VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

OPTIMALIZACE PRACOVNÍHO PROSTŘEDÍ PROSTŘEDNICTVÍM TECHNOLOGIÍ INTERNET OF THINGS
OPTIMISING THE WORKING ENVIRONMENT THROUGH INTERNET OF THINGS TECHNOLOGIES

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE Martin Šebo
AUTHOR

VEDOUCÍ PRÁCE Ing. Petr Sedlák
SUPERVISOR

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Martin Šebo**
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2023/24
Studijní program:	Informační management

Garant studijního programu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Optimalizace pracovního prostředí prostřednictvím technologií Internet of Things

Charakteristika problematiky úkolu:

Úvod
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr

Cíle, kterých má být dosaženo:

Cílem práce je analýza pracovního prostředí společnosti pomocí zařízení IoT, které jsou součástí ekosystému Cisco Meraki, a následně návrh jeho optimalizace tak, aby byla dosažena maximální efektivita a životnost použitých aktivních síťových prvků.

Základní literární prameny:

ČSN EN ISO/IEC 27001 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí Systémy managementu informační bezpečnosti - Požadavky, 2023. [Praha]: Česká agentura pro standardizaci.

ČSN EN ISO/IEC 27002 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí Opatření informační bezpečnosti, 2023. [Praha]: Česká agentura pro standardizaci.

DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk, 2019. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing. ISBN isbn978-80-88260-39-4.

SEDLÁK, Petr a KONEČNÝ, Martin, 2023. Přeměna ISMS v manažerské informatice. Brno: CERM, akademické nakladatelství. ISBN isbn978-80-7623-110-8.

SEDLÁK, Petr a KONEČNÝ, Martin, 2021. Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru. Brno: CERM, akademické nakladatelství. ISBN isbn978-80-7623068-2.

NIST Special Publication 800-213 IoT Device Cybersecurity Guidance: Establishing IoT Device Cybersecurity Requirements, Annapolis: NIST, 2021.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2023/24

V Brně dne 4.2.2024

L. S.

doc. Ing. Miloš Koch, CSc. garant	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Táto diplomová práca je zameraná na analýzu pracovného prostredia spoločnosti Stellnaris s.r.o. prostredníctvom zariadení Internet of Things, a to po stránke teploty, vlhkosti, kvality vzduchu a hlučnosti. Cieľom práce je analyzovať a navrhnúť optimalizáciu monitorovaných priestorov tak, aby sieťové prvky (najmä aktívne) bežali čo najefektívnejšie, bola dosiahnutá ich vysoká životnosť a taktiež, aby bol dosiahnutý komfort pre osoby nachádzajúce sa v priestoroch v prípade výkonu práce. Predmetom tejto práce nie je monitoring celých priestorov firmy, ale len vybraných miestností, ktoré sú bližšie špecifikované v kapitole Analýza súčasného stavu.

Kľúčové slová: *IoT, monitoring, teplota, kvalita, meranie, efektivita, spoľahlivosť, zabezpečenie*

Abstract

This master's thesis is focused on the analysis of the working environment of Stellnaris s.r.o. through the Internet of Things devices in terms of temperature, humidity, air quality and noise. The aim of the thesis is to analyze and propose the optimization of the monitored premises so that the network elements (especially the active ones) run as efficiently as possible, their long lifetime is achieved and also so that the comfort of the persons present in the premises is achieved in case of work performance. The subject of this work is not the monitoring of the entire company premises, but only selected areas, which are specified in more detail in the chapter Analysis of the current state.

Key words: *IoT, monitoring, temperature, quality, measuring, effectivity, reliability, security*

Bibliografická citace

ŠEBO, Martin. *Optimalizace pracovního prostředí prostřednictvím technologií Internet of Things* [online]. Brno, 2024 [cit. 2024-04-23]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/158740. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Ing. Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 23. 4. 2024

Bc. Martin Šebo
autor

POĎAKOVANIE

Rád by som touto cestou poďakoval vedúcemu diplomovej práce, Ing. Petrovi Sedlákovi, za ním poskytnutú možnosť písania práce s danou témou a jeho následným dozorom nad prácou samotnou. Taktiež by som chcel poďakovať Ing. Matejovi Zápotočnému, Ph.D. za konzultácie a Ing. Matejovi Havlasovi za oponentúru. V neposlednom rade chcem poďakovať vedeniu samotnej spoločnosti Stellnaris s.r.o. za možnosť nasadenia riešenia, ktoré je predmetom práce, v ich priestoroch počas môjho pôsobenia v spoločnosti samotnej.

Obsah

Úvod

Problematika monitorovania prostredia slúžiaceho na výkon práce nie je žiadnou novinkou, no dnešný prístup sa skôr zameriava na optimalizáciu prostredia ako z hľadiska zvýšenia komfortu zamestnancov, tak aj predlžovania životnosti a dostupnosti prvkov technickej infraštruktúry.

Vďaka presunu mnohých služieb do prostredia cloud je možné vytvoriť celé monitorovacie systémy postavené na technológiách, ktorých správu po stránke údržby a zabezpečenia tým pádom nemusí riešiť samotná spoločnosť, ktorá ich využíva, ale tieto záležitosti pripadajú na poskytovateľa služieb.

Jednou z mnohých výhod v tomto prípade je, že zabezpečenie je na naozaj vysokej úrovni odpovedajúcej medzinárodným bezpečnostným štandardom, čo má za následok vysokú spoľahlivosť a dostupnosť. V neposlednom rade ide o vysoko modifikovateľný a škálovateľný nástroj, ktorý je možné implementovať ako v rozsiahlych korporátnych spoločnostiach, tak aj v menších firmách s desiatkami zamestnancov.

Ciele práce, metódy a postupy spracovania

Práca sa zameriava na problematiku monitorovania a optimalizácie pracovného prostredia v spoločnosti, ktorá sa venuje vývoju softvéru, marketingovým službám a grafickému dizajnu. Spočiatku v spoločnosti, ktorá je predmetom tejto práce, nebol implementovaný žiadny systém, ktorý by umožňoval sledovať a zlepšovať podmienky v kanceláriách a serverovniach, kde sa nachádzajú dôležité zdroje, zariadenia a, v neposlednom rade, aj zamestnanci.

Cieľom práce je analyzovať aktuálny stav a potreby spoločnosti v tejto oblasti a navrhnúť riešenie založené na zariadeniach internetu vecí (IoT), ktoré by umožňovali meranie a reguláciu teploty, vlhkosti a kvality ovzdušia v rôznych priestoroch a vyhodnotiť vplyv tohto riešenia na zvýšenie komfortu a produktivity zamestnancov, ako aj na predĺženie životnosti a zníženie prevádzkových nákladov na aktívne sieťové prvky.

Práca sa skladá z troch častí. V teoretickej časti sa popisujú základné pojmy a princípy IoT, existujúce technológie a platformy pre prevádzku IoT zariadení, ako aj možnosti a výzvy spojené s monitorovaním a optimalizáciou pracovného prostredia. Taktiež je jej súčasťou detailný opis zvoleného nástroja.

V analytickej časti je priblížený aktuálny stav v spoločnosti a taktiež proces zberu údajov prostredníctvom IoT. Ďalej sa popisuje spôsob spracovania, analýzy a prezentácie získaných dát.

Posledná časť slúži na prezentáciu navrhovaných riešení vytvorených na základe zozbieraných dát, ako pomocou zariadení, tak priamo od zamestnancov prostredníctvom ankiet. Týmto je pravdepodobnosť, že budú navrhované riešenia prínosné, skutočne vysoká. Okrem toho je celý proces ešte na záver zhodnotený aj po ekonomickej stránke.

1. Teoretické východiská práce

Táto kapitola zahŕňa rôzne informácie slúžiace na lepší opis a teda pochopenie metód a postupov pri monitorovaní prostredia prostredníctvom zariadení internetu vecí. V prvom rade definuje základné pojmy ako je internet vecí alebo IoT, monitoring, opisuje nástroj Cisco Meraki a následne pojmy, s ktorými sa už priamo v prostredí Cisco Meraki pracuje. Hlavným cieľom je teda pochopenie princípov a problematiky, ktorými sa diplomová práca zaoberá a to ako z hľadiska hardvérových, tak aj softvérových prostriedkov.

1.1. Meraki

Meraki bola pôvodne spoločnosť, respektíve startup, ktorá navrhla svoju technológiu na základe projektu Roofnet, experimentu vyvinutého Laboratóriom počítačovej vedy a umelej inteligencie (CSAIL) Massachusettského technologického inštitútu. Jeho tvorcovia chceli vytvoriť samo sa organizujúcu bezdrôtovú sieť, ktorá by mohla smerovať dátové pakety preskakovaním z jednej antény namontovanej na streche na druhú (uzly, ktoré prijímajú a vysielajú dáta).

Keď spoločnosť Cisco v roku 2012 získala spoločnosť Meraki, získala aj jej odborné znalosti a priekopnícke projekty v oblasti cloudovo riadených sietí. Dnes je spoločnosť Cisco Meraki najdôveryhodnejšou značkou pre bezpečnú a škálovateľnú cloudovú architektúru, ktorú možno ľahko nasadiť a spravovať na diaľku.

Spoločnosť teraz ponúka širokú škálu produktov a služieb. Veľkou výhodou tejto služby je, že používatelia môžu integrovať produkty Meraki a vytvoriť tak ucelený ekosystém spravovaný v cloude, v ktorom môžu bezproblémovo spolupracovať bezpečnostné riešenia, prepínače a ďalšie IT funkcie. Čím viac produktov a riešení Cisco Meraki užívateľ disponuje, tým lepšie výsledky môže dosiahnuť. [1]

1.2. Cloud

Cloud, známy aj ako cloud computing, je na internete založený model vývoja a používania počítačových technológií. Je to koncept, ktorý sa týka integrácie fyzických objektov do digitálnej sféry prostredníctvom použitia rôznych technológií, ako sú snímače, softvér a sieťové pripojenia.

Cloud je virtuálny priestor v dátových centrách, ktorý prevádzkovateľ cloudových služieb poskytuje klientom. Prostredníctvom internetu klienti pristupujú k svojim dátam uloženým v tomto dátovom centre. Dáta sú umiestnené v dátových centrách na fyzických serveroch.

Podľa potreby vie poskytovateľ zákazníkovi zväčšovať priestor, ak potrebuje uložiť viac dát a takisto upravovať výkon cloudu. Cloudové úložiská rozdeľujeme na verejné cloudové úložisko, súkromné cloudové úložisko a hybridné cloudové úložisko.

Cloud computing sa často stretáva s tromi modelmi cloudových služieb: Software as a Service (SaaS), Platform as a Service (PaaS) a Infrastructure as a Service (IaaS).

Cloud computing je významný krok vpred v oblasti technologickej inovácie, ktorý otvára nové možnosti pre vývoj inteligentných systémov a služieb, ktoré môžu výrazne zlepšiť naše životy a spôsobiť hlboké zmeny v mnohých oblastiach, vrátane priemyslu, dopravy, zdravotníctva a domácností. [2]

1.3. IoT (Internet of Things)

Internet vecí (IoT) predstavuje koncept, ktorý sa týka integrácie fyzických objektov do digitálnej sféry prostredníctvom použitia rôznych technológií, ako sú snímače, softvér a sieťové pripojenia. Medzi tieto "veci" patria napríklad: domáce spotrebiče, automobily, termostaty, ale aj sofistikované priemyselné nástroje.

Podľa odhadov je v súčasnosti pripojených viac ako 10 miliárd zariadení internetu vecí a očakáva sa, že do roku 2025 ich počet vzrastie na 22 miliárd. Tento nárast je dôsledkom pokračujúcej digitalizácie a technologickej inovácie, ktorá umožňuje pripojenie stále väčšieho počtu zariadení k internetu.

V posledných rokoch sa internet vecí stal jednou z najdôležitejších technológií 21. storočia. Jeho význam spočíva v schopnosti pripojiť každodenné predmety, ako sú kuchynské spotrebiče, autá, termostaty a detské opatrovateľky, k internetu prostredníctvom vstavaných zariadení. Toto prepojenie umožňuje rýchlu komunikáciu medzi ľuďmi, procesmi a vecami, čo vedie k výraznému zlepšeniu efektívnosti a pohodlia.

Vďaka pokrokom v oblasti výpočtovej techniky, cloudu, veľkých dát, analytických a mobilných technológií môžu fyzické veci zdieľať a zhromažďovať údaje s minimálnym zásahom človeka. V tomto prostredí môžu digitálne systémy zaznamenávať, monitorovať a upravovať každú interakciu medzi prepojenými vecami. Tento proces umožňuje vytváranie inteligentných systémov, ktoré sú schopné automaticky reagovať na zmeny v prostredí a optimalizovať svoje operácie na základe získaných údajov.

Takže, internet vecí predstavuje významný krok vpred v oblasti technologickej inovácie, ktorý otvára nové možnosti pre vývoj inteligentných systémov a služieb, ktoré môžu výrazne zlepšiť naše životy a spôsobiť hlboké zmeny v mnohých oblastiach, vrátane priemyslu, dopravy, zdravotníctva a domácností. [3]

1.4. Monitoring

Monitoring je proces, ktorý zahŕňa systematické sledovanie, zhromažďovanie, analýzu a interpretáciu dát. Tento proces je kľúčový pre efektívne riadenie a kontrolu systémov a procesov v rôznych oblastiach, vrátane IT, zdravotníctva, výroby, vedy a výskumu a mnohých ďalších.

V kontexte informačných technológií sa monitoring používa na sledovanie a vyhodnocovanie výkonu a spoľahlivosti hardvéru a softvéru. To zahŕňa sledovanie výkonu serverov, databáz, sietí a aplikácií, ako aj sledovanie bezpečnostných hrozieb a incidentov.

Existuje niekoľko typov monitoringu v IT:

1. **Systémový monitoring**: Systémový monitoring sa zaoberá sledovaním výkonu a stavu fyzických alebo virtuálnych serverov. To zahŕňa sledovanie takých metrík, ako je vyťaženie procesora, využitie pamäte a diskového priestoru, ako aj stav a výkon operačného systému a jeho služieb.

2. **Aplikačný monitoring (APM)**: APM sa zaoberá sledovaním a riadením výkonu a dostupnosti softvérových aplikácií. To zahŕňa sledovanie takých metrík, ako je čas odozvy, chybovosť, využitie zdrojov a kvalita služieb.

3. **User experience monitoring**: Tento typ monitoringu sa zaoberá sledovaním a vyhodnocovaním toho, ako užívatelia interagujú s aplikáciami a službami. To môže zahŕňať sledovanie takých metrík, ako je čas odozvy, chybovosť, využitie zdrojov a spokojnosť užívateľov.

4. **Sieťový monitoring**: Sieťový monitoring sa zaoberá sledovaním a riadením výkonu a spoľahlivosti počítačových sietí. To zahŕňa sledovanie takých metrík, ako je priepustnosť, oneskorenie, strata paketov, dostupnosť a stav sieťových zariadení, ako sú switche a routery.

Každý z týchto typov monitoringu má svoje vlastné nástroje, techniky a postupy, ktoré sa používajú na zhromažďovanie, analýzu a interpretáciu dát. Tieto informácie môžu byť použité na identifikáciu a riešenie problémov, optimalizáciu výkonu a zlepšenie kvality služieb. [4]

1.5. Hardware

Ako už bolo spomenuté, v rámci IoT je zahrnuté široké spektrum rôznych zariadení, prevažne slúžiacich na sledovanie alebo monitoring iných zariadení, osôb, či celých prostredí. V tomto prípade ide konkrétne o inteligentné kamery a senzory od spoločnosti Cisco. Do spoločnosti Stellnaris bolo zakúpené hardwarové vybavenie, ktoré je kompatibilné s už používaným systémom na správu koncových zariadení, Cisco Meraki. Firma teda disponuje dvomi kusmi kamery Cisco Meraki MV2 a dvomi kusmi senzorov, MT-10 a MT-14.

1.5.1. Senzory

V prípade senzorov boli zvolené modely, ktorých účelom je primárne meranie teploty a vlhkosti vzduchu. Oba senzory sú napájané z batérií, no v prípade zariadenia MT14 je možné dodatočné napájanie cez USB-C konektor, čo následne umožňuje meranie hodnôt PM2.5. Keďže sa nepodarilo túto funkciu spojazdniť ani po komunikácii s podporou Cisco, nebude v práci riešená.

MT10

- senzor disponuje schopnosťou merať teplotu vzduchu (°C/°F)
- taktiež meria vlhkosť vzduchu (RH%)

MT14

- senzor disponuje schopnosťou merať rovnaké údaje ako MT-10
- navyše umožňuje merať kvalitu vzduchu (TVOC, PM2.5) a hluk

Obrázok 1: Cisco Meraki MT10 a MT14
(zdroj: vlastné spracovanie)

1.5.2. Kamery

Čo sa týka použitých kamier, ich hlavné využitie je na monitorovanie zvolených priestorov naživo v prípade potreby a na zachytávanie udalostí pomocou detekcie pohybu na časovú os. Keďže kamery disponujú kvalitným senzorom citlivým na infračervené svetlo, poskytujú použiteľný živý prenos a záznamy vo forme fotiek aj v noci. Parametre kamier sú špecifikované nižšie.

MV2

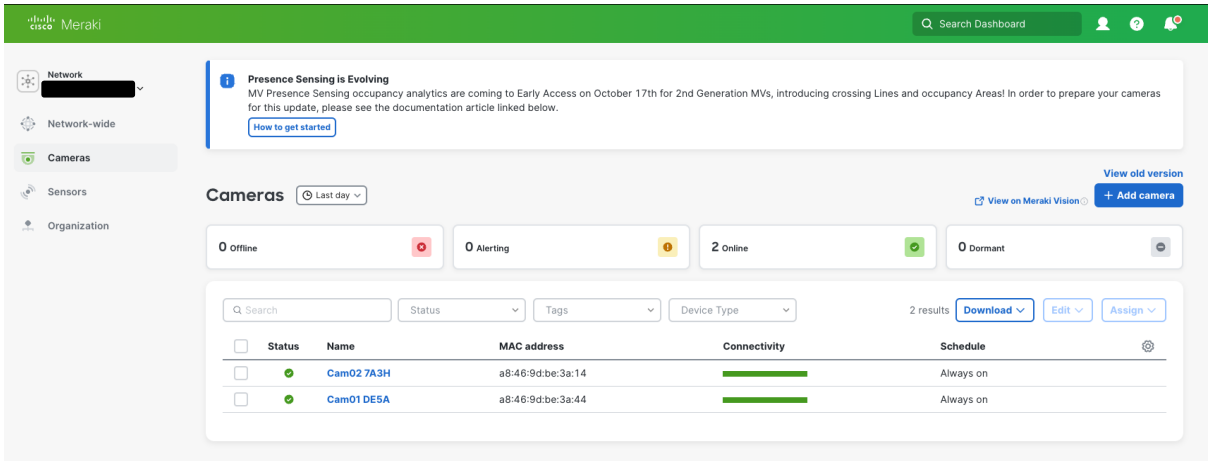
- umožňuje nahrávanie videozáznamu v rozlíšení 1080p (enkódovanie H.264)
- uhol nahrávania je 103 stupňov
- komunikuje prostredníctvom Wi-Fi (802.11ac)
- živý prenos s možnosťou tvorby záznamu
- reakcia na pohyb (udalosti sú zaznačované na časovú osu vo forme tagov)

Obrázok 2: Cisco Meraki MV2
(zdroj: [5])

1.6. Software

Bez nástroja priamo určeného na správu zariadení by nebolo možné vytvorenie monitorovacieho systému. V tomto prípade je teda využívaný nástroj priamo vyvinutý spoločnosťou Cisco. Konkrétne ide o Cisco Meraki, ktorý okrem správy koncových uzlov (PC, mobilné zariadenia) a sieťových prvkov podporuje správu IoT.

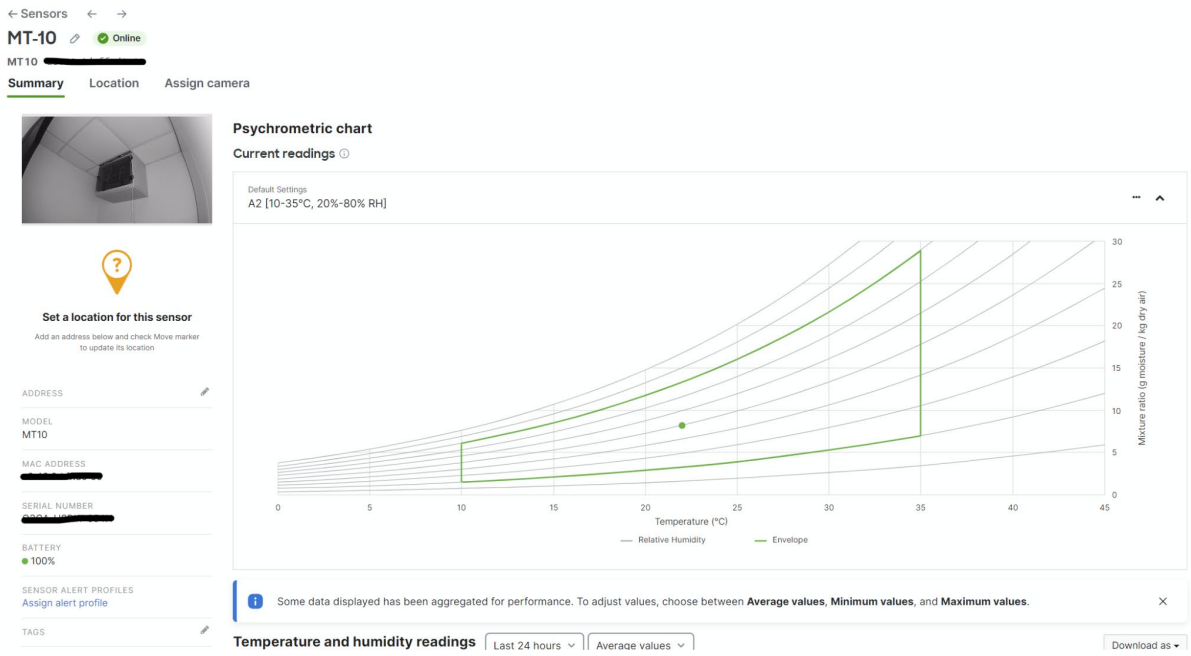
Cisco Meraki poskytuje užívateľom prehľad enrollnutých zariadení vo forme zoznamu obsahujúceho základné informácie.



Obrázok 3: Cisco Meraki
(zdroj: vlastné spracovanie)

1.6.1. Prehľad senzorov

V prípade senzorov je menu veľmi podobné tomu, ktoré slúži na zobrazenie kamier, preto ho nie je nutné znázorňovať. Dôležitý je detailný prehľad v prípade konkrétnych zariadení.



Obrázok 4: Dashboard senzoru MT10
(zdroj: vlastné spracovanie)

Systém poskytuje základné informácie ako aktuálne meranie údajov vo forme psychrometrického grafu. Tento graf znázorňuje údaje z takzvaného mokrého a suchého teplomeru pre zmesi vzduchu a vodnej pary pri atmosférickom tlaku.

Zóny označené zeleným obrysom v psychrometrických grafoch vychádzajú z odporúčaní noriem ASHRAE na udržiavanie teplotných a vlhkostných podmienok rôznych typov dátových centier. Nižšie sú uvedené 4 odporúčané rozsahy:

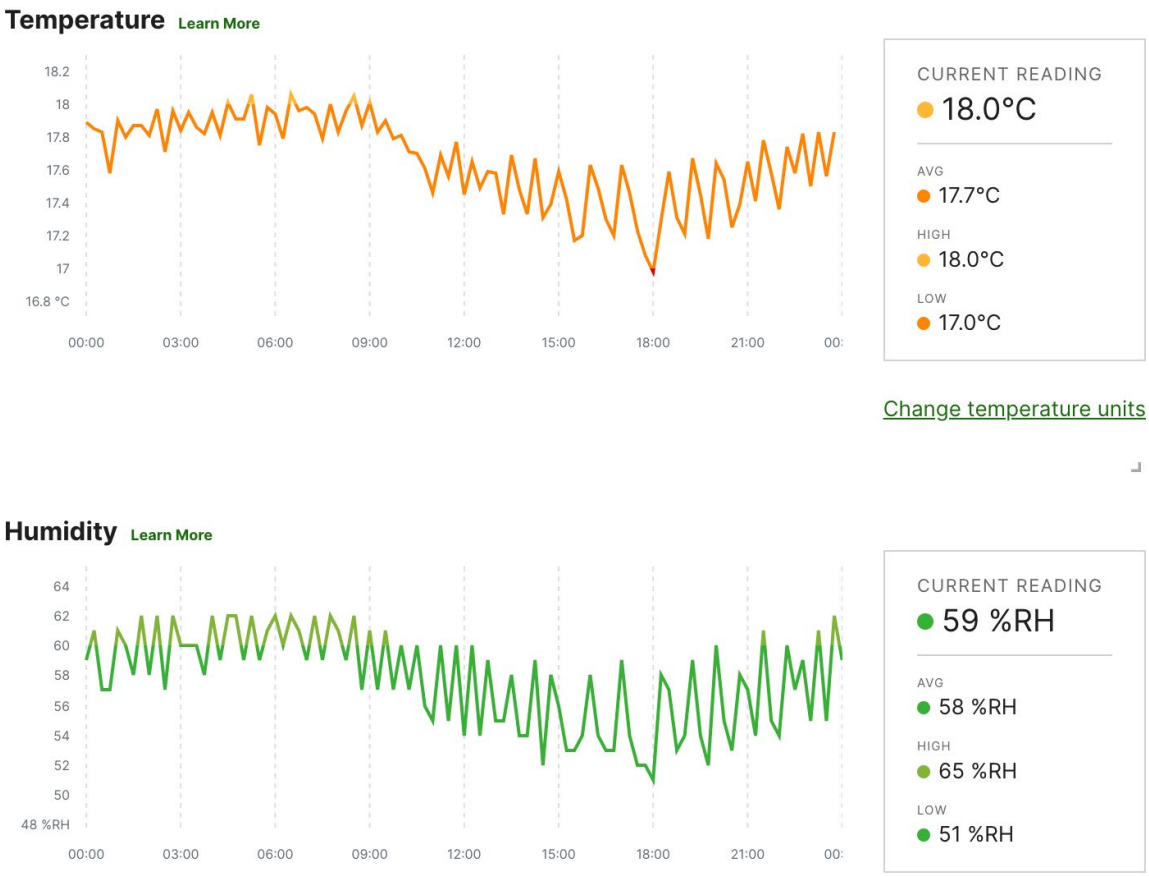
A1 [15 - 32 °C, 20 - 80 % relatívnej vlhkosti] - typické dátové centrum s prísne kontrolovanými parametrami prostredia

A2 [10-35 °C, 20 % - 80 % relatívnej vlhkosti] - typický priestor informačných technológií s určitou kontrolou parametrov prostredia

A3 [5-40 °C, 8 % - 85 % relatívnej vlhkosti] - typicky skladovací priestor so záložnými diskami

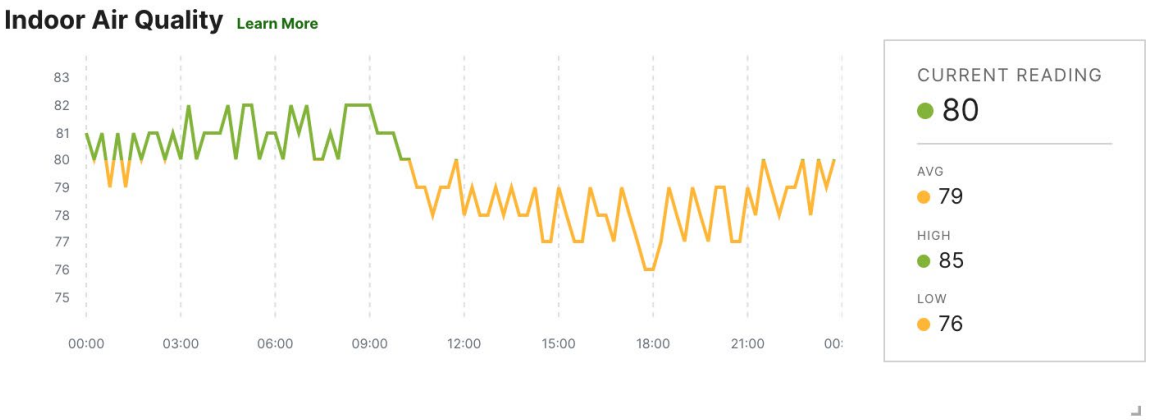
A4 [5-45 °C, 8 % - 90 % relatívnej vlhkosti] - Najmenej citlivé priestory z hľadiska životného prostredia.

Oba senzory sú pomocou dashboard naviazané na individuálne kamery, s ktorou zdieľajú miestnosti, kvôli prehľadnosti.



Obrázok 5: Meranie teploty a vlhkosti vzduchu MT14
(zdroj: vlastné spracovanie)

Obidva senzory podporujú meranie teploty, ktoré je uvedené buď v stupňoch Celzia alebo Fahrenheita a vlhkosti vzduchu vyjadrenej množstvom vodnej pary prítomnej vo vzduchu v percentách relatívnej vlhkosti (%RH). Keďže MT14 podporuje navyše meranie iných hodnôt, nižšie sú znázornené merania tohto senzoru.



Obrázok 6: Meranie kvality vzduchu MT14
(zdroj: Meraki Dashboard)

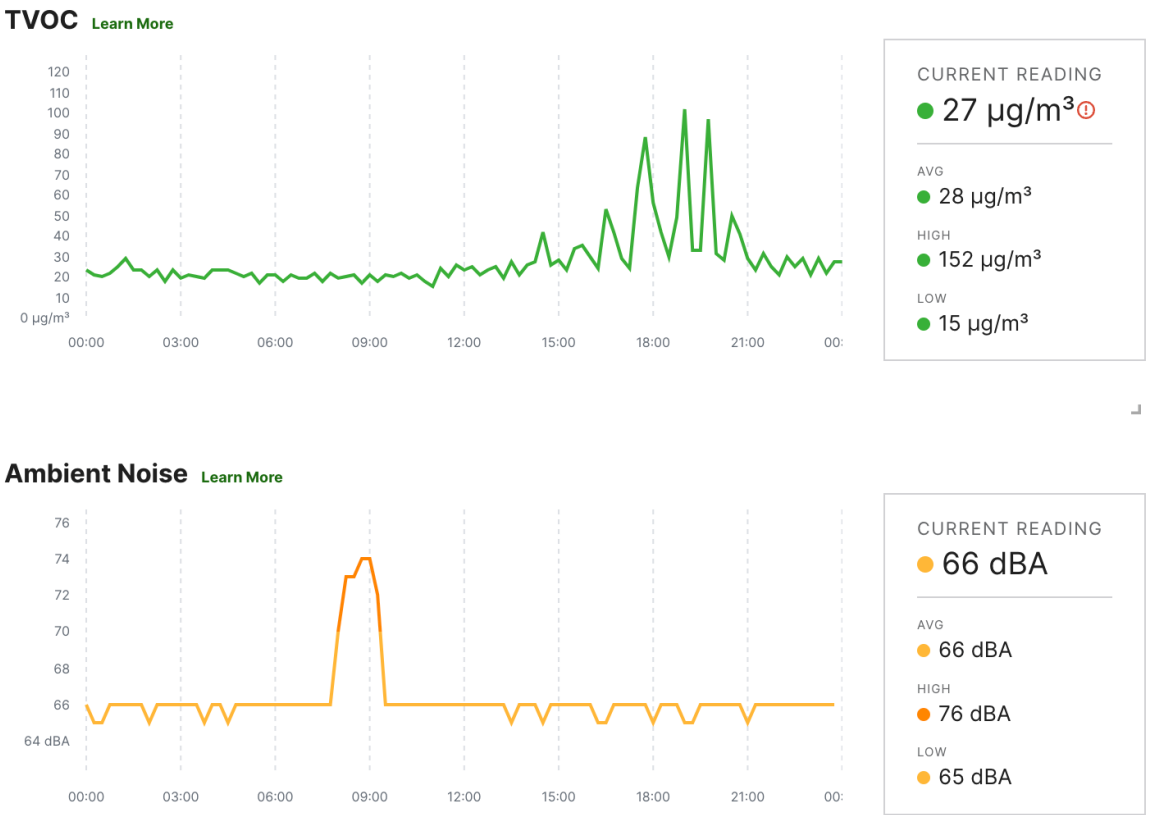
IAQ - Ide v tomto prípade o kvalitatívne súhrnné hodnotenie, ktoré možno použiť ako všeobecný ukazovateľ celkovej kvality ovzdušia. IAQ má päť úrovní hodnotenia: vynikajúce, dobré, primerané, zlé a nedostatočné. Zahŕňa teplotu, vlhkosť, TVOC a v prípade aktivácie aj PM2.5. IAQ nezahŕňa úrovne hluku v okolí. Osa hodnotenia je znázornená nižšie.

Obrázok 7: Osa hodnotenia IAQ
(zdroj: vlastné spracovanie)

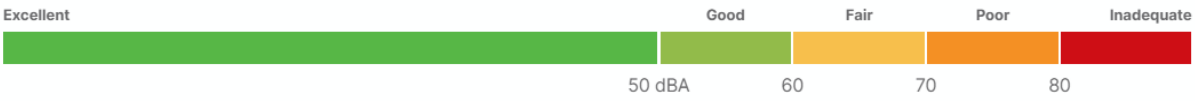
TVOC - Meria celkové množstvo prchavých organických zlúčenín v oblasti v mikrogramoch na meter kubický. Medzi VOC patria rôzne chemické látky, ako sú farby, aerosólové spreje, čistiace prostriedky, pesticídy a automobilové výrobky. Môžu zahŕňať aj chemikálie z fajčenia elektronických cigariet, známeho aj ako vaping.

Obrázok 8: Osa hodnotenia TVOC
(zdroj: vlastné spracovanie)

Senzor v neposlednom rade meria úroveň okolitého hluku v dBA alebo tzv. A-weighted Decibeloch, ktoré sú najvhodnejšie pre znázornenie toho, ako je hlučnosť vnímaná ľudským uchom.



Obrázok 9: Znázornenie TVOC a okolitého hluku
(zdroj: vlastné spracovanie)



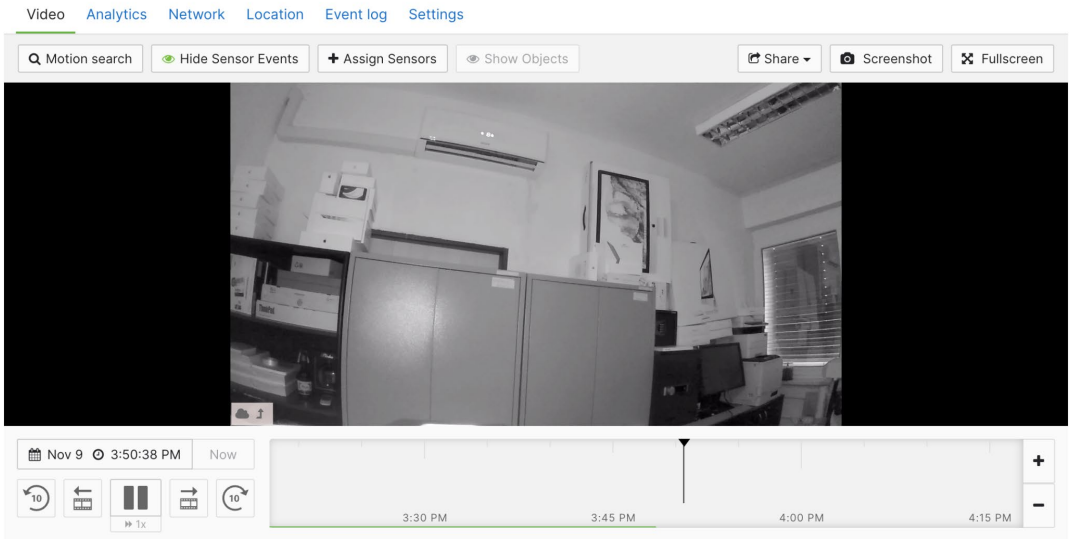
Obrázok 10: Osa hodnotenia okolitého hluku
(zdroj: vlastné spracovanie)

1.6.2. Prehľad kamier

Na správu kamier sú v súčasnej dobe k dispozícii dve rôzne kontrolné strediská. Obe umožňujú sledovanie živého prenosu. V prípade dokúpenia archívnej licencie aj sledovanie záznamu, ktorého kvalita závisí od nastavení v sekcii Settings. Ak užívateľ nedisponuje archívnou licenciou, ako je to v tomto prípade, kamera pri detekcii pohybu na časovej osi znázorňuje udalosti vo forme snapshotov.

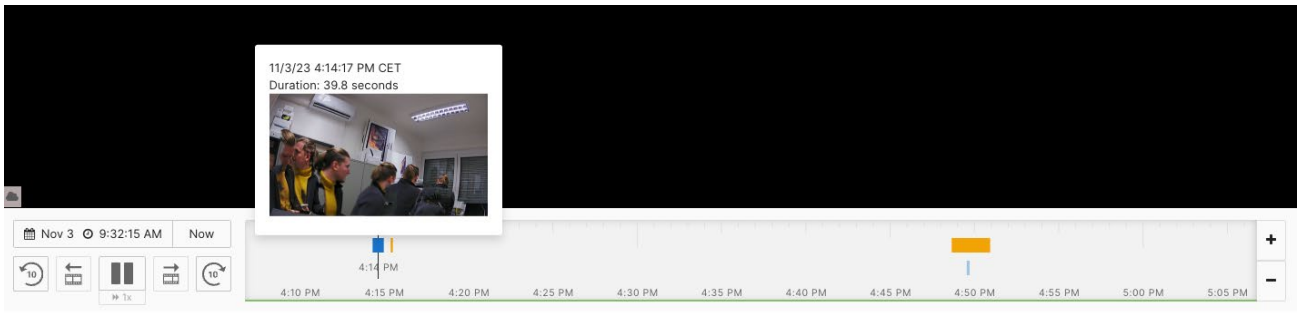
Správca má tiež možnosť vytvorenia screenshotu v akomkoľvek momente sledovania živého prenosu, označiť v rámci záberu zónu sledovania pohybu (Motion search) a taktiež môže konkrétnym kamerám priradiť dostupné senzory.

Základný ovládací panel



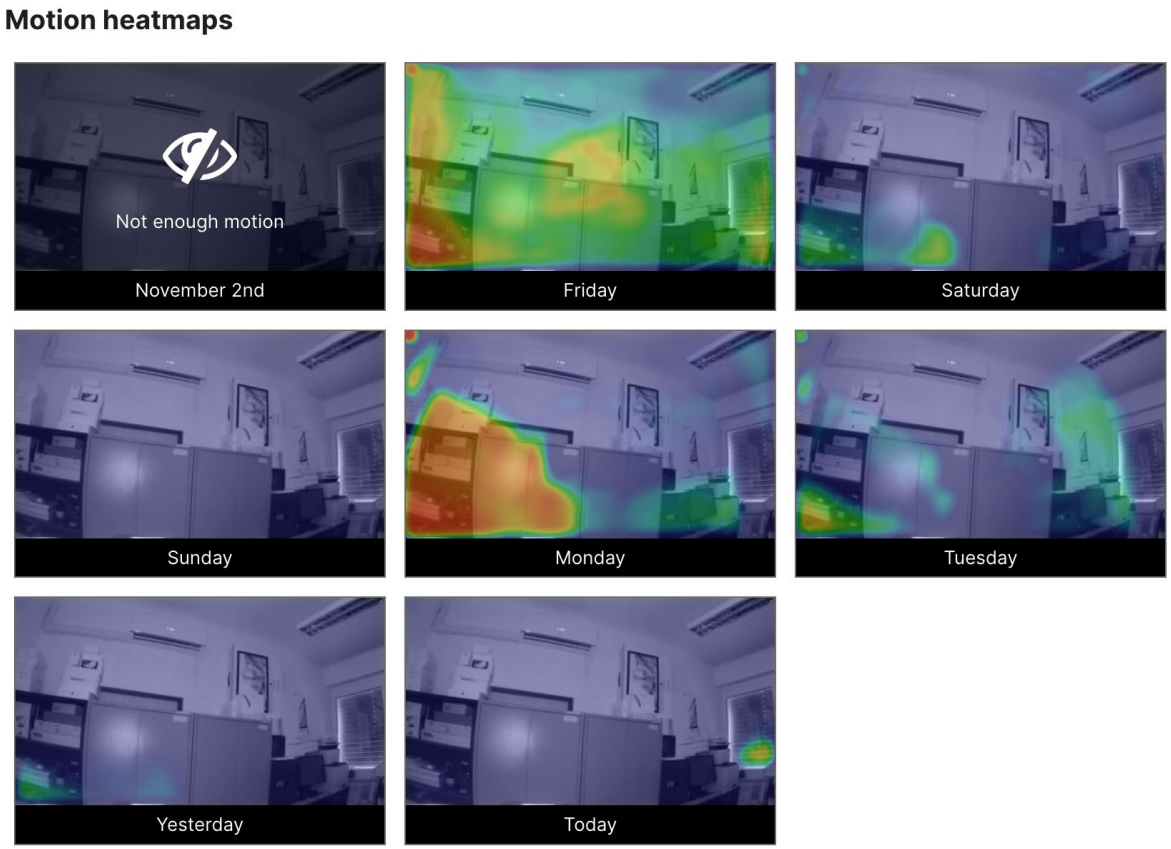
Obrázok 11: Video control
(zdroj: vlastné spracovanie)

Prehľad a možnosť zobrazenia udalostí na časovej osi



Obrázok 12: Videová os
(zdroj: vlastné spracovanie)

V sekcii Analytics je zas možné zobrazenie takzvaných Motion heatmaps, ktoré slúžia na vizualizáciu teplotných zón zapríčinených pohybom osôb v sledovaných priestoroch. Ich zobrazenie je možné nastaviť vo frekvencii minút, hodín až dní.



Obrázok 13: Motion heatmaps
(zdroj: vlastné spracovanie)

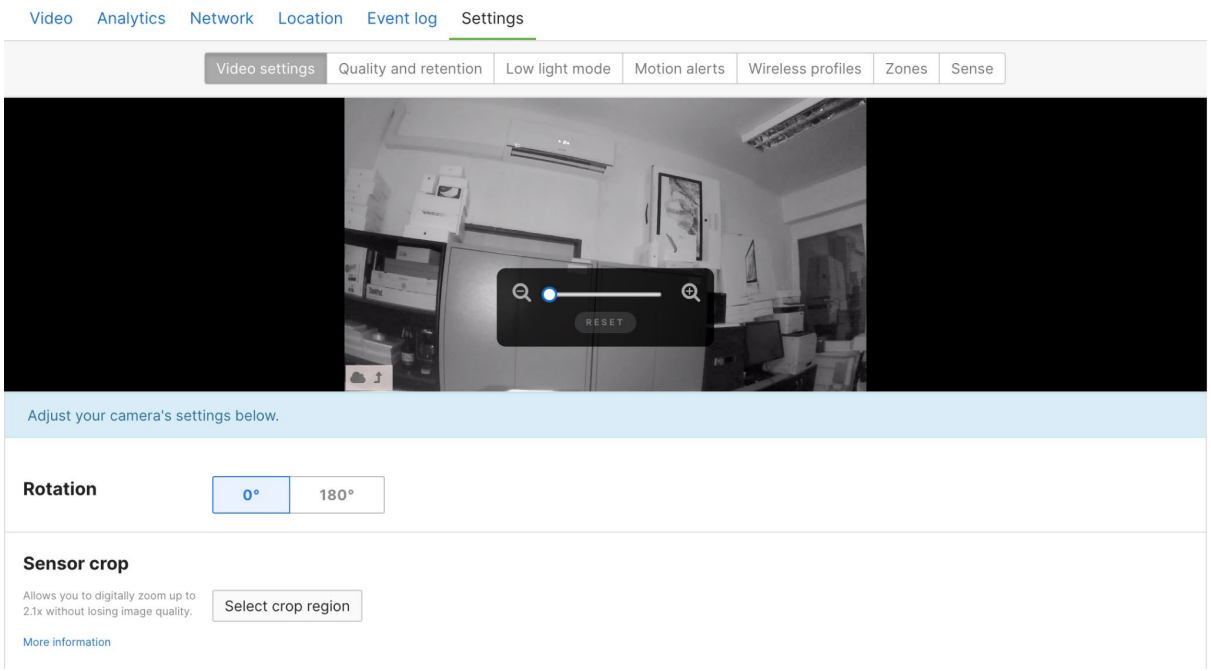
V sekcii Network sú zobrazené sieťové údaje, ako z hľadiska Ethernet, tak aj WiFi. Patrí medzi ne v tomto prípade fyzická adresa, lokálna adresa, verejná adresa, gateway zariadenia a úroveň

signálu v dB. Ďalej je možné použiť príkaz ping na samotné zariadenie alebo na doménu, na ktorú je zariadenie pripojené. Taktiež je možné kameru reštartovať alebo poslať príkaz traceroute.

V prípade sekcie Location je možné nastaviť umiestnenie kamery v rámci predtým stanovenej mapy objektu. Event log slúži len na zachytávanie informácií o realizovaných nastaveniach kamery správcom.

Poslednou sekciou sú nastavenia alebo Settings, v ktorých je možné nakonfigurovať záležitosti ako orientácia kamery, orezanie záberu, tvorba takzvaných Privacy windows, čo sú vo svojej podstate len bloky zakrývajúce zvolené zóny záberu.

Ďalej je možné zvoliť kvalitu prenosu, čo zahŕňa rozlíšenie a snímkovú frekvenciu, prepínanie medzi dvoma verziami detekcie pohybu a možnosťou povoliť alebo zakázať aj nahrávanie zvuku.



Obrázok 14: Nastavenie videa
(zdroj: vlastné spracovanie)

Taktiež je možné nastavenie režimu v nízkom svetle. Ako už bolo spomenuté, kamery disponujú senzormi schopnými nahrávať aj v tme pomocou infračerveného žiarenia. Správca má na výber medzi permanentným vypnutím alebo zapnutím tejto funkcie, no môže tiež v

prípade jej zapínania a vypínania zvoliť aj automatickú metódu, ktorá sa riadi množstvom svetla detegovaným v miestnosti.

V prípade Motion alerts, ako už názov napovedá, má zas správca možnosť v prípade zapnutia upozornení o pohybe nastaviť ich frekvenciu, dĺžku a citlivosť takzvaných triggers alebo spúšťačov. Ďalej je možné kameru zaradiť do predom vytvorenej zóny alebo jej priradiť bezdrôtový profil. Kamery tiež disponujú funkciou Sense, ktorá slúži na pokročilé rozpoznávanie osôb.

Meraki Vision

Ako už bolo spomenuté, nástroj Meraki v prípade správy kamier disponuje okrem toho základného aj mierne iným odlišným nástrojom s názvom Meraki Vision. Ten poskytuje správcovi možnosť tvorby takzvaných Video Walls alebo video stien, čo sú rôzne kombinovateľné zostavy vysielaní zo zvolených kamier.

Obrázok 15: Meraki Vision
(zdroj: vlastné spracovanie)

Okrem toho je pomocou tohto nástroja možná tvorba reportov a vyhľadávanie udalostí (zatiaľ len v Beta verzii).

2. Analýza súčasného stavu

Táto kapitola je zameraná na zhodnotenie súčasnej situácie v spoločnosti Stellnaris s.r.o., čo konkrétne znamená, že v nej bude opísaná spoločnosť samotná, ďalej stav aktuálneho vybavenia, ktoré má za účel meniť atribúty ovzdušia, ako napríklad teplota, vlhkosť, množstvo nežiadúcich častíc vo vzduchu a hluk. V neposlednom rade odpovedá na otázky, aké riziká vyplývajú z inštalácie zariadení IoT na monitoring spomenutých atribútov.

V spoločnosti sa v každej miestnosti nachádza klimatizačná jednotka, pomocou ktorej je možné do značnej miery regulovať teplotu a vlhkosť vzduchu. Aktuálne však jednotky nie sú nastavené podľa žiadnych výstupných údajov získaných na základe reálnych testov, ale ide len o akési nastavovanie, ktoré sa odráža od rôznych odhadov alebo pocitov.

Ako už bolo spomenuté, predmetom tejto práce je meranie a vyhodnocovanie dát v rámci štyroch zvolených priestorov, z ktorých je jeden serverová miestnosť na druhom poschodí (ďalej serverovňa), miestnosť s dátovým rozvádzačom na prízemí (ďalej rozvodňa), kúpeľňa na prízemí a kuchynka na druhom poschodí.

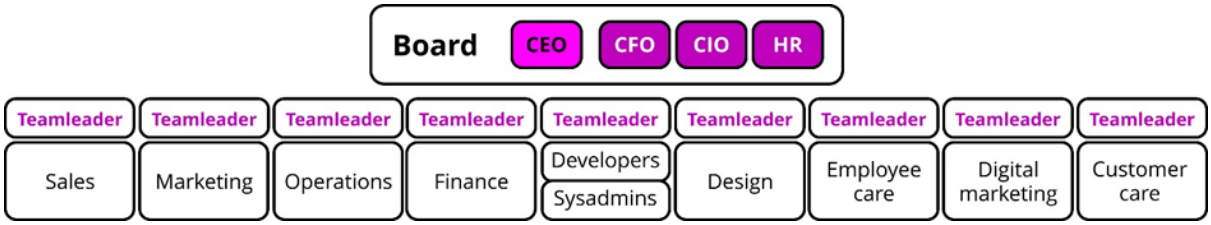
Do spoločnosti bolo zakúpené hardwarové vybavenie, ktoré je kompatibilné s už dlhodobo používaným systémom na správu koncových zariadení, Cisco Meraki. Firma teda disponuje dvomi kusmi kamery Cisco Meraki MV2 a dvomi kusmi senzorov (MT-10 a MT-14) s príslušnými licenciami, bez ktorých by správa zariadení nebola v rámci SW nástroja možná.

2.1. Opis spoločnosti

Stellnaris s.r.o. bola v roku 2007 založená ako reklamná a marketingová agentúra. Pôsobí na trhu už vyše 15 rokov a spočiatku bola zameraná na tvorbu grafického dizajnu rôznych propagačných materiálov. Neskôr sa jej zameranie primárne uprelo na poskytovanie digitálnych riešení a rozšírila tak významne svoje portfólio o softvérové produkty. Primárne sa dnes venuje vývoju SW, čo zahŕňa tvorbu menších projektov pre rôzne firmy, ale taktiež ponúka aj vlastné komplexné nástroje. Spoločnosť primárne sídli v meste Brno, no má taktiež pobočku v Prahe. V tejto práci je predmetom riešenia nasadenie IoT v hlavnom sídle.

2.1.1. Organizačná štruktúra

V prípade Stellnaris s.r.o. ide o takzvanú agilnú štruktúru, ako ju označuje firma samotná. Pozostáva z 10 oddelení: Sales, Marketing, Operations, Finance, Developers, Sysadmins/IT Support, Design, Employee care, Digital marketing a Customer care. Prevažnú časť zamestnancov tvoria ale softvéroví vývojári.

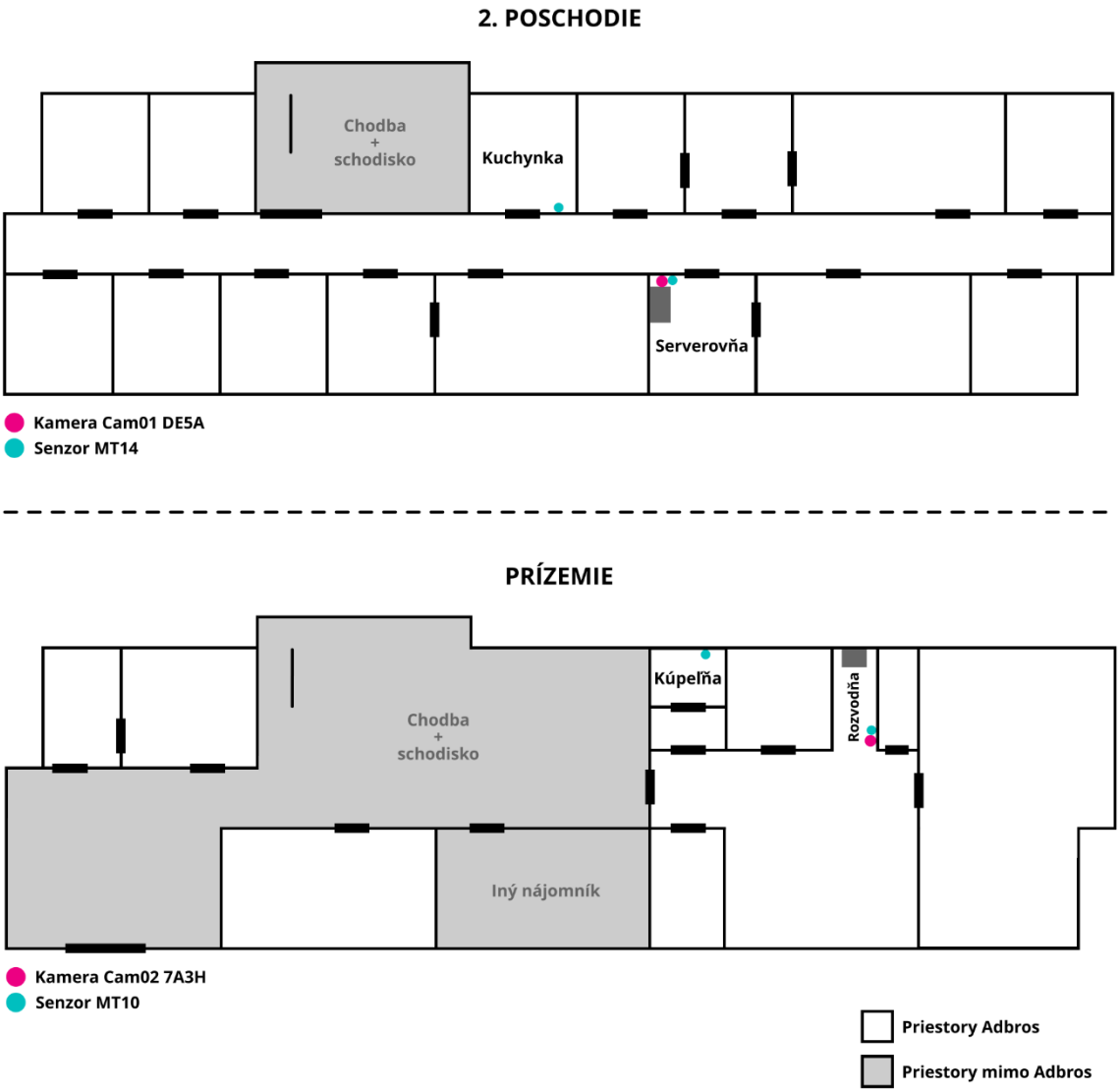


Obrázok 16: Organizačná štruktúra spoločnosti (zdroj: vlastné spracovanie)

Firma sa ďalej rozdeľuje na tímy, ktoré sa rozprestierajú aj naprieč oddeleniami. V rámci nich sa riešia rôzne projekty a môžu mať v ich rámci zamestnanci iných vedúcich než v rámci svojho oddelenia. Tieto skutočnosti majú za následok, že druh organizačnej štruktúry spoločnosti Stellnaris možno považovať za hybridný.

2.1.2. Plán budovy

Ako už bolo spomenuté, predmetom tejto práce je riešenie IoT problematiky v hlavnom sídle spoločnosti v meste Brno. Ide o dvojposchodovú budovu. Konkrétne o vybrané priestory v prízemí budovy a jej celé druhé poschodie. Prvé poschodie majiteľ budovy prenajíma iným spoločnostiam, tak ako aj určitú časť prízemia. Umiestnenie zariadení je špecifikované formou máp vytvorených na základe pôdorysov oboch spomenutých poschodí.



Obrázok 17: Plán budovy - druhé poschodie a prízemie
(zdroj: vlastné spracovanie)

Na analýzu súčasného stavu poslúžia dáta získané primárne prostredníctvom senzorov, ale aj kamier. V neposlednom rade budú do procesu vstupovať aj dáta získané na základe dotazníkov zamestnancov, ktorí sa vo vybraných priestoroch zdržiavajú. Namerané dáta použité na tvorbu analýzy v prípade serverovne a rozvodne boli zozbierané od inštalácie infraštruktúry, dňa 02.11.2023 o 16. hodine, do dňa 02.12.2023 o 16. hodine, kedy bolo meranie ukončené a došlo k presunu senzorov na nové miesta. Keďže systém Meraki poskytuje najlepší súhrn dát v rozmedzí maximálne jedného mesiaca, bolo zvolené toto časové okno. Pokiaľ ide o priestory kuchynky na druhom poschodí a kúpeľne na prízemí, dáta boli merané od 02.01.2024 do dňa

01.02.2024, z rovnakých dôvodov ako v prípade prvého merania. Analýza sa zameriava na údaje z celého monitorovacieho obdobia.

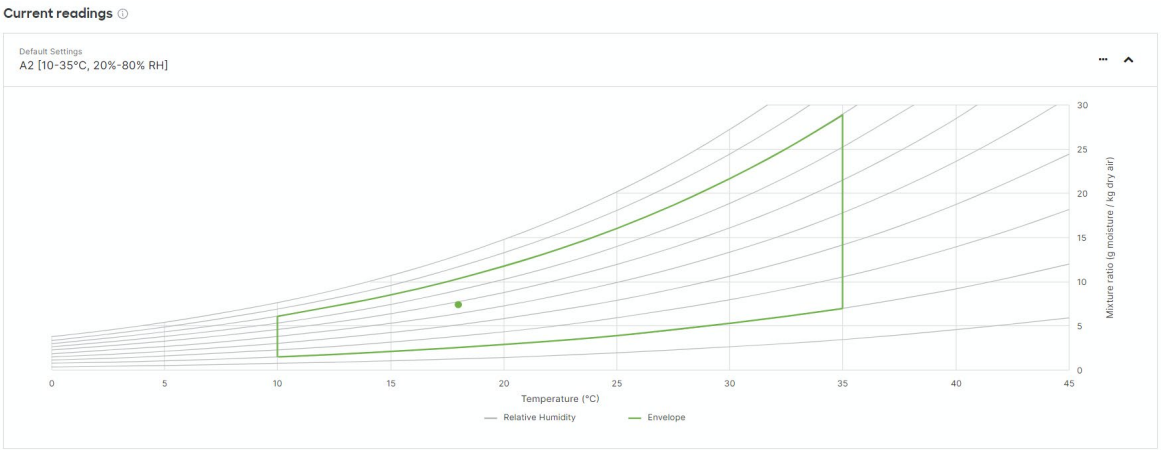
2.2. Serverovňa

V prípade serverovej miestnosti bol zvolený senzor MT14 a kamera Cam02 7AH3. Ide o izolovanú miestnosť so serverovým rackom, ktorý obsahuje rôzne routery, switche, patchpanely a NAS. Ďalej sa v priestore nachádza klimatizačná jednotka a rôzne PC, ktorých prevádzka je prerušovaná. To znamená, že niekedy sú niektoré z nich spustené dni bez prestávky, no naopak môžu byť následne vypnuté aj po dobu niekoľkých týždňov. Klimatizačná jednotka je konštantne spustená, nastavená na 18 stupňov Celzia a základný režim chladenia.

Inštrumentáciou boli merané údaje o teplote (°C), vlhkosti (%RH), kvalite ovzdušia (zahŕňajúce teplotu, vlhkosť, TVOC), hluku (dBA) a TVOC - celkového množstva prchavých organických zlúčenín (µg/m3).

2.2.1. Senzor MT14

Na psychrometrickom grafe senzoru MT14 možno identifikovať namerané hodnoty v priestore prostredníctvom zelenej bodky, ktorá sa nachádza v oblasti so zeleným obrysom. Táto poloha signalizuje súlad s odporúčanými normami ASHRAE pre udržiavanie teplotných a vlhkostných podmienok v prostredí informačných technológií (rozsah A2).



Obrázok 18: Senzor MT14 – Serverovňa - Psychrometric chart
(zdroj: vlastné spracovanie)

Líniové grafy merania kvality vzduchu, teploty a vlhkosti poskytujú dôležité informácie o prostredí miestnosti, kde je umiestnené zariadenie servera. Na osi x je znázornený čas v dňoch, zatiaľ čo os y zobrazuje merané parametre. Kontinuálne sledovanie takýchto grafov je kritické pre zachovanie optimálnych podmienok pre fungovanie serverových zariadení a minimalizáciu rizika porúch. Stabilná teplota je kľúčovým faktorom pre prevenciu prehrievania a správne fungovanie aktívnych prvkov. Stabilná úroveň vlhkosti je dôležitá pre prevenciu korózie a správne fungovanie serverových zariadení.

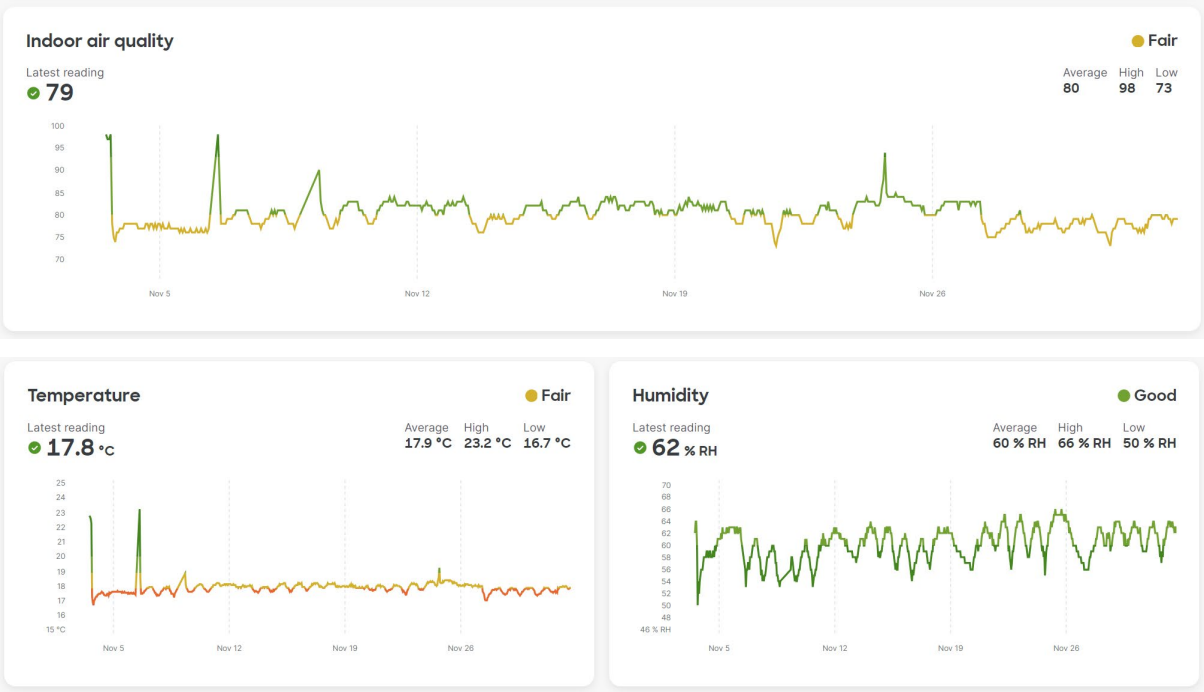
Kvalita a teplota

Grafy zobrazujú v prvotných hodinách merania veľmi vysoké hodnoty. Táto skutočnosť je jednoducho vysvetliteľná tým, že senzor sa v tom čase kalibroval pre meranie správnych hodnôt. Priemerné hodnoty kvality ovzdušia sa za meraný mesiac pohybovali okolo hodnoty 80 bodov. Priemerná teplota v serverovni sa držala na hodnote 17,9 stupňov Celzia.

Líniový graf kvality ovzdušia a teploty ukazujú vysoký výkyv v nameraných hodnotách dňa 6. novembra a taktiež v neskorších hodinách 8. novembra, čo pretrvávalo do rána 9. novembra. V oboch prípadoch išlo o dočasný výpadok senzora. Po oprave sa senzor sám skalibroval a pokračoval v meraní hodnôt.

Vlhkosť

Graf vlhkosti v miestnosti serverovne vykazuje výrazné fluktuácie, ktoré sa prejavujú striedaním medzi vysokými a nízkymi hodnotami. Tieto oscilácie môžu mať rôzne príčiny a vplyvy na prostredie v serverovni. V prvých dvoch dňoch merania sledujeme z grafu pomalé stúpanie vlhkosti k hodnote okolo 58 percent . Po výpadku senzoru 6. novembra sa vyššie hodnoty vlhkosti objavujú v nočných a skorých ranných hodinách. Z dlhodobého hľadiska sa ale miera vlhkosti vzduchu pohybuje v priemere okolo hodnoty 60 percent. Je možné povedať, že ide o najvýraznejšie fluktuujúcu hodnotu, čo je pripisované nastaveniu klimatizačnej jednotky.

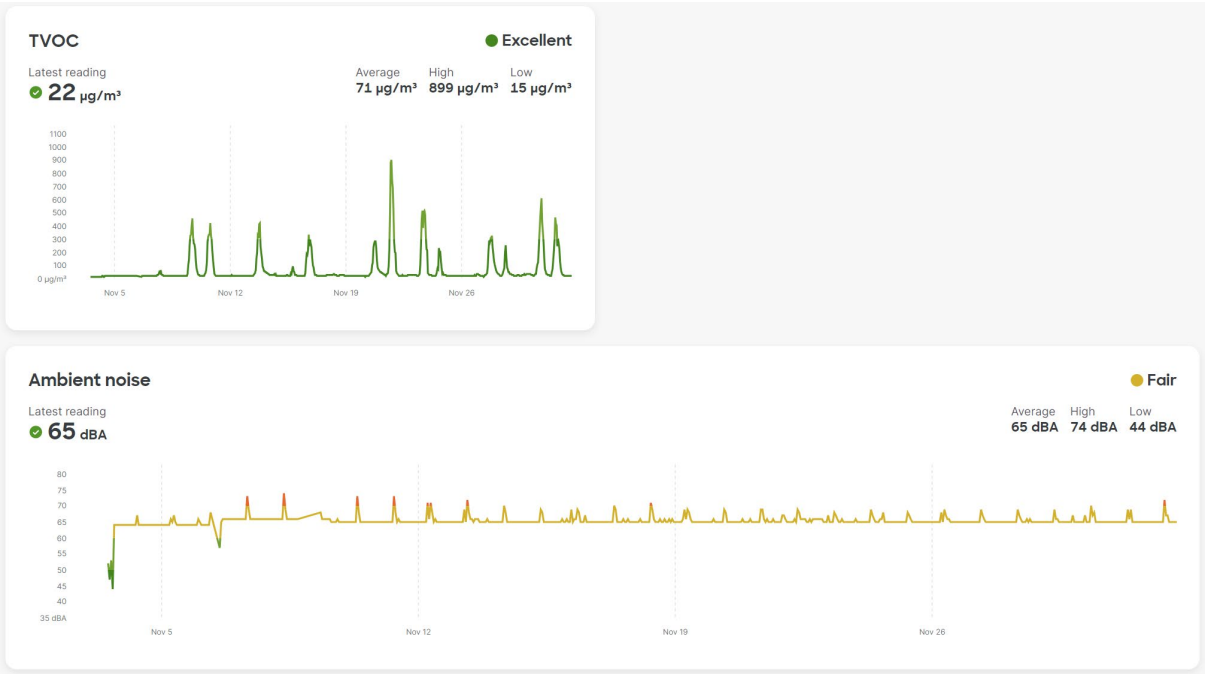


Obrázok 19: Senzor MT14 – Serverovňa - Kvalita, teplota a vlhkosť vzduchu (zdroj: vlastné spracovanie)

TVOC a ambientný hluk

Na nasledujúcich dvoch grafoch sú zobrazené hodnoty prchavých organických zlúčenín (TVOC) v danej oblasti a úroveň okolitého hluku. Priemerná hodnota TVOC v serverovni dosahuje úroveň 71 µg/m3. Pozorujeme najvýraznejší nárast hodnôt dňa 21. Novembra a to až na úroveň 899 µg/m3 a značné, aj keď menej podstatné zvýšenia v dňoch 23.11., 30.11. A 01.12.. Vzhľadom na ale inak bežne nízke hodnoty v radoch nižších desiatok µg/m3, sú vyššie namerané hodnoty považované skôr za anomálie.

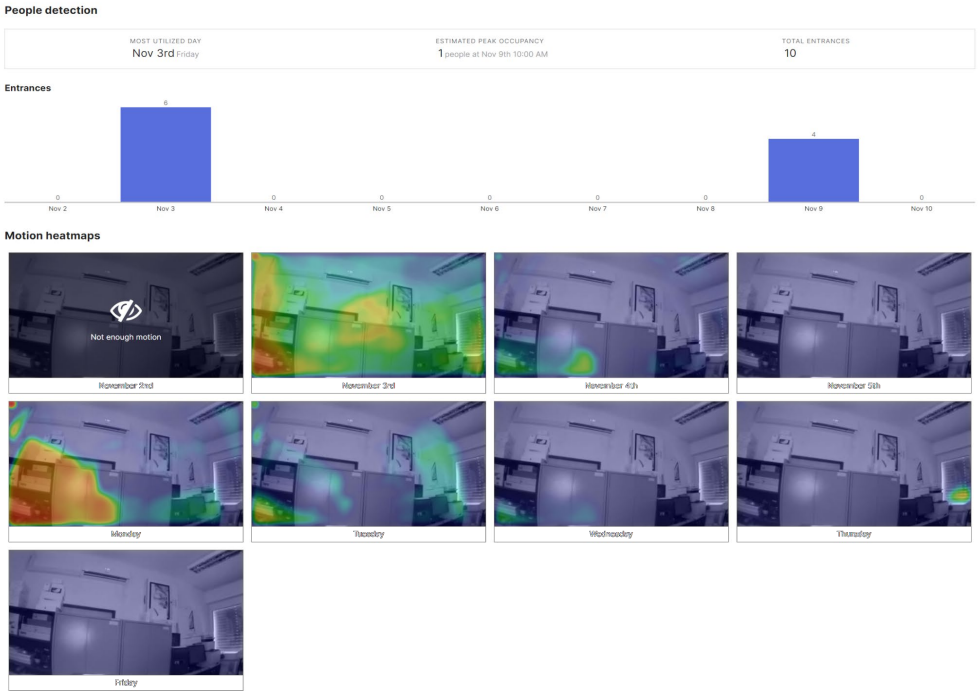
Priemerná úroveň okolitého hluku v miestnosti serverovne počas meraného obdobia dosahovala 65 dBA. Táto vyššia hodnota je daná najmä aktívnym chladením sieťových prvkov. Dňa 6. novembra jasne vidíme pokles hodnôt v dôsledku výpadku senzora. Napriek tomu pozorujeme každý deň v ranných hodinách zvýšenie úrovne hluku v prostredí na úroveň zhruba 70 dBA. Počas niektorých dní dosahuje dokonca hodnôt okolo 75 dBA, čo je na grafe znázornené červenou farbou. Ide skrátka o dni, keď sa v priestoroch zdržiavali zamestnanci.



Obrázok 20: Senzor MT14 – Serverovňa - TVOC a ambientný hluk
(zdroj: vlastné spracovanie)

2.2.2. Kamera č. 2 - Cam02 7A3H

Ako už bolo spomenuté, kamera číslo 2 zachytáva priestory serverovne. V priestoroch bol zachytený najvyšší teplotný výkyv 3. novembra, kedy doň bola kamera inštalovaná. V ostatných dňoch sa udržiavala teplota na nižších hodnotách, až na pár výnimiek, kedy technik opäť navštívil serverovňu. V nadchádzajúcich dňoch a teda od 10. novembra až do ukončenia merania neboli ďalej údaje z kamery sledované, keďže na analýzu s prehľadom stačili údaje získané prostredníctvom senzorov.



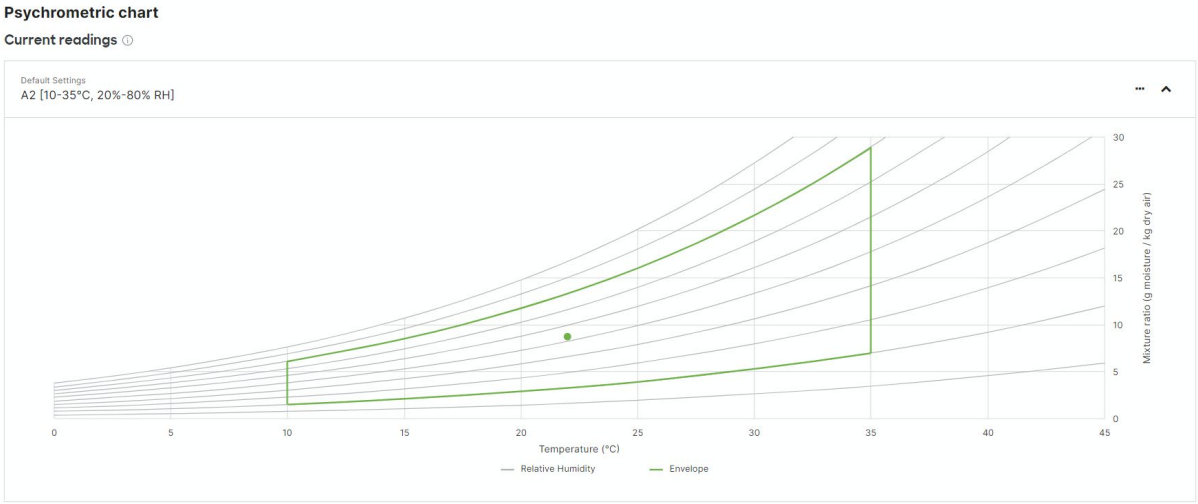
Obrázok 21: Kamera MV2 Cam02 – Serverovňa – Heatmaps
(zdroj: vlastné spracovanie)

2.3. Rozvodňa

V prípade rozvodne a s ním spojeného kancelárskeho priestoru bol zvolený senzor MT10 a kamera MV2 Cam01 DE5A. Keďže ide o miestnosť, kde sa každý pracovný deň vyskytujú zamestnanci, hodnoty sa značne líšia od tých nameraných v predchádzajúcich priestoroch. V priestoroch sa okrem zamestnancov a ich počítačov nachádzajú aj dve klimatizačné jednotky. Tie v tomto prípade vzhľadom na obdobie merania ale slúžia skôr na dodatočné vykurovacie účely, ako nadstavba konvenčného vykurovania pomocou radiátorov. Inštrumentáciou boli merané iba údaje o teplote (°C) a vlhkosti (%RH), čo vyplýva z funkcionality senzoru MT10.

2.3.1. Senzor MT10

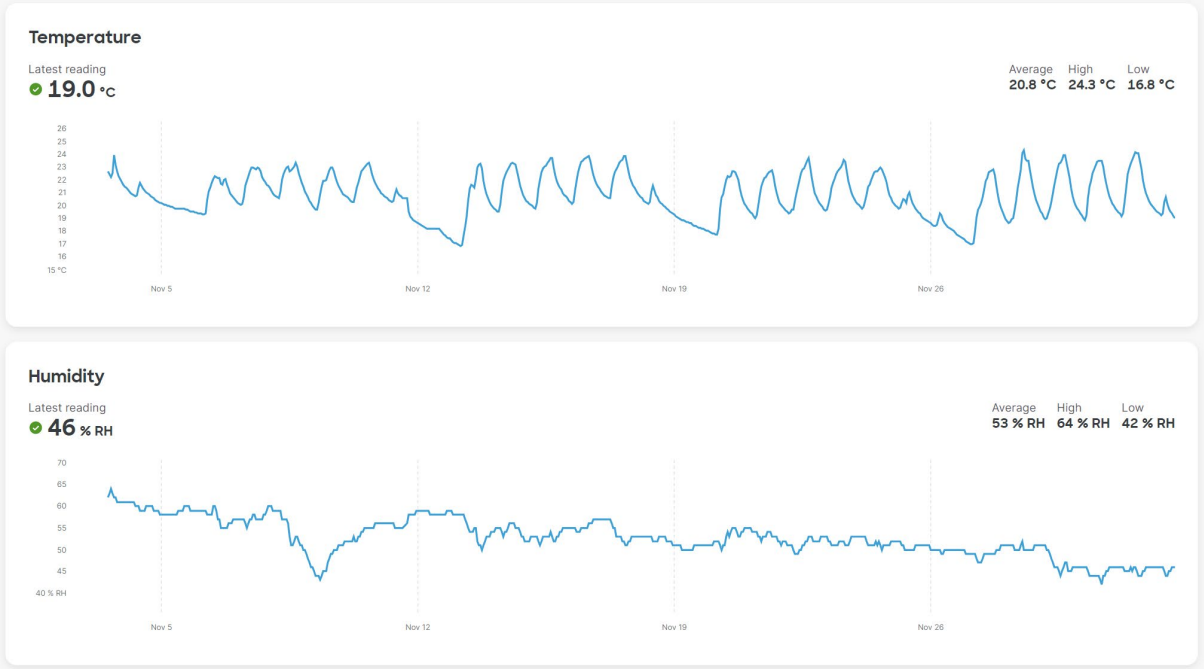
Poloha zelenej bodky na psychrometrickom grafe identifikujúca namerané hodnoty v miestnosti prostredníctvom senzoru MT10 naznačuje zhodu s odporúčanými normami ASHRAE pre udržiavanie teplotných a vlhkostných podmienok v prostredí informačných technológií v rámci rozsahu A2. V tomto prípade je ale navyše zrejmé, že sa teplota nachádzala bližšie k optimálnym hodnotám, čo je pre priestory, kde sa zdržujú zamestnanci každý pracovný deň podstatné.



Obrázok 22: Senzor MT10 – Rozvodňa - Psychrometric chart (zdroj: vlastné spracovanie)

Teplota a vlhkosť vzduchu

Ako už bolo spomenuté, nasledujúce líniové grafy senzoru MT10 znázorňujú namerané hodnoty teploty a vlhkosti v miestnosti rozvodne v období od 2. novembra do 2. decembra, tak ako v prípade serverovne. Počas sledovaného obdobia dosiahla priemerná teplota v prostredí 20,8 stupňov Celzia. Z grafu vyplývajú výrazné fluktuácie teploty, pričom v nočných hodinách mala teplota tendenciu klesať až na 17 stupňov, v poobedňajších a skorých večerných hodinách sa zvyšovala na maximálne hodnoty okolo 23 stupňov Celzia. Priemerná hodnota vlhkosti dosahovala 53 percent, pričom počas sledovaného obdobia pozorujeme postupné poklesy vlhkosti a to najmä ku koncu mesiaca november. Okrem výrazného poklesu hodnoty na 42 % ale k ďalším anomáliám po zvyšok obdobia merania nedošlo.

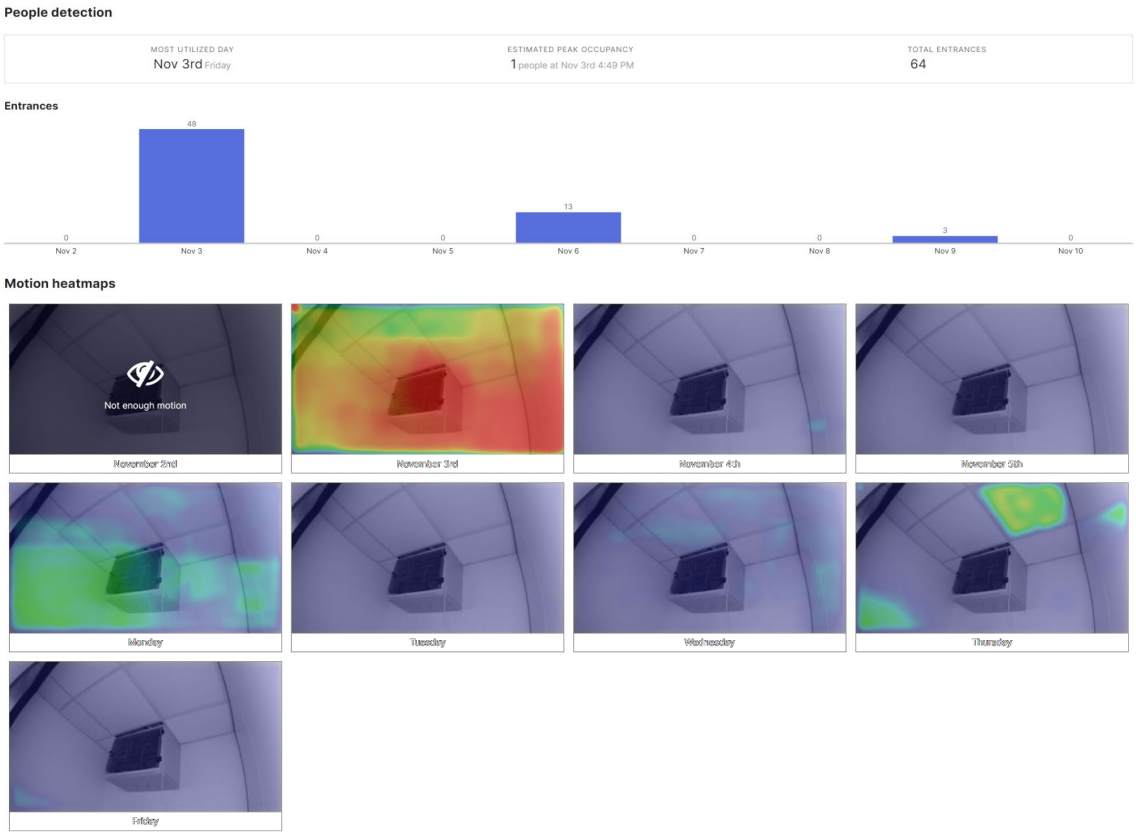


Obrázok 23: Senzor MT10 – Rozvodňa - Teplota a vlhkosť vzduchu (zdroj: vlastné spracovanie)

2.3.2. Kamera č. 1 - Cam01 DE5A

Na základe Heat maps je zrejmé, že dňa 3. novembra, kedy bola kamera nainštalovaná do miestnosti rozvodne, boli zachytené výkyvy vo forme výrazného zvýšenia teploty v okolí kamery samotnej. Tieto zmeny v teplotách sú primárne výsledkom toho, že bola v tom čase kamera inštalovaná technikom, no zároveň nemožno úplne vylúčiť možnosť ovplyvnenia meraní v dôsledku kalibrácie senzoru po jeho počiatočnej inštalácii.

Následne je na snímkach možné pozorovať pokles teploty. Dňa 6. novembra a 9. novembra vidíme mierne zvýšenie teploty, ktoré bolo opäť spôsobené prítomnosťou zamestnancov v danej miestnosti. Tak ako v prípade serverovne, ani v tejto miestnosti už po dni 10.11. nebolo ďalej nutné sledovať údaje prostredníctvom kamery, keďže kľúčové dáta bolo možné v plnej miere získať vďaka nainštalovanému senzoru.



Obrázok 24: Kamera MV2 Cam01 – Rozvodňa – Heatmaps
(zdroj: vlastné spracovanie)

2.4. Kuchynka

Proces monitoringu v prípade tohto priestoru už nezahŕňal parametre získané kamerou, ale spočíval len v použití senzoru MT14. Inštrumentáciou boli teda merané údaje o teplote (°C), vlhkosti (%RH), kvalite ovzdušia (zahŕňajúce teplotu, vlhkosť, TVOC), hluku (dBA) a TVOC - celkového množstva prchavých organických zlúčenín (µg/m3) ako v prípade serverovne. Ako už bolo špecifikované, senzor MT14 disponuje širšou funkcionalitou než ako je to v prípade modelu MT10. Jeho voľba bola v tomto prípade zrealizovaná z toho dôvodu, že frekvencia zdržiavania sa zamestnancov v miestnosti kuchynky je podstatne vyššia ako v prípade kúpeľne na prízemí, a preto sa zber väčšieho množstva atribútov považuje za prínosnejší.

Kvalita vzduchu

Na základe zmeraných údajov vo forme grafu je zrejmé, že kvalita vzduchu sa udržiava v rámci povolených hodnôt. K výrazným poklesom dochádza pravidelne len v čase mimo pracovnej doby, respektíve až vo večerných a nočných hodinách a aj vtedy sa udržiava hodnota kvality okolo hodnoty 80 bodov zo 100. Avšak, počas sledovaného obdobia došlo k trom anomáliám. V dňoch 7., 14. a 21. januára hodnoty klesli až na 70 bodov. Tieto výrazné poklesy možno pripísať výraznému ochladeniu a následne nedostatočnej reakcie centrálneho vykurovacieho systému budovy. Ako je možné vidieť, dňa 28. januára už k rovnakému poklesu nedošlo.

Obrázok 25: Senzor MT14 – Kuchynka - Kvalita, teplota a vlhkosť vzduchu (zdroj: vlastné spracovanie)

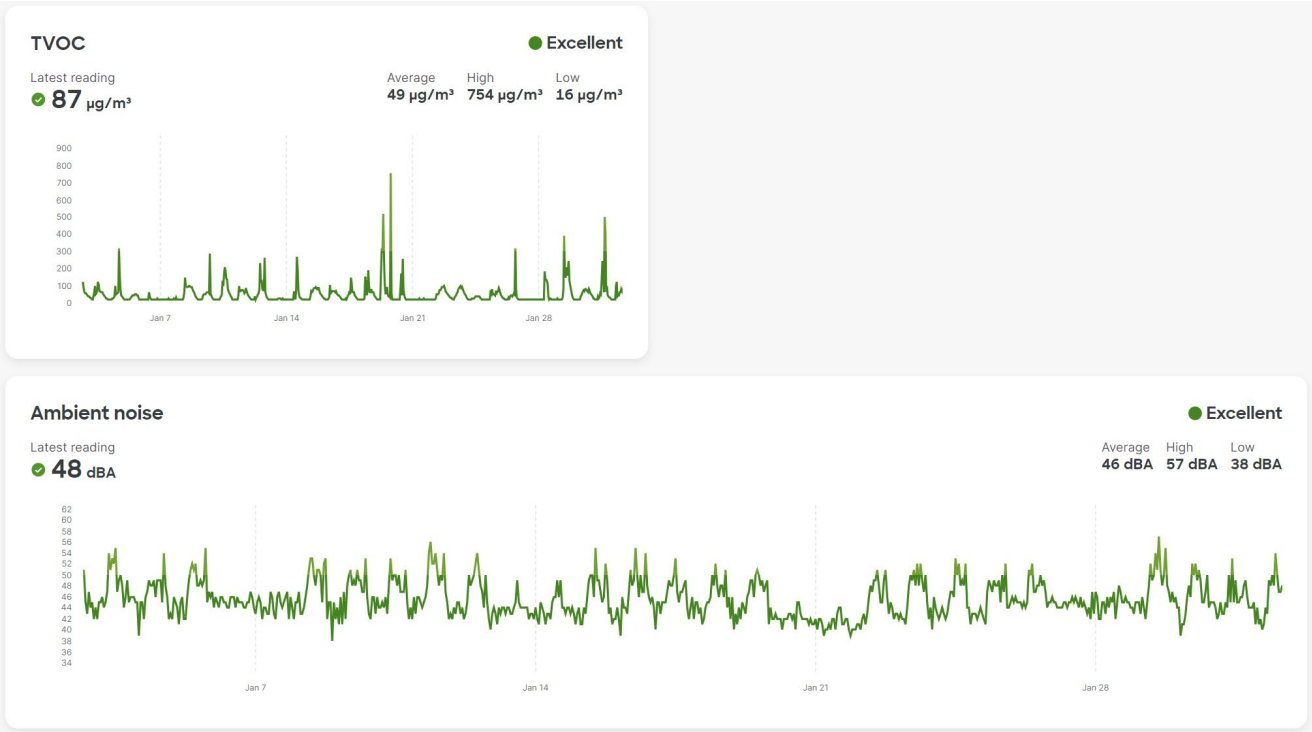
Teplota a vlhkosť

V prípade teploty je možné povedať, že takmer totožne kopíruje trend nameraných hodnôt kvality vzduchu. V dňoch 7., 14. a 21. januára boli zaznamenané jej výrazné poklesy. V priemere pod 16 stupňov Celzia, no dňa 21. januára až takmer len 15 stupňov. Tieto extrémy sa však prestali v nasledujúcich dňoch vyskytovať, ako to bolo aj v prípade celkovej kvality vzduchu. Priemerná teplota sa ale pohybovala v okolí hodnoty 19 stupňov, čo nie je priaznivé.

Pokiaľ ide o vlhkosť, bola výrazne stabilnejším atribútom, no je evidentné, že z dlhodobého hľadiska mala tendenciu skôr klesať a ku koncu obdobia sa držala jej priemerná hodnota na úrovni 51 percent.

TVOC a ambientný hluk

V období monitoringu sa hodnoty prchavých organických zlúčenín TVOC udržiavali na priemernej hodnote 49 µg/m3. Vzhľadom na to, že jednak ide o kuchynské priestory, kde dochádza minimálne k tepelnej úprave rôznych jedál a skladovaniu potravín sú hodnoty viac než priaznivé. Za zmienku určite stoja ale výrazne vyššie namerané hodnoty a to najmä v dňoch 19., 26., 29. a 31. januára, keď sa im podarilo dosiahnuť trojciferných čísiel. Išlo o večerné hodiny, keď sa realizovalo v miestnosti rozsiahle upratovanie. Samozrejme, nešlo o prekročenie povolených, respektíve bezpečných hodnôt.

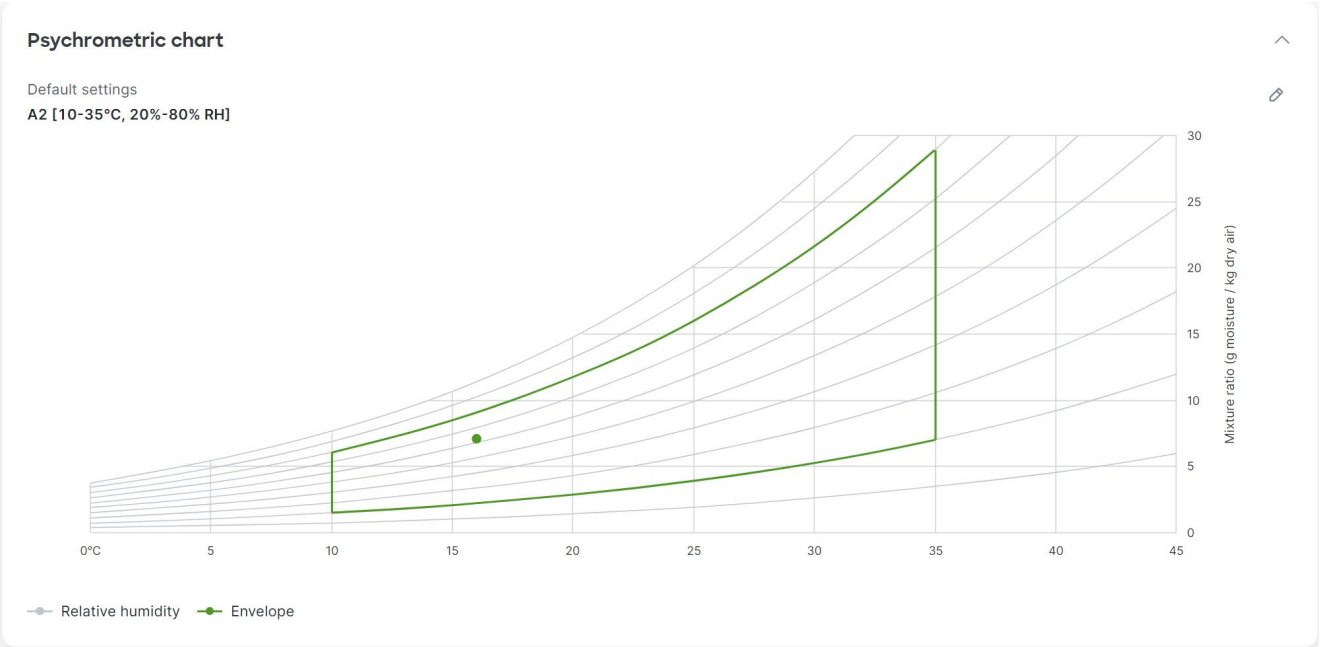


Obrázok 26: Senzor MT14 – Kuchynka – TVOC a ambientný hluk (zdroj: vlastné spracovanie)

Parameter ambientného hluku sa za celý čas merania pohyboval okolo hodnoty 46 dBA. V prípade najviac frekventovaných hodín išlo skôr o hodnoty v rámci 50 až 55 dBA a naopak vo večerných alebo nočných hodinách, prípadne počas víkendov dosahovali skôr hodnoty nižšie ako 40 dBA. V tomto prípade nejde o nič, čo by sa vymykalo norme.

2.5. Kúpeľňa

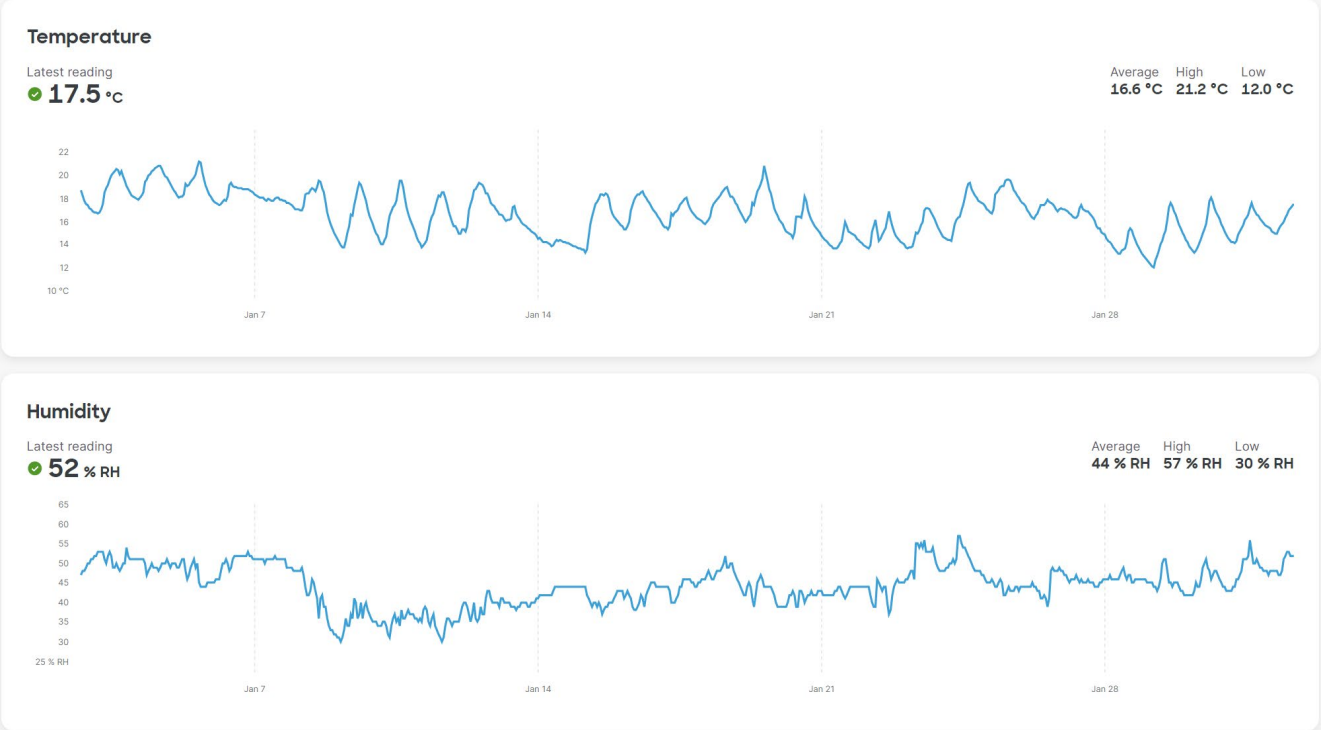
Na základe psychrometrického grafu je ihneď možné identifikovať nevhodné podmienky vyplývajúce najmä z nízkej teploty nameranej v danom priestore. Umiestnenie zelenej bodky v rámci grafu síce stále značí zhodu s odporúčanými normami ASHRAE pre udržiavanie teplotných a vlhkostných podmienok v prostredí informačných technológií v rámci rozsahu A2, no ide skôr o hraničné hodnoty a preto sú pre komfort na pracovisku považované za nevyhovujúce.



Obrázok 27: Senzor MT10 – Kuchynka – Psychrometric chart (zdroj: vlastné spracovanie)

Teplota a vlhkosť

Ako už bolo naznačené predchádzajúcim grafom, priemerné namerané údaje v priestoroch kúpeľne skutočne nie sú optimálne. Pokiaľ ide o teplotu, maximá počas pracovných dní zvyčajne dosahujú približne 18 stupňov Celzia. Je pravda, že sprcha, ktorá je súčasťou kúpeľne nie je v zimných mesiacoch takmer nikdy využívaná, no aj v prípade jej občasného použitia je prostredie nekomfortné. Nad teplotu 20 stupňov sa vzduch dostal len párkrát začiatkom mesiaca január. Vlhkosť sa v priemere dlhodobo udržiava na hodnote 44 %, no na grafe je viditeľné, v ktoré dni bola sprcha používaná na základe opakovaného zvyšovania vlhkosti na úroveň okolo 55 %. Najväčšie extrémy boli namerané v prvej polovici januára, keď vlhkosť poklesla až na 30 %.



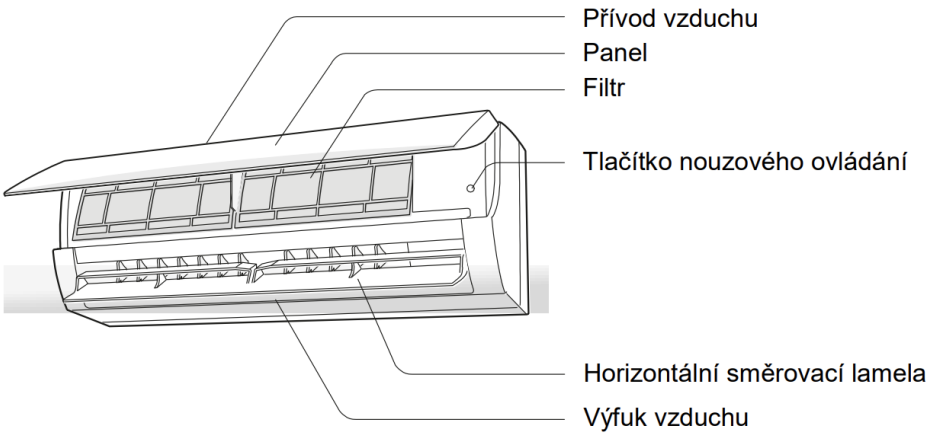
Obrázok 28: Senzor MT10 – Kuchynka – Teplota a vlhkosť
(zdroj: vlastné spracovanie)

2.6. Klimatizačné jednotky

Keďže sa v každom zo spomenutých priestorov nachádza klimatizačná jednotka, je dôležitý aspekt aj ich nastavení. Samozrejme ide o prostriedky, ktoré majú hneď po centrálnom vykurovacom systéme na atribúty vzduchu najväčší vplyv.

Aktuálne sa na tieto účely využívajú jednotky od výrobcu Sinclair, konkrétne model Vision ASH-12BIV Wi-Fi. Ide o typ splitovej nástennej klimatizácie, ktorá ponúka možnosť chladiť a zároveň zohrievať vzduch v interiéri. Klimatizácie tiež podporujú WiFi ovládanie pomocou mobilnej aplikácie a disponujú funkciou "I FEEL", ktorá automaticky nastavuje teplotu podľa senzora na diaľkovom ovládači.

Taktiež je ich súčasťou filter s katechínom a aktívnym uhlím, ktorý znižuje množstvo baktérií, vírusov a nepríjemných pachov vo vzduchu. Okrem toho je tento model vybavený cold plasma generátorom, ktorý produkuje negatívne ióny a zvyšuje kvalitu vzduchu v miestnosti. Klimatizácie majú chladiaci výkon 3,2 kW a kúriaci výkon 3,5 kW, čo je dostatočné pre miestnosti do 40 m2. [6]

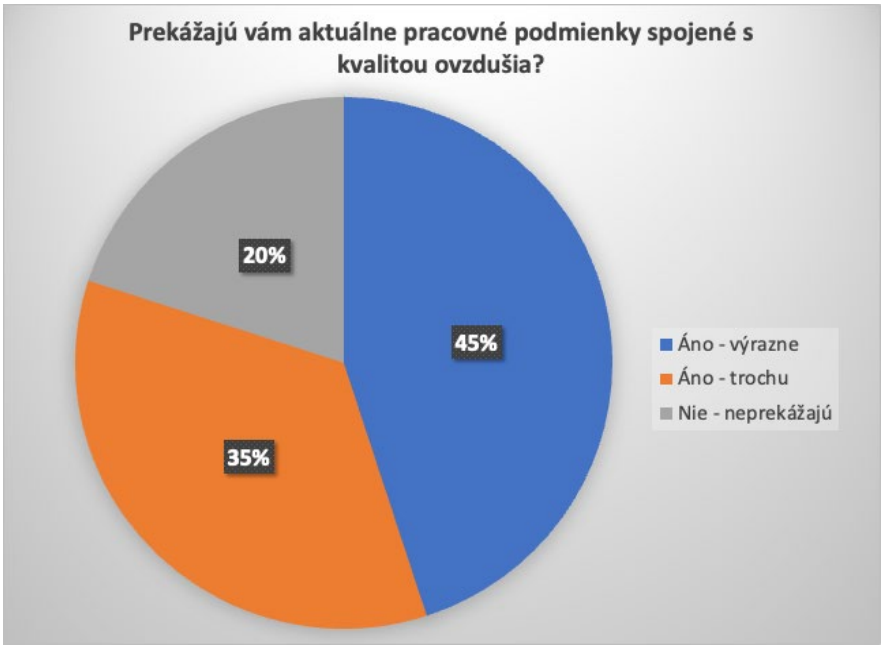


Obrázok 29: Vnútorná jednotka klimatizácie
(zdroj: [7])

2.7. Prieskum vo forme dotazníkov

Vzhľadom na to, že serverovňa predstavuje uzavretý a samostatný priestor, jeho podmienky sa neodrážajú na pracovnom prostredí zamestnancov spoločnosti. Preto táto časť analýzy nekladie dôraz na serverovňu. Naopak, v prípade rozvodne, ktorá predstavuje menší priestor, zdieľaný s rozsiahlym kancelárskym prostredím, kuchynky, kde sa zamestnanci okrem svojho pracovného miesta a zasadačiek zdržiavajú najviac a kúpeľne, bolo rozhodnuté sústrediť sa na prieskum, ktorý by poskytol náhľad do skutočných podmienok pracovného prostredia zamestnancov.

V nadväznosti na toto rozhodnutie bol vykonaný prieskum kvality ovzdušia, ktorý pomohol lepšie pochopiť vplyv pracovného prostredia na zdravie a komfort zamestnancov. Prieskum bol zrealizovaný vo forme dotazníkov mierených priamo na zamestnancov zdržiavajúcich sa vo vybraných priestoroch. Koláčový graf nižšie znázorňuje výsledky dotazníku o tom, či zamestnancom všeobecne prekážajú aktuálne pracovné podmienky po stránke teploty a kvality vzduchu ako takej.



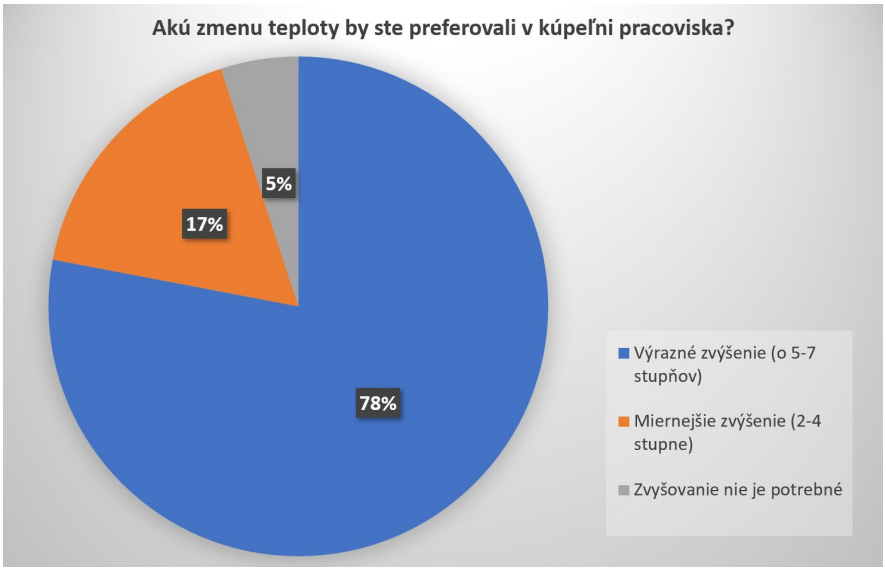
Obrázok 30: Výsledky prieskumu o kvalite ovzdušia (zdroj: vlastné spracovanie)

Na základe výsledkov je možné povedať, že väčšine zamestnancov aspoň do istej miery aktuálne podmienky prekážajú. A to ako v priestoroch kancelárií, ktorých súčasťou je rozvodňa, tak aj kuchynky a kúpeľne.

Ďalší graf zas znázorňuje odpovede zamestnancov konkrétne na atribút zmeny teploty v priestoroch. Ako už bolo spomenuté, počas sledovaného obdobia sa v priestoroch rozvodne pohybovala priemerná úroveň teploty okolo 20,5 stupňa Celzia. V prípade kuchynky išlo zas o 22 stupňov a v miestnosti kúpeľňa sa priemer udržiava len na cca 16,5 stupňoch. Zamestnanci mali priestor vyjadriť sa k teplotným podmienkam v prípade kancelárií spojených s rozvodňou a kúpeľne.

Obrázok 31: Výsledky prieskumu o teplote – rozvodňa / kancelária (zdroj: vlastné spracovanie)

Výsledky dotazníka jasne naznačujú, že prevažná väčšina zamestnancov preferuje zvýšenie teploty v priestoroch kancelárie.



Obrázok 32: Výsledky prieskumu o teplote - kúpeľňa (zdroj: vlastné spracovanie)

Ako bolo aj očakávané, zamestnanci by v prípade priestorov kúpeľne takmer jednohlasne uvítali zvýšenie teploty a väčšina dokonca jej výrazné zvýšenie.

Obrázok 33: Výsledky prieskumu o teplote - kuchynka
(zdroj: vlastné spracovanie)

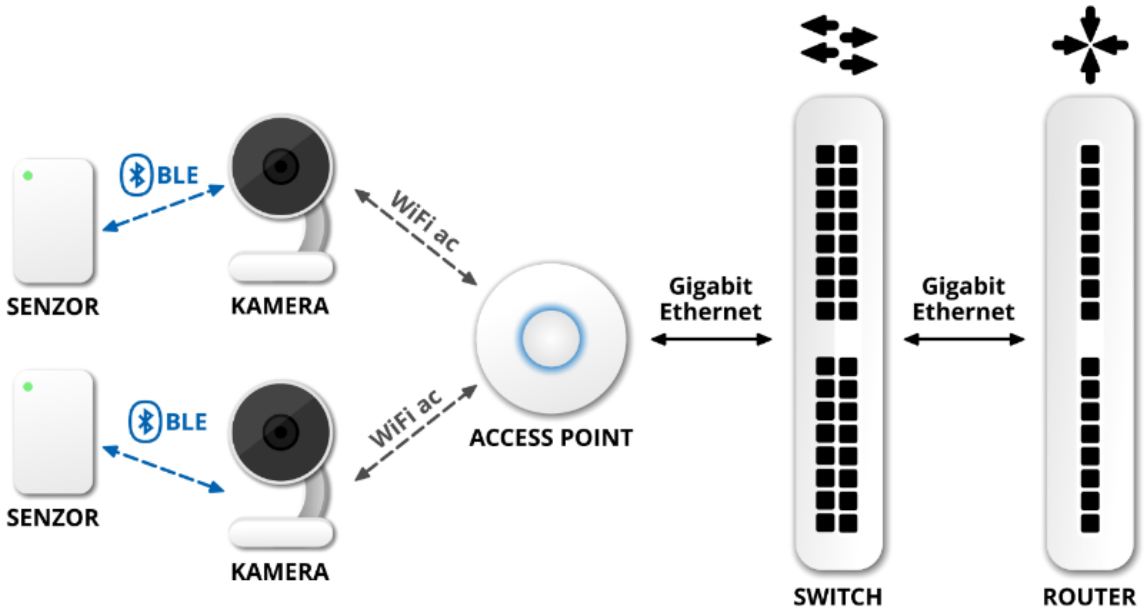
V neposlednom rade bola položená zamestnancom otázka ohľadom priestorov kuchynky. V tomto prípade sa ukázalo, že drvivá väčšina z opýtaných je s aktuálnym stavom spokojná.

Zároveň bol braný do úvahy platný zákon (nařízení vlády č. 361/2007 Sb.), ktorý stanovuje maximálnu povolenú teplotu v priestore vyhradenom pre kancelársku, či administratívnu prácu na 26 °C a minimálnu teplotu na 20 °C. Táto úprava by reflektovala nielen preferencie zamestnancov, ale aj právne normy, prispievajúce k celkovému pohodliu a produktivite pracovníkov.

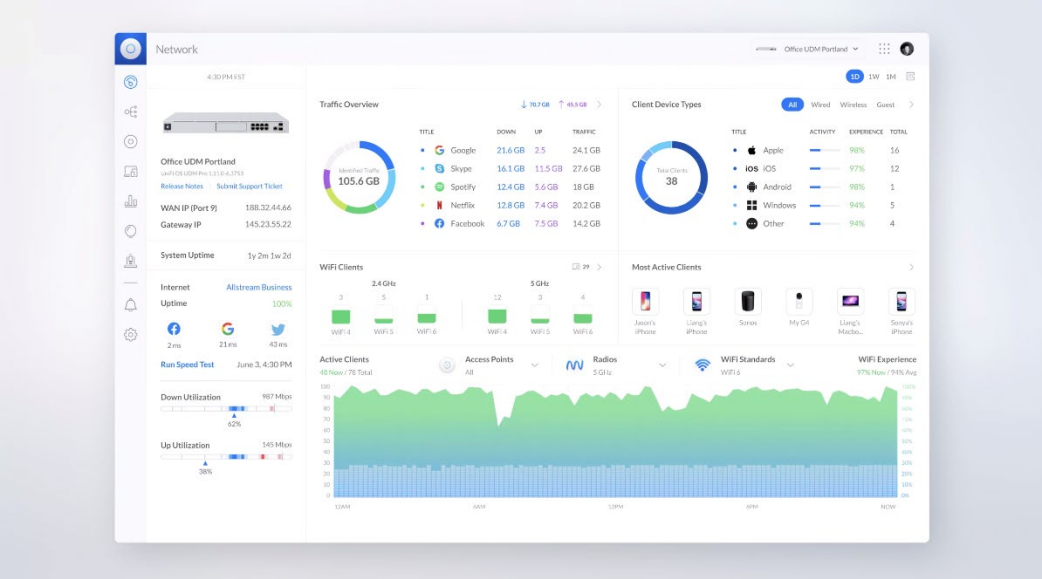
2.8. Sieťová konfigurácia

Aktuálne sú zariadenia pripojené priamo na firemnú sieť prostredníctvom štandardu Wi-Fi 2,4/5GHz. V spoločnosti sa využíva WLAN s SSID AdS, do ktorej sa počas prihlasovania užívateľ autentizuje pomocou WPA2-PSK a AdStaff, kde je zas využívané WPA2-Enterprise, čo má za následok, že každý užívateľ má vlastný alias a heslo, ktoré na pripojenie používajú. Taktiež sa pri overovaní využíva bezpečnostný certifikát. V neposlednom rade sa na oddelenom VLAN nachádza AdNet, ktorý slúži na pripájanie nefiremných zariadení, akými sú napríklad TV, mobily zamestnancov atď. IoT zariadenia sú aktuálne pripojené na SSID AdNet, pri ktorom je na autentifikáciu opäť využitý protokol WPA2-PSK.

Ako už bolo spomenuté, komunikačný systém Meraki je postavený na princípe takzvaných brán alebo gateways. Brány, ktoré v tomto prípade predstavujú IP kamery, sa prostredníctvom Wi-Fi 5 priamo pripájajú na access pointy v spoločnosti, ktoré ich tým pádom pripoja na router, a senzory následne nadväzujú spojenie prostredníctvom technológie Bluetooth Low Energy (BLE) s kamerami. Toto má za následok, že dané IoT zariadenia môžu trpieť na bežné zraniteľnosti IoT, keďže ide o značne otvorenú bezdrôtovú komunikáciu.



Obrázok 34: Aktuálne sieťové zapojenie IoT - zjednodušené (zdroj: vlastné spracovanie)



Obrázok 35: UniFi Controller v7
(zdroj: [8])

2.9. Kvalita a riziká

Celkovo je kvalita systému Cisco Meraki a IoT zariadení na vysokej úrovni. Za zmienku ale určite stojí opakované vypadávanie, respektíve odpájanie senzorov od gateways. Keďže senzory ako gateway využívajú kamery a ich výber je úplne náhodný, čo bolo overené priamo Meraki technikmi, ich pripojenie nie je vždy 100%. Konkrétne sa oba senzory pokúšali o pripájanie na jednu kameru, čo zapríčinilo, že v prípade senzoru nachádzajúceho sa na inom poschodí ako spomenutá kamera dochádzalo k výpadkom v dôsledku slabého signálu. Pri hodnote pod -85dB sa senzor odpojí a nesnaží sa pripojiť na kameru, ktorá sa fyzicky nachádza prakticky hneď vedľa neho. Toto zapríčinilo výkyvy nameraných hodnôt v prípade MT 14.

2.9.1. Uloženie dát

Za zmienku taktiež stojí fakt, že namerané údaje sú priamo ukladané do cloud-u spoločnosti Cisco, čo prináša riziká odhalenia, ukradnutia a ich potencionálnej zmeny. Spoločnosť Cisco taktiež získava údaje z nástrojov na zber údajov a riešení priamo od zákazníkov, čo zahŕňa telemetrické údaje, údaje potrebné pre poskytnutie podpory, údaje o hrozbách, informácie o softvérových licenciách a inštaláciách aplikácií.

Spoločnosť Cisco ale zohľadňuje princípy dôveryhodnosti, transparentnosti a zodpovednosti. Údaje sú zbierané bezpečným pripojením a chránené počas celého životného cyklu údajov pomocou Cisco Secure Development Lifecycle. Transparentnosť je zachovaná využívaním údajov len na stanovené účely a ich zdieľanie s dôveryhodnými partnermi. Zodpovednosť sa prejavuje v dodržiavaní najvyšších štandardov bezpečnosti a ochrany osobných údajov, súladu so zákonnými predpismi a zmluvami so zákazníkmi, ktorým sú služby poskytované.

2.9.2. Zraniteľnosti infraštruktúry

Pokiaľ ide o riziká spojené so zraniteľnosťou systémov (CVE), v prípade zariadení Cisco Meraki vo všeobecnosti boli v závislosti od série zariadenia zistené rôzne potencionálne hrozby. Keďže sa ale žiadna z týchto zraniteľností netýka modelov MT ani MV, bolo zhodnotené, že na základe mnohých bezpečnostných certifikácií, ktorými sa spoločnosť Cisco preukazuje sú spoločnosťou využívané zariadenia IoT dokonale zabezpečené.

Na druhej strane, pokiaľ ide o zariadenia MikroTik, v ich prípade je známych výrazne vyššie množstvo CVE. Keďže všetky zariadenia MikroTik v spoločnosti Stellnaris na svoju prevádzku využívajú operačný systém RouterOS, budú v tejto časti uvedené a opísané niektoré konkrétne zraniteľnosti. Aktuálne je na všetkých sieťových prvkoch nainštalovaný systém RouterOS 6.47.

Zoznamy zraniteľností (CVE) v prípade systému RouterOS a zvyšných Cisco Meraki produktov sú uvedené v tabuľkách nižšie.

Tabuľka 1: Zoznam zraniteľností Cisco Meraki
(zdroj: [9])

Názov	Popis hrozby
CVE-2023-20029	A vulnerability in the Meraki onboarding feature of Cisco IOS XE Software could allow an authenticated, local attacker to gain root level privileges on an affected device. This vulnerability is due to insufficient memory protection in the Meraki onboarding feature of an affected device. An attacker could exploit this vulnerability by modifying the Meraki registration parameters. A successful exploit could allow the attacker to elevate privileges to root.
CVE-2022-20933	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z3 Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit this vulnerability by crafting a malicious request and sending it to the affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to crash and restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and re-authenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention. Cisco Meraki has released software updates that address this vulnerability.
CVE-2018-0284	A vulnerability in the local status page functionality of the Cisco Meraki MR, MS, MX, Z1, and Z3 product lines could allow an authenticated, remote attacker to modify device configuration files. The vulnerability occurs when handling requests to the local status page. An exploit could allow the attacker to establish an interactive session to the device with elevated privileges. The attacker could then use the elevated privileges to further compromise the device or obtain additional configuration data from the device that is being exploited.
CVE-2014-7999	Cisco-Meraki MS, MR, and MX devices with firmware before 2014-09-24 allow remote authenticated users to install arbitrary firmware by leveraging unspecified HTTP handler access on the local network, aka Cisco-Meraki defect ID 00478565.
CVE-2014-7995	Cisco-Meraki MS, MR, and MX devices with firmware before 2014-09-24 allow physically proximate attackers to obtain shell access by opening a device's case and connecting a cable to a serial port, aka Cisco-Meraki defect ID 00302077.
CVE-2014-7994	Cisco-Meraki MS, MR, and MX devices with firmware before 2014-09-24 allow remote attackers to execute arbitrary commands by leveraging knowledge of a cross-device secret and a per-device secret, and sending a request to an unspecified HTTP handler on the local network, aka Cisco-Meraki defect ID 00301991.
CVE-2014-7993	Cisco-Meraki MS, MR, and MX devices with firmware before 2014-09-24 allow remote attackers to obtain sensitive credential information by leveraging unspecified HTTP handler access on the local network, aka Cisco-Meraki defect ID 00302012.

Tabuľka 2: Zoznam zraniteľností MikroTik RouterOS od verzie 6.47 (zdroj: [10])

Názov	Popis hrozby
CVE-2023-41570	MikroTik RouterOS v7.1 to 7.11 was discovered to contain incorrect access control mechanisms in place for the Rest API.
CVE-2023-30800	The web server used by MikroTik RouterOS version 6 is affected by a heap memory corruption issue. A remote and unauthenticated attacker can corrupt the server's heap memory by sending a crafted HTTP request. As a result, the web interface crashes and is immediately restarted. The issue was fixed in RouterOS 6.49.10 stable. RouterOS version 7 is not affected.
CVE-2023-30799	MikroTik RouterOS stable before 6.49.7 and long-term through 6.48.6 are vulnerable to a privilege escalation issue. A remote and authenticated attacker can escalate privileges from admin to super-admin on the Winbox or HTTP interface. The attacker can abuse this vulnerability to execute arbitrary code on the system.
CVE-2023-24094	An issue in the bridge2 component of MikroTik RouterOS v6.40.5 allows attackers to cause a Denial of Service (DoS) via crafted packets.
CVE-2022-45315	Mikrotik RouterOs before stable v7.6 was discovered to contain an out-of-bounds read in the snmp process. This vulnerability allows attackers to execute arbitrary code via a crafted packet.
CVE-2022-45313	Mikrotik RouterOs before stable v7.5 was discovered to contain an out-of-bounds read in the hotspot process. This vulnerability allows attackers to execute arbitrary code via a crafted nova message.
CVE-2022-36522	Mikrotik RouterOs through stable v6.48.3 was discovered to contain an assertion failure in the component /advanced-tools/nova/bin/netwatch. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.
CVE-2022-34960	The container package in MikroTik RouterOS 7.4beta4 allows an attacker to create mount points pointing to symbolic links, which resolve to locations on the host device. This allows the attacker to mount any arbitrary file to any location on the host.
CVE-2021-41987	In the SCEP Server of RouterOS in certain Mikrotik products, an attacker can trigger a heap-based buffer overflow that leads to remote code execution. The attacker must know the scep_server_name value. This affects RouterOS 6.46.8, 6.47.9, and 6.47.10.
CVE-2021-36614	Mikrotik RouterOs before stable 6.48.2 suffers from a memory corruption vulnerability in the tr069-client process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).
CVE-2021-36613	Mikrotik RouterOs before stable 6.48.2 suffers from a memory corruption vulnerability in the ptp process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).
CVE-2021-3014	In MikroTik RouterOS through 2021-01-04, the hotspot login page is vulnerable to reflected XSS via the target parameter.
CVE-2020-22845	A buffer overflow in Mikrotik RouterOS 6.47 allows unauthenticated attackers to cause a denial of service (DOS) via crafted FTP requests.
CVE-2020-22844	A buffer overflow in Mikrotik RouterOS 6.47 allows unauthenticated attackers to cause a denial of service (DOS) via crafted SMB requests.

CVE-2020-20267	Mikrotik RouterOs before 6.47 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/resolver process. An authenticated remote attacker can cause a Denial of Service due to invalid memory access.
CVE-2020-20266	Mikrotik RouterOs before 6.47 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/dot1x process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).
CVE-2020-20265	Mikrotik RouterOs before 6.47 (stable tree) suffers from a memory corruption vulnerability in the /ram/pckg/wireless/nova/bin/wireless process. An authenticated remote attacker can cause a Denial of Service due via a crafted packet.
CVE-2020-20264	Mikrotik RouterOs before 6.47 (stable tree) in the /ram/pckg/advanced-tools/nova/bin/netwatch process. An authenticated remote attacker can cause a Denial of Service due to a divide by zero error.
CVE-2020-20262	Mikrotik RouterOs before 6.47 (stable tree) suffers from an assertion failure vulnerability in the /ram/pckg/security/nova/bin/ipsec process. An authenticated remote attacker can cause a Denial of Service due to an assertion failure via a crafted packet.
CVE-2020-20254	Mikrotik RouterOs before 6.47 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/lcdstat process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).
CVE-2020-20253	Mikrotik RouterOs before 6.47 (stable tree) suffers from a divison by zero vulnerability in the /nova/bin/lcdstat process. An authenticated remote attacker can cause a Denial of Service due to a divide by zero error.
CVE-2020-20252	Mikrotik RouterOs before stable version 6.47 suffers from a memory corruption vulnerability in the /nova/bin/lcdstat process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).
CVE-2020-20250	Mikrotik RouterOs before stable version 6.47 suffers from a memory corruption vulnerability in the /nova/bin/lcdstat process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference). NOTE: this is different from CVE-2020-20253 and CVE-2020-20254. All four vulnerabilities in the /nova/bin/lcdstat process are discussed in the CVE-2020-20250 github.com/cq674350529 reference.
CVE-2020-20249	Mikrotik RouterOs before stable 6.47 suffers from a memory corruption vulnerability in the resolver process. By sending a crafted packet, an authenticated remote attacker can cause a Denial of Service.
CVE-2020-20248	Mikrotik RouterOs before stable 6.47 suffers from an uncontrolled resource consumption in the memtest process. An authenticated remote attacker can cause a Denial of Service due to overloading the systems CPU.

Keďže ale na základe zdroja ide o zraniteľnosti, ktoré je možné vyriešiť aktualizáciou systému na najnovšiu verziu, nemala by byť ich eliminácia príliš zložitá,

3. Návrhy riešení

Táto kapitola sa zaoberá návrhom riešení v nadväznosti na problémy, prípadne riziká zistené vďaka získaným dátam počas doby analýzy súčasného stavu. Jednak ide o surové dáta namerané prostredníctvom zariadení IoT, ktoré boli následne spracované pomocou systému Meraki, vlastnou analýzou rizík, údajmi získanými priamo od zamestnancov prostredníctvom dotazníkov a vlastnými úsudkami, ktoré sú založené na skúsenostiach so správou sieťových zariadení a vedomostí z oblasti kyberbezpečnosti, pokiaľ ide o nastavenie zabezpečenia IoT.

3.1. Návrhy po stránke kvality vzduchu

Keďže je komfort zamestnancov pochopiteľne jedným z najdôležitejších aspektov ovplyvňujúcich ich produktivitu, táto práca sa, ako už bolo mnohokrát naznačené priamo zaoberá jeho zvýšením, čo je vďaka IoT skutočne jednoduchšie realizovateľné.

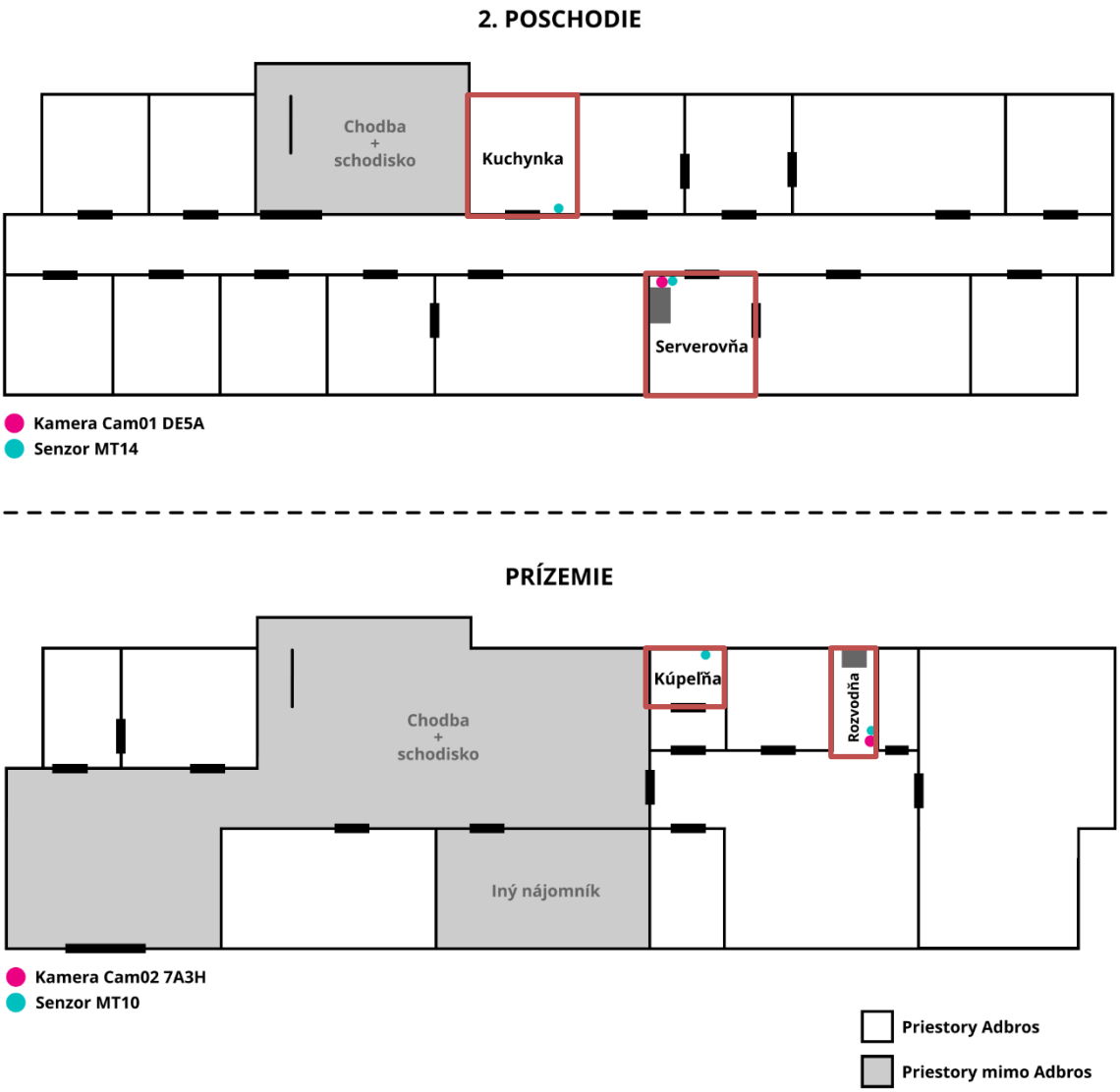
Aktuálne je preto navrhované mierne zníženie teploty v serverovej miestnosti, kde sa nachádzajú mnohé aktívne prvky a NAS s tým, že na klimatizačnej jednotke by bol zvolený režim vysušovania vzduchu, aby bola optimalizovaná taktiež miera vlhkosti v danej miestnosti.

V prípade rozvodne, kde ide primárne o komfort zamestnancov, keďže sa v nej síce nachádzajú sieťové prvky, ale primárne nie aktívne a aj tie sú chladené pasívne, je zas navrhnuté mierne zvýšenie teploty. Tento návrh je považovaný za relevantný aj napriek tomu, že sa síce podľa odporúčaní aktuálna teplota nachádza v povolenom rozsahu, no na základe dotazníkov je zvýšenie teploty jednoznačne vyžadované zamestnancami.

V neposlednom rade, pokiaľ ide o zmeny teploty, v prípade kúpeľne je odporučené jej výrazné zvýšenie, čo ako už bolo spomenuté, bude mať preukázateľne pozitívny dopad na komfort zamestnancov.

Tieto návrhy môžu byť realizované ako zmenou vykurovacieho režimu po strane centrálneho kúrenia prostredníctvom radiátorov, tak aj zmenou nastavení klimatizačných jednotiek v chladných obdobiach.

Keďže majú zamestnanci plnú kontrolu nad ovplyvnením teploty a vlhkosti vzduchu prostredníctvom klimatizačných jednotiek, návrh je postavený na základe ich konfigurácie.



Obrázok 36: Plán budovy - druhé poschodie a prízemie
(zdroj: vlastné spracovanie)

3.1.1. Serverovňa

V tejto miestnosti je odporúčané znížiť teplotu na najnižšiu možnú hodnotu, čo je v prípade klimatizačných jednotiek 16 stupňov a zvoliť režim vysušovania vzduchu s tým, že budú následne monitorované teploty HW a rýchlosť otáčok ventilátorov aktívnych prvkov.

3.1.2. Rozvodňa

Pokiaľ ide o túto miestnosť, na základe nameraných údajov a spätnej väzby od zamestnancov sa odporúča mierne navýšenie teploty v základnom chladiacom režime bez vysušovania vzduchu, aby bol zachovaný čo najvyšší možný komfort zamestnancov v chladných obdobiach. V prípade letných období už regulácia teploty v interiéri pripadá na momentálne preferencie zamestnancov a táto práca sa zameriava len na zvyšok roku, keď je potrebné priestory vykurovať, ako už bolo spomenuté.

3.1.3. Kuchynka

Ako už bolo naznačené, v prípade tejto miestnosti je doporučené najmä zvýšenie teploty, aby bola zaručená jej stabilizácia počas pracovných dní. Pokiaľ ide o vlhkosť, nie je nutné meniť žiadne ďalšie nastavenia, keďže aj počas analýzy boli namerané optimálne hodnoty a v týchto priestoroch sa samozrejme nenachádzajú žiadne zariadenia kritickej infraštruktúry.

3.1.4. Kúpeľňa

V prípade tejto miestnosti je jednoznačne najdôležitejšie zvýšenie teploty a to výrazné. Okrem toho by bolo vhodné prepnúť klimatizáciu na režim vysušovania, keďže pri dlhodobejšom používaní zariadení v týchto priestoroch má vlhkosť tendenciu značne stúpať a zamestnanci v nich nikdy dlhodobo nezdržiavajú, takže niekedy potencionálne suchší vzduch nebude mať na nich negatívny vplyv.

3.2. Návrhy po stránke zabezpečenia IoT

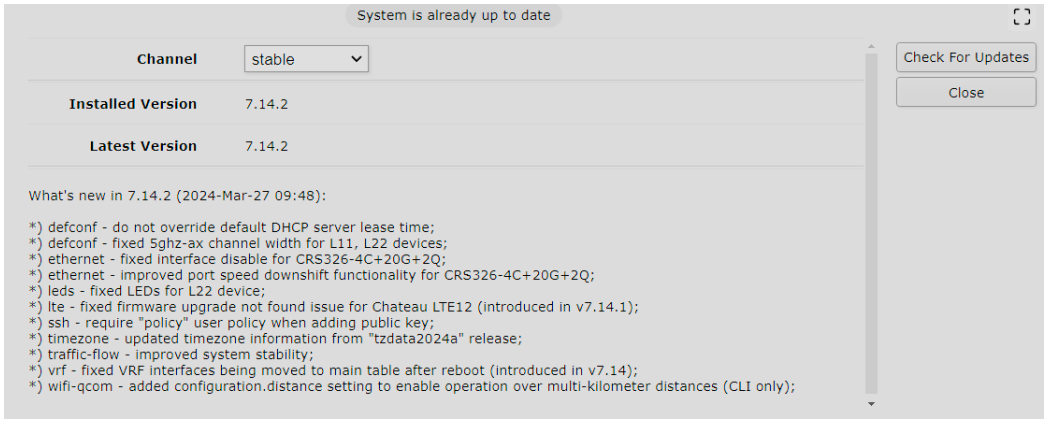
Táto kapitola je zameraná na návrhy zabezpečenia samotnej infraštruktúry a zariadení IoT. Jej predmetom bude opis rôznych metód alebo nástrojov, ktoré by viedli k zníženiu rizík spojených s prevádzkou zariadení tohto charakteru vzhľadom k ich relatívne otvorenej komunikácii. Keďže sa mi nepodarilo nájsť žiadne aktuálne bezpečnostné zraniteľnosti (CVE) v prípade zariadení Cisco Meraki MV/MT a Cisco sa odkazuje na spĺňanie širokého množstva bezpečnostných štandardov, ktorými môže dokázať ich zabezpečenie, táto kapitola bude riešiť zabezpečenie infraštruktúry z hľadiska sieťových prvkov MikroTik, access pointov Ubiquiti UniFi a technológií, ktoré využívajú na vzájomnú komunikáciu a samotnú konfiguráciu týchto sieťových prvkov.

Medzi rozsiahle množstvo štandardov, ktoré Cisco spĺňa a zaraďuje ich pod takzvaný Cisco Cloud Controls Framework (CCF) patrí napríklad: SOC 2, ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC 27701:2019, ISO/IEC 22301:2019, ENS, IRAP December 2021, PCI-DSS v3.2.1, ISMAP, C5, CoC, CCC, FedRAMP LI-SAAS/Tailored, NIST 800-171, EUCS a SecNumCloud. [11]

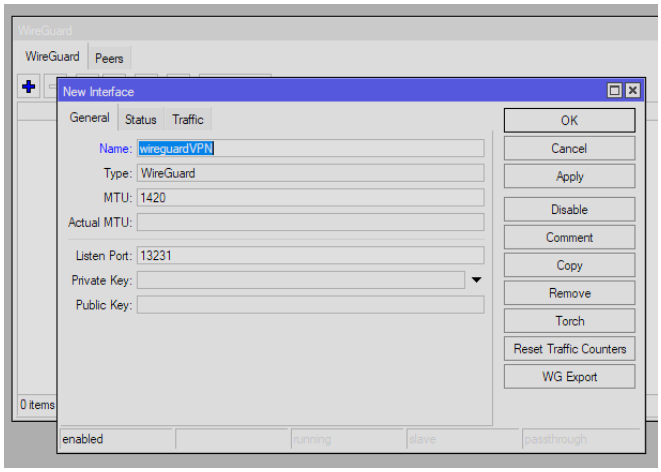
3.2.1. Aktualizácia aktuálnej infraštruktúry

Dôležitým aspektom zabezpečenia sieťovej infraštruktúry je jednoznačne udržiavanie všetkých jej prvkov na aktuálnych verziách firmvéru. Tento krok by mal byť zrealizovaný ako prvý, keďže nie je v jeho prípade potrebný nákup žiadneho nového HW, ani zložitá konfigurácia rôznych bezpečnostných funkcií.

V prípade MikroTik routerov a switchov by bola zrealizovaná aktualizácia ich FW z aktuálnej na verziu 7.14.2. Pred realizáciou aktualizácie by bola prevedená záloha konfigurácie zariadení. Po realizácii bude router disponovať možnosťou implementácie VPN prostredníctvom protokolu WireGuard, ktorý by priniesol so sebou ďalšie bezpečnostné benefity v porovnaní s aktuálne používaným L2TP.



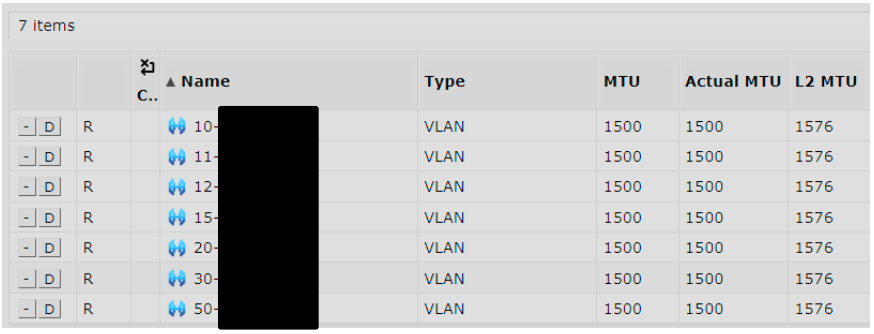
Obrázok 37: Aktualizácia MikroTik
(zdroj: vlastné spracovanie)



Obrázok 38: WireGuard v rámci RouterOS
(zdroj: vlastné spracovanie)

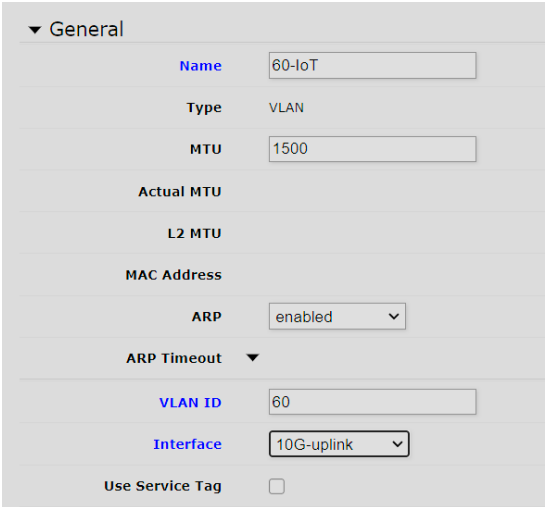
3.2.2. Vytvorenie dedikovanej VLAN pre IoT zariadenia

Jedným z návrhov možností zabezpečenia je tvorba dedikovanej virtuálnej lokálnej siete len pre IoT zariadenia. Navrhuje sa založenie siete AdIoT s overovaním WPA3, do ktorej sa okrem daných zariadení nebude môcť pripojiť žiadne iné. Toto bude zohľadnené a formalizované aj v bezpečnostných politikách spoločnosti. Tento VLAN bude zabezpečený navyše dedikovaným firewallom.



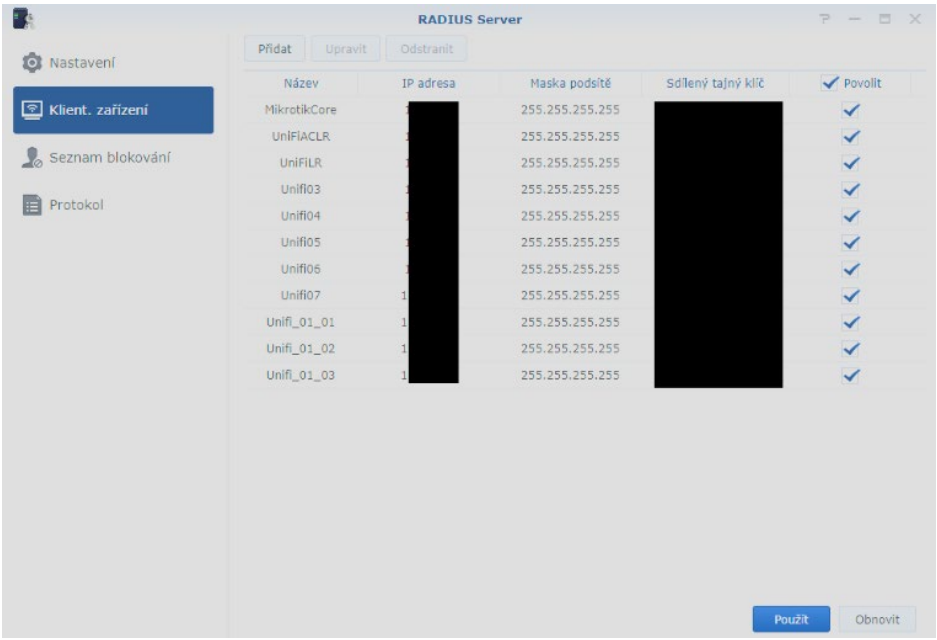
Obrázok 39: Aktuálne nastavenie VLAN
(zdroj: vlastné spracovanie)

Konkrétne by počiatočne bola vytvorená virtuálna sieť s názvom 60-IoT, aby zapadla do aktuálne zaužívaného pomenovacieho systému. Bola by naviazaná priamo na interface 10G-uplink, ktorý slúži ako primárne pripojenie infraštruktúry pomocou VLAN.



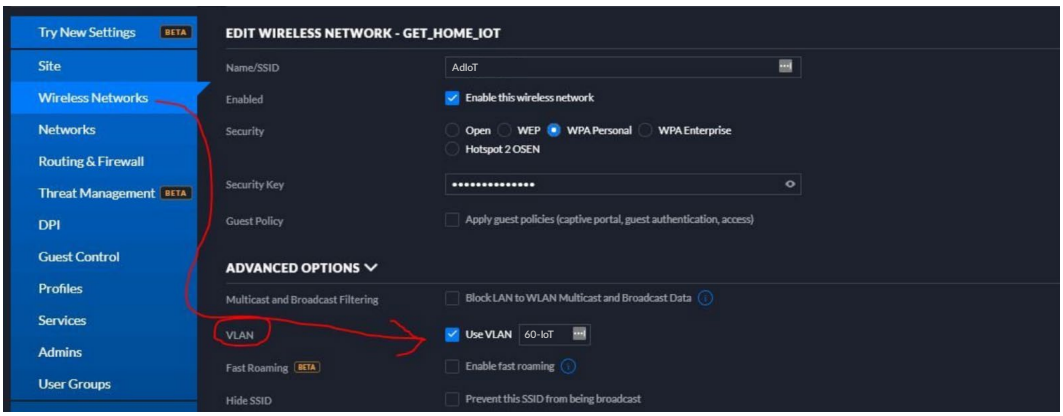
Obrázok 40: Konfigurácia nového VLAN
(zdroj: vlastné spracovanie)

V ďalšom kroku by následne v rámci UniFi controlleru AP bolo vytvorené nové SSID s názvom AdIoT a to naviazané na VLAN 60-IoT. Zabezpečovacie heslo by bolo zdieľané len naprieč administrátormi.



Obrázok 41: Aktuálne nastavenie Radius serveru
(zdroj: vlastné spracovanie)

Nasledujúci screenshot znázorňuje, ako by vytvorenie AdIoT bolo zrealizované pomocou aktuálnych AP, ktoré WiFi 6 a teda ani zabezpečenie WPA3 nepodporujú.



Obrázok 42: Nastavenie bezdrôtovej siete v rámci UniFi controller-u
(zdroj: vlastné spracovanie)

Tabuľka 2: Zoznam SSID po zmene
(zdroj: vlastné spracovanie)

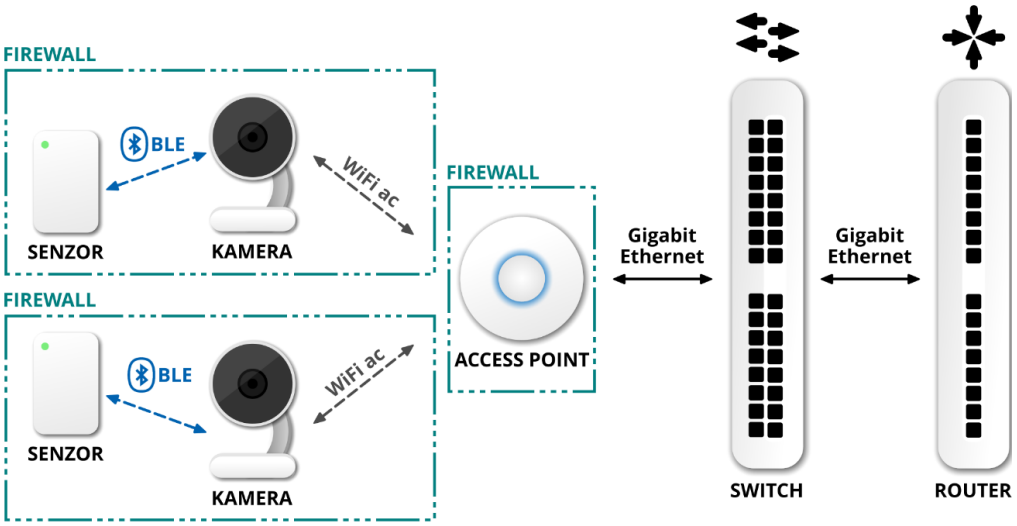
SSID	VLAN	MTU	Security	Interface
AdS	20-STAFF	1500	WPA2 Personal	10G-Uplink
AdStaff	20-STAFF	1500	WPA2 Enterprise	10G-Uplink
AdNet	30-AdNet	1500	WPA2 Personal	10G-Uplink
AdHost	50-HOST	1500	WPA2 Personal	10G-Uplink
AdIoT	*60-IoT*	*1500*	*WPA3 Personal**	*10G-Uplink*

**V prípade, že by boli zakúpené nové AP s podporou WiFi 6*

3.2.3. Nasadenie Client Firewalls

Ďalší návrh riešení spočíva v nasadení tzv. Client Firewalls. Ide o firewally pre jednotlivé zariadenia, aby komunikácia v rámci internej siete bola ohraničená a teda ochránená na oboch stranách. Vzhľadom na to, že klientské firewally musia byť nainštalované a udržiavané individuálne na každom zariadení, potenciál pre škálovateľnosť je obmedzený. Napriek tomu poskytujú dôležitú vrstvu ochrany pre jednotlivé zariadenia, najmä v prípade, že sú pripojené k otvoreným sieťam, ako je internet.

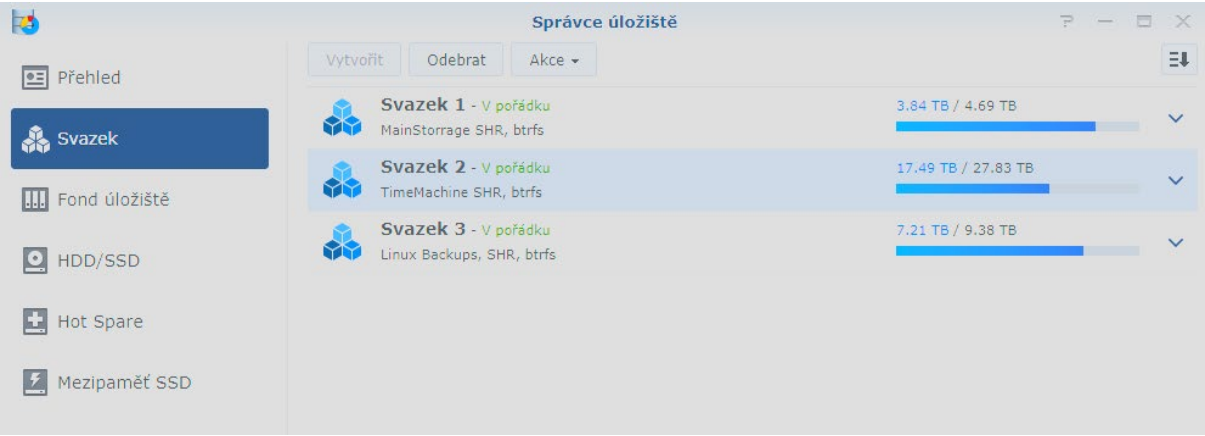
Diagram nižšie v zjednodušenej forme znázorňuje, ako by zhruba mohlo vyzerať zapojenie s nasadenými firewallmi. Boli by zvolené dedikované segmenty pre kamery a senzory a pre jednotlivé access pointy. Okrem toho je navyše použitý firewall pre celú virtuálnu lokálnu sieť obsahujúcu IoT.



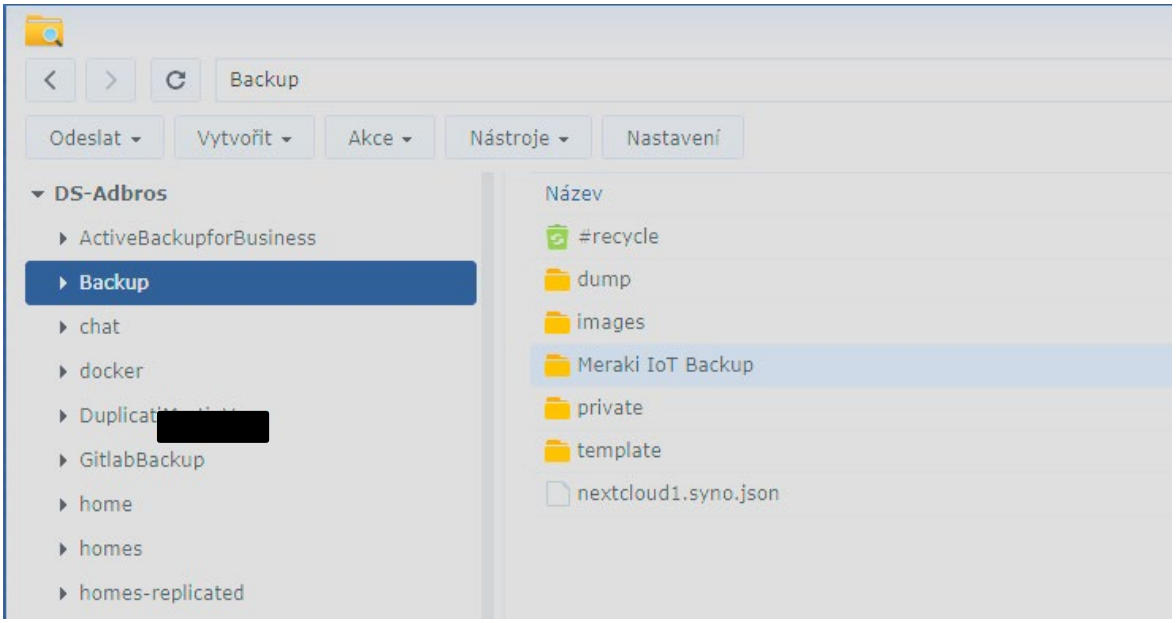
Obrázok 43: Nasadenie client firewalls - zjednodušené
(zdroj: vlastné spracovanie

3.2.4. Lokálne zálohovanie dát zo zariadení

Zálohovanie sa dnes už považuje za neoddeliteľnú súčasť bezpečnostných postupov. Toto platí aj v prípade zhromažďovaných dát prostredníctvom IoT. Okrem ich neustáleho zálohovania v rámci cloud služieb Cisco Meraki sa navrhuje pravidelná tvorba záloh v rámci NAS, ktorým spoločnosť disponuje, aby sa zaistila ich on-premise dostupnosť. Tento krok by aj do budúcna zjednodušil ďalšie analýzy dát. Konkrétne by boli na tieto účely využité Synology NAS, ktorými spoločnosť disponuje.

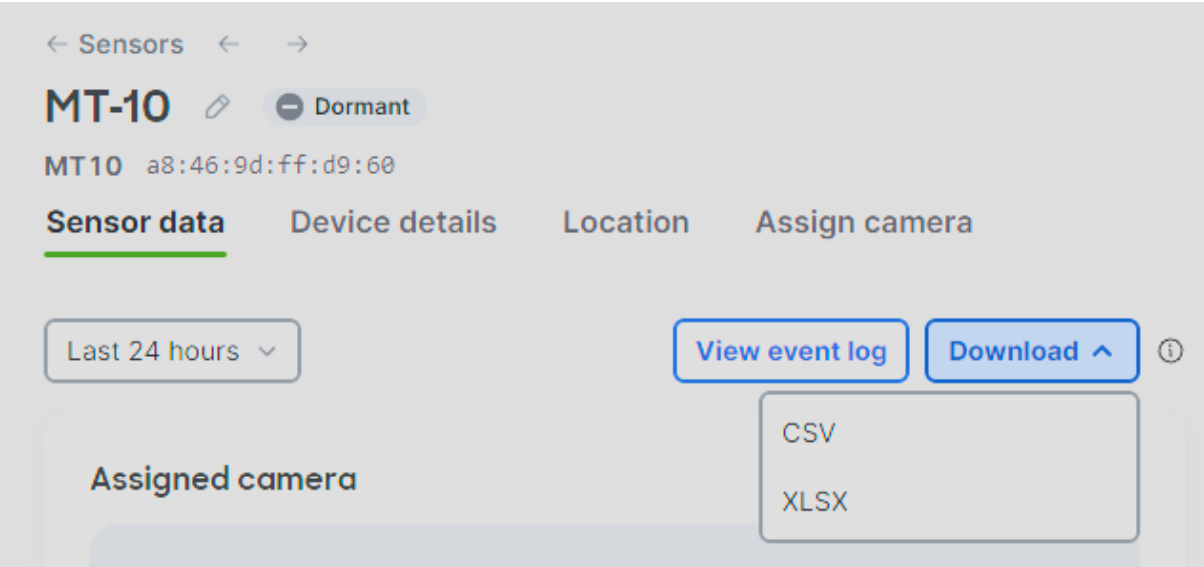


Obrázok 44: Vyhradenie priestoru v rámci NAS
(zdroj: vlastné spracovanie)



Obrázok 45: Vyhradenie priestoru v rámci NAS II
(zdroj: vlastné spracovanie)

Jedinou nevýhodou by v tomto prípade bol fakt, že aktuálne nie je možné automatizovať zálohovanie v rámci nástroja Cisco Meraki . Preto by bolo nutné v pravidelných intervaloch (napríklad raz mesačne) vytvárať zálohy manuálne prostredníctvom vytvárania exportov a ich následného nahrávania na NAS.

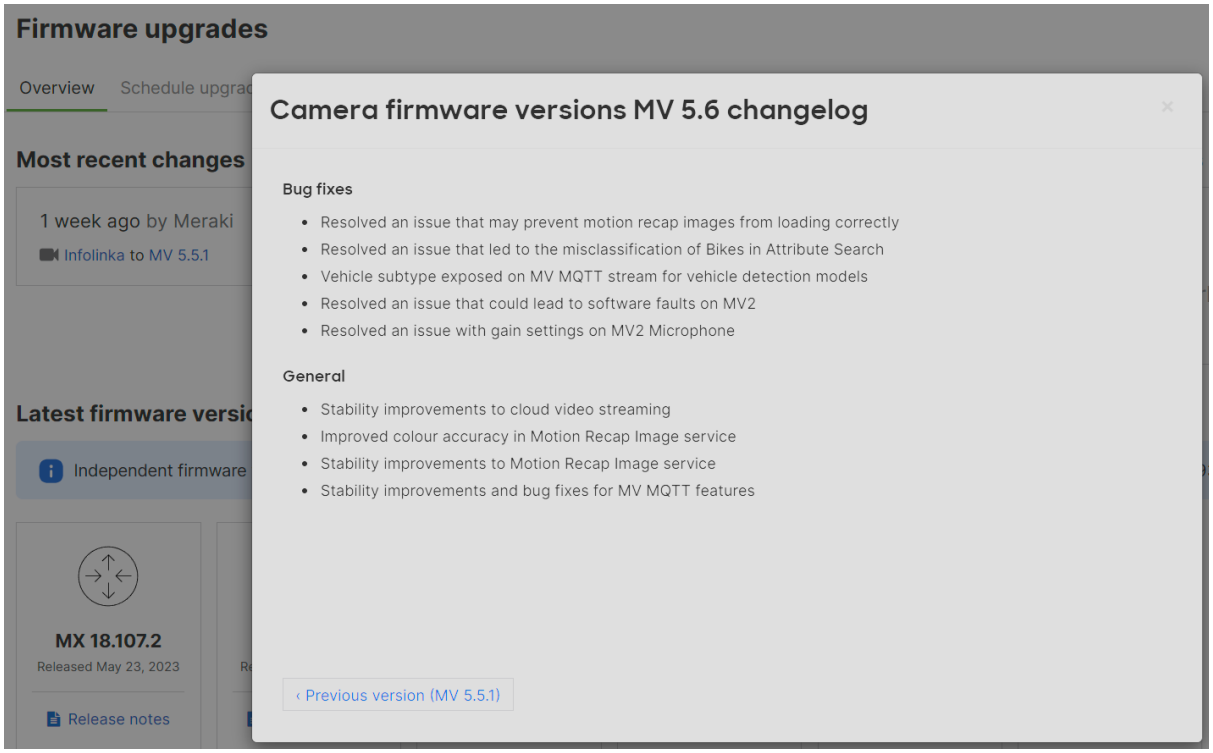


Obrázok 46: Tvorba exportov v rámci Cisco Meraki
(zdroj: vlastné spracovanie)

3.2.5. Aktualizácia a konfigurácia IoT

Ako už bolo spomenuté v prechádzajúcej kapitole, pri monitorovaní pomocou senzorov Meraki dochádzalo k výpadkom z dôvodu nedostatočne silného signálu. Po konzultácií s podporou Cisco sa odporúča aktualizácia firmvéru na verziu 5.3, ktorá značne zlepšuje možnosti prenosu signálu medzi kamerami a senzormi. Taktiež sa odporúča opätovná inicializácia oboch kamier tak, aby boli senzory v ich blízkosti prinútené pripojiť sa na k sebe najbližšie umiestnenú kameru, teda gateway. Keďže je voľba pripojenia žiaľ kompletne závislá od zariadenia samotného a nie je možné ju manuálne nastaviť, bude tento krok vyžadovať niekoľko pokusov.

Ku dňu 12.4.2024 je dokonca možné firmvér aktualizovať na verziu MV 5.6, ktorá poskytuje ďalšie opravy.



Obrázok 47: Centrum aktualizácií Cisco Meraki
(zdroj: vlastné spracovanie)

3.3. Návrhy po stránke zakúpenia ďalšieho vybavenia

Samozrejme, okrem dodatočnej konfigurácie alebo aktualizácie súčasne používaných sieťových prvkov je odporučený aj upgrade infraštruktúry. V tejto časti je bližšie špecifikované, o ktoré prvky by mohlo ísť a akým spôsobom by sa ich výmena, prípadne doplnenie zvýšila bezpečnosť a efektivita systému.

3.3.1. Upgrade AP na WiFi 6

Keďže je aktuálne bezdrôtová časť infraštruktúry založená na už relatívne neaktuálnej technológii WiFi 802.11ac z roku 2012, navrhuje sa prechod na access pointy s technológiou WiFi 6 (802.11ax), prípadne 6E. Síce nejde o najnovší druh tejto bezdrôtovej technológie, no vzhľadom na zvyšok infraštruktúry a optimálne vynaložené finančné náklady v rámci obmedzeného rozpočtu je jej voľba opodstatnená. Išlo by o výmenu aktuálnych všetkých 6 kusov AP, z ktorých sa 3 nachádzajú na prízemí a zvyšné na druhom poschodí.

Vďaka využitiu overenia WPA3 bude sieť oveľa viac zabezpečená prostredníctvom 192 bitového šifrovania, v porovnaní so 128-bit v prípade WPA2 a implementácii SAE (na rozdiel od PSK), takže bude výrazne znížená šanca zraniteľností zvonku aj po stránke zabránenia útokom formou reinštalácie kľúča a off-line slovníkovým útokom.

WiFi 6 totiž spolu s WPA3 prináša takzvanú vylepšenú predbežnú utajenosť (forward secrecy), čo zabezpečuje, že aj keď by hacker odchytil šifrovací kľúč, nemôže dešifrovať už nadviazanú komunikáciu. To znamená, že akékoľvek odchytené dáta zostávajú zabezpečené, čo bráni neoprávnenému prístupu k citlivým informáciám.

Vďaka funkcií TWT (Target Wake Time) WiFi 6 umožňuje zariadeniam plánovať časy registrácie v routeri a tým sa skracuje čas, ktorý musia tráviť hľadaním siete. To má za následok, že je minimalizované okno zraniteľnosti, počas ktorého sú zariadenia náchylné na neoprávnený prístup alebo útoky.

V neposlednom rade, vylepšená účinnosť a zníženie latencie v rámci technológie WiFi 6 znamenajú, že bezpečnostné protokoly a firewally môžu pracovať efektívnejšie, analyzovať a filtrovať dátové pakety s vyššou presnosťou a rýchlosťou. To umožňuje rýchlejšiu detekciu a reakciu na akékoľvek potenciálne bezpečnostné hrozby, čím sa posilňuje celková bezpečnosť.

Tabuľka č. 2: Porovnanie WiFi 5 a 6
(zdroj: vlastné spracovanie)

-	WiFi 5 (802.11ac)	WiFi 6 (802.11ax)
Rok	2012	2019
Max data rate	3,5 Gb/s	9,6 Gb/s
Pásma	2,4 + 5 GHz	2,4 + 5 + 6 GHz
Zabezpečenie	WPA 2	WPA 3
Šifrovanie	128 - bit	192 - bit
Technológie	PSK	SAE, TWT, Enhanced MAC Address Privacy, BSS Coloring

3.3.2. Rozšírenie množstva kamier a senzorov

Taktiež sa odporúča dokúpenie viacerých kusov kamier a senzorov. Vzhľadom na funkcionalitu infraštruktúry Meraki by nebolo nutné nakúpiť veľké množstvo kamier, keďže jednu kameru dokáže ako gateway používať viacero senzorov zároveň. Preto sa za relevantný považuje dodatočný nákup 1 kamery a 3 kusov senzorov na pokrytie všetkých dôležitých oblastí v rámci spoločnosti.

Keďže sa počas monitorovacieho obdobia najviac osvedčil senzor MT14 vďaka svojej rozšírenej funkcionalite v porovnaní s modelom MT10, pri nákupe by bol zvolený tento model. Tým by sa dosiahlo paralelné a kontinuálne monitorovanie vo všetkých spomenutých miestnostiach vyššie a teda serverovni, rozvodni, kuchynke a kúpeľni, no bolo by možné monitorovať aj kuchyňu na prízemí a hlavnú chodbu na druhom poschodí.

Kamery by boli umiestnené na chodbách, čím by sa značne zlepšilo pokrytie monitorovaných oblastí spoločných priestorov a zároveň by kamery boli umiestnené tak, aby poskytovali dostatočne silný signál na pripojenie pre senzory.

Taktiež by so sebou mohlo priniesť množstvo výhod kúpenie ďalších modelov senzorov. Napríklad, modely MT40 alebo MT15.

MT40, ako monitor spotreby energie, poskytuje informácie o využití energie, inteligentné upozornenia a diaľkové ovládanie stavu napájania. Týmto spôsobom prispieva k udržateľnosti, zrýchľuje riešenie problémov pri vzdialených nasadeniach a zefektívňuje prevádzku tým, že umožňuje efektívnejšiu reakciu na výpadky napájania. [12]

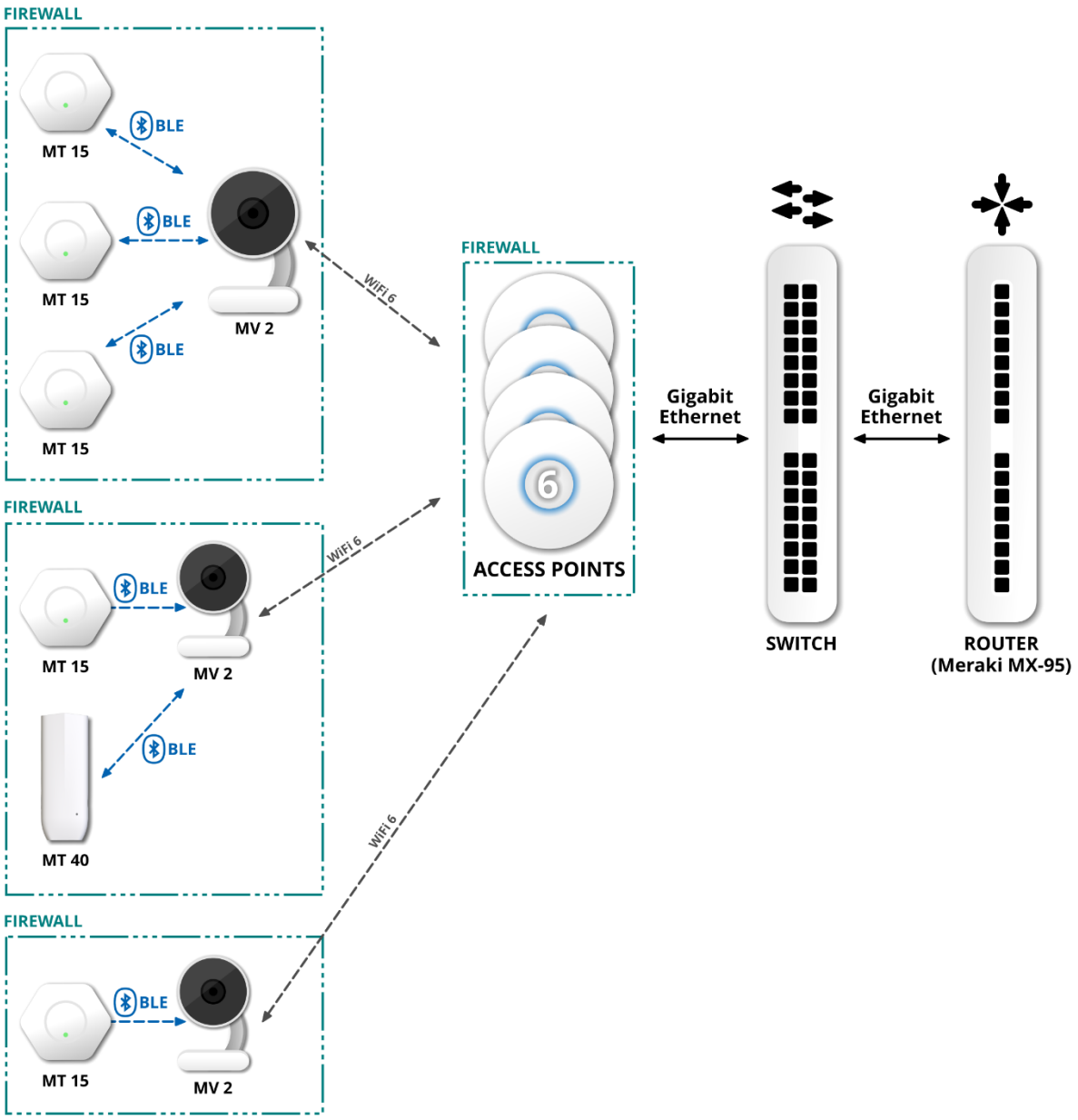
MT15 je veľmi podobný modelu MT14, no okrem TVOC, PM2.5, teploty, vlhkosti a okolitého hluku monitoruje navyše reálny CO2. Okrem toho ponúka LED vizuálny indikátor, ktorý poskytuje informácie o kvalite vzduchu ľuďom v miestnosti. Nakoniec, MT15 má flexibilné možnosti napájania, vrátane USB-C a PoE portu na zariadení, ktoré sú umiestnené tak, aby káble boli skryté. V ideálnom prípade by bol tento model zvolený ako náhrada aj za aktuálne zakúpené MT10 a MT14. [13]

Obrázok 48: Cisco Meraki MT40
(zdroj: [12])

Obrázok 49: Cisco Meraki MT15
(zdroj: [13])

Obrázok 50: Finálne umiestnenie IoT na základe návrhov (zdroj: vlastné spracovanie)

Ak by bola zrealizovaná kúpa nových access points s technológiou WiFi 6 a dokúpenie ďalších IoT zariadení, mohla by výsledná situácia vyzerať približne tak, ako je znázornená vyššie na pôdoryse a nižšie vo forme diagramu. V konečnom dôsledku by sa na prízemí delili o jednu kameru ako o svoju gateway 3 senzory a v prípade druhého poschodia by zas každý zo senzorov využíval jednu z dostupných kamier.



Obrázok 51: Finálne zapojenie v rámci siete na základe návrhov (zdroj: vlastné spracovanie)

Nasadenie viacerých zariadení by samozrejme so sebou prinieslo aj potrebu zakúpenia ďalších licencií. Taktiež by stálo za zváženie dokúpenie už spomenutých licencií, ktoré umožňujú užívateľovi archiváciu záznamu z kamier prostredníctvom Meraki Vision.

3.3.3. Zaobstaranie Cisco routeru

Vzhľadom na to, že modelový rad Meraki obsahuje aj business routery, za zváženie by stála taktiež výmena terajšieho MikroTik routera za model od spoločnosti Cisco. Konkrétne by vzhľadom na veľkosť firmy a požiadavky bol vhodný model MX95. Týmto by sa maximalizovala kompatibilita celej infraštruktúry, minimálne po stránke nainštalovaných IoT zariadení a celú by ju bolo možné spravovať priamo cez nástroj Cisco Meraki.

MX95 disponuje 4 kusmi dedikovaných WAN uplink portov, 2 kusmi 10G SFP+ portov a 2 kusmi RJ45 2,5G mGig portov. LAN porty zahŕňajú 4x RJ45 1 GbE porty a 2x SFP+ 10G porty. Navyše tento router disponuje jedným USB konektorom, ktorý je možné využiť na takzvaný „cellular failover“. Ide o možnosť redundantného pripojenia prostredníctvom mobilnej siete. Táto konektivita by bola pre aktuálny stav firmy viac než dostatočná a samotný výrobca uvádza, že je daný model vhodný do organizácií, ktoré majú až do 500 užívateľov, takže by bola infraštruktúra nadimenzovaná aj do budúcna so značnou rezervou. [14]

Obrázok 52: Cisco MX95
(zdroj: [15])

3.4. Analýza rizík

V priebehu implementácie nových technológií vznikajú komplikácie, napríklad v oblasti komunikácie so zamestnancami, školenia zamestnancov, či celkového riadenia projektu. Počas testovacieho nasadenia IoT a následného monitoringu prostredia, ktoré boli riešené v kapitolách analýza súčasného stavu a v návrhu riešení, boli zistené hrozby, ktoré by pri širšej implementácii do budúcna, ktorá bola tiež navrhnutá vyššie, mohli nastať. V následku toho bola v tejto kapitole zrealizovaná analýza rizík.

Využitá bola skórovacia metóda. Konkrétne boli priradené pravdepodobnosti výskytu a dopadu na implementáciu zmeny ku každému riziku. Ďalším krokom je identifikácia opatrení pre zníženie dopadov rizík a na základe toho stanovenie hodnôt nových. V tabuľke nižšie je znázornená stupnica hodnotenia pravdepodobnosti výskytu jednotlivých rizík, ktoré by mohli mať vplyv na úspešnosť realizácie zmeny.

Tabuľka 3: Pravdepodobnosť výskytu
(zdroj: vlastné spracovanie)

Číselná hodnota	Percentuálna hodnota	Slovný opis
1-2	0 - 20 %	Vysoko nepravdepodobné
3-4	21 - 40 %	Nepravdepodobné
5-6	41 - 60 %	Možné
7-8	61 - 80 %	Pravdepodobné
9-10	81 - 100 %	Vysoko pravdepodobné

Nasledujúca tabuľka zas znázorňuje jednotlivé stupne dopadu týchto rizík a ich slovný popis. Vynásobením týchto dvoch hodnôt získame celkovú hodnotu rizika.

Tabuľka 4: Vyjadrenie dopadu rizík
(zdroj: vlastné spracovanie)

Hodnota	Slovný opis
1-2	Bezvýznamný
3-4	Málo významný
5-6	Významný
7-8	Veľmi významný
9-10	Kriticky významný

V nasledujúcej tabuľke sú identifikované riziká, ku ktorým by konkrétne mohlo dôjsť pri plnohodnotnom nasadení technológií.

Tabuľka 5: Prehľad rizík
(zdroj: vlastné spracovanie)

Číslo	Riziko	Označenie
1	Nedostatok komunikácie naprieč oddeleniami	R1
2	Neochota zo strany zamestnancov	R2
3	Nedostatočne skúsený personál	R3
4	Nevhodný čas na implementáciu	R4
5	Nejasne stanovené ciele	R5
6	Nedostatok zdrojov	R6
7	Nepripravenosť infraštruktúry	R7
8	Neefektívne riadenie projektu	R8
9	Nedostatok podpory od vedenia	R9
10	Zraniteľnosť systému	R10
11	Závislosť od kľúčových zamestnancov	R11

Po identifikácií daných rizík je ich potrebné následne ohodnotiť. V tabuľke nižšie je stanovená pravdepodobnosť rizík a aj ich dopad. Tieto dve hodnoty budú vynásobené a tým získame celkovú hodnotu jednotlivých rizík. V prípade prvej tabuľky sú uvedené možné scenáre ako následky rizík. V ďalšej tabuľke sú uvedené už opatrenia, pomocou ktorých je možné hodnoty dopadu týchto rizík znížiť.

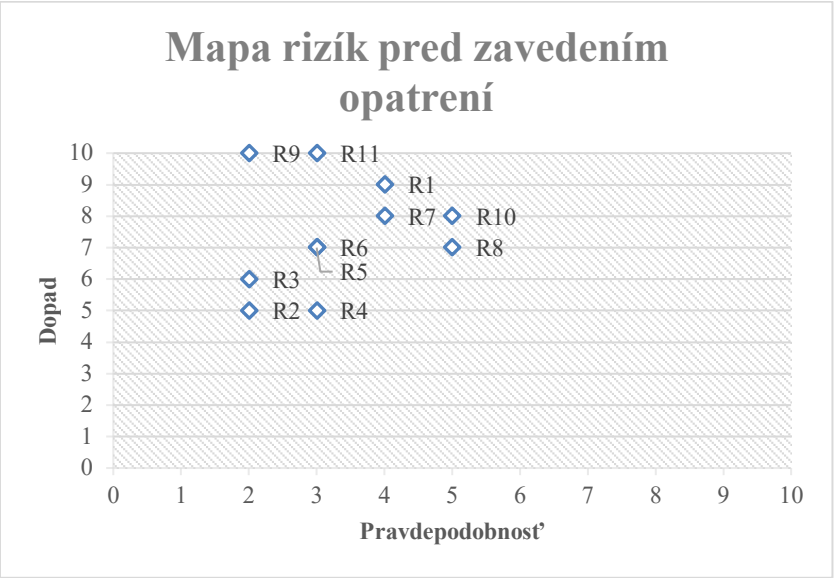
Tabuľka 6: Ohodnotenie rizík
(zdroj: vlastné spracovanie)

	Riziko	Scenár	P-ST	Dopad	Celková hodnota
R1	Nedostatok komunikácie naprieč oddeleniami	Kvôli nesprávnemu vykomunikovaniu zámerov a stratégií naprieč oddeleniami môže dôjsť k neefektívnej realizácii implementácie	4	9	36
R2	Neochota zo strany zamestnancov	V dôsledku nedôvery zamestnancov voči implementácii by bola znížená úroveň ich produktivity	2	5	10
R3	Nedostatočne skúsený personál	Nedostatok znalostí a skúseností v prípade zamestnancov by mohol viesť k neefektívnej implementácii zmien	2	6	12
R4	Nevhodný čas na implementáciu	Na základe nesprávneho načasovania by mohlo dôjsť k oneskoreniu implementácie	3	5	15
R5	Nejasne stanovené ciele	Vznik neefektívnych procesov, čo by malo za následok neuspokojivé výsledky implementácie	3	7	21
R6	Nedostatok zdrojov	V prípade nedostatku zdrojov, či už po časovej a finančnej stránke alebo ľudských zdrojov by došlo k oneskoreniu alebo nesprávnej implementácii	3	7	21
R7	Nepripravenosť infraštruktúry	Ak by nebola aktuálna infraštruktúra dostatočne prispôsobená nárokom vyplývajúcim z implementácie nových technológii, vznikli by problémy s funkcionalitou	4	8	32
R8	Neefektívne riadenie projektu	Oneskorenia, nedorozumenia a následne neefektívna implementácia	5	7	35
R9	Nedostatok podpory od vedenia	Na základe konfliktov medzi vedením a zamestnancami by vznikli komplikácie, ktoré by mohli viesť k samotnému zlyhaniu celého projektu	2	10	20
R10	Zraniteľnosť systému	V dôsledku nedostatočnej pripravenosti systému by sa mohol stať terčom mnohých bezpečnostných hrozieb napádajúcich celú infraštruktúru	5	8	40
R11	Závislosť od kľúčových zamestnancov	V prípade stratenia kľúčových zamestnancov by v lepšom prípade došlo k oneskoreniu a v krajnom až k neúspechu projektu	3	10	30

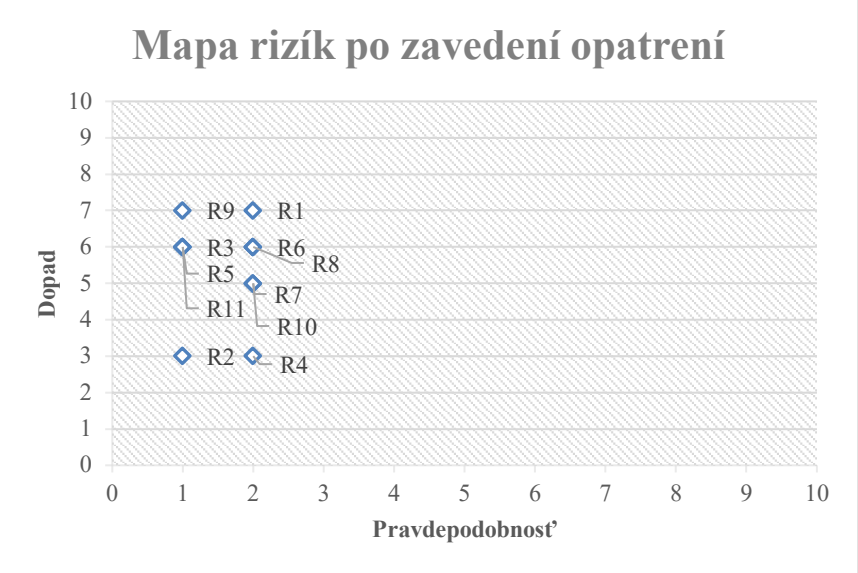
Tabuľka 7: Ohodnotenie rizík po zavedení opatrení
(zdroj: vlastné spracovanie)

	Riziko	Opatrenie	P-ST	Dopad	Celková hodnota
R1	Nedostatok komunikácie naprieč oddeleniami	Zavedenie efektívnych komunikačných kanálov a realizácia pravidelných tímových meetingov na zdieľanie informácii medzi oddeleniami	2	7	14
R2	Neochota zo strany zamestnancov	Vytvorenie motivačných programov a školení, aby sa zamestnancom priblížil proces implementácie.	1	3	3
R3	Nedostatočne skúsený personál	Vzdelávanie personálu v kľúčových oblastiach pre správnu implementáciu.	1	6	6
R4	Nevhodný čas na implementáciu	Dôkladné plánovanie a sledovanie časových rámcov pre jednotlivé úlohy, aby boli dodržané deadlines.	2	3	6
R5	Nejasne stanovené ciele	Tvorba jednoznačných pokynov, smerníc a postupov naprieč oddeleniami.	1	6	6
R6	Nedostatok zdrojov	Dôkladné rozplánovanie množstva a využitia zdrojov v rámci celého trvania implementácie.	2	6	12
R7	Nepripravenosť infraštruktúry	Kontrola infraštruktúry a následná konfigurácia spojená s aktualizáciou systémov na základe technologických štandardov.	2	5	10
R8	Neefektívne riadenie projektu	Realizácia pravidelných meetingov naprieč oddeleniami a vedením na základe vopred stanovenej časovej osi s míľnikmi.	2	6	12
R9	Nedostatok podpory od vedenia	Zaistenie dostatočného zapájania vedenia do implementácie a informovania vedenia o prebiehajúcich činnostiach.	1	7	7
R10	Zraniteľnosť systému	Zjednotenie nastavení aktuálneho systému a nových technológií s bezpečnostnými štandardmi.	2	5	10
R11	Závislosť od kľúčových zamestnancov	Prehodnotenie štruktúry zamestnancov tak, aby bol čo do najväčšej miery zachovaný znalostný kapitál a motivácia zotrvania zamestnancov formou poskytnutia ďalšieho profesného rozvoja.	1	6	6

Na nasledujúcich mapových grafoch sú znázornené hodnoty rizík pred a po zavedením opatrení:



Graf 1: Mapa rizík pred zavedením opatrení (zdroj: vlastné spracovanie)

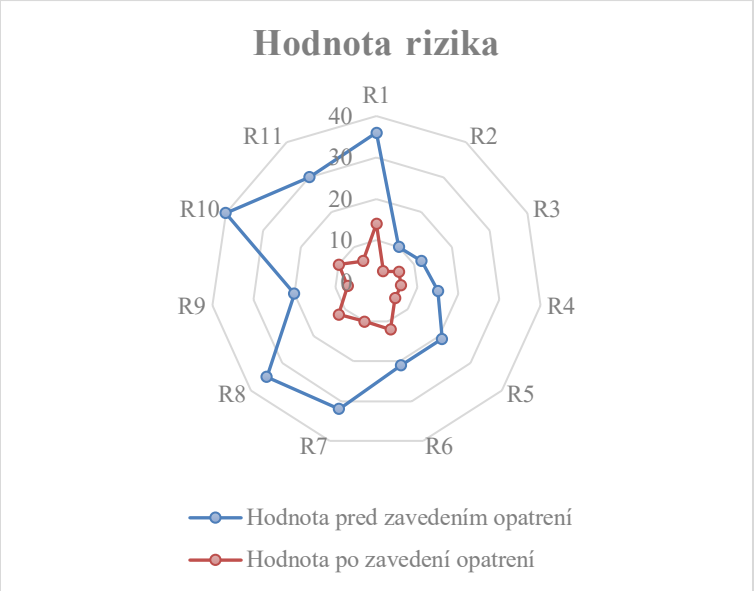


Graf 2: Mapa rizík po zavedení opatrení (zdroj: vlastné spracovanie)

V nasledujúcej tabuľke sú uvedené jednotlivé riziká s hodnotami pred a po zavedení opatrení. Ide o priamejšie porovnanie údajov v tejto forme a následne vo forme pavučinového grafu.

Tabuľka 8: Porovnanie celkových hodnôt rizík
(zdroj: vlastné spracovanie)

	Riziko	Hodnota pred zavedením opatrení	Hodnota po zavedení opatrení
R1	Nedostatok komunikácie naprieč oddeleniami	36	14
R2	Neochota zo strany zamestnancov	10	3
R3	Nedostatočne skúsený personál	12	6
R4	Nevhodný čas na implementáciu	15	6
R5	Nejasne stanovené ciele	21	6
R6	Nedostatok zdrojov	21	12
R7	Nepripravenosť infraštruktúry	32	10
R8	Neefektívne riadenie projektu	35	12
R9	Nedostatok podpory od vedenia	20	7
R10	Zraniteľnosť systému	40	10
R11	Závislosť od kľúčových zamestnancov	30	6



Graf 3: Pavučinový graf porovnania celkových hodnôt rizík
(zdroj: vlastné spracovanie)

Riziká sú analyzované skórovacou metódou a súčasťou návrhu je aj finančné hodnotenie.

3.5. Ekonomické zhodnotenie a prínosy

Vynaložené náklady

Táto kapitola sa zaoberá finančnou stránkou celého projektu. Celkový rozpočet bol stanovený na 100 000 Kč s tým, že by mal byť v cene zahrnutý nákup zariadení a preplatený čas zamestnancov vynaložený na ich úvodné nastavenie. V nasledujúcej tabuľke je zhrnuté, koľko jednotlivé senzory a kamery stáli. V neposlednom rade je započítaná práca dvoch technikov, ktorí vynaložili zhruba 30 hodín na realizáciu, kedy mali na starosť výber nástroja, nákup a implementáciu.

Tabuľka č. 8: Ekonomické zhodnotenie
(zdroj: vlastné spracovanie)

Názov	Cena / jednotku	Množstvo	Cena celkom v Kč
Senzor MT14	$267.47*	1 kus	6 125
Senzor MT10	$167.08*	1 kus	3 827
Kamera MV2	$515.42*	2 kusy	11 805
Meraki MT/MV licencia	2952 Kč*	2 kusy	5904
Zamestnanci technického oddelenia	500 Kč/hod/os	2 zamestnanci po dobu 30 hodín	30 000
Celkové výdaje			**57 661**

*Ceny zariadení a licencií sú orientačné, keďže sa neustále menia.

Prínosy sú v tomto okamihu ťažko vyčísliteľné, pretože hlavným cieľom je zvýšenie komfortu zamestnancov a tým aj ich produktivita. Tá sa v tento krátky okamih zaznamenať a vyčísliť nedá, avšak náklady vo výške 57 661 Kč nie sú pre spoločnosť Stellnaris nijak závratne vysoké a tak zvýšenie produktivity pri malom počte zamestnancov môže pre spoločnosť znamenať významný prínos a výsledky budú určite viditeľné v budúcnosti.

Taktiež je nutné podotknúť, že je vďaka zariadeniam zvýšená bezpečnosť po stránke monitorovania. V neposlednom rade sa dá počítať so zvýšením životnosti sieťových a to hlavne aktívnych prvkov zmenou nastavenia klimatizačných jednotiek v závislosti od nameraných dát. V pláne je pravidelné meranie spokojnosti zamestnancov.

Potencionálne náklady

V prípade, že by došlo k výmene už spomenutých access points (ako príklad bol zarátaný do tabuľky model TP-Link EAP 670), doplneniu senzorov, respektíve ich výmene za modely Cisco Meraki MT15, dokúpenie modelu MT40 a výmeny routeru za Cisco MX95, ďalšie vynaložené náklady by sa pohybovali zhruba okolo hodnoty 226 000 Kč. V tomto prípade neboli zarátané náklady spojené s inštaláciou nových zariadení, keďže je odhad trvania zložitý a to hlavne v prípade konfigurácie nového routeru.

Išlo by o skutočne signifikantnú čiastku pre spoločnosť o veľkosti Stellnaris, takže je možné, že by bolo jej opodstatnenie reálnejšie v prípade budúceho rastu firmy, a teda nie v dobe blízkej.

Tabuľka 9: Ekonomické zhodnotenie potencionálnych nákladov (zdroj: vlastné spracovanie)

Názov	Cena / jednotku	Množstvo	Cena celkom v Kč
Senzor MT15	$477.70*	5 kusov	57 324
Senzor MT40	$267.47*	1 kus	6 420
Kamera MV2	$515.42*	1 kus	11 805
Router MX95	112 691 Kč*	1 kus	112 691
Meraki MT/MV licencia	2 952 Kč*	5 kusov	14 760
AP TP-Link EAP 670	3 909 Kč*	6 kusov	23 454
Celkové výdaje			**226 454**

*Ceny zariadení a licencií sú orientačné, keďže sa neustále menia.

Záver

Cieľom práce bolo navrhnúť a zaviesť systém na optimalizáciu pracovného prostredia spoločnosti Stellnaris prostredníctvom zariadení IoT, a to po stránke teploty, vlhkosti a kvality vzduchu a hlučnosti. Taktiež bolo cieľom navrhnúť optimalizáciu monitorovaných priestorov tak, aby sieťové prvky bežali čo najefektívnejšie, bola dosiahnutá ich vysoká životnosť a taktiež, aby bol dosiahnutý komfort pre osoby nachádzajúce sa v priestoroch v prípade výkonu práce. Predmetom práce boli navyše návrhy lepšieho zabezpečenia aktuálne používanej infraštruktúry a taktiež tvorba opatrení pri hromadnom nasádzaní spomenutých zariadení do budúcna na základe výsledkov analýzy rizík.

Prostredie bolo monitorované pomocou systému Cisco Meraki, senzorov a kamier. Meranie dát prebiehalo v horizonte niekoľkých mesiacov, celkovo pre všetky monitorované priestory od 02.11.2023 do dňa 01.02.2024. Stanovený celkový rozpočet na 100 000 Kč bol dodržaný, pretože finálna implementácia vrátane ľudských zdrojov a prístrojov stála 57 661 Kč. Pokiaľ ide o investície spojené s návrhmi riešení, ich celková suma by sa mala pohybovať okolo hodnoty 226 000 Kč bez zahrnutia práce spojenej s ich realizáciou po stránke inštalácie.

Zoznam zdrojov

[1] STRATUS INFOSYSTEMS. *What is Cisco Meraki?* [online]. Dostupné z: https://www.stratusinfosystems.com/news/what-is-cisco-meraki/

[2] SYCOM. *Čo je to cloud? Spoznajte Cloud computing služby* [online]. Dostupné z: https://www.sycom.sk/co-je-to-cloud

[3] ORACLE. *What is IoT?* [online]. Dostupné z: https://www.oracle.com/internet-of-things/what-is-iot/

[4] DIGMIA. *Čo je monitoring siete a prečo sa firmám oplatí?* [online]. Dostupné z: https://www.digmia.sk/co-je-monitoring-siete

[5] CISCO MERAKI. *MV2 Indoor Security Camera* [online]. Dostupné z: https://meraki.cisco.com/product/security-cameras/indoor-security-cameras/mv2/

[6] SINCLAIR SOLUTIONS. *ASH-12BIV - Sinclair Solutions* [online]. Dostupné z: https://www.sinclair-solutions.com/cs/produkty/nastenne-klimatizace-168/vision-serie/6455-ash-12biv-053011000003240.html

[7] KONÍČEK, Tomáš. *SINCLAIR VISION ASH-12BIV* [online]. Dostupné z: https://www.tomaskonicek.cz/files/product/additionalFiles/sinclair-um-vision-ash-xxbiv-cz.pdf

[8] UBIQUITI INC.. *UniFi Network Version 7.0* [online]. Dostupné z: https://blog.ui.com/2022/03/01/unifi-network-version-7-0-introduces-revamped-settings-to-simplify-system-configuration/

[9] MITRE. *CVE - Meraki* [online]. Dostupné z: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Meraki

[10] MITRE. *CVE - RouterOS* [online]. Dostupné z: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=RouterOS

[11] CISCO. *What is the Cloud Controls Framework?* [online]. Dostupné z: https://www.cisco.com/c/en/us/about/trust-center/compliance/ccf.html#~what-is-the-cloud-controls-framework

[12] CISCO MERAKI. *MT40 Datasheet - Smart Power Controller* [online]. Dostupné z: https://documentation.meraki.com/MT/MT_Datasheets/MT40_Datasheet_-_Smart_Power_Controller

[13] CISCO MERAKI. *MT15 Datasheet - Indoor Air Quality w/CO2* [online]. Dostupné z: https://documentation.meraki.com/MT/MT_Datasheets/MT15_Datasheet_-_Indoor_Air_Quality_w%2F%2FCO2

[14] STINSON, Amon; VO, Don; SINGH, Simarbir. *CISCO MX95/105 Datasheet* [online]. Dostupné z: https://documentation.meraki.com/MX/MX_Overviews_and_Specifications/MX95%2F%2F105_Datasheet

[15] CISCO MERAKI. *MX95 Medium Branch Security & SD-WAN* [online]. Dostupné z: https://meraki.cisco.com/product/security-sd-wan/medium-branch/mx95/

Zoznam obrázkov

Zoznam tabuliek

Zoznam grafov