální prací nebo mycí programy, které se přizpůsobují typu tkaniny nebo nádobí a mají zabudovaný analyzátor znečištění a automatická doporučení pro efektivní čištění. Pračky LG mají zabudovanou umělou inteligenci. [16]

- Chytré vysavače a úklidové systémy umožňují kontrolovat proces, když jste mimo domov, a přizpůsobit proces čištění. Některé robotické vysavače mají například systém automatického dobíjení, obnovení úklidu po dobití, hlasové ovládání. [16]

2.2.3 Chytrá zdravotnická zařízení

Dalším trendem, který pandemie urychlila, je to, že mnoho technologií pro inteligentní domácnosti se začalo zaměřovat buď výhradně na zdravotní přínosy, nebo alespoň zdůrazňují potenciál aplikací v této oblasti. Například chytré termostaty již dlouho patří mezi nejoblíbenější zařízení, ale nyní mají některé z nich integrované funkce, jako jsou senzory vlhkosti, které pomáhají zlepšovat kvalitu vzduchu. [16] [18]

Vzrostl také prodej chytrých čističek vzduchu a klimatizací, které umožňují pomáhat zlepšovat a udržovat kvalitu ovzduší v době této celosvětové zdravotní krize. Některé chytré domovní zvonky integrují funkci snímání teploty, takže lidé mohou své hosty před vpuštěním do domu zkontrolovat podle jednoho z nejzákladnějších ukazatelů Covid-19 . [16] [18]

V menší míře přispívají ke zlepšení celkového zdravotního stavu chytré systémy filtrace vody inspirované Covidem. Dnešní chytré toalety jdou daleko za hranice běžných toalet a využívají senzory pro analýzu odpadu a pokožky, aby poskytly přehled o zdravotním stavu uživatele a upozornily ho na případné problémy v naději, že uživatel může vyhledat odbornou pomoc dříve, než se problém zhorší. [16] [18]

V roce 2021 bude i nadále růst význam trendu, který se týká zdraví a který byl během pandemie podpořen také v důsledku zavírání tělocvičen a fitness studií, tedy zvyšování času stráveného doma. Zvýšený zájem vyvolávají chytrá fitness zařízení, jako je Mirror, Smart Trainer od Samsungu a aplikace Ultrahuman vytvořená pro připojení k hodinkám Apple Watch uživatele. Díky nim můžete cvičit doma a dostávat odborné tréninky od asistenta s umělou inteligencí. [16] [18]

2.2.4 Vysokorychlostní připojení k internetu

Jedním z hlavních předpokladů pro inteligentní domy budoucnosti je vysokorychlostní připojení k internetu prostřednictvím mesh Wi-Fi nebo jiné podobné technologie. Pomalé připojení a hluchá místa, která se objevují, když se vzdálíte od svého routeru, se stanou problémem minulosti, když mesh Wi-Fi propojí váš primární router se všemi vašimi zařízeními bez ztráty kvality. Celý dům bude mít vysokorychlostní připojení pro všechna zařízení chytré domácnosti, která v něm budou nainstalována. [16][17]

2.2.5 Použití technologií autonomního bydlení

Lidé začali používat inteligentní domy, aby mohli vést udržitelnější a pohodlnější životní styl. V nadcházejících letech se budou trendy vývoje těchto technologií točit kolem tohoto

konceptu. Udržitelnost bude na vrcholu seznamu trendů v oblasti technologií pro chytré domácnosti. [16][17]

Využití autonomních technologií je jedním ze způsobů, jak řešit složité výzvy udržitelnější budoucnosti. Již nyní existuje řada řešení, která umožňují autonomní provoz inteligentních domů v případě nouzových situací nebo výpadků. Mezi taková řešení patří využívání systémů pro ukládání energie a solárních systémů, které omezují závislost na externích organizacích a snižují uhlíkovou stopu. Technologie napájení mimo síť jsou jedním z trendů inteligentních domů, který bude pokračovat ještě mnoho let. [16]

2.2.6 Bezkontaktní technologie

Tento trend již začal pronikat do oblasti chytrých domácností a pandemie Covid-19 jej v posledních letech ještě urychlila. Mnoho lidí je již zvyklých na bezkontaktní dávkovače dezinfekce rukou v maloobchodě, a i když tyto pravděpodobně nejsou vybaveny chytrým systémem, potenciál tu je a koncept bezkontaktních zařízení se rozšiřuje. [16]

Bezkontaktní zvonky jsou například novinkou, která umožňuje hostům ohlásit svůj příchod, aniž by se dotýkali běžných povrchů, kde se mohou šířit bakterie. A samozřejmě mnoho domácích zařízení se ovládá prostřednictvím mobilních aplikací, takže každá osoba s těmito systémy se dotýká pouze svého telefonu, nikoliv samotného zařízení. Totéž platí pro zadávání příkazů hlasem, které se již začíná rozšiřovat díky hlasovým "asistentům", jako jsou Amazon Alexa a Siri. [16][17]

2.2.7 Domácí roboti

Pokroky v oblasti umělé inteligence, využití laserového mapování a vývoj vztahů mezi lidmi a roboty pomáhají zlepšit schopnost robotů vykonávat běžné domácí práce. Již za několik let nám budou roboti vařit jídlo, uklízet v našich domácnostech, prát oblečení, zalévat květiny a dokonce se starat o naše domácí mazlíčky. Kamery, které robotům nahradí oči, budou schopny rozpoznávat předměty a mikrofony, které jsou ušima, budou schopny rozpoznávat řeč. Díky tomu budou roboti schopni být lidem nejen skvělými pomocníky, ale také se starat o jejich bezpečnost. Kromě toho se tito vyspělí roboti budou schopni přizpůsobovat měnícímu se prostředí pomocí pokročilých algoritmů strojového učení. Budou vybaveny senzory, které jim umožní přesněji vnímat své okolí a činit chytřejší rozhodnutí. Důležitým prvkem jejich funkčnosti bude schopnost sdílet data s ostatními zařízeními v domácnosti, což umožní lepší koordinaci úkolů a vytvoření integrovaného prostředí pro pohodlnější a komfortnější

bydlení. Takto technologicky vyspělí roboti nejen zvýší efektivitu procesů v domácnosti, ale také zlepší bezpečnost a pohodlí uživatelů. [16]

2.3 Typy komunikačních protokolů chytré domácnosti

Komunikační protokol je soubor pravidel a standardů, které definují způsob vzájemné komunikace zařízení. Komunikační protokoly se používají k přenosu informací mezi počítači, servery, chytrými zařízeními a dalšími objekty. Definují formát dat, způsob odesílání a přijímání informací a jejich ochranu. Komunikační protokoly hrají důležitou roli při zajišťování bezpečnosti a spolehlivosti sítí a zvyšování efektivity zařízení. [19][20]

Některé značky používají pro svá zařízení standardní protokoly, které všichni známe: Wi-Fi a Bluetooth. V poslední době je však stále populárnější vytvářet pro chytrá zařízení vlastní komunikační protokoly. Zpočátku společnosti vytvářely vlastní sítě, ale pro uživatele to nebylo příliš pohodlné, protože zařízení s různými značkami a protokoly fungovala špatně nebo nefungovala vůbec. Proto se všechny značky rozhodly používat speciálně vyvinutý protokol: ZigBee. Ten umožňuje organizovat práci se zařízeními různých značek. Zároveň není závislý na platebním signálu internetové sítě. Ten je nutný pouze pro programování. ZigBee se tak stal nejoblíbenějším komunikačním protokolem pro chytrá zařízení. Úplně každý komunikační protokol má své pro a proti a já bych si rád prošel ty nejpoužívanější a pochopil, jak fungují. [19][20]

2.3.1 Bluetooth

Bluetooth je protokol, který uživatelé znají již čtvrt století. Existují také zařízení chytré domácnosti, která lze ovládat prostřednictvím Bluetooth, například některá světla Yeelight Mijia a Philips Hue. Tento typ rádiové komunikace je skvělým způsobem, jak začít s automatizací domácnosti, protože všechny chytré telefony mají zabudované rozhraní Bluetooth. Hlavní výhodou technologie Bluetooth je, že je spolehlivá a lokalizovaná, což znamená, že není závislá na internetu. Chytrá zařízení obvykle používají levné moduly Bluetooth s nízkou spotřebou energie. Například BLE je poměrně spolehlivý komunikační protokol, který umožňuje, aby zařízení dlouho fungovalo na baterii. Dosah Bluetooth je obvykle krátký - asi 10 metrů, takže "chytrá" zařízení můžete ovládat hlavně v jedné místnosti. K rozšíření systému se používá technologie Bluetooth Mesh. Tato technologie umožňuje každému zařízení komunikovat s ostatními zařízeními a ovládání se provádí pomocí brány, která takové spojení podporuje. [19] [21]

2.3.2 Wi-Fi

Wi-Fi bylo vyvinuto ve stejné době jako Bluetooth. Podívejme se na principy protokolu Wi-Fi na příkladu zásuvky Wi-Fi. Připojí se k domácímu směrovači, získá IP adresu a stane se samostatným uzlem v síti, takže nepotřebuje žádnou bránu. Pokud máte přístup k internetu, můžete zásuvku sledovat a ovládat z chytrého telefonu kdekoli na světě. Wi-Fi má vysokou šířku pásma, například Wi-Fi 6. generace - až 11 Gb/s - a Wi-Fi 7. generace - až 30 Gb/s, vysoké přenosové rychlosti a širokou konektivitu. [19]

Tento protokol je vhodný pro vytvoření inteligentní domácnosti, protože většina lidí již má router Wi-Fi. Wi-Fi se často používá, když je vyžadována vysoká šířka pásma. Jednou z nevýhod tohoto typu připojení je nízká energetická účinnost a poměrně slabé routery. Bohužel mnoho poskytovatelů internetových služeb často nabízí svým zákazníkům levné a slabé Wi-Fi routery. To vede k tomu, že velké rodiny mají problémy s pokrytím, stabilním signálem a omezeným počtem připojených chytrých zařízení. Některé směrovače podporují pouze deset bezdrátových připojení. Vzhledem k tomu, že k routeru jsou již připojeny např. televizory, mobilní telefony, tablety, počítače, notebooky atd., dochází po přidání nových chytrých zařízení k rychlému přetížení routerů. Wi-Fi je také velmi vytížený a hlučný protokol, zejména v obytných domech. Pokud například využíváte celou šířku pásma Wi-Fi ke sledování videa v rozlišení 4K, může se signál pro zapnutí a vypnutí světel zaseknout ve frontě, což zpomaluje celý proces interakce s vaší chytrou domácností. Pokud se tedy rozhodnete pro vybudování svého ekosystému využívat Wi-Fi, pořiďte si nejprve výkonný router, který pracuje na různých frekvencích: 2,4; 5; 6 GHz a dokáže připojit desítky chytrých zařízení. [21]

2.3.3 Z-Wave

Protokol Z-Wave je bezdrátová verze protokolu pro domácí automatizaci. Vytvořila jej společnost Zensys, nyní Sigma Designs, která v roce 2013 aktualizovala jeho funkce a nazvala jej Z-Wave Plus. Na rozdíl od technologií Bluetooth a Wi-Fi, které byly vytvořeny z jiných důvodů a poté přijaty průmyslem inteligentních domácností, byl protokol Z-Wave navržen speciálně pro domácí automatizaci. Mezi výhody protokolu Z-Wave patří vysoká bezpečnost síťového protokolu, nízká spotřeba energie, schopnost provozovat zařízení až několik let na jednu baterii, stabilita komunikace, ovládání na vzdálenost až 100 metrů volného prostoru a kompatibilita s chytrými zařízeními od různých výrobců s logem Z-Wave. Z-Wave je nízkofrekvenční síť pracující v pásmu 900 MHz, které již není využíváno jinými rádiovými

zařízeními. Díky tomu je síť méně náchylná k rádiovému rušení a kratší vlnová délka umožňuje signálu snadněji procházet zdmi a jinými rušivými vlivy. Rozšíření Smart Home je vždy k dispozici a umožňuje připojit až 232 chytrých zařízení k jednomu ekosystému. [19] [21]

Protokol Z-Wave vytváří síť, která zvyšuje dosah a flexibilitu komunikace. Síť mesh je síť, která je tím silnější a spolehlivější, čím více chytrých zařízení je k ní připojeno. Je to proto, že zařízení Z-Wave připojená ke zdroji napájení mohou fungovat jako opakovače, ke kterým lze připojit další malá zařízení. Ty přenášejí signály od zařízení k zařízení, dokud nedosáhnou řídicí jednotky. Z-Wave je plně lokalizovaná síť, která umožňuje chytrým zařízením fungovat i při výpadku internetového připojení. [21]

Nevýhodou sítě je omezená šířka pásma: rychlost i u nejnovějších zařízení řady 700 se pohybuje kolem 100 kb/s, což je mnohem pomalejší než Wi-Fi a dokonce i Bluetooth, takže na ni můžete zapomenout při streamování HD videa nebo používání kamer. Zařízení Z-Wave jsou také dražší než jejich protějšky Bluetooth, Zigbee a Wi-Fi. Vzhledem k tomu, že standard byl uzavřen až do roku 2019, je nabídka zařízení značně omezená. [19] [21]

Pokud plánujete v chytré domácnosti používat zařízení s nízkou šířkou pásma, jako jsou inteligentní senzory, chytré osvětlení, zámky, teplotní čidla atd. A pokud jste v situaci, kdy jsou zařízení pro automatizaci domácnosti vzdálená, můžete přidat zařízení Z-Wave, abyste posílili síť ve vzdálených koutech budovy.[21]

2.3.4 ZigBee

Protokol Zigbee existuje již od 90. let minulého století, takže má za sebou dlouhou historii a etabloval se jako spolehlivý protokol pro domácí automatizaci. Zjednodušeně řečeno se jedná o lokální a šifrovaný komunikační protokol s nízkou spotřebou energie pro chytré domácnosti. Počet produktů Zigbee dostupných online je impozantní. [22]

V současné době je Zigbee nejoblíbenějším a nejpoužívanějším komunikačním protokolem pro produkty internetu věcí. Protokol Zigbee podporuje až 65 000 připojených zařízení v jedné topologii sítě. Zigbee 3.0 vytváří síť tak, že prakticky jakékoli drátové zařízení přidané do ekosystému může fungovat jako rozbočovač, čímž se celý systém stává spolehlivějším a odolnějším. K vytvoření celé sítě a připojení dalších chytrých zařízení k ní slouží brána Zigbee. Drátové modely fungují jako mosty, podporují až 20 koncových zařízení a rozšiřují dosah ekosystému. [21] [22]

Stejně jako Z-Wave vytváří Zigbee místní síť, která je nezávislá na připojení k internetu. Data přenášená mezi zařízeními jsou přitom šifrovaná a spotřebovávají velmi málo energie. Protokol Zigbee má malou šířku pásma, přibližně 250 kb/s. To je dvaapůlkrát rychlejší než Z-Wave, ale stále příliš pomalé pro streamování videa. Stejně jako v případě protokolu Z-Wave má i Zigbee organizaci výrobců a certifikační program. Jeho kvalita se však u jednotlivých výrobců liší, protože není důsledně testován. [22]

2.3.5 Thread

Thread je nový protokol pro inteligentní domy, který je velmi podobný protokolu Zigbee. V podstatě je Thread založen na rádiových zařízeních používaných v Zigbee. Při použití stejného rádiového spektra 2,4 GHz a šířky pásma například 250 kb/s vytváří Thread šifrovanou síť, která je bezpečná a má nízkou spotřebu energie. Thread má dokonce certifikační program podobně jako Z-Wave a Zigbee. Dá se tedy říci, že Thread v sobě zahrnuje všechny výhody předchozích protokolů. [21] [23]

Thread však obsahuje důležité změny, díky kterým je lepší než ostatní. Thread se od ostatních liší tím, že je založen na internetovém protokolu IPv6. Jeho hlavní výhodou je, že podporuje více uzlů v jednom ekosystému. Pokud například selže brána Z-Wave nebo Zigbee, selže celý ekosystém. Pokud si koupíte nový zámek, je třeba znovu připojit všechna zařízení. Jednou z hlavních výhod technologie Thread je, že v jednom ekosystému můžete mít více bran. Jedna z nich je vybrána jako hlavní brána a stává se správcem sítě. Pokud tato hlavní brána selže nebo dojde k jejímu výpadku, nastoupí na její místo jiná, díky čemuž je celá síť odolnější a méně náchylná k selhání. [23]

Zařízení Smart Thread mohou také vypínat své vlastní rádiové signály, pokud nejsou potřeba, a jsou tak energeticky úspornější než zařízení Zigbee a Z-Wave. Například zařízení Zigbee vydrží na baterii rok, zatímco podobné zařízení Thread dva až tři roky. [23]

A konečně, Thread používá protokol IPv6, což znamená, že je snadno kompatibilní se zařízeními Wi-Fi a Bluetooth. Síť Thread je odolná vůči poruchám a vytváří bezpečnou, spolehlivou a stabilní síť bez výpadků, inteligentní zařízení, která se snadno připojují a podporují cloudový provoz. S protokolem Thread lze vytvořit rozsáhlý ekosystém, protože systém může mít 1 hlavní bránu podporující připojení k internetu a 31 dalších bran, z nichž každá připojuje více než 500 zařízení. [23]

2.3.6 Matter

Matter je globální protokol, který v roce 2019 spustila globální společnost zabývající se technologiemi a platformami IoT. Protože žádná společnost nedokáže pokrýt celý ekosystém svých zařízení, rozhodli se giganti v oblasti IoT vytvořit protokol, který by propojil vše, a tím se stal Matter. Na tom, aby byla zařízení chytré domácnosti používající výše uvedené protokoly interoperabilní prostřednictvím čisté rádiové komunikace, se podílí již více než 300 společností. Cílem Matteru je učinit chytrou domácnost dostupnější, modernější, pohodlnější a jednodušší na používání. Komunikační standard Matter je určen k ovládání všech zařízení v domácnosti: osvětlení, vytápění, zabezpečení, větrání, spotřebičů, různých senzorů, audio a video zařízení atd. Matter si bere to nejlepší, co nabízejí ostatní protokoly. Matter lze použít pro bezpečnou komunikaci mezi aplikacemi internetu věcí. K ochraně dat před neoprávněným přístupem využívá šifrování pomocí veřejného klíče a autorizaci na základě certifikátu. Matter je speciálně navržen pro chytré produkty všech výrobců a platforem. [24]

Do konce roku 2022 obdrží některé produkty internetu věcí softwarové aktualizace a budou podporovat protokol Matter a v roce 2023 bude k dispozici přibližně 1 000 certifikovaných chytrých zařízení. Protokol Matter využívá standardní internetové technologie, jako je IP adresa a Wi-Fi, takže je flexibilnější a přizpůsobivější než mnoho jiných protokolů. Stará zařízení není třeba vyměňovat, ale lze je integrovat do nového systému. Díky protokolu Matter se navíc spotřebitelé a vývojáři chytrých domácností nemusí obávat nekompatibility chytrých zařízení. [24]

Protokoly zkrátka zajišťují bezproblémovou komunikaci a interakci mezi zařízeními a systémy. Vzhledem k tomu, že poptávka po technologiích chytré domácnosti stále roste, je důležité, aby výrobci a vývojáři využívali a integrovali nejnovější protokoly a zdokonalovali tak technologie internetu věcí, aby je mohl využívat každý. [19]

3 ZÁKLADNÍ TERMINOLOGIE

V této části bych chtěl podrobněji rozebrat pojmy nezbytné pro další práci, jako jsou aktiva, hrozby, rizika a bezpečnostní opatření. Dále se budu zabývat hlubšími pojmy, jako jsou hmotná a nehmotná aktiva, vnitřní a vnější hrozby, způsoby identifikace a analýzy rizik a bezpečnostní opatření k minimalizaci rizik. Podrobné pochopení těchto pojmů umožní nejen hlubší porozumění analyzovanému problému, ale také poskytne účinnější řešení pro zajištění bezpečnosti a odolnosti systému inteligentní domácnosti.

3.1 Aktivum

V kontextu bezpečnosti je aktivem jakýkoli objekt nebo zdroj, který má pro vlastníka nemovitosti nebo podniku hodnotu. Při analýze rizik je třeba řádně zohlednit všechna aktiva, protože jejich ochrana je základním cílem každého systému řízení bezpečnosti. Jakákoli ztráta aktiva může vlastníkovi způsobit nejen finanční škody, ale také škody na pověsti. A tak se aktiva dělí na hmotná a nehmotná.

3.1.1 Hmotná aktiva

Hmotná aktiva jsou všechny fyzické předměty nebo zdroje, které jsou ve vlastnictví osoby nebo podniku a mají určitou finanční hodnotu. Tato aktiva mohou být snadno měřitelná a hmatatelná. Hmotná aktiva jsou například infrastruktura, dopravní prostředky, zařízení a výrobky.

3.1.2 Nehmotná aktiva

Nehmotná aktiva jsou všechny nehmotné zdroje, které jsou ve vlastnictví osoby nebo podniku a mají významnou hodnotu. Tato aktiva nejsou hmatatelná ani fyzicky měřitelná, ale mohou mít významný vliv na činnost, cenu a pověst podniku. Mezi nehmotná aktiva mohou patřit například lidské zdroje, které zahrnují znalosti, dovednosti a zkušenosti zaměstnanců, duševní vlastnictví, jakákoli data a informace a také pověst a značka.

3.2 Hrozba

Podle Ministerstva vnitra České republiky je hrozba „Jakýkoli fenomén, který má potenciální schopnost poškodit zájmy a hodnoty chráněné státem. Míra hrozby je dána velikostí možné škody a časovou vzdáleností (vyjádřenou obvykle pravděpodobností čili rizikem) možného uplatnění této hrozby[25].“

V závislosti na zdroji lze hrozby rozdělit na vnitřní a vnější.

3.2.1 Vnitřní hrozby

Vnitřní hrozby jsou hrozby, které pocházejí zevnitř objektu nebo společnosti. Tyto hrozby mohou být způsobeny buď zaměstnanci organizace, anebo různými procesy a systémy v rámci organizace. Vnitřními hrozbami mohou být například technické poruchy, které mohou vést ke ztrátě důležitých dat nebo k úplnému zastavení některých procesů organizace. Nedodržení bezpečnostních pravidel může mít pro organizaci rovněž vážné důsledky.

3.2.2 Vnější hrozby

Vnější hrozby jsou hrozby vyskytující se mimo organizaci nebo zařízení, které by mohly negativně ovlivnit činnost vlastníka nebo jeho aktiva. Vnějšími hrozbami mohou být například přírodní katastrofy, jako jsou zemětřesení, povodně, uragány nebo lesní požáry, které mohou zničit infrastrukturu podniku. Vnějšími hrozbami jsou také jednání konkurentů, jejichž cílem může být snížení konkurenceschopnosti podniku.

3.3 Riziko

Podle Ministerstva vnitra České republiky je riziko „Možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí. Riziko je vždy odvoditelné a odvozené z konkrétní hrozby.[26]“

3.3.1 Identifikace rizik

Identifikace rizik je proces identifikace a popisu možných rizik, která mohou ovlivnit různé procesy v organizaci nebo objektu. Tento proces zahrnuje několik klíčových činností, jejichž výsledek bude nezbytný pro další analýzu rizik. Při identifikaci rizik je třeba vzít v úvahu aktiva, která mohou být ohrožena riziky, a také vnější a vnitřní hrozby. Na základě všech těchto údajů je třeba identifikovat slabá místa v systémech, procesech nebo již existující ochraně aktiv. Po identifikaci slabých míst je třeba vypracovat různé scénáře, v nichž by se teoreticky mohla určitá rizika realizovat.

3.3.2 Analýza rizik

Analýza rizik je proces stanovení pravděpodobnosti výskytu rizik a možných nepříznivých dopadů na organizaci. Při provádění analýzy rizik je nutné určit pravděpodobnost výskytu rizik, například v procentech, a také posoudit možné důsledky realizovaných rizik, například

poškození pověsti, finanční ztráty nebo únik informací. Existuje obrovské množství metod analýzy rizik, všechny se liší svou složitostí a rozsahem. Každá organizace si vybírá jednu nebo více metod analýzy rizik, které nejlépe vyhovují jejím konkrétním cílům a potřebám.

Identifikace a analýza možných rizik umožňuje organizaci včas se připravit na možné ohrožení a vypracovat scénáře řešení problémů nebo minimalizovat rizika jejich výskytu. Všechny tyto procesy přispívají k udržitelnému, bezpečnému a trvalému fungování organizace.

3.4 Bezpečnostní opatření

Bezpečnostní opatření jsou konkrétní kroky, které organizace přijímá k minimalizaci, prevenci a řízení rizik a hrozeb, které mohou nepříznivě ovlivnit aktiva nebo provoz organizace. Zahrnují vypracování bezpečnostních politik, fyzická ochranná opatření, jako jsou režimová opatření a kamerový dohled, ochranu informací prostřednictvím šifrování a používání antivirového softwaru, školení zaměstnanců, zkušební mimořádné situace a bezpečnostní audity. Bezpečnostní opatření jsou nedílnou součástí zajištění nepřetržitého a bezpečného provozu každé organizace nebo objektu. Základem efektivního návrhu a realizace bezpečnostních opatření je analýza rizik, která by měla být provedena předem.

II. PRAKTICKÁ ČÁST

4 ANALÝZA BEZPEČNOSTI CHYTRÉ DOMÁCNOSTI

V této části své bakalářské práce se zabývám bezpečnostní analýzou systémů inteligentních domácností. Hlavním cílem této části je identifikovat bezpečnostní aktiva a hrozby, se kterými se může setkat každý majitel chytrých domácích zařízení. V této analýze budou zohledněna jak hmotná, tak nehmotná aktiva, stejně jako vnější a vnitřní hrozby pro bezpečnost uživatele a jeho majetku.

4.1 Aktiva chytré domácnosti

Aktiva chytré domácnosti jsou všechny fyzické i nefyzické prvky v domácnosti, které mohou být jakýmkoli způsobem ovlivněny zařízeními chytré domácnosti. Všechny tyto prvky je třeba vzít v úvahu při posuzování potenciálních hrozeb, jako jsou například kybernetické útoky, neoprávněný přístup nebo fyzické poškození. Tato část se zaměřuje na identifikaci aktiv inteligentní domácnosti, aby bylo možné lépe pochopit možné hrozby a následně analyzovat rizika.

4.1.1 Hmotná aktiva chytré domácnosti

V současné době roste aktuálnost a zájem o chytrá domácí zařízení, která zjednodušují nebo plně automatizují různé domácí a rutinní procesy. Většina lidí však vůbec nepřemýšlí o nebezpečích, která mohou při používání těchto zařízení vzniknout. Na začátek bych chtěl určit, jaké hmotná aktiva mohou být potenciálně ohrožena zařízeními chytré domácnosti.

V první řadě jsou hmotnými aktivy samotná zařízení chytré domácnosti. Může se s nimi stát cokoli, od samovznícení až po fyzické poruchy, které mohou způsobit škody na okolních předmětech, a dokonce i na lidech. Nejdůležitějším hmotným aktivem v systémech chytré domácnosti je však lidský život. Je důležité si uvědomit, že všechna zařízení chytré domácnosti jsou elektrická zařízení, která mohou člověka nejen zasáhnout elektrickým proudem, ale také se mohou vznítit, což může také potenciálně ohrozit život člověka. Mnoho lidí používá chytrá zařízení také pro domácí mazlíčky, například chytrá pítka a hračky. Život domácích mazlíčků je také důležitým aktivem.

Dalším hmotným aktivem chytrých domácích systémů je nábytek v bytě nebo domě. Nesprávné používání nebo konstrukce elektrických zařízení může poškodit nebo dokonce zničit nábytek v domácnosti. Byt nebo dům, kde jsou umístěna zařízení chytré domácnosti, je jednoznačně dalším hmotným aktivem systémů chytré domácnosti. Zařízení chytré domácnosti

jsou hořlavá, což může zcela zničit byt i se vším, co se v něm nachází. Sem mohou patřit i dopravní prostředky, které v současné době stále častěji využívají různá chytrá zařízení, například k dálkovému ovládání vytápění vozu. Jakékoli z těchto zařízení může selhat a vznítit se, což může rovněž zničit vozidlo. Důležitým hmotným aktivem jsou také řídicí jednotky, které jsou důležitou součástí pokročilejších systémů chytrých domácností. Mohou totiž způsobit selhání celého systému.

Na závěr této části bych chtěl zdůraznit důležitost definování hmotných aktiv inteligentní domácnosti v kontextu zajištění bezpečnosti a funkčnosti celého systému. Na základě této analýzy je možné formulovat konkrétní hrozby, které mi v budoucnu pomohou při práci. Je také důležité poznamenat, že bezpečnost celého systému inteligentní domácnosti nezávisí na výrobci nebo ceně jednotlivých zařízení, ale na správné konfiguraci a integraci všech zařízení jako celku. Pozornost je třeba vždy věnovat spolupůsobení jednotlivých komponent, aby byl veškerý hmotný majetek dobře chráněn.

4.1.2 Nehmotná aktiva chytré domácnosti

V analýze bezpečnosti systémů chytré domácnosti jsou nesmírně důležitá nehmotná aktiva, která jsou nedílnou součástí těchto technologií. Zabezpečení těchto aktiv musí být na nejvyšší úrovni, protože ztráta jakéhokoli nehmotného aktiva může vést k mimořádně vážným důsledkům pro pověst uživatele i výrobce systému chytré domácnosti.

Nehmotná aktiva zahrnují především osobní údaje uživatelů. Pro ovládání téměř všech zařízení je nutné se zaregistrovat v aplikaci se svými osobními údaji. Také během provozu mnoha zařízení chytré domácnosti se shromažďuje obrovské množství různých osobních údajů o uživatelích, které slouží k personalizaci a zlepšení fungování systému. V případě úniku těchto údajů může být ohrožen život člověka. Dalším nehmotným aktivem systémů inteligentní domácnosti je software. Jeho součástí jsou operační systémy, platformy a mobilní aplikace pro správu chytrých domácností a také cloudové služby pro ukládání dat a vzdálenou správu zařízení chytrých domácností.

Důležitým nehmotným aktivem, které je třeba při konstrukci zařízení zohlednit, jsou také různé algoritmy a analytické údaje. Mnoho systémů pro inteligentní domácnosti má speciální algoritmy strojového učení, které optimalizují výkon zařízení a také předpovídají potřeby uživatelů. Významným nehmotným aktivem v systémech inteligentní domácnosti je také způsob šifrování dat, komunikační protokoly pro bezpečný přenos dat a technologie pro ověřování a autorizaci uživatelů. Bezpečnost těchto aktiv musí být udržována na nejvyšší

úrovni, protože prolomením šifrování může potenciální útočník získat údaje ke všem ostatním nehmotným aktivům.

Nehmotná aktiva systémů chytré domácnosti tak hrají zásadní roli při zajišťování důvěrnosti, integrity a dostupnosti dat a různých funkcí těchto systémů. Klíčovými aspekty pro minimalizaci rizik a zajištění bezpečného a pohodlného používání technologií inteligentní domácnosti jsou efektivní správa a neustálé zlepšování bezpečnosti systémů inteligentní domácnosti.

4.2 Hrozby chytré domácnosti

Dostupnost a popularita systémů inteligentních zařízení každým rokem roste. Tyto systémy umožňují nejen automatizovat mnoho běžných domácích procesů, ale také zlepšit úroveň života zavedením nových technologií do života běžných lidí. S rostoucí oblibou těchto systémů však roste i riziko bezpečnostních hrozeb. Ohrožen může být nejen samotný systém chytré domácnosti, ale také důležité osobní údaje a bezpečnost obyvatel domu. Na základě specifikovaných aktiv systémů chytrých domácností v minulé části bych chtěl identifikovat hrozby, které jsou s nimi spojeny. Hrozby jsou rozděleny do 2 hlavních kategorií: vnější a vnitřní.

4.2.1 Vnější hrozby chytré domácnosti

Vnější hrozby jsou hrozby z vnějšího prostředí, které mohou ovlivnit funkčnost nebo bezpečnost systémů inteligentní domácnosti nebo jejich majitele. Zahrnují širokou škálu různých hrozeb, od kybernetických útoků až po krádeže zařízení. Je velmi důležité, aby všechny součásti systémů chytré domácnosti měly zavedena robustní bezpečnostní opatření, která minimalizují možnost vnějších útoků. V této části bych chtěl identifikovat vnější hrozby, abych je mohl zohlednit ve své další části práce při analýze rizik.

Jednou z nejvýznamnějších vnějších hrozeb pro systémy inteligentní domácnosti je hackerský útok. Hacking znamená neoprávněný přístup k systémům inteligentní domácnosti prostřednictvím zneužití zranitelností v softwaru zařízení nebo nedostatečně zabezpečených sítí. Hackeři mohou získat přístup ke všem osobním údajům uživatelů, ovládacím prvkům celého systému, a dokonce způsobit fyzické poškození zařízení prostřednictvím neomezené manipulace s těmito zařízeními. Dále může hacker získané údaje použít k osobním účelům, například k vydírání oběti.

Instalace škodlivého softwaru (Malware) do chytrých domácích zařízení může také způsobit různé typy škod. Malware může například monitorovat činnost uživatele a krást citlivé informace pomocí senzorů, kamer a mikrofonů, stejně jako sledovat historii prohlížeče, kterou lze následně využít k vydírání nebo prodeji informací. Škodlivý software může také narušit jednotlivá zařízení, což může negativně ovlivnit celý systém a poškodit jak oficiální programové vybavení zařízení, tak i zařízení jako celek. Malware může být nainstalován hackerem při vloupání do systému chytré domácnosti, neopatrným jednáním uživatele nebo dokonce obyčejným kurýrem při doručování zařízení do domu zákazníka.

Phishing je další bezpečnostní hrozbou pro inteligentní domácí systémy. Phishing představuje podvodné metody, jejichž cílem je získat údaje o účtu nebo jiné citlivé informace od uživatelů chytrých domácností. Útočník může používat falešné e-maily, SMS nebo speciálně vytvořené webové stránky, které se liší pouze jedním znakem v adresovém řádku. Nepozorní uživatelé mohou omylem uložit soubor zaslaný do pošty pod záminkou oficiálního dopisu od poskytovatele internetu a tento soubor může obsahovat virus, který ukradne citlivé informace ze všech systémů inteligentní domácnosti. Podvodníci mohou tyto údaje použít k získání neoprávněného přístupu ke všem systémům inteligentní domácnosti.

Vážnou hrozbou pro systémy chytré domácnosti je také sociální inženýrství. Sociální inženýrství je druh psychologické manipulace s osobou za účelem získání citlivých informací nebo přístupu k systémům. Útočníci se mohou vydávat za technickou podporu a trvat na změně nastavení zabezpečení nebo požadovat přihlašovací údaje uživatele. Mohou se také nabourat do stránek vaší rodiny a přátel na sociálních sítích a pomocí chatu se pokusit získat vaše údaje. V současné době je mnoho procesů automatizováno pomocí umělé inteligence, což riziko této hrozby ještě zvyšuje.

Mezi fyzické vnější hrozby patří krádež zařízení. Mnoho lidí umisťuje různé senzory, kamery nebo chytré domofony mimo budovu, což velmi usnadňuje krádež těchto zařízení. Pomocí získaných zařízení mohou narušitelé získat také přístup k síti a osobním údajům celého systému, což pak může vést k vážným následkům. To s sebou nese i finanční ztráty pro majitele ukradených zařízení.

Vandalismus je další bezpečnostní hrozbou pro chytré systémy v domácnostech. Někteří lidé mohou jen tak pro zábavu rozbít kamery nebo senzory, což může ovlivnit funkčnost některých částí systému chytré domácnosti. Vandalismus také zvyšuje náklady na opravy nebo případnou výměnu zařízení novými.

Hrozbou jsou také přírodní katastrofy, jako jsou zemětřesení, povodně, uragány nebo lesní požáry. Přírodní katastrofy v podstatě způsobují fyzické poškození zařízení inteligentní domácnosti, což zvyšuje náklady na celý systém. Mnoho lidí na přírodní katastrofy při nákupu různých zařízení pro chytrou domácnost vůbec nemyslí, což může ve výsledku způsobit vážné finanční ztráty.

Existují také síťové hrozby, mezi které patří DDoS útoky. Cílem těchto útoků je přetížit celou síť systému chytré domácnosti pomocí nelegitimního datového přenosu. Útoky DDoS jsou díky své jednoduchosti pro malé systémy rok od roku častější. V rámci prevence proti takovým útokům zavádí mnoho dodavatelských firem softwarová omezení, například na počet možných připojených uživatelů nebo zařízení, ale to není dostačující. Útok DDoS představuje vážnou hrozbu, protože může vést k závažným selháním systému a úplné ztrátě dat zařízení.

Další síťovou hrozbou pro systémy chytré domácnosti jsou zranitelnosti v komunikačních protokolech, jako jsou Wi-Fi, Zigbee a další. Každý systém má vždy své chyby, neexistují stoprocentně bezpečná zařízení. Včasná řešení však mohou zabránit vážným následkům pro uživatele. Zranitelnosti v komunikačních protokolech lze zneužít k zachycení, manipulaci nebo nahrazení dat ze zařízení, například k nahrazení videa z kamerového systému videozáznamem ve smyčce, aby bylo možné vniknout do domu a ukrást majetek. Hackeři mohou tyto zranitelnosti využít také k získání přístupu do sítě inteligentní domácnosti za účelem další manipulace.

4.2.2 Vnitřní hrozby chytré domácnosti

Vnitřní hrozby jsou hrozby, které se vyskytují v samotném systému inteligentní domácnosti. Může jít o chyby v konfiguraci systému až po zranitelnosti v softwaru. Je důležité identifikovat co nejvíce vnitřních hrozeb, aby se zabránilo možným následkům pro uživatele zařízení chytré domácnosti.

Nejpopulárnější vnitřní hrozbou mezi nezkušenými uživateli je nesprávná nastavení zařízení. Mnoho lidí používá k přihlašování příliš jednoduchá hesla, což hackerům značně usnadňuje průnik do systému. Nepoužívání dvoufaktorového ověřování a nedostatečně nastavená síťová ochrana mohou rovněž zvýšit zranitelnost systému vůči kybernetickým útokům.

Další bezpečnostní hrozbou je zakázání aktualizací softwaru a firmwaru chytrých zařízení. Každý rok se objeví desítky nových způsobů, jak získat přístup k různým systémům. Pravidelné aktualizace od vývojářů pomáhají řešit zranitelnosti, jakmile jsou objeveny. Mnoho uživatelů však automatické aktualizace zařízení vypíná, což vede ke zvýšené bezpečnostní hrozbě pro systémy chytré domácnosti.

Chyby v softwarovém kódu jsou také vážnou bezpečnostní hrozbou. Většina softwaru je psána ručně lidmi, takže vždy existuje možnost chyb nebo omylů na straně programátorů. Útočníci mohou tyto chyby odhalit dříve než vývojáři a využít je k získání neoprávněného přístupu nebo narušení systému. Proto je důležité nevypínat automatické aktualizace zařízení.

Další vnitřní hrozbou je nedostatečná ochrana přístupových práv. Někteří uživatelé nevěnují dostatečnou pozornost ochraně přístupových práv ke svým systémům chytré domácnosti a dávají nadměrná práva všem svým známým a dočasným pracovníkům. Nadměrný počet uživatelů s přístupovými právy k systému může negativně ovlivnit bezpečnost celého systému. Telefon vašeho známého s přístupem ke kameře v domě může být prolomen a útočník může využít přístup do systému pro své vlastní účely. Lidé také často nenakonfigurují metody ověřování uživatelů, což má velký vliv na zabezpečení.

Nerozdělení přístupových práv do různých úrovní má také negativní dopad na bezpečnost celého systému. Je důležité řádně zvážit, komu a jaká práva udělit. Pokud nejsou práva správně rozdělena, mohou uživatelé s minimálními právy přistupovat ke kritickým funkcím systému a měnit důležitá nastavení zabezpečení bez vašeho vědomí.

Ukládání všech dat musí být také řádně zabezpečeno. Zranitelné úložiště může vést ke krádeži nebo úniku dat do internetu. Používání neověřených nebo bezplatných cloudových úložišť také zvyšuje riziko zneužití dat třetími stranami. Každé zařízení také ukládá obrovské množství dat a musí být zabezpečeno.

Další vnitřní hrozbou je nešifrování při přenosu dat. Každé zařízení by mělo používat moderní metody šifrování pro přenos dat v rámci celého systému chytré domácnosti, mobilních telefonů a cloudových úložišť. Při absenci šifrování mohou být citlivá data a důvěrné informace zachyceny za účelem získání přístupu do systému nebo pozdějšího prodeje.

Jednou z vnitřních hrozeb jsou také chyby uživatelů. Kvůli neznalosti nebo nepozornosti uživatele může být systém zranitelný vnějšími hrozbami. Přestože phishing je vnější hrozbou, bez chyby uživatele uvnitř systému nemůže útočník získat přístup do systému

prostřednictvím phishingu. Otevření phishingových e-mailů nebo instalace podezřelých aplikací může nakonec vést k vážným důsledkům pro zabezpečení celé chytré domácnosti.

Každá z hrozeb uvedených v tomto bloku vyžaduje specifická bezpečnostní opatření a strategie prevence. Ve své bakalářské práci se zaměřím na analýzu rizik na základě těchto hrozeb a navrhnu způsoby jejich minimalizace. Již nyní však lze říct, že k eliminaci mnoha hrozeb stačí, aby se uživatelé řídili pokyny výrobce.

5 ANALÝZA RIZIK A JEJÍ VYHODNOCENÍ

Analýza rizik je důležitou součástí zajištění bezpečnosti v mnoha oblastech. V oblasti zabezpečení chytrých domácností je také nutné provádět analýzy rizik, aby bylo možné identifikovat a řešit různé zranitelnosti, které pak mohou vést k vážným následkům. Existuje obrovské množství metod analýzy rizik, které se liší především svou složitostí, rozsahem a požadavky na osoby, které ji provádějí. V této bakalářské práci budu používat metodu FMEA, která je jednou z nejpopulárnějších metod na celém světě. Na základě výsledků této analýzy rizik navrhnu různé způsoby řešení hrozeb a rizik, se kterými se může setkat každý uživatel systémů chytré domácnosti.

5.1 Metoda FMEA

FMEA (Failure Modes and Effects Analysis, Analýza způsobů a následků selhání) je metoda analýzy rizik, která představuje systematický přístup k identifikaci a analýze potenciálních hrozeb a rizik ve výrobcích nebo procesech, jakož i jejich příčin a důsledků. Hlavním cílem FMEA je zlepšit kvalitu a spolehlivost systémů a proaktivně řešit problémy již v raných fázích vývoje, výroby nebo provozu. Pro mě je tato metoda analýzy rizik nejnázornější a nejzajímavější, protože okamžitě vidíte problémové oblasti, které je třeba řešit.

Pro plnohodnotnou analýzu rizik je nutné postupně projít jednotlivými fázemi. Prvním krokem analýzy rizik FMEA je identifikace možných hrozeb, které mohou v systému nebo v procesu jeho provozu nastat. Dalším důležitým krokem je určení, k jakým důsledkům mohou hrozby v analyzovaném systému nebo procesu vést. Důležité je také zjistit příčiny, proč k těmto hrozbám dochází, protože pokud odstraníte příčinu, nebude hrozba existovat. Po určení hrozeb, jejich příčin a důsledků je nutné posoudit riziko každé poruchy podle tří kritérií: pravděpodobnost výskytu, závažnost a zjistitelnost. Každé kritérium bylo vyhodnoceno dle tabulky 1, která obsahuje hodnotící stupnici.

Tab. 1 Stanovené stupnice hodnocení intervalů pravděpodobnost výskytu, vážnosti a odhalení hrozeb [vlastní]

Pravděpodobnost výskytu (P)	**Stupnice hodnocení**	**Vážnost (V)**	**Stupnice hodnocení**	**Odhalení (O)**	**Stupnice hodnocení**
Velmi nízká	<0;2>	Nepatrná	<0;2>	Velmi nízká	<0;2>

Nízká	<2,4>	Přijatelná	<2,4>	Nízká	<2,4>
Střední	<4,6>	Významná	<4,6>	Střední	<4,6>
Vysoká	<6,8>	Velmi významná	<6,8>	Vysoká	<6,8>
Velmi vysoká	<8,10>	Kritická	<8,10>	Velmi vysoká	<8,10>

Dalším krokem analýzy rizik FMEA byl výpočet RPN (Rizikové prioritní číslo). RPN se vypočítá na základě předchozích údajů. Je třeba jednoduše vynásobit všechna 3 dříve získaná čísla. Hodnota RPN je potřebná pro stanovení priorit opatření ke zmírnění rizik mezi všemi uvažovanými daty. Pro usnadnění jsem rozdělil možné hodnoty RPN do 4 intervalů, které můžete vidět v tabulce 2.

Tab. 2 - Stanovené intervaly rizikového prioritního čísla [vlastní]

Intervaly RPN	**Míra rizika**
<1,30>	**Nízké riziko**
<31,60>	**Střední riziko**
<61,90>	**Vysoké riziko**
<91,125>	**Velmi vysoké riziko**

Jsou stanoveny 4 intervaly: nízké, střední, vysoké a velmi vysoké riziko ohrožení. Při nízkém riziku fungují systémy a procesy v rámci přijatelných hodnot a hrozby nevyžadují okamžitý zásah. Přesto nelze sledování těchto hrozeb pozastavit, protože se může kdykoli něco změnit. Hrozby střední úrovně již mohou vyžadovat určitá nápravná opatření a jejich změny by měly být monitorovány a vyhodnocovány. Vysoké riziko je již významnou hrozbou, která vyžaduje rychlá opatření ke zmírnění rizika. Je důležité nadále sledovat, vyvíjet a zavádět různá opatření k prevenci a zmírnění těchto rizik. Velmi vysoká rizika mají nejvyšší prioritu, protože se již jedná o kritické hrozby, které mohou vést k velmi závažným důsledkům pro celý systém nebo proces. Hrozby s velmi vysokým rizikem vyžadují okamžitou pozornost a naléhavá opatření k řešení těchto rizik.

Na základě údajů získaných ze všech předchozích kroků je třeba vypracovat a zavést opatření ke zmírnění rizik a vyhodnotit výsledky podle stejných tří kritérií: pravděpodobnost výskytu (P), vážnost (V) a odhalitelnost (O). Tento krok je pro celou analýzu rizik poslední, ale neméně důležitý.

Metoda FMEA je důležitým nástrojem pro identifikaci, hodnocení a prevenci rizik spojených s různými systémy a procesy. Tato metoda se používá v mnoha oblastech a patří k nejlepším. Proto jsem si vybral právě tuto metodu analýzy rizik.

Tab. 3 Část analýzy FMEA [vlastní]

Typ hrozby	**Hrozba**	**Potenciální příčina hrozby**	**Potenciální důsledky chyby**	**Současný stav**				**Bezpečnostní opatření**
				P	**V**	**O**	**RPN**	
Vnější hrozby	Hackerský útok	Zranitelnosti softwaru, slabá hesla	Neoprávněný přístup k systému	4	5	3	60	Pravidelné aktualizace softwaru, používání složitých hesel
	Malware	Instalace napadených aplikací	Krádež dat, narušení provozu systému	3	4	2	24	Antivirový software, kontrola aplikací před instalací
	Phishing	Podvodné e-maily, napadené aplikace	Krádež dat	4	4	4	64	Proškolení uživatelů, používání antiphishingových filtrů
	Sociální inženýrství	Neoprávněný přístup	Krádež osobních údajů	4	4	4	64	Zaškolení uživatelů
	Krádež zařízení	Únik dat, narušení provozu	Ztráta zařízení, finanční ztráty	3	4	3	36	Fyzická ochrana zařízení, šifrování dat v zařízeních

Tabulka 3, kterou vidíte výše, je pouze částí celé analýzy rizik FMEA, celá tabulka analýzy je uvedena v příloze I. Snažil jsem se najít nejčastější hrozby mezi běžnými uživateli systémů chytré domácnosti a na základě analýzy rizik jsem navrhl způsoby jejich minimalizace. Výsledkům analýzy rizik se budu věnovat v další části mé bakalářské práce.

5.2 Výsledky analýzy

Hlavním účelem analýzy rizik FMEA bylo identifikovat a posoudit možná rizika v systémech chytré domácnosti, jakož i jejich příčiny a možné důsledky. To vše bylo nezbytné pro nalezení možných řešení, která mohou zvýšit spolehlivost a bezpečnost zařízení IoT. Analyzoval jsem možné hrozby, jejichž původcem mohou být buď samotní uživatelé, chyby při výrobě, nebo útoky hackerů. Hrozby byly hodnoceny podle tří kritérií, mezi něž patřila pravděpodobnost výskytu, vážnost problému a odhalitelnost těchto hrozeb. Po posouzení hrozeb podle všech kritérií bylo vypočteno číslo priority rizika (RPN), aby bylo možné stanovit priority rizik a naplánovat opatření k jejich zmírnění. Každá hrozba byla zařazena mezi 4 kategorie uvedené v tabulce 2. Na základě komplexní analýzy rizik byla navržena doporučení pro zlepšení bezpečnosti, která budou podrobněji rozebrána v následující části.

Na základě příčin hrozeb lze s jistotou říci, že největší hrozbou pro systémy inteligentní domácnosti je nedostatek znalostí a zkušeností uživatelů. Právě majitelé chytrých zařízení mohou způsobit většinu problémů vedoucích k vážným následkům. Nedostatek času, lenost nebo prostě neochota přečíst si návod k obsluze chytrých zařízení může vést k problémům se zabezpečením celého systému chytré domácnosti.

Dalším velkým problémem jsou zranitelnosti v softwaru chytrých domácích zařízení. Důvodů je několik, od chyb programátorů až po neustálý vývoj nových technologií, které mohou obejít současné metody ochrany. Ochránit se před všemi hrozbami je nemožné na 100 %, ale pečlivé testování hardwaru, pravidelné aktualizace a vylepšení mohou pomoci v boji proti mnoha závažným hrozbám.

Na základě získaných údajů jsem navrhl několik způsobů jejich odstranění. Teoreticky může realizace navržených opatření výrazně zvýšit spolehlivost a bezpečnost systémů inteligentních domácností. Důkladnější analýza všech mnou doporučených bezpečnostních opatření, stejně jako testování v praxi, bude provedena později v této bakalářské práci.

Závěrem lze říct, že analýza rizik FMEA ukázala, že zavedení navrhovaných opatření může významně zvýšit bezpečnost a spolehlivost systémů chytré domácnosti. Nicméně se také doporučují pravidelné revize, aktualizace a doplňování analýzy rizik s ohledem na změny ve vývoji technologií a nové údaje. Věřím, že v budoucnu se díky začlenění umělé inteligence a strojového učení do systémů inteligentních domácností přestaneme obávat chyb uživatelů. Počítače mohou zohlednit mnohem více dat najednou a lépe a rychleji vyhodnocovat uživatelské akce již nyní.

6 NÁVRH BEZPEČNOSTNÍCH OPATŘENÍ

V této části své bakalářské práce bych se chtěl blíže podívat na všechna mnou navržená bezpečnostní opatření ke zmírnění rizik, která si můžete podrobně prohlédnout v příloze I. Projdu jednotlivé hrozby a navrhovaná opatření, abych lépe vysvětlil důvody, proč jsem tato řešení navrhl.

6.1 Hackerský útok

První hrozbou, kterou jsem při analýze rizik FMEA zvažoval, byl hackerský útok. Po analýze možných příčin jsem navrhl pravidelné aktualizace softwaru a používání složitých hesel jako opatření ke zmírnění bezpečnostních rizik systémů inteligentní domácnosti. Opatření, která jsem navrhl, významně zvyšují úroveň zabezpečení chytré domácnosti, minimalizují pravděpodobnost úspěšného vnějšího hackerského útoku a chrání citlivé údaje uživatelů i systém jako celek.

Pravidelné aktualizace softwaru často obsahují opravy nově objevených zranitelností, které mohou útočníci zneužít ke vstupu do systému. Pravidelné aktualizace významně zvyšují aktuálnost systému a ochranu před nově zjištěnými hrozbami. Vývojáři také neustále pracují na zlepšování funkčnosti a zabezpečení svých zařízení. A automatické aktualizace minimalizují riziko, že uživatel důležité aktualizace přehlédne.

Dalším opatřením, které navrhuji, je používání složitých hesel. Mnoho lidí o složitosti svých hesel nepřemýšlí, ale mnozí hackeři používají metodu dolování hesel, při které se pomocí počítačů jednoduše zkouší všechny možné kombinace hesel. Složitá hesla, která používají kombinaci velkých a malých písmen, číslic a speciálních znaků, výrazně ztěžují nalezení hesla. Pokud použijete dostatečně složité heslo, budou hackeři potřebovat mnohem více času a prostředků k prolomení systému. Důležité je také používat různá hesla pro přihlašování do různých systémů. Předejdete tak riziku průniku až do několika systémů najednou, pokud dojde k úniku jednoho z nich.

6.2 Malware

Další bezpečnostní hrozbou pro systémy chytré domácnosti je malware. Doporučil jsem používat antivirový software a kontrolovat aplikace před jejich instalací. Tato opatření výrazně snižují pravděpodobnost úspěšného útoku malwaru a chrání systém inteligentní domácnosti před potenciálními bezpečnostními hrozbami.

Používání antivirových programů umožňuje pravidelné a automatické skenování celého systému a pomáhá identifikovat škodlivý software a odstranit jej ze všech zařízení. Antivirové programy jsou také neustále aktualizovány, objevují se a zavádějí nové technologie, které umožňují lepší a rychlejší odhalení škodlivého softwaru, který může ohrozit bezpečnost nebo provoz jednotlivých zařízení. S použitím antivirových programů se výrazně snižuje negativní dopad na systém chytré domácnosti, což vede ke zvýšení spolehlivosti všech komponent.

Kontrola aplikací před jejich instalací je také bezpečnostním opatřením, které jsem navrhl ke snížení rizika negativních důsledků malwaru. Internet je obrovským místem pro sdílení souborů a mnoho lidí slepě důvěřuje všem stránkám, které tam jsou. Útočníci však často zavádějí různé počítačové viry uvnitř programů nebo dokonce filmů, které si lidé mohou najít a stáhnout přes internet. Pro zajištění bezpečnosti systémů inteligentní domácnosti je nutné kontrolovat soubory, které uživatelé stahují z internetu. Mnoho prohlížečů již zavedlo automatickou kontrolu souborů před jejich stažením. Velmi důležité je také používat ke stahování souborů a aplikací oficiální zdroje.

6.3 Phishing

Phishing je také bezpečnostní hrozbou pro systémy chytré domácnosti. Jako první bezpečnostní opatření jsem navrhl proškolit uživatele. Mnoho lidí se nevědomky dopouští chyb, které mohou mít fatální následky. Uživatelé by měli být schopni rozpoznat phishingové aktivity od podvodníků. Uživatelé by měli být obezřetní při otevírání odkazů, které najdou na internetu, kontrolovat e-mailové adresy odesílatele a neotevírat podezřelé aplikace. Školení uživatelů o možnostech ochrany proti phishingu zvyšuje jejich povědomí o hrozbách, což výrazně zvyšuje bezpečnost při používání internetu.

Dalším navrhovaným opatřením ke snížení bezpečnostního rizika systémů chytré domácnosti je použití antiphishingových filtrů. V současné době bohužel neexistují 100% účinné filtry, které by dokázaly rozpoznat phishingové e-maily nebo webové stránky. To se však brzy změní díky využití umělé inteligence. Navzdory extrémně slabým antiphishingovým filtrům pomůže jejich používání zabránit alespoň některým phishingovým stránkám a e-mailům. Všechny filtry jsou navíc pravidelně aktualizovány a vylepšovány, takže jejich používání je důležitou součástí zajištění bezpečnosti uživatelů chytré domácnosti.

6.4 Sociální inženýrství

Sociální inženýrství je také významnou hrozbou pro bezpečnost systémů chytré domácnosti. Jako první bezpečnostní opatření jsem navrhl školení uživatelů. Vzhledem k tomu, že každý rok se objevují nové způsoby manipulace s lidmi, je důležité zvyšovat povědomí uživatelů systémů chytré domácnosti o metodách sociálního inženýrství a také školit, jak rozpoznat phishingové útoky. Čím více lidí si bude vědomo existence a metod sociálního inženýrství, tím menší bude bezpečnostní hrozba.

Použití antiphishingových filtrů také zvyšuje bezpečnost uživatelů před útočníky. Jak jsem uvedl v minulém bloku, antiphishingové filtry nejsou v současné době nijak zvlášť účinné, ale přesto je nejlepší je používat pro zvýšení spolehlivosti a bezpečnosti systémů inteligentní domácnosti.

6.5 Krádež zařízení

Jako další bezpečnostní hrozbu jsem zvažoval krádež chytrých zařízení. Podle mého názoru je tento problém v dnešní době poměrně častý. Proto jsem navrhl poměrně účinná bezpečnostní opatření, která by tomu měla zabránit. Jako první návrh jsem zvolil fyzickou ochranu zařízení. Mezi ně patří složitější upevňovací prvky a také zámky. To vše ztěžuje krádež zařízení nepovolaným osobám. Koneckonců je mnohem těžší odstranit detektor přišroubovaný ke zdi než detektor připevněný lepicí páskou.

Pro zabránění úniku informací z odcizených zařízení jsem navrhl používat šifrování dat. I když se někomu podaří zařízení ukrást, je nepravděpodobné, že by se dostal k informacím uloženým v zařízení. Bez správných klíčů nebudou narušitelé schopni přečíst zašifrovaná data, což výrazně zvyšuje spolehlivost systémů chytré domácnosti.

6.6 Vandalismus

Vandalismus je také významnou hrozbou pro bezpečnost systémů chytrých domácností. Zničená zařízení mohou ovlivnit funkčnost celého systému a také výrazně zvýšit náklady na údržbu. Použití fyzického zabezpečení může riziko vandalismu výrazně snížit. Kromě složitých držáků a zámků, o kterých jsem psal v části věnované krádežím zařízení, můžete použít také speciální odolné skříně proti vandalům, které zvyšují odolnost proti úplnému zničení zařízení. Důležité je také umístit zařízení na těžko přístupná místa, například vysoko

nad zemí nebo do specializovaných skříní. Snížíte tak riziko, že vandalové získají přímý přístup k vašim zařízením.

Instalace kamerového systému může také výrazně zvýšit bezpečnost vašich zařízení. Pokud umístíte kamery na viditelné místo, budou sloužit jako odstrašující prostředek. Vandalové budou méně pravděpodobně páchat trestnou činnost, pokud budou vědět, že jejich jednání je zaznamenáno na kameru. Mnoho kamer v dnešní době také vysílá signál přímo do telefonu a má možnost monitorovat různé oblasti a posílat upozornění na porušení přímo na telefon majitele. Díky tomu můžete okamžitě reagovat na podezřelé aktivity nebo pokusy o vandalismus.

6.7 Přírodní katastrofy

Přírodní katastrofy jsou v České republice poměrně vzácnou hrozbou, ale klimatické změny mohou v příštích letech statistiku upravit. Proto se jedná o další bezpečnostní hrozbu pro systémy chytré domácnosti. Jako první opatření ke zmírnění rizik jsem navrhl fyzickou ochranu. V předchozích dvou dílech jsem již dostatečně rozebral klady této ochrany. Kromě toho bych chtěl upozornit na to, že rizika poškození přírodními podmínkami se výrazně snižují použitím silných upevňovacích prvků a ochranných krytů.

Dalším opatřením, jak předejít vážným problémům, které mohou způsobit přírodní katastrofy, je zálohování dat uložených v chytrých domácích zařízeních. V případě ztráty nebo zničení zařízení lze všechna data snadno vrátit zpět. Použitím zálohování nebude systém nijak vážně ovlivněn.

Navrhl jsem také pojištění zařízení. Pokud používáte drahé systémy chytré domácnosti, pojištění komponent by bylo skvělým způsobem, jak snížit náklady na údržbu. Během silné bouřky může být zařízení zničeno bleskem nebo silným větrem. Pojištěná zařízení vám pojišťovací agent uhradí a vy neutrpíte žádnou škodu.

6.8 DDoS útoky

Další bezpečnostní hrozbou jsou útoky DDoS. Jako opatření ke zmírnění rizika jsem navrhl používat speciální ochranu proti těmto útokům, například Arbor Networks nebo Cloudflare. Díky této ochraně bude příchozí provoz analyzován v reálném čase. Taková ochrana dokáže odhalit anomální a potenciálně nebezpečné aktivity typické pro útoky DDoS. Okamžitá reakce takové ochrany umožňuje celému systému odolat a propustit pouze legitimní systémové

požadavky. Moderní systémy ochrany také dokáží automaticky navýšit zdroje a přerozdělit zátěž v reakci na zvýšení příchozího provozu, což umožňuje odolat zátěži i při intenzivních útocích.

Použití síťového klonování (Network Cloning) umožňuje rozložit zátěž mezi více serverů v různých částech světa a snížit tak pravděpodobnost přetížení jednoho z nich. Úplné selhání hardwaru by bylo mnohem obtížnější díky rozložení zátěže do více uzlů. Také v případě selhání jednoho klonu budou ostatní klony fungovat dál, čímž bude zajištěna nepřetržitý provoz celého systému.

6.9 Zranitelnosti v komunikačních protokolech

Poslední vnější hrozbou pro systémy chytré domácnosti, kterou jsem v analýze rizik zvažoval, jsou zranitelnosti v komunikačních protokolech. Jako první bezpečnostní opatření jsem navrhl používat bezpečné protokoly, například TLS (Transport Layer Security). Tento protokol poskytuje vysoce kvalitní šifrování dat při přenosu informací mezi externími servery a zařízeními chytré domácnosti. I v případě zachycení zašifrovaných dat nebudou narušitelé schopni data přečíst, což chrání důvěrnost a celistvost informací. Zabezpečené protokoly mají také mechanismy, které ověřují a verifikují příchozí data. To umožňuje zachovat celistvost dat během přenosu.

Pravidelné bezpečnostní audity mohou odhalit zranitelnosti komunikačních protokolů dříve, než je najdou útočníci. Tyto audity mohou testovat a analyzovat vnitřní kód systému a také posuzovat soulad s novými bezpečnostními standardy, které jsou pravidelně aktualizovány. Na základě výsledků auditů se také vypracovávají plány na odstranění zranitelností a případná vylepšení zabezpečení systému.

6.10 Nesprávná nastavení zařízení

První vnitřní hrozbou pro systémy chytré domácnosti je nesprávná nastavení zařízení. Hlavním bezpečnostním opatřením, které jsem navrhl, je vzdělávání uživatelů. Jak jsem napsal na začátku, největší hrozbou pro zabezpečení systému chytré domácnosti je uživatel. Nezkušení majitelé těchto systémů mohou omylem změnit důležitá nastavení, čímž ohrozí celý systém. Jako školení by se měla zvyšovat informovanost uživatelů a získané znalosti by se měly pravidelně aktualizovat. Díky školení lidé lépe chápou důležitost správného nastavení a mohou sami analyzovat rizika spojená se změnou nastavení systému. U proškolených

uživatelů je méně pravděpodobné, že se při nastavování systémů chytré domácnosti dopustí chyb.

Pravidelná kontrola nastavení zabezpečení také zvyšuje spolehlivost celého systému chytré domácnosti. Můžete tak identifikovat a opravit zranitelná místa nebo nezabezpečená nastavení a zabránit tak jejich zneužití narušiteli. Během kontroly lze také odhalit nesoulad s aktuálními bezpečnostními standardy. V dnešní době je k dispozici mnoho automatizovaných nástrojů pro kontrolu bezpečnostních nastavení, které tento proces značně urychlují a usnadňují a mohou najít zranitelnosti, kterých by si člověk nevšiml.

6.11 Zakázání aktualizací softwaru

Vypnutí aktualizací softwaru rovněž ohrožuje bezpečnost systémů chytré domácnosti. Někteří lidé nechtějí svá zařízení aktualizovat, ale to má velký dopad na bezpečnost celého systému. Každý den se objevují nové způsoby, jak obejít bezpečnostní systémy, a vývojáři se snaží včas najít řešení těchto problémů. Zakázání automatických aktualizací může snížit účinnost celého systému a zvyšuje riziko průniku útočníka do systému. Automatické aktualizace zajišťují včasný příjem bezpečnostních oprav, které zvyšují odolnost systému proti vnějším hrozbám.

Kontrola dodržování zásad také zajišťuje, že verze softwaru na všech zařízeních v systému chytré domácnosti jsou aktuální. Může také odhalit závady v samotných zařízeních a navrhnout jejich odstranění.

6.12 Chyby v softwarovém kódu

Pro minimalizaci rizik spojených s chybami v softwarovém kódu jsem navrhl testování softwaru a také jeho pravidelnou aktualizaci. Testování softwaru v rané fázi umožňuje identifikovat zranitelnosti ještě předtím, než uživatel získá přístup k systému nebo aktualizaci. Také pro testování kvality je třeba používat různé metody pro komplexní testování softwarového kódu. V současné době je k dispozici také mnoho metod automatizovaného testování. Umělá inteligence výrazně zjednodušuje hledání chyb v kódu a včasné odstraňování zranitelností.

Pravidelné aktualizace softwaru pomáhají minimalizovat riziko problémů již po uvedení softwaru na trh. Každé zařízení může časem ztratit na aktuálnosti a aktualizace pomáhají udržovat bezpečnost celého systému. Aktualizace také obsahují vylepšení a nové funkce,

které zvyšují bezpečnost systému jako celku. A automatické aktualizace pomáhají zabránit nepozornosti uživatelů, kteří by důležité aktualizace přehlédli.

6.13 Nedostatečná ochrana přístupových práv

Další hrozbou pro systémy chytré domácnosti je nedostatečná ochrana přístupových práv. Jako bezpečnostní opatření jsem navrhl zavedení vícefaktorové autentizace a také kontrolu přístupových práv. Vícefaktorové ověřování uživatelů je vynikajícím řešením problému spojeného s neoprávněným přístupem do systému. Při přihlašování bude vícefaktorové ověřování (MFA) vyžadovat nejen heslo, ale také například jednorázový kód nebo biometrické údaje uživatele. Dodatečná úroveň ověření při přihlášení zamezí pochybným změnám bezpečnostních nastavení ze strany neoprávněných osob.

Pravidelná kontrola nastavení přístupových práv uživatelů rovněž zlepší zabezpečení systému chytré domácnosti. Při kontrole lze identifikovat nepotřebné uživatele s přístupem do systému. Umožní také přísnější kontrolu přístupu neoprávněných osob do systému.

6.14 Nerozdělení přístupových práv

Nedostatečné rozdělení přístupových práv je také vážnou hrozbou pro systémy chytrých domácností. Mnoho uživatelů o tom ani nepřemýšlí, ale je to důležitý aspekt zabezpečení celého systému a minimalizuje rizika spojená s neoprávněným přístupem k systému a datům. Zajišťování omezení přístupových práv minimalizuje přístupová práva pro určité osoby. Každý uživatel by měl mít pouze taková práva, která jsou nezbytná k plnění jeho úkolů. Je také možné rozlišovat přístupová práva na základě rolí. Každému uživateli je přidělena určitá role, na jejímž základě mu budou přidělena určitá uživatelská práva. Tato metoda zjednodušuje správu přístupu k systému a datům a poskytuje jasné vymezení práv v závislosti na funkčních potřebách uživatele.

Vícefaktorové ověřování také řeší řadu problémů spojených s touto hrozbou. Rozšířené vícefaktorové ověřování vyžaduje ověření identity uživatele, což výrazně zvyšuje úroveň zabezpečení ve srovnání s použitím pouze hesla. Také v případě odhalení hesla nebude útočník schopen získat plný přístup do systému chytré domácnosti. Vícefaktorové ověřování může také pomoci chránit před phishingovými útoky, protože kromě hesla bude útočník potřebovat jednorázový kód nebo biometrické údaje uživatele.

6.15 Nezabezpečené ukládání dat

K vyřešení hrozby nezabezpečeného ukládání dat jsem navrhl používat šifrování dat i bezpečné ukládání dat. Šifrování převádí data do nečitelného formátu, který nelze dešifrovat bez speciálního klíče. Tím je zajištěno, že data jsou v bezpečí před narušiteli i při získávání zašifrovaných dat. Použití moderních asymetrických metod šifrování umožní odolat i silným útokům. Šifrování také pomáhá zachovat důvěrnost a celistvost důležitých dat.

Bezpečným ukládáním dat mám na mysli používání zabezpečených úložišť. V současné době existuje obrovské množství takových úložišť, uživatel si musí vybrat takové, které mu vyhovuje. Například použití speciálních úložišť s hardwarovým šifrováním umožní uživateli minimalizovat riziko neoprávněného přístupu k datům a v případě poškození úložiště bude moci data vrátit do původního stavu. Pravidelné zálohování také umožní mít důležitá data vždy rychle a bezpečně k dispozici.

6.16 Nešifrování při přenosu dat

Další vnitřní hrozbou pro systémy chytré domácnosti je nepoužívání šifrování při přenosu dat. Použití šifrovacích protokolů, jako je SSL nebo TSL, poskytuje silnou ochranu dat při přenosu dat mezi zařízeními chytré domácnosti, uživatelským mobilem nebo cloudovým úložištěm. Šifrování převádí všechna data do nečitelného formátu, čímž zajišťuje, že data jsou při přenosu mezi zařízeními v bezpečí a důvěrná. Také protokoly SSL a TSL jsou ověřené a spolehlivé, což zvyšuje bezpečnost dat v případě jejich neoprávněné manipulace.

6.17 Chyby uživatelů

Jak jsem již psal, hlavní bezpečnostní hrozbou je sám uživatel. Jeho chyby mohou vést k výraznému zhoršení odolnosti systému vůči různým hrozbám. V rámci bezpečnostních opatření by uživatelé měli být proškoleni, jak správně spravovat systém chytré domácnosti. Zvyšování povědomí o možných rizicích pomáhá uživatelům pochopit důležitost správné správy zařízení chytré domácnosti. Každý uživatel by měl znát správná bezpečnostní nastavení, složitá hesla, techniky phishingu a sociálního inženýrství a měl by být schopen rozpoznat podezřelé zprávy a požadavky.

Také dodatečná kontrola činností ze strany poskytovatele systému chytré domácnosti může zvýšit úroveň zabezpečení celého systému. Pravidelnou kontrolou celého systému inteligentní domácnosti lze odhalit neoprávněné činnosti, softwarové chyby nebo poruchy

různých zařízení. Monitorování činností odhalí možné příčiny poruch a nesprávných činností uživatelů.

Bezpečnostní hrozby je důležité prozkoumat, aby byla zajištěna dobrá ochrana osobních údajů a správná funkce všech zařízení v systému chytré domácnosti. V této části své bakalářské práce jsem se zabýval různými vnitřními a vnějšími hrozbami, které mohou negativně ovlivnit zabezpečení celého systému. Prostřednictvím provedené analýzy rizik FMEA bylo možné identifikovat nejzranitelnější a nejnebezpečnější zranitelnosti v systémech chytré domácnosti. Každá hrozba byla vyhodnocena a byla navržena bezpečnostní opatření, která mají minimalizovat její následky. Každé navržené opatření bylo podrobně popsáno a byla zdůvodněna jeho účinnost. Implementace navržených bezpečnostních opatření tak zajistí, že celý systém chytré domácnosti bude spolehlivě fungovat a že osobní údaje uživatelů budou bezpečně chráněny před uvažovanými hrozbami. V další části své práce ověřím vhodnost a úspěšnost těchto bezpečnostních opatření v praxi.

7 OVĚŘENÍ VHODNOSTI NÁVRHU V PRAXI

Pro ověření vhodnosti mnou navržených opatření jsem vybral 3 různé domácnosti s různými chytrými zařízeními. První skupina používala zařízení jako chytrý reproduktor s hlasovým asistentem, termostat, chytrý robotický vysavač a bezpečnostní kameru. Druhá skupina používala 2 chytré bezpečnostní kamery, chytrý reproduktor s hlasovým asistentem, chytrá světla, pohybový senzor a chytrý videozvonek. Třetí skupina měla chytrý reproduktor s hlasovým asistentem, jednu bezpečnostní kameru, chytrou zásuvku, chytrou rychlovarnou konvici a hub pro vzájemné propojení zařízení. Každá skupina představovala uživatele různého věku a technických dovedností. S každou skupinou jsem pracoval zvlášť, abych kvalitativně identifikoval jejich problémy a využil různá bezpečnostní opatření.

Prvním krokem při testování mých návrhů bylo zaškolení každé skupiny ve formátu online schůzky pomocí služby Google Meets. Pro přesnější školení byla naše setkání rozdělena do tří hlavních bloků. Během prvního setkání jsem uživatelům vysvětlil základní bezpečnostní pravidla, jako je používání silných hesel a zapojení vícefaktorového ověřování. Vzhledem k tomu, že téměř každý den dochází k únikům databází z velkých společností, začal jsem tím, že jsem každé skupině uživatelů ukázal, jak si zkontrolovat, zda jejich přihlašovací jména a hesla nebyla odcizena. K tomu byla použita stránka haveibeenpwned.com. Pro kontrolu stačí zadat svou e-mailovou adresu a na stránce se zobrazí informace, zda se váš e-mail stal předmětem úniku dat. Všechny skupiny měly pozitivní výsledek. Proto bylo mým doporučením změnit e-mailovou adresu ve všech propojených programech.

Po kontrole e-mailů jsem vysvětlil, jak je důležité používat silná hesla. Každá skupina tvrdila, že k přihlašování používá silná hesla. Ke kontrole síly hesla jsem použil webový portál passwordmonster.com. Pomocí této stránky si můžete zkontrolovat sílu hesla a také zjistit, jak dlouho bude trvat prolomení hesla. Většina skupin měla silná hesla, nejslabší hesla byla ve skupině starších uživatelů. Všechna nejistá hesla byla změněna na silnější, s použitím velkých a malých písmen, číslic a speciálních znaků.

Za účelem posílení bezpečnosti osobních údajů uživatelů jsme také společně připojili vícefaktorové ověřování k nejdůležitějším systémům uživatelů. Při přihlašování byli uživatelé požádáni o jednorázový kód z aplikace Google Authenticator a také o jednorázový kód zaslaný na mail. Poté se jednomu z uživatelů po dobu jednoho měsíce někdo pokoušel získat přístup k jeho elektronické poště, ale díky vícefaktorovému ověřování se útočníkům nepodařilo získat přístup.

Během druhého setkání byli uživatelé seznámeni s možnými phishingovými útoky a možnostmi jejich identifikace. K proškolení uživatelů byly použity informace z webových stránek Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Uživatelé byli rovněž proškoleni v rozpoznávání phishingu a podezřelých požadavků. Všichni uživatelé měli v prohlížečích na svých počítačích a mobilních telefonech automaticky zapnuté antiphishingové filtry. Byly také zkontrolovány e-maily každé skupiny uživatelů a nalezeny desítky zpráv obsahujících phishingové odkazy. Všechny byly označeny jako spam a smazány. [27][28]

Během druhého setkání byli uživatelé také poučeni o antivirových programech. Mnoho uživatelů nemělo nainstalované žádné antivirové programy, protože si mysleli, že jsou automaticky nainstalovány s operačním systémem. Pro spolehlivou ochranu před viry byl použit placený antivirový program od společnosti Eset, který patří k cenově nejvýhodnějším produktům. Po kontrole systému antivirem bylo na počítačích nejstarší skupiny zjištěno několik virů. Ukázalo se, že nejzkušenější v oblasti kybernetické bezpečnosti je nejmladší skupina. Všechny viry byly odhaleny a odstraněny, což výrazně zvýšilo bezpečnost zařízení uživatelů. Aby se snížilo riziko další instalace virů, bylo na všech počítačích povoleno kontrolování stahovaných souborů. Všechny prohlížeče mají tuto funkci ve výchozím nastavení povolenou, ale já jsem povolil dodatečnou kontrolu souborů antivirovým programem.

Během třetího online setkání jsem uživatelům vysvětlil důležitost aktualizací softwaru pro všechna zařízení, včetně chytrých domácích zařízení. Při kontrole aktualizací bylo zjištěno, že polovina uživatelů má vypnutou funkci automatické aktualizace chytrých zařízení. Některá zařízení neměla aktualizaci softwaru až od roku 2019. Po úplné aktualizaci všech systémů byli uživatelé překvapeni, že jejich zařízení fungují lépe. Pomohl jsem také nastavit časy automatických aktualizací pro uživatele tak, aby se s aktualizacemi nesetkali například při práci na počítači. Všechna zařízení budou automaticky instalovat aktualizace v noci, takže si toho uživatelé nevšimnou.

Také během třetího setkání jsem všem skupinám vysvětlil důležitost správného nastavení zabezpečení systémů chytré domácnosti. S každým uživatelem jsme prošli důležitá bezpečnostní nastavení. V případě jakýchkoli nejasností jsem vysvětlil význam určitých nastavení pro zabezpečení chytré domácnosti.

Tím školení uživatelů skončilo. Výsledkem bylo nalezení 11 e-mailových adres, které byly ohroženy únikem dat, nalezení 27 slabých hesel, nastavení vícefaktorového ověřování pro

přihlašování do důležitých systémů, uživatelé se také naučili rozpoznávat phishingové odkazy, byly povoleny automatické aktualizace pro všechna zařízení a vysvětlena důležitá nastavení systému chytré domácnosti. Všechny skupiny se zdokonalily v zabezpečení svých zařízení, což výrazně snížilo riziko několika bezpečnostních hrozeb systému chytré domácnosti najednou.

Pro testování fyzické ochrany chytrých domácích zařízení jsem pracoval pouze s jednou skupinou, protože další dvě používaly pouze kamery uvnitř bytu ke sledování malého dítěte a kočky. Třetí skupina používala chytrý videozvonek a jednu kameru pro venkovní sledování. Při kontrole fyzického zabezpečení zařízení se ukázalo, že obě zařízení byla připevněna oboustrannou lepicí páskou. Pro dostatečné zabezpečení těchto zařízení jsem navrhl, aby byl videodomofon připevněn k plotu pomocí šroubů a kamera zavěšena přímo pod střechou domu a rovněž připevněna šrouby. Kromě ochrany kamery před přírodními katastrofami byl použit speciální kryt, který chrání kameru před hromaděním prachu, nečistot a vody na kameře. Kryt také dále chrání kameru před fyzickým poškozením. Videodomofon má pevné kovové pouzdro, takže další ochrana by byla zbytečným plýtváním penězi. Za dobu používání ochranného krytu na kameře si uživatelé všimli, že již není nutné každý den čistit kameru od nahromaděného sněhu nebo nečistot. Kamera pracuje přehledně a nezanáší se. Vzhledem k tomu, že všechny skupiny uživatelů mají malý počet chytrých domácích zařízení, je další pojištění zbytečné. Pro majitele složitějších a dražších systémů však bude mít toto bezpečnostní opatření význam.

Dále jsem zkontroloval, zda jsou data uložená v samotných zařízeních chytré domácnosti šifrovaná. Jak se ukázalo, všechna moderní a kvalitní zařízení již mají vlastní metody šifrování zabudované v operačním systému. Toto bezpečnostní opatření je však stále relevantní pro starší systémy chytré domácnosti. U všech uživatelů se šifrování dat používá jak při ukládání dat, tak při jejich přenosu mezi zařízeními, takže v případě krádeže zařízení nebudou data použita pro osobní potřebu útočníka.

Co se týče zálohování dat, mnoho uživatelů tyto funkce vypnulo, i když je cloudové úložiště poskytované dodavateli zdarma. Každá skupina tuto funkci nevyužívala vůbec. Nejvýhodnější možností pro ukládání záloh dat uživatelů byl Google drive. Tento způsob ukládání záloh jsme zvolili proto, že společnost Google poskytuje silnou ochranu pomocí šifrování pomocí protokolu HTTPS jak při přenosu dat do cloudového úložiště, tak při jejich ukládání. Uživatelé byli také spokojeni s příznivou cenou a možnostmi vhodného nastavení úložiště. Používáním spolehlivého cloudového úložiště, šifrování při přenosu a ukládání dat a záloh

se minimalizuje několik potenciálních bezpečnostních hrozeb pro systémy chytré domácnosti.

Při kontrole přístupových práv se ukázalo, že žádná ze skupin nepoužívá rozdělení přístupových práv a nijak je nekontroluje. Společně s uživateli jsme jednotlivým uživatelům přidělili role a v každé skupině určili jednu osobu, která jako jediná mohla měnit bezpečnostní nastavení celého systému chytré domácnosti. Každá role měla určitá omezení týkající se bezpečnosti systému inteligentní domácnosti. Také bylo zavedeno vícefaktorové ověřování uživatelů, aby bylo zajištěno co nejlepší zabezpečení přístupových práv. Tím se zamezí neoprávněnému použití systému bez vědomí hlavního uživatele. I když se útočník dozví přihlašovací heslo, bude muset získat přístup k poště majitele a také k jeho mobilu, aby mohl zadat jednorázový kód z aplikace Google Authenticator.

Hrozba chyb v softwaru chytrých domácích zařízení spočívá výhradně na straně vývojářů těchto zařízení. Bohužel neznám nikoho, kdo v této oblasti pracuje, ale jsem si jistý, že každý kód napsaný programátorem prochází před uvedením na trh kontrolou kvality. Pravidelné aktualizace závisí také na výrobci zařízení. V každém případě se objevují nová zařízení a nekonečná podpora pomocí aktualizací pro všechna zařízení je zbytečná. Je na každém výrobci, jak dlouho bude zařízení podporovat. Všechna zařízení však dostávají aktualizace, které řeší bezpečnostní problémy, po dobu několika let.

Důležitou součástí zabezpečení celého systému chytré domácnosti je také použití bezpečných komunikačních protokolů. Každý rok se bezpečnostní protokoly zdokonalují, vyvíjejí se nové protokoly a některé přestávají být aktuální. Všechna moderní zařízení používají k vzájemnému přenosu dat poměrně bezpečné protokoly. Všechny skupiny mají nainstalovány nejnovější aktualizace a používají kvalitní a moderní komunikační protokoly.

Navzdory nebezpečnosti útoků DDoS se s nimi běžní uživatelé setkávají jen zřídka. Moderní zařízení chytré domácnosti však proti těmto útokům používají dostatečnou ochranu. Po analýze systémů používaných v mých testovacích skupinách jsem zjistil, že nejběžnější technologií pro zabezpečení proti útokům DDoS je rozdělení mezi více serverů, aby se zabránilo přetížení systému, a také filtrování příchozích a odchozích požadavků. Také ochrana proti těmto útokům vyžaduje poměrně velké investice a prostředky, které nejsou pro malé systémy chytrých domácností tak nezbytné.

Po ověření mnou navržených bezpečnostních opatření v praxi ve třech různých skupinách jsem zjistil, že všechny mé návrhy jsou velmi účinné pro snížení rizik systémů chytrých

domácností. Nejlepší výsledky vykázalo školení uživatelů, které vedlo k výraznému snížení počtu phishingových útoků a neoprávněných přístupů do systémů chytrých domácností. Uživatelé ve všech skupinách byli s výsledkem a novými znalostmi v oblasti kybernetické bezpečnosti spokojeni a uváděli zvýšený pocit bezpečí. V další části své bakalářské práce zhodnotím vhodnost a úspěšnost mých bezpečnostních opatření.

8 VYHODNOCENÍ VHODNOSTI A ÚSPĚŠNOSTI NÁVRHU

Implementace mnou navržených bezpečnostních opatření založených na analýze rizik FMEA ve třech různých testovacích skupinách používajících různá zařízení chytré domácnosti a reprezentujících různé věkové skupiny prokázala jejich vysokou účinnost při snižování rizik v systémech chytré domácnosti. Nejúspěšnějším návrhem bylo školení uživatelů a implementace monitorovacích nástrojů. Výsledkem testovacích skupin bylo výrazné snížení úrovně rizik, zejména phishingových útoků a neoprávněného přístupu do systému. Uživatelé podrobně pochopili základy kybernetické bezpečnosti a byli příjemně překvapeni jednoduchostí a účinností mnou navržených opatření.

Z hlediska vhodnosti mnou navržených opatření se většina z nich ukázala jako účinná a spolehlivá při snižování bezpečnostních rizik systémů chytrých domácností. Navzdory neustálému technologickému vývoji mnoho drobných problémů uniká pozornosti vývojářů softwaru. Podobný výzkum pomáhá upoutat pozornost jak běžných uživatelů systémů chytré domácnosti, tak vývojářů softwaru a výrobců zařízení chytré domácnosti. Spokojenost uživatelů a zvýšený pocit bezpečí svědčí o vhodnosti mých návrhů v rámci snižování rizik. Také hodnota RPN v mé analýze rizik FMEA potvrzuje to, co tvrdím. Úplná analýza rizik FMEA je uvedena v příloze I. Díky mnou navrženým bezpečnostním opatřením se podařilo výrazně snížit číslo RPN, takže vhodnost všech mých návrhů je vysoká.

Mnou navržená bezpečnostní opatření jsou úspěšná na základě výsledků tří velmi odlišných testovacích skupin. Uživatelé byli spokojeni a pokračují ve studiu kybernetické bezpečnosti, aby lépe porozuměli různým bezpečnostním hrozbám pro systémy chytrých domácností. Jejich školení proběhlo úspěšně bez jakýchkoli problémů nebo nedorozumění. Informace, které byly zjištěny pro tuto bakalářskou práci, jsou důležitou součástí pro zvýšení informovanosti a vzdělání běžných nezkušených uživatelů s cílem zlepšit bezpečnost celého systému i pocit bezpečnosti a důvěry uživatelů. Prostřednictvím mnou navržených bezpečnostních opatření lze zajistit nejen vysokou úroveň bezpečnosti systémů chytré domácnosti, ale také spokojenost a důvěru uživatelů v nové technologie chytré domácnosti.

ZÁVĚR

Cílem mé bakalářské práce bylo identifikovat, klasifikovat a analyzovat rizika spojená se systémy chytrých domácností a vyvinout a zavést bezpečnostní opatření ke zmírnění těchto rizik. V teoretické části bakalářské práce byly podrobně zkoumány technologie, jako je internet věcí a chytrá domácnost. Oblasti použití technologií internetu věcí jsou úžasné svou rozmanitostí a rozsáhlostí. Další zdokonalování těchto technologií umožní lidem výrazně zlepšit kvalitu jejich života a zjednodušit většinu procesů, které lidé vykonávají. Již dostupné technologie chytré domácnosti mají silný dopad na kvalitu života uživatelů, což výrazně urychluje tempo zavádění technologií do každodenního života. Byly také zjištěny budoucí perspektivy této technologie a současné způsoby komunikace mezi zařízeními. Celá teoretická část byla nezbytná pro kvalitativní analýzu rizik spojených se systémy chytré domácnosti.

V praktické části byla identifikována aktiva chytré domácnosti, na jejichž základě byly zjištěny vnější a vnitřní bezpečnostní hrozby. Díky získaným údajům jsem provedl analýzu rizik pomocí metody FMEA, která mi umožnila identifikovat příčiny problémů a stanovit priority rizik. Na základě analýzy rizik jsem navrhl různá bezpečnostní opatření ke zmírnění rizik spojených se systémy inteligentní domácnosti. Všechna opatření jsem také ověřil na třech velice odlišných skupinách lidí, kteří používali různá zařízení, patřili do různých věkových skupin a měli různé znalosti o zabezpečení systémů chytré domácnosti. Všechna mnou navržená bezpečnostní opatření se ukázala jako vhodná, účinná a úspěšná při uvedení do praxe. Uživatelé byli spokojeni a výrazně si rozšířili své znalosti o zabezpečení systémů chytré domácnosti. Výrazně se také zvýšil pocit bezpečí, což je důležitý faktor při používání jakékoli technologie.

Tato bakalářská práce přispívá k lepšímu pochopení principů fungování systémů inteligentních domácností a možných bezpečnostních rizik a poskytuje praktická doporučení, jak je zmírnit. Věřím, že tato práce bude užitečná nejen pro zkušené uživatele, ale i pro nováčky v této oblasti. Účinnost navrhovaných opatření byla ověřena jak teoreticky, tak v praxi. Všechny cíle stanovené na začátku bakalářské práce byly úspěšně splněny.

SEZNAM POUŽITÉ LITERATURY

[1] IBM. What is internet of things? Online. 2023. Dostupné z: https://www.ibm.com/topics/internet-of-things. [cit. 2023-12-08].

[2] GEEKBRAINS. Internet věcí: historie vzniku a charakteristické rysy. Online. 2022. Dostupné z: https://gb.ru/blog/internet-veschej/. [cit. 2023-12-08].

[3] IOT. Internet věcí. Online. 2020. Dostupné z: https://iot.ru/wiki/internet-veshchey. [cit. 2023-12-08].

[4] SURESH, P.; J. VIJAY, Daniel; PARTHASARATHY, V. a ASWATHY, R. H. A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. *International Conference on Science Engineering and Management Research (ICSEMR)*. 2015, roč. 2014, č. 10.1109/ICSEMR.2014.7043637, s. 10.

[5] ARAFAT ALI, Hesham; ALI, Zainab a BADAWY, Mahmoud. Internet of Things (IoT): Definitions, Challenges, and Recent Research Directions. International Journal of Computer Applications. October 2015, roč. 2015, č. 128(1):975-8887, s. 11.

[6] K-ELECTRO. SYSTÉM INTELIGENTNÍ DOMÁCNOSTI - FUNKCE A VÝHODY. Online. 2023. Dostupné z: https://freehomeabb.ru/info/umnyy-dom-osobennosti-i-preimushchestva/. [cit. 2023-12-15].

[7] KNX24. Výhody chytré domácnosti. Online. 2023, 16.03.2023. Dostupné z: https://knx24.com/news/base/plyusy_umnogo_doma/. [cit. 2024-01-03].

[8] BLOG DG-HOME. CHYTRÉ SVĚTLO: PODROBNÝ PRŮVODCE SYSTÉMEM CHYTRÉHO OSVĚTLENÍ. Online. 2021, 08.06.2021. Dostupné z: https://dg-home.ru/blog/umnyj-svet-sistema-upravleniya-osveshcheniem_b565145/. [cit. 2024-01-03].

[9] SHEFINVEST. Chytrá domácnost: vytápění, osvětlení a zavlažování. Online. 2021, 10.02.2021. Dostupné z: https://shefinvest.ru/100221. [cit. 2024-01-03].

[10] TELEMETRICA. Bezpečnostní systém v chytré domácnosti. Online. 2023. Dostupné z: https://telemetrica.ru/faq/sistema_bezopasnosti_v_umnom_dome/. [cit. 2024-01-03].

[11] AMAZIN. Chytré zámky - co jsou a k čemu slouží? Online. 2022. Dostupné z: https://amazin.su/publ/dlja_doma/sistemy_umnyj_dom/umnye_zamki_chto_ehto_takoe_i_dlja_chego_oni_nuzhny/28-1-0-49. [cit. 2024-01-05].

[12] FACETER. Chytrý kamerový systém. Online. 2020, 05.09.2020. Dostupné z: https://faceter.cam/ru/blog/umnaya-sistema-videonablyudeniya/. [cit. 2024-01-05].

[13] VIDEOGLAZ. Chytrý kamerový systém. Online. 2022, 29.06.2022. Dostupné z: https://videoglaz.ru/blog/umnoe-videonablyudenie-principy-organizacii-i-sovremennye-resheniya#1. [cit. 2024-01-05].

[14] PORTER, Michael E. a HEPPELMANN, James E. How Smart, Connected Products Are Transforming Competition. Online. 2014. Dostupné z: https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition. [cit. 2024-01-05].

[15] ALI, Bako a Ali AWAD. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. Sensors [online]. 2018, 18(3), 817. ISSN 1424-8220. Dostupné z: doi:10.3390/s18030817

[16] STARTUS INSIGHTS. Top 9 Smart Home Trends & Innovations in 2023. Online. 2023. Dostupné z: https://www.startus-insights.com/innovators-guide/smart-home-trends-innovations/. [cit. 2024-01-05].

[17] STERGIOU, Christos; PSANNIS, Kostas E.; BYUNG-GYU, Kim a GUPTA, Brij. Secure integration of IoT and Cloud Computing. Future Generation Computer Systems. 2018, roč. 2016, č. 10.1016/j.future.2016.11.031, s. 25. ISSN 0167-739X.

[18] INVEST-FORSAJT. 16 chytrých gadgetů pro lékaře a pacienty. Online. 2020. Dostupné z: https://www.if24.ru/16-umnyh-gadzhetov-dlya-vrachej-i-patsientov/. [cit. 2024-01-05].

[19] DIACHENKO, Ruslan. Top 7 Smart Home Protocols Compared. Online. 2023, 17.07.2023. Dostupné z: https://lembergsolutions.com/blog/smart-home-protocols-explained. [cit. 2024-01-07].

[20] ČÍKA, Petr, 2017. Internet věcí pro inteligentní domácnost: Internet of things for smart home : zkrácená verze habilitační práce. Brno: Vysoké učení technické v Brně, nakladatelství VUTIUM. ISBN 978-80-214-5559-7.

[21] SONOFF. Smart Home Protocols. Online. 2021. Dostupné z: https://sonoff.tech/news-and-events/works-with/smart-home-protocols/#2. [cit. 2024-01-07].

[22] TEXAS INSTRUMENTS. Zigbee. Online. 2023. Dostupné z: https://www.ti.com/technologies/wired-wireless-connectivity/zigbee/overview.html?utm_source=google&utm_medium=cpc&utm_campaign=epd-con-null-58700007750932412_zigbee_overview_rsa-cpc-pp-google-wwe_int&utm_content=what_is_zigbee_technology&ds_k=zigbee+wireless+networking&gad_source=1&gclid=Cj0KCQiAtO-msBhCnARIsAGPa5yaOGjHwc5h0w_M2UNcJ1vuMKqmAoyMaRe8bsh-9xlb85BXSq4nbXxMaAvb4EALw_wcB&gclsrc=aw.ds#zigbee. [cit. 2024-01-07].

[23] THREAD GROUP. What is Thread? Online. 2023. Dostupné z: https://www.threadgroup.org/BUILT-FOR-IOT/Smart-Home. [cit. 2024-01-07].

[24] WIRED. Here's What the 'Matter' Smart Home Standard Is All About. Online. 2023, 23.10.23. Dostupné z: https://www.wired.com/story/what-is-matter/. [cit. 2024-01-07].

[25] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Hrozba. Online. 2003. Dostupné z: https://www.mvcr.cz/clanek/hrozba.aspx. [cit. 2024-03-23].

[26] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Riziko. Online. 2003. Dostupné z: https://www.mvcr.cz/clanek/riziko.aspx#:~:text=Mo%C5%BEnost%2C%20%C5%BEe%20s%20ur%C4%8Ditou%20pravd%C4%9Bpodobnost%C3%AD,mo%C5%BEno%20posoudit%20na%20z%C3%A1klad%C4%9B%20tzv.. [cit. 2024-03-23].

[27] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST [NUKIB]. Doporučení k ochraně počítačů a chytrých zařízení v domácností. Online. Dostupné z: https://www.nukib.cz/cs/infoservis/doporuceni/1512-ochrante-svuj-domov-proti-hackerum/. [cit. 2023-11-14].

[28] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST [NUKIB]. Phishing - stále aktuální hrozba. Online. Dostupné z: https://nukib.gov.cz/cs/infoservis/doporuceni/1494-phishing-stale-aktualni-hrozba/. [cit. 2024-05-20].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

FMEA	Failure Mode and Effects Analysis.
IoT	Internet of Things.
IBM	International Business Machines.
NEST	Novell Embedded Systems Technology.
IPX	Internetwork Packet Exchange
LED	Light Emitting Diode
SMS	Short Message Service
Gb/s	Gigabit per second
GHz	Gigahertz
MHz	Megahertz
kb/s	Kilobit per second
IPv6	Internet Protocol version 6
DDoS	Distributed Denial of Service
P	Pravděpodobnost výskytu
V	Vážnost
O	Odhalení
RPN	Risk Priority Number
TLS	Transport Layer Security
MFA	Multi-Factor Authentication
SSL	Secure Sockets Layer
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
HTTPS	HyperText Transfer Protocol Secure

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA I: ANALÝZA FMEA

Typ hrozby	Hrozba	Potenciální příčina hrozby	Potenciální důsledky chyby	Současný stav				Bezpečnostní opatření	Stav po opatřeních			
				P	V	O	RPN		P	V	O	RPN
Vnější hrozby	Hackerský útok	Zranitelnosti softwaru, slabá hesla	Neoprávněný přístup k systému	4	5	3	60	Pravidelné aktualizace softwaru, používání složitých hesel	2	5	2	20
	Malware	Instalace napadených aplikací	Krádež dat, narušení provozu systému	3	4	2	24	Antivirový software, kontrola aplikací před instalací	2	4	2	16
	Phishing	Podvodné e-maily, napadené aplikace	Krádež dat	4	4	4	64	Proškolení uživatelů, používání antiphishingových filtrů	2	4	2	16
	Sociální inženýrství	Neoprávněný přístup	Krádež osobních údajů	4	4	4	64	Zaškolení uživatelů, antiphishingové filtry	2	4	2	16
	Krádež zařízení	Únik dat, narušení provozu	Ztráta zařízení, finanční ztráty	3	4	3	36	Fyzická ochrana zařízení, šifrování dat v zařízeních	2	4	2	16

	Vandalismus	Úmyslný účinek	Poškození zařízení	2	4	2	16	Fyzická ochrana zařízení, bezpečnostní kamery	1	4	2	8
	Přírodní katastrofy	Narušení provozu	Poškození zařízení, finanční ztráty	2	5	1	10	Zálohování dat, pojištění zařízení, fyzická ochrana	1	5	1	5
	DDoS útoky	Přetížení sítě požadavky	Narušení provozu sítě	3	4	3	36	Speciální ochrana proti útokům DDoS, používání síťových clon	2	4	2	16
	Zranitelnosti v komunikačních protokolech	Porucha systému	Odposlech nebo falšování dat	4	5	3	60	Používání zabezpečených protokolů, pravidelné bezpečnostní audity	2	5	2	20
Vnitřní hrozby	Nesprávná nastavení zařízení	Chyby uživatele	Zranitelnosti v systému	3	3	3	27	Zaškolení uživatelů, ověření nastavení zabezpečení	2	3	2	12
	Zakázání aktualizací softwaru	Zranitelnosti systému	Selhání a vniknutí do systému	3	4	3	36	Automatické aktualizace, kontrola dodržování zásad	1	4	2	8
	Chyby v softwarovém kódu	Chyby programátorů	Porucha provozu systému	3	4	2	24	Testování softwaru, pravidelné aktualizace	2	4	2	16
	Nedostatečná ochrana přístupových práv	Špatně nastavená přístupová práva	Neoprávněný přístup do systému	4	4	3	48	Zavedení vícefaktorového ověřování, kontrola přístupových práv	2	4	2	16

	Nerozdělení přístupových práv	Nesprávné nastavení přístupových práv	Neoprávněný přístup ke kritickým funkcím	3	4	3	36	Rozdělení přístupových práv, vícefaktorové ověřování	2	4	2	16
	Nezabezpečené ukládání dat	Žádné šifrování	Únik citlivých informací	4	5	2	40	Šifrování dat, bezpečné ukládání	2	5	2	20
	Nešifrování při přenosu dat	Žádné šifrování	Únik citlivých informací	4	5	3	60	Zavedení šifrování (např. SSL/TLS)	2	5	2	20
	Chyby uživatelů	Nesprávné činnosti	Neoprávněné činnosti	2	4	3	24	Zaškolení uživatelů, kontrola činnosti	1	4	2	8