VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

ANALÝZA ZABEZPEČENÍ FIREMNÍ SÍTĚ STŘEDNÍHO PODNIKU A IMPLEMENTACE NAVRHOVANÝCH BEZPEČNOSTNÍCH OPATŘENÍ

ANALYSIS OF THE SECURITY OF THE CORPORATE NETWORK OF A MEDIUM-SIZED ENTERPRISE AND THE IMPLEMENTATION OF CONTROLS

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — Ondřej Havlíček

AUTHOR

VEDOUCÍ PRÁCE — Ing. Petr Sedlák

SUPERVISOR

BRNO 2023

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Student:	**Ondřej Havlíček**
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2022/23
Studijní program:	Manažerská informatika

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 bakalářskou práci s názvem:

Analýza zabezpečení firemní sítě středního podniku a implementace navrhovaných bezpečnostních opatření

Charakteristika problematiky úkolu:

Úvod
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr

Cíle, kterých má být dosaženo:

Cílem této práce je analyzovat zabezpečení firemní sítě a jejich vnitřních procesů a zhodnotit je dle standardů vydaných Národním úřadem kybernetické a informační bezpečnosti a následně navrhnout adekvátní bezpečnostní opatření.

Základní literární prameny:

DOUCEK Petr, Martin KONEČNÝ a Luděk NOVÁK. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing, 2020. ISBN 978-80-88260-39-4.

JORDÁN Vilém a Viktor ONDRÁK. Infrastruktura komunikačních systémů II - Kritické aplikace. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-80-214-5240-4.

ONDRÁK Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

SEDLÁK Petr, Martin KONEČNÝ a kolektiv. Kybernetická (ne)bezpečnost. CERM, Akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2022/23

V Brně dne 5.2.2023

L. S.

Ing. Jiří Kříž, Ph.D. garant	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Tato bakalářská práce analyzuje zabezpečení a vnitřní procesy firemní sítě středního podniku a popisuje implementaci navrhovaných bezpečnostních opatření. Teoretická část popisuje základní pojmy použité ve vlastním návrhu řešení. V analytické části je zhodnocen současný stav zabezpečení firmy. Praktická část řeší samotnou implementaci navrhovaných řešení tak, aby odpovídaly minimálním bezpečnostním standardům vydaných Národním úřadem kybernetické a informační bezpečnosti.

Abstract

This bachelors thesis analyses security and inner processes of a medium-sized enterprise and describes implementation of suggested controls. Teoretical part describes basic terms used in the main part of the thesis. In the analytical part is reviewed present state of security. Practical part deals with the implementation of controls in a way, that is acceptable for minimal secure standards published by Národní ústav kybernetické a informační bezpečnosti.

Klíčová slova

Kybernetická bezpečnost, bezpečnostní opatření, informační systém, firemní síť

Key words

Cybersecurity, safety measures, information system, firm network

Bibliografická citace

HAVLÍČEK, Ondřej. *Analýza zabezpečení firemní sítě středního podniku a implementace navrhovaných bezpečnostních opatření.* Brno, 2023. Dostupné také z: https://www.vut.cz/studenti/zav-prace/detail/151298. Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák**.**

Čestné prohlášení

Prohlašuji, že jsem svoji bakalářskou práci vypracoval samostatně s využitím zdrojů, které jsem řádně ocitoval a neporušil jsem autorská práva stanovená Zákonem č.121/2000 Sb., o právu autorském.

V Brně, 14. května 2023 …..…….

Ondřej Havlíček

Poděkování

Rád bych poděkoval svému vedoucímu práce panu Ing. Petru Sedlákovi, že mi byl vždy nápomocný a svými radami přispěl k vypracování mé závěrečné práce. Dále bych chtěl poděkovat správci sítě firmy, kde jsem měl možnost zpracovat svoje téma. V neposlední řadě svojí sestře, která mi byla nápomocná při zpracovávání této práce.

Obsah

Úvod 13

1 Teoretická východiska práce 14

1.1 Logické zapojení hvězda 14

1.2 Router 14

1.3 Switch 14

1.4 Server 14

1.5 Informační systém QI 15

1.6 Operační systém 15

1.7 Segmentace sítě 15

1.8 UPS 15

1.9 Antivirus 16

1.10 Firewall 16

1.11 Zálohování 16

1.12 RAID 10 16

1.13 Kyberprostor 17

1.14 Bezpečnostní incident 17

1.15 Bezpečnostní riziko 17

1.16 Bring your own device 17

1.17 B2B prodej 17

1.18 Šifrování dat 18

1.19 Dvoufázové ověření 19

1.20 Disaster recovery plan 19

1.21 Audit kybernetické bezpečnosti 20

1.22 Malware 20

1.23 Phishing 21
1.24 Sociální inženýrství 21
1.25 CISO 22
1.26 Střední podnik 22
1.27 VLAN 22
1.28 Access mode 22
1.29 Trunk mode 23
1.30 Síťový port přepínače 23
1.31 Penetrační testování 23
1.32 Outsourcing 23
2 Popis současného stavu 24
2.1 Oblast technická 24
2.1.1 Schéma logického zapojení 24
2.1.2 Síťové prvky 26
2.1.3 Server 27
2.1.4 Koncové zařízení 27
2.1.5 Software na koncových zařízeních 27
2.1.6 Firewall 28
2.1.7 Omezení provozu 28
2.1.8 Zálohování dat 28
2.1.9 Tok dat 29
2.1.10 E-shop 29
2.2 Oblast řízení 30
2.2.1 Klasifikace a ochrana informací 30
2.2.2 Docházkový systém 30
2.2.3 Udělování přístupů 30

2.2.4 Bezpečnostní povědomí zaměstnanců 31
2.2.5 Fyzické zabezpečení ve firmě 31
2.2.6 Disaster recovery plan 31
2.2.7 Bring your own device 32
2.2.8 Evidence bezpečnostních incidentů a bezpečnostních událostí 32
2.2.9 Personál správy sítě 32
2.2.10 Dodavatelé a odběratelé 32
2.2.11 Organizační hierarchie 33
3 Analýza současného stavu 34
3.1 Oblast technická 34
3.2 Oblast řízení 35
4 Výsledek analýzy současného stavu 36
4.1 Graf výsledku analýzy 36
4.2 Zhodnocení výsledku analýzy 37
5 Vlastní návrh řešení 38
5.1 Školení zaměstnanců 38
5.1.1 Vytvoření programu školení 38
5.1.2 Očekávané přínosy 39
5.1.3 Role a odpovědnosti ve školícím programu 39
5.1.4 Výběr školícího programu a zhodnocení nákladů 42
5.1.5 Přidělení školících programů pracovním pozicím 43
5.1.6 Bezpečný pohyb v kybersvětě 44
5.2 Segmentace stě 46
5.2.1 Identifikace switchů 46
5.2.2 Logické rozdělení sítě 47
5.2.3 Navrhované opatření 47

5.2.4 Současné nastavení sítě v programu Cisco Packet Tracer 48
5.2.5 Nastavení switchů 49
5.2.6 Nastavení routeru 52
5.2.7 Logické schéma zapojení pro kanceláře 53
5.2.8 Logické schéma zapojení pro sklad a výrobu 53
5.3 Další navrhované řešení 54
5.3.1 Klasifikace dat 54
5.3.2 Evidence bezpečnostních incidentů 54
5.3.3 Audit zabezpečení sítě 57
5.3.4 Záložní zdroj elektřiny 57
5.3.5 Dvoufázové ověřování 58
5.3.6 Disaster recovery plan 59
5.3.7 Manažer bezpečnosti ICT 60
5.3.8 Šifrování dat na disku 62
5.3.9 Zabezpečení serveru proti vnějším vlivům 62
5.3.10 Aplikační bezpečnost 63
5.4 Závěrečná kalkulace výdajů 64
6 Výstupní analýza po zavedení navrhovaných opatření 65
6.1 Oblast technická 65
6.2 Oblast řízení 66
6.3 Vyhodnocení navrhovaných opatření a jejich přínos 67
7 Závěr 68
Použité zdroje 69
Seznam obrázků 74
Seznam tabulek 75
Přílohy 76

Příloha 1: Certifikát Bvk! – Základní verze 76

Příloha 2: Základy kybernetické bezpečnosti 77

Příloha 3: Kurz pro manažery kybernetické bezpečnosti 78

Úvod

V dnešní době zpříjemňují život běžným uživatelům moderní technologie. Čím dál více obsahu a služeb se přesouvá na internet. Tohoto trendu se v průběhu posledních let zúčastňují i firmy a modernizují svoje zázemí. To ale sebou přináší i spoustu rizik. Internetoví útočníci se zaměřují nejen na soukromé osoby, ale hlavně na větší organizace a firmy, ze kterých mohou získat větší zisk.

Chránit firemní síť je velmi důležitý úkol a firma by ho měla svěřit takovému člověku, který je velmi zkušený a vyzná se v oboru kybernetické bezpečnosti. Řada firem tento problém řeší najmutím bezpečnostních odborníků, kteří jsou smluvně vázáni plnit povinnosti. Firma tak předá svoje odpovědnosti poskytovateli těchto služeb a zároveň tak ušetří lidské a finanční zdroje.

Některé organizace ale zaměstnávají odborníky přímo ve svých řadách. Tito zaměstnanci nesou odpovědnost za zabezpečení celé sítě organizace a musí jednotlivé oblasti vyřešit efektivně a znát všechny potřebné opatření pro zlepšení zabezpečení.

Národní úřad kybernetické a informační bezpečnosti vydal doporučení na minimální bezpečnostní standardy, které upřesňují, co je považováno za minimální opatření v různých oblastech kybernetické bezpečnosti. Toto doporučení je zatím jen dobrovolné a je na uvážení jednotlivých organizací, zda se rozhodnou tato opatření implementovat ve svých firemních sítích. V budoucnu je ale v plánu z těchto doporučení vytvořit povinné opatření, které bude muset vykázat každá organizace, že je v plném rozsahu splňuje. Je to reakce na nové, efektivnější a agresivnější útoky, které se současně s rozvojem informačních technologií také neustále zdokonalují.

Toto téma jsem si vybral, jelikož je tato problematika stále více a více probíraná ve společnosti a spousta firem stále používá zastaralá opatření, technické vybavení a procesy v boji proti kybernetické kriminalitě.

Osobně se o toto téma zajímám a ve svém okolí jsem našel firmu, která tato opatření nesplňuje v celém rozsahu. Aby si firma ochránila svoje jméno, zůstane anonymní. S firmou jsem podepsal smlouvu o mlčenlivosti, a tak v celé mé práci zůstane anonymní.

1 Teoretická východiska práce

V této části popíšu všechny pojmy, které se nacházejí v textu a které je potřeba objasnit.

1.1 Logické zapojení hvězda

Jedná se o takové zapojení, kde ve středu je jeden aktivní prvek, například switch, a na něj se napojují buď koncové uzly nebo další aktivní prvky rozšiřující síť. Každý tento koncový uzel je připojen přímo na aktivní prvek nezávisle na ostatních zařízeních. V případě vypadnutí jednoho z uzlů je celá síť stále funkční.[1]

1.2 Router

Router neboli směrovač je aktivní prvek sítě pracující na 3. vrstvě síťového modelu ISO/OSI. Jeho úkolem je směrovat pakety do okolních sítí, tzv. routing a odesílání paketů tou nejvýhodnější cestou, tzv. forwarding. K tomu mu slouží routovací tabulka, kde si zapisuje nejbližší další routery včetně jejich vzdálenosti ohodnocené číslem.[1]

1.3 Switch

Switch neboli přepínač slouží pro rozesílání paketů konkrétním koncovým uzlům v síti. Toto dokáže díky tabulce MAC adres. Tabulka obsahuje MAC adresy koncových zařízení a port, skrze který je připojen. Paket poté pošle přes daný port danému uzlu.[1]

1.4 Server

Sever je stanice, která poskytuje ostatním zařízením v síti služby. Tyto služby mohou být souborové, aplikační, tiskové, poštovní, databázové nebo terminálové.[1]

1.5 Informační systém QI

QI je podnikový informační systém, určený pro střední a velké podniky, zaměřený mimo jiné na řízení vztahů se zákazníkem. Je velmi vhodný pro firmy, které se zabývají výrobou a zákaznickým servisem. Systém je možno upravit dle vlastních potřeb odebráním nebo přidáním modulů.[4][5]

1.6 Operační systém

„Operační systém je sada programů (software) umožňujících co nejefektivnější využití hardwaru počítače. Operační systém patří mezi tzv. systémový software a hlavním úkolem operačního systému je zabezpečit běh a programovou podporu aplikačních programů“. Operační systém je ten systém, se kterým pracuje uživatel, a je tak k tomu uzpůsoben. Podporuje běh jiných aplikací a dokáže jim přiřazovat hardware pro jejich plynulý běh.[6]

1.7 Segmentace sítě

Segmentace sítě je opatření zlepšující celkové zabezpečení sítě. Jedná se o rozdělení sítě, ať už logicky nebo fyzicky, na jednotlivé vzájemně oddělené podsítě. Díky tomuto rozdělení nemůže dojít k průniku z jedné sítě do druhé. Pro koncové zařízení je tedy podsíť jeho limitem, kam se v rámci celé sítě dokáže dostat.[2]

1.8 UPS

UPS neboli záložní zdroj napájení je přístroj, který v případě výpadku elektrického proudu je schopen napájet zařízení po dobu potřebnou pro obnovu zdroje nebo zajištění náhradního.[3]

1.9 Antivirus

„Antivirus je zjednodušené označení bezpečnostního programu, který vyhledá, detekuje, blokuje a odstraňuje kybernetické hrozby“. Dá se říci, že antivirus je hradní stráž, která prochází hradby a hledá zločince uvnitř hradu. Novodobé antiviry rozpoznávají škodlivé programy na základě porovnání vzorků v antivirové databázi, která se neustále aktualizuje i několikrát za den. K detekci mu slouží nástroje jako je emulace kódu, heuristika a analýza chování programu.[7]

1.10 Firewall

„Firewall je bezpečnostní systém, který v počítačové síti zkoumá a omezuje síťový provoz na základě předdefinovaných nebo dynamických pravidel a politik“. Firewall se zapojuje nejen do perimetru celé sítě, aby ochránil všechny zařízení v síti, ale i na samotná koncová zařízení. Velice zjednodušeně je firewall strážce brány do hradu a zabraňuje vniknutí nepřítele. Firewall kontroluje jednotlivé pakety a zkoumá jejich základní informace. Z paketu vyčte zdrojového adresáta, cílového adresáta a porty pro tuto komunikaci a její protokoly. Díky tomu dokáže detekovat potenciální útoky a zabránit jim ještě předtím, než se dostane do koncového zařízení.[8]

1.11 Zálohování

Zálohování dat je proces, při kterém vytváříme kopii dat na jiný datový nosič. Tímto je zajištěna dostupnost dat při poškození datového nosiče, nedostupnost připojení ke cloudovému úložišti nebo úmyslným či neúmyslným lidským zásahem. Důležitá je i frekvence zálohování. To můžeme provádět denně, týdně nebo měsíčně. Obecně ale platí, že čím častěji provádíme zálohu, tím lépe.[9][28]

1.12 RAID 10

RAID je technologie zrcadlení disků. Jedná se o ukládání dat na vzájemně nezávislé disky, kdy v případě selhání jednoho z nich, je umožněna snadná a rychlá obnova dat. RAID 10 je typ zrcadlení, ve kterém se disky rozdělí na dvě dvojice, které se vzájemně zrcadlí. Díky tomu máme vysokou rychlost čtení i zápisu a zároveň vysokou bezpečnost.[10]

1.13 Kyberprostor

Pojem kyberprostor je vymezen v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti §2 písmena a) „Kybernetickým prostorem rozumíme digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informační systémy a službami a sítěmi elektronických informací“.[11]

1.14 Bezpečnostní incident

Bezpečnostní incident je porušení nebo bezprostřední hrozba porušení bezpečnostních politik, bezpečnostních zásad nebo standardních bezpečnostních pravidel provozu informační a komunikační technologie v důsledku kybernetické bezpečnostní události.[12][28]

1.15 Bezpečnostní riziko

„Souhrn možností, že hrozba využije zranitelnosti aktiva nebo skupiny aktiv a tím způsobí organizaci škodu“. Jedná se tedy o pravděpodobnost, že dojde k bezpečnostnímu incidentu. Číselně jej můžeme vyjádřit hodnotou v rozsahu <0,1>, přičemž 0 představuje téměř žádné riziko a 1 jistotu vzniku.[12][13]

1.16 Bring your own device

Jedná se o koncept, který umožňuje zaměstnancům používat jejich osobní zařízení jako notebook nebo mobilní telefon, se kterými se dostanou do firemní sítě a mohou používat firemní data pro plnění jejich pracovních povinností.[14]

1.17 B2B prodej

Rozdělení trhu, ve kterém působí jen společnosti. Je to prodej jedné firmy druhé firmě. Tento trh je větší než trh spotřebitelů (B2C). Dochází zde k prodejům a nákupům ve velkém množství. Výrobky a služby, nabízené i poptávané na trhu, slouží pro další výrobu nebo poskytnutí další služby.[15]

1.18 Šifrování dat

Šifrování dat neboli kryptografie slouží pro zakódování obsahu datových nosičů, aby se člověk, který nemá klíč pro zpětné dešifrování, nemohl snadno dostat k citlivým datům. Pro šifrování se používají různé metody:

- Ruční kryptografie
    - Substituční šifry
        - Nahrazení znaku původního řetězce novým znakem.
    - Transpoziční šifry
        - Pořadí znaků v řetězci se mění podle určitých pravidel.
- Symetrická kryptografie
    - Proudové šifry
        - Algoritmus šifruje buď jednotlivé bity nebo celé byty aniž by byla známa délka celého řetězce.
    - Blokové šifry
        - Algoritmus šifruje bloky dat o délce 64, 128 nebo 256 bitů.
- Asymetrická kryptografie
    - Asymetrické kryptografické algoritmy využívají matematické jednocestné funkce:
        - Faktorizační systémy
        - Logaritmické veřejné kryptosystémy
        - Kryptosystémy na bázi eliptických křivek
- Hashovací funkce
    - Z jakkoliv dlouhého řetězce se vytvoří zkrácený identifikátor. Výstupem této funkce je blok pevné délky (128 nebo 160 bitů).
- Generátory náhodných posloupností
    - Generují se nezávislé a vzájemně spolu nesouvisející binární hodnoty.[16]

1.19 Dvoufázové ověření

Kromě klasického přihlašování uživatelským jménem a heslem jsou některé systémy chráněny dvoufázovým ověřením. Uživateli se po přihlášení zašle unikátní bezpečnostní kód na mobilní telefon nebo e-mail, který má se svým účtem spojen. Tento kód se generuje jen na dobu nezbytnou pro ověření identity a poté vyprší.[17]

1.20 Disaster recovery plan

V případě pohromy je potřebné nastavit pravidla a určit postupy, díky kterým firma minimalizuje potenciální škody a dokáže v co nejkratším čase obnovit stav firmy před pohromou. K tomu slouží Disaster recovery plan, česky plán obnovy po pohromě, který přesně určí, jak se má postupovat, aby byla firma schopna vyřešit nejrůznější možné scénáře.[18][28]

1.21 Audit kybernetické bezpečnosti

„Audit je obecně řečeno systematický, nezávislý a dokumentovaný proces pro získání důkazů z auditu a pro jeho objektivní hodnocení s cílem stanovit rozsah, v němž jsou splněna kritéria auditu“. V jednoduchosti porovnáváme současný stav s ideálním stavem stanoveným souborem politik a postupů.

Auditní tým by měl být v průběhu samotného auditu nedůvěřivý a kriticky hodnotit všechny důkazy vedoucí k výsledku auditu. Základními principy auditu jsou integrita, spravedlivé prezentování, profesionální přístup, důvěrnost, nezávislost, průkaznost.

Rozlišujeme následující druhy auditů:

- Interní
    - Audit 1. strany
        - Interní auditor posuzuje samotné procesy nastavené ve firmě a výsledek slouží pro potřebné zlepšení.
- Externí
    - Audit 2. strany
        - Audit provádí zákazník nebo organizace svého dodavatele.
    - Audit 3. strany
        - Pro účely zákonů nebo certifikace.[28]

1.22 Malware

Malware je označení pro škodlivý software. Tento software se svévolně chová v zařízení a způsobuje jeho zpomalení, vyšší využití operační paměti, zvýšenou spotřebu baterie nebo sám instaluje další programy. Takový škodlivý software se do zařízení může dostat skrze zranitelnost zabezpečení, ale nejčastěji to bývá za použití sociálního inženýrství.[20]

1.23 Phishing

Phishing je jedna z praktik sociálního inženýrství. Útočník se snaží ze své oběti dostat citlivé údaje a ty pak zneužít. Analogie vychází z průběhu útoku. Útočník nahodí „návnadu“, často ve formě podvodného e-mailu a čeká, než se někdo chytí. Jedná se tedy o „rybaření“ – fishing. Záměna ph za f vychází ze slova „phreaks“, což je hackerská skupina v USA. Samotný phising se dělí na:

- E-mail phishing
  - Zprávy rozesílané hromadně na e-mail bez konkrétní adresace.
- Spear phishing
  - Vytvoření zprávy přímo na míru díky veřejně známým informacím oběti.
- Whaling
  - Cílené útoky na manažery nebo majitele firem nebo organizací.
- CEO fraud
  - Tyto útoky jsou mířeny na nižší pozice ve firmě, které se maskují jako zprávy od vyšších manažerů.
- Vishing
  - Jedná se o útoky realizované přes telefonní hovor.
- Smishing
  - Jedná se o útok, kdy se rozesílají podvodné SMS zprávy.
- Page hijacking
  - Oběť je navedena na podvodnou webovou stránku, která zdánlivě vypadá jako ta, kterou požadují.[21]

1.24 Sociální inženýrství

Jedná se o sociotechniku, při které dochází k manipulaci a přesvědčování lidí s cílem vylákat z nich citlivé osobní údaje. Útočník manipuluje s obětí, aby u ní navodil pocit důvěryhodnosti a bylo pro něj snadné s ní pracovat. V ideálním případě pro útočníka by si oběť neměla uvědomit, že je s ní manipulováno ani po samotném útoku.[22]

1.25 CISO

Jinými slovy Chief information security officer, manažer bezpečnosti informací, je role v ISMS – systém řízení informační bezpečnosti, kdy je tato osoba odpovědná a má řídící pravomoci nad celou informační bezpečností organizace.[13]

1.26 Střední podnik

Označení střední podnik má firma dle kritérií Evropské komise, vydané v roce 2005, pokud:

- Zaměstnává do 250 zaměstnanců.
- Roční obrat je do 50 milionů EUR nebo celková bilance je do 43 milionů EUR.[24]

1.27 VLAN

VLAN, Virtual Local Area Network je jeden z nástrojů dělení sítě, aniž by se měnilo její fyzické zapojení. Takto vytvořené podsítě jsou vzájemně nedostupné. V nastavení přepínače se nastaví různé VLAN a té se přiřadí jednotlivé porty za využití Access Mode, které pak budou komunikovat pouze s porty stejné VLAN. Propojení přepínačů, aby se zachovalo nastavení VLAN a dostupnost zařízení stejné VLAN v rámci celé sítě, slouží Trunk Mode.[25]

1.28 Access mode

Access mode je konfigurace portů na přepínači, díky které přiřazujeme jednotlivým portům VLAN. Pro přepínač je možné nastavit více VLAN, ale port může být součástí jen jedné VLAN. Zařízení na druhé straně, většinou se jedná o koncové zařízení, netuší, že se v nějaké VLAN nachází, jelikož přepínač vyjme z rámce informace o VLAN.[25]

1.29 Trunk mode

Tento mód slouží pro přenášení rámců skrze více VLAN. Nejčastěji se nastavuje při propojení více přepínačů nebo ve spojení přepínač směrovač. Na obou stranách spojení musí být tento mód nastaven, aby bylo zajištěno správné zasílání rámců. Do samotného rámce je důležité vložit informaci, které VLAN je tento rámec součástí.[25]

1.30 Síťový port přepínače

Port je zdířka na přepínači, do které si připojují další síťové prvky nebo koncové uzly do Ethernetu. Port může, ale nemusí být součástí některé VLAN. Do portu lze zapojit metalické kabely nebo optické kabely, liší se v technickém provedení zásuvky. Pro Ethernet se v dnešní době stále nejčastěji používají metalické přípojky RJ-45 a již méně používané RJ-11.

1.31 Penetrační testování

Penetrační testování je takový test, při kterém se počítačový odborník, jinými slovy etický hacker, snaží překonat bezpečnostní opatření sítě, s cílem zjistit a upozornit na zranitelnosti v zabezpečení. Výsledkem je soupis trhlin, které je potřeba co nejdříve opravit. Obsah závěrečné zprávy z testování by měl znát pouze zadavatel a osoba nebo skupina provádějící samotné testování. Důvodem je ochránění firmy v případě bezpečnostních nedostatků před potenciálním využitím nedostatků a následným útokem.[26]

1.32 Outsourcing

„Outsourcingem se řeší vyčlenění činností, které nesouvisí s hlavním předmětem podnikání, za účelem uvolnění finančních prostředků, lidských zdrojů, a to externímu poskytovateli těchto činností, který je vázán smluvně zajistit tyto činnosti v určité kvalitě a za úplatu“.

V oblasti kybernetické bezpečnosti je velmi důležité vymezit pravomoci a zodpovědnosti poskytovatele těchto služeb v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti.[27]

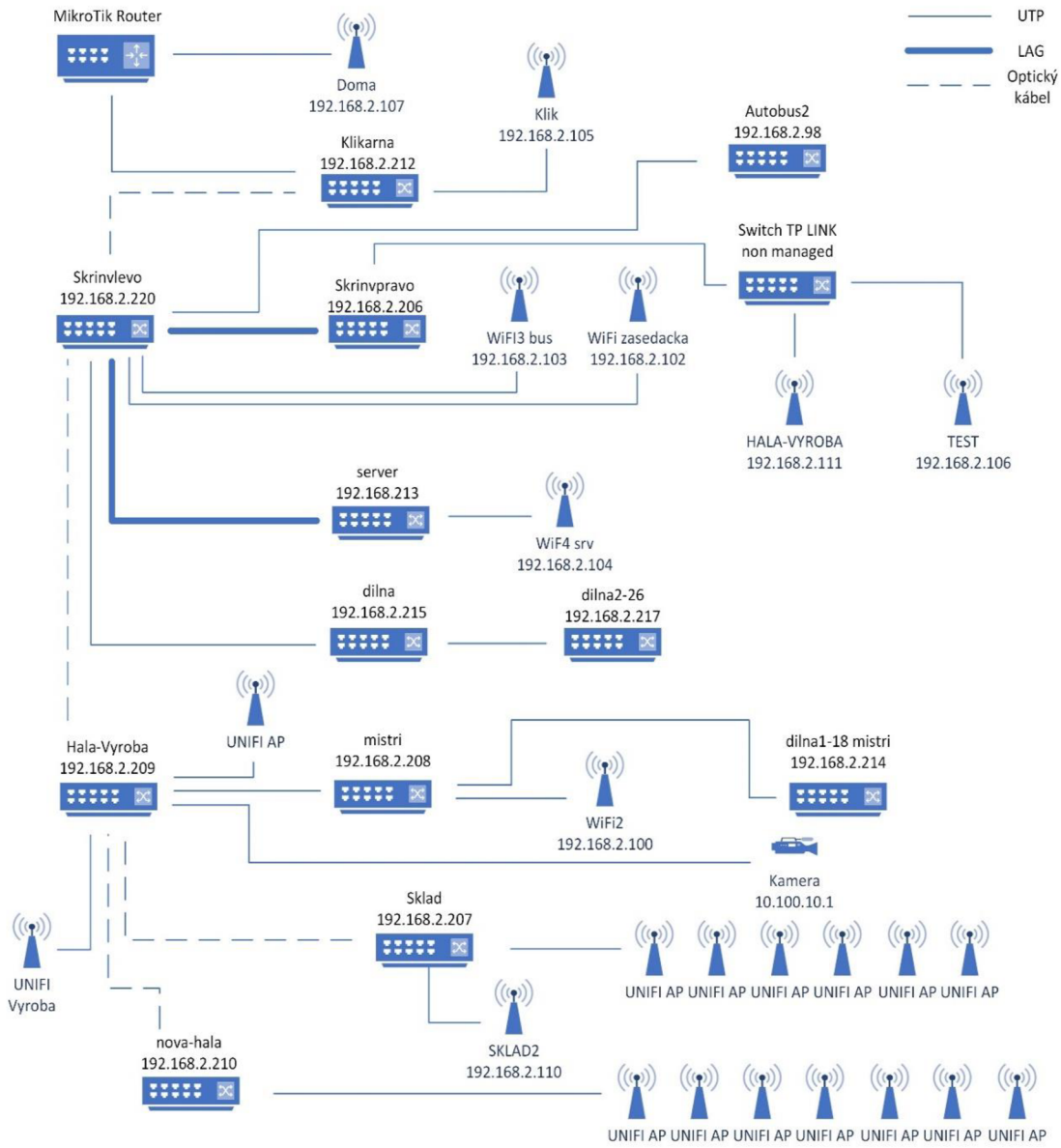
2 Popis současného stavu

2.1 Oblast technická

V následujících podkapitolách si popíšeme jednotlivé ICT vybavení firmy, topologii a logické schéma zapojení, popis hardwaru a tok dat firmy.

2.1.1 Schéma logického zapojení

Síť je realizována do zapojení hvězdy. Z routeru, který je z připojen optickým kabelem na poskytovatele internetu, je napojen switch v serveru. Z něj se postupně rozvádí připojení kabelem do jednotlivých částí firmy a zde jsou pak zapojeny koncové zařízení jako jsou firemní počítače, Wi-Fi a terminály lisů. Těchto switchů je třináct. Tři z nich jsou Power over Ethernet switche, jelikož slouží zároveň jako zdroje proudu pro UNIFI antény a jeden je Non managed. Spojení switche Skrinvlevo a Skrinvpravo je realizováno LAG zapojením. Stejně tak i Skrinvlevo a server.



Obrázek 1: Schéma logického zapojení

2.1.2 Síťové prvky

Aktivní prvek	Model	Název	Doplňující informace	Síť
Switch 1	Cisco SG300 28	Klikarna	-	192.168.2.212
Switch 2	Cisco SG300 28	Autobus2	-	192.168.2.98
Switch 3	Cisco SG300 28	Skrinvlevo	-	192.168.2.220
Switch 4	Cisco SG300 28	Skrinvpravo	-	192.168.2.206
Switch 5	Cisco SG300 28	Server	-	192.168.2.213
Switch 6	Cisco SG300 28	Dilna	-	192.168.2.215
Switch 7	Cisco SG300 28	Dilna2-26	-	192.168.2.217
Switch 8	Cisco SG300 28	Mistri	-	192.168.2.208
Switch 9	Cisco SG300 28	Hala-VYROBA	POE	192.168.2.209
Switch 10	Cisco SG300 28	Dilna1-18 mistri	-	192.168.2.214
Switch 11	Cisco SG300 28	Sklad	POE	192.168.2.207
Switch 12	Cisco SG300 28	Nova-hala	POE	192.168.2.210
Switch 13	Cisco SG300 28	TPI LINK	Non managed	-
Router	Mikrotik RB951G-2HnD	MikroTik Router	Na routeru je první nastavení firewallu	192.168.2.101
UPS	Smart UPS 1500		-	192.168.2.95

Tabulka 1: Tabulka síťových prvků

2.1.3 Server

Prvek	Model	Operační systém
Server	Supermicro E5-1620 v3	Debian 7.8 xen 4.1.4
Server	Supermicro E5-1620 v3	Debian 7.8 xen 4.1.4
Rack server	Lenovo ThinkSystem SR590 machine type 7X99CTO1WW	VMware vSphere 6 Hypervisor 6.7.0
RackStation	Synology RS812	DSM 4.0-2219
DiskStaion	Synology DS414j	DSM 6.1.4-15217
Úložný systém NAS	DS 1016RE2	Firmware 6.62B.10
APC	Back UPS 950	-

Tabulka 2: Tabulka prvků připojených v serveru

2.1.4 Koncové zařízení

Pro svoje zaměstnance vedení kupuje použité zařízení z bazarů. Dokud zařízení funguje, není důvod jej měnit za nové. Zařízení jsou tak několik let stará. Je zde tedy velké riziko napadení, jelikož hardware není aktuální a jeho ovladače již mohou být zastaralé. Opět se jedná o rozhodnutí managementu, které v tom nevidí prioritu.

2.1.5 Software na koncových zařízeních

Firma pro svoje vnitřní procesy využívá informačního systému QI. Tento informační systém dokonale plní veškeré požadavky firmy, a to v oblasti TPV a kalkulace, plánování výroby a skladování polotovarů a hotových výrobků. Veškeré návrhy součástek a dílů vytváří projektoví manažeři ve Solidworks. Pro administrativní a obchodní účely se využívají aplikace balíčku Adobe Acrobat.

Služba	Software
Operační systém	Windows 10 Home 64bit
Antivir	ESET Secure Office
Aplikace pro projektové manažery	Solidworks
Aplikace pro administrativu	Adobe Acrobat

Tabulka 3: Tabulka využívaných SW

2.1.6 Firewall

Na routeru je první úroveň nastavení firewallu, kde probíhá veškeré routování, forwarding, filtry a jiná omezení. Zároveň zde probíhá i antispam pošty. Na koncových zařízeních je nastavena druhá úroveň firewallu přes ESET konzoli.

2.1.7 Omezení provozu

Firma kromě denního provozu, kde se odehrává administrativa, objednávky a prodej, lisuje na nepřetržitý třísměnný provoz plastové díly. V noční dobu, kdy jsou všechny firemní procesy omezeny jen na obsluhu lisovacích strojů, je úplně omezen přístup na internet. Je to z důvodu, aby se operátoři nerozptylovali ničím jiným a plně se věnovali svoji pracovní náplni.

V běžné pracovní době není žádné speciální omezení. Pomocí jedné z funkcí antiviru ESET je blokována nelegální tématika webových stránek jako je erotika, zbraně, násilí a jiné.

2.1.8 Zálohování dat

Firma si svoje data zálohuje pro případ zničení nebo ztráty. Zálohování dat probíhá jednou za týden vždy v pátek po pracovní době, kdy je síť nejméně vytížená a nemůže tak dojít k narušení zálohování. Disky jsou umístěny v serverovně přímo v racku a situovány do diskových polí RAID 10.

2.1.9 Tok dat

2.1.9.1 Příjem dat

Většina komunikace probíhá přes e-mail, a ty jsou často s přílohami. Zákazníci volají na zákaznický servis v menší míře. Je to z důvodu, aby zákazník nemohl rozporovat znění svojí objednávky, archivace těchto objednávek a systémovosti, jelikož se v budoucnu může opakovat některá z objednávek, a snadno se tak dohledá a znovu zpracuje. Fyzicky se žádné flashdisky od zákazníků nebo cizích lidí do firmy nenosí. Vnitropodnikové přenosy jsou odesílání dat na server. Tato komunikace není šifrovaná.

2.1.9.2 Odesílání dat

Z firmy odchází pouze telefonická a e-mailová komunikace, v jejíž příloze jsou potřebné dokumenty. Pouze výjimečně se vynáší ven soubory na flashdisku nebo papírovou formou.

2.1.10 E-shop

Samotná firma má web pouze prezentační. Je zde přehled toho, co firma produkuje. Její minoritní produktová skupina má svůj e-shop, na kterém se nabízejí produkty zejména koncovým zákazníkům. Je zde možné vytvořit účet pro budoucí objednávky. Tento web spravuje externista. Komunikace s ním probíhá pouze elektronicky nebo telefonicky.

2.2 Oblast řízení

2.2.1 Klasifikace a ochrana informací

Firma svoje údaje pravidelně zálohuje na disk, ale k žádné kategorizaci, klasifikaci nebo šifrování nedochází. Data jsou uložena na jednom diskovém poli a nejsou nijak rozlišena. Podstatná data k provozu a obyčejná nedůležitá data jsou na stejné úrovni. Kdo si jaká data může zobrazit se realizuje pomocí udělování přístupů zaměstnanců.

2.2.2 Docházkový systém

Zaměstnanci mají svůj vlastní čip, kterým evidují příchod a odchod z firmy. Každý průchod terminálem musí být zaznamenán. Zaměstnavatel má tedy přehled o tom, kdo se v jaký čas nacházel ve firmě. Každý zaměstnanec má k sobě přiřazený právě jeden čip, který zároveň slouží pro pohyb po areálu firmy. V případě poškození nebo ztráty je zaměstnanec povinen tuto skutečnost nahlásit, aby se přístup odstranil a žádná neoprávněná osoba se nedostala do budov.

2.2.3 Udělování přístupů

Zaměstnanci při nástupu do pracovního poměru získávají přihlašovací jméno a heslo, které si musí změnit. Díky těmto údajům se dostávají do firemní sítě. Toto heslo se neměnní po intervalech, ale spíše z důvodu toho, že zaměstnanec svoje heslo zapomene. To, kam se v rámci sítě můžou zaměstnanci dostat, určují přístupová práva rozdělená podle jejich role ve firmě. Oprávnění nejsou kategorizována do tříd, pouze se podle pracovní náplně urči, co ve firemní síti bude potřebovat a podle toho bude udělen přístup. Role jsou rozděleny na:

- Kancelář
- Výroba
- Sklad

V momentě, kdy zaměstnanec ukončí pracovní poměr ve firmě, všechny jeho přístupové údaje se mažou.

2.2.4 Bezpečnostní povědomí zaměstnanců

Zaměstnanci v kanceláři i ve výrobě neprochází žádným školením o bezpečném pohybu v kyberprostoru. Vyšší management tento krok bere jako zbytečný z pohledu finanční stránky. Je tedy veliké riziko napadení skrze neopatrnost zaměstnanců. E-maily mají často přílohy, které mohou obsahovat škodlivý obsah. Na počítačích není nastavené zamykání nebo automatické odhlašování v případě delší nečinnosti.

2.2.5 Fyzické zabezpečení ve firmě

Do objektů firmy se nepovolaný člověk nedostane bez doprovodu zaměstnance. Veškeré dveře jsou na zámek, včetně serverovny. Je tedy potřeba klíčů, a ty se také dávají jen podle potřeby pracovní náplně zaměstnanců. Dříve se také používal čip, který omezoval a odděloval zaměstnance ve výrobě od administrativní části. V dnešní době od tohoto ale firma odstoupila a přístup je pro všechny stejný.

2.2.6 Disaster recovery plan

Firma nemá žádný konkrétní plán pro obnovu. Správce sítě pouze vychází z nějaké osobní zkušenosti. V případě havárie by vše řešil sám a postupoval podle logického plánu v hlavě. Nejsou zavedena ani žádná preventivní opatření. Firma nemá žádný záložní zdroj energie, který by udržoval v chodu důležité zařízení pro funkci sítě nebo výrobu. V případě výpadku lisů z jakéhokoliv důvodu přichází firma o důležité příjmy. Ve výrobní hale je umístěno 30 strojů. Ty dokáží fungovat bez terminálu, který slouží jen pro přeprogramování výroby, ale samy bez energie nepracují. Jeden takový stroj dokáže generovat zisk 5 000 Kč za hodinu. Pokud by tedy stály nečinně po dobu dvou hodin, přijde firma o potenciálních 300 000 Kč.

2.2.7 Bring your own device

Každý ze zaměstnanců dostane k vykonávání svojí práce firemní zařízení, a nemusí si tak nosit svoje vlastní. Firma tuto možnost ani nepodporuje. Co je ovšem možné je odnést si firemní zařízení domů. Toto zařízení, které se využívá pouze k administrativním nebo kancelářským procesům, je omezeno ve funkčnosti a nelze ho použít pro osobní volnočasové aktivity, jako jsou třeba počítačové hry.

2.2.8 Evidence bezpečnostních incidentů a bezpečnostních událostí

V případě výskytu bezpečnostního incidentu není připraven žádný plán postupu. Pokud se z incidentu stane událost, správce sítě nijak skutečnost neeviduje. Neexistuje tedy žádná historie, ze které by se dalo vycházet pro předejití budoucích incidentů.

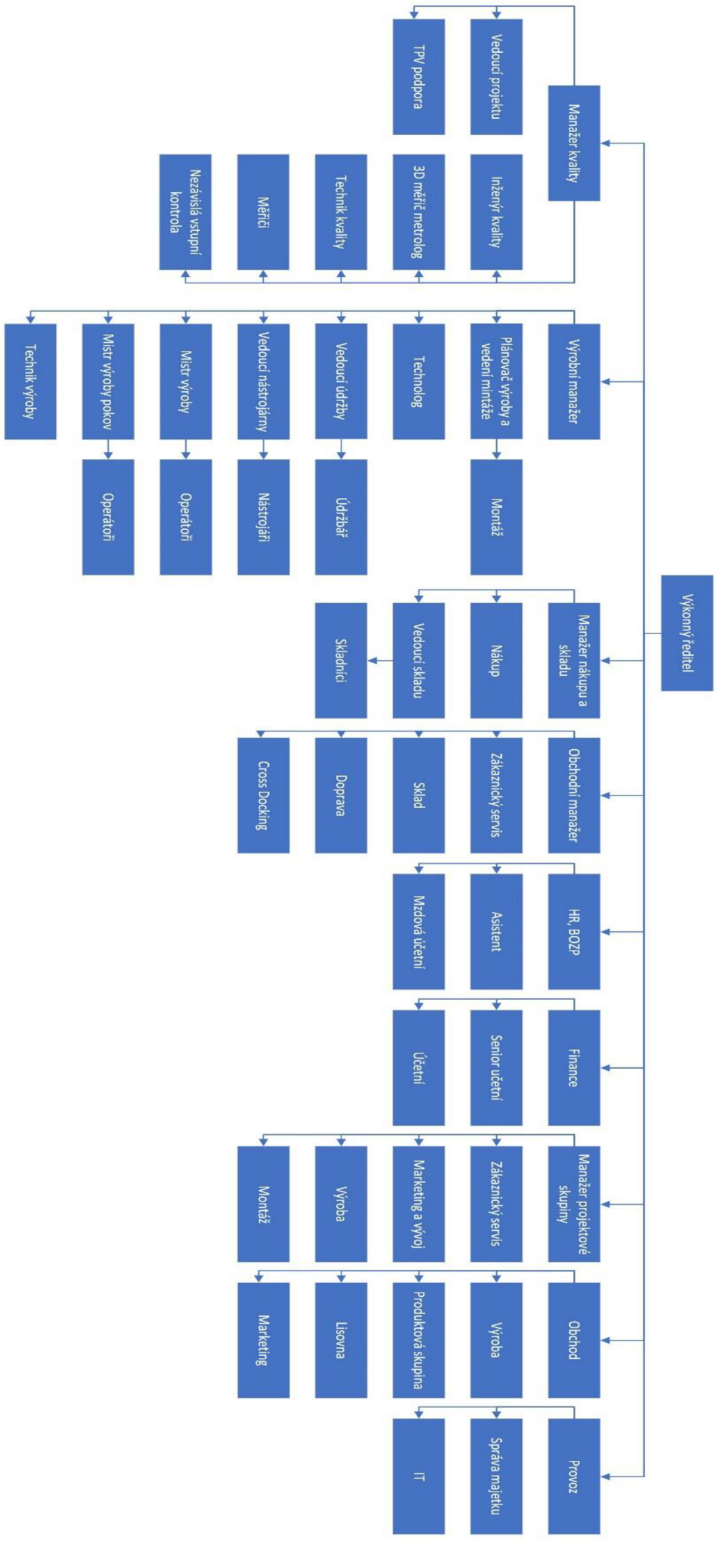
2.2.9 Personál správy sítě

Správu firemní sítě má na starosti jeden zaměstnanec. Ten řeší problematiku zapojení prvků v síti, správu firemních zařízení, obsluhu serverů a správu firemních zařízení. Vykonává tak zároveň i funkci manažera bezpečnosti ICT.

2.2.10 Dodavatelé a odběratelé

Svoje produkty firma převážně prodává jiným společnostem, které je dále využívají pro svoji výrobu. Jedná se tedy o B2B prodej. Některé svoje výrobky prodává přímo koncovým zákazníkům. Výrobu rozděluje na automotive a non automotive. Pro výrobu a lisování odebírá plastové granuláty a jiný materiál. Hotové výrobky expeduje mezinárodními i vnitrostátními dopravními společnostmi.

2.2.11 Organizační hierarchie



Obrázek 2: Organizační hierarchie

3 Analýza současného stavu

3.1 Oblast technická

Oblast	Čím plněno	Poznámka	Hodnocení
Záloha dat.	Záloha se provádí na konci každého pracovního týdne.		**Splňuje**
Segmentace sítě.	Firemní síť není nijak rozdělená.	Jediná segmentace je Wi-Fi pro hosty.	**Nesplňuje**
Antiviry.	Na zařízeních je nainstalovaný antivir.	Esset Secure office.	**Splňuje**
Aplikační bezpečnost.	Provádí se pouze penetrační testy, a to bez pravidelnosti.	Testy zajišťuje externí firma.	**Částečně splňuje**
Šifrování.	Šifrování dat na disku není zajištěno.		**Nesplňuje**
Omezení přístupu na internet.	Filtrace nelegálních témat a noční omezení přístupu na internet.	Pro noční směny je omezen přístup pouze na nezbytné procesy pro výrobu.	**Splňuje**
Aktivní blokování nežádoucí komunikace.	Zajištěno firewallem.	Nastavený antispam.	**Splňuje**
Použití dvoufázového ověření.	Zaměstnanci pro přístup do firemní sítě používají pouze přihlašovací údaje a heslo.		**Nesplňuje**
Záložní zdroj elektřiny.	Firma nemá žádný záložní generátor, který by udržoval důležité zařízení v provozu.		**Nesplňuje**
Fyzické zabezpečení serveru.	Zamykatelné dveře i samotná skříň.		Splňuje
Zabezpečení serveru proti vnějším vlivům.	Nezávislá klimatizace bez požárního hlásiče.	V místnosti je pouze hasící přístroj.	**Částečně splňuje**

Tabulka 4: Tabulka současného stavu oblasti technické

3.2 Oblast řízení

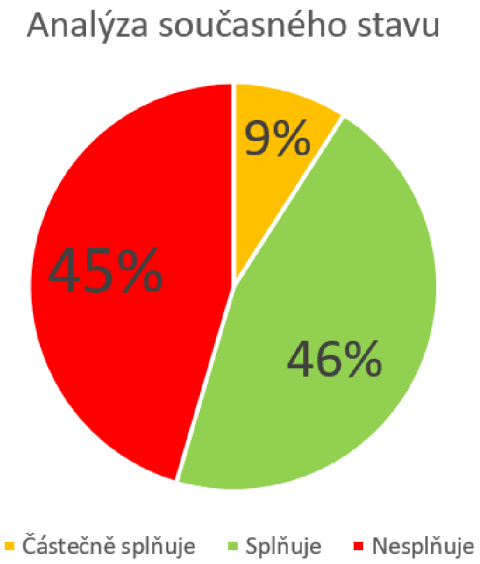
Oblast	Čím plněno	Poznámka	Hodnocení
Klasifikace informací.	Firma nijak neklasifikuje svoje data.	Přístup k datům řídí pomocí udělení rolí.	Nesplňuje
Školení zaměstnanců o bezpečnostním povědomí.	Žádné školení neprobíhá.	Management toto nepovažuje jako prioritu.	Nesplňuje
Udělování přístupů zaměstnancům.	Role v systému odpovídají pracovním pozicím.		Splňuje
Disaster recovery plan.	Firma nemá svůj plán na obnovu	Správce sítě vychází ze zkušeností.	Nesplňuje
Audit bezpečnosti ICT.	Audity bezpečnosti neprobíhají.	Management toto nepovažuje jako prioritu.	Nesplňuje
Fyzická bezpečnost.	Důležité místnosti pro chod sítě a celý areál firmy je pro veřejnost nedostupný.	Pro pohyb je potřeba klíče nebo čipu.	Splňuje
Evidence bezpečnostních incidentů.	Žádná evidence neprobíhá.		Nesplňuje
Bring your own device.	Používání vlastních zařízení firma nepodporuje.	firma poskytuje svým zaměstnancům zařízení.	Splňuje
Oddělení povinností správce.	Správce je zároveň i manažer bezpečnosti.		Nesplňuje
Evidence pohybu zaměstnanců.	Firma používá docházkový systém.	Zaměstnanec pro příchod a odchod používá čip.	Splňuje
Evidence hesel.	Hesla jsou uložena v Keypass.	Hesla se nemění pravidelně.	Splňuje

Tabulka 5: Tabulka současného stavu oblasti řízení

4 Výsledek analýzy současného stavu

4.1 Graf výsledku analýzy

Hodnocení jednotlivých bodů analýzy jsem zanesl přehledně do grafu.



Obrázek 3: Graf analýzy současného stavu

4.2 Zhodnocení výsledku analýzy

Z grafu vidíme, že firma ze 45 % nesplňuje minimální standardy bezpečnosti a 9 % jen částečně splňuje. Pouze 46 % bodů analýzy vyhovuje standardům. Nejdůležitější nedostatky jsou:

- Firma nijak neodlišuje důležitost svých dokumentů. Zaměstnanci, kteří nejsou součástí vrcholného managementu se mohou dostat k důležitým dokumentům.
- Je velké riziko napadnutí firemní sítě skrze neopatrnost zaměstnanců, kteří nemají školení o tom, jak se pohybovat v kyberprostoru.
- V případě vyskytnutí nestandartní situace není přesně popsaný postup řešení takové situace. Může dojít ke zmatkům, které povedou k větším škodám.
- Firemní zařízení se kupují z bazarů. Věk většiny počítačů přesahuje 5 let a stávají se hrozbou pro síť.
- V případě výpadku elektrické sítě není firma zajištěna náhradním zdrojem energie. Uniklé potenciální zisky v době nečinnosti strojů mohou být velmi vysoké.

V praktické části této práce rozeberu všechny nedostatky a navrhnu řešení, které bude splňovat minimální standardy zabezpečení vydané Národním úřadem kybernetické a informační bezpečnosti.

5 Vlastní návrh řešení

V této části navrhnu řešení u některých bodů tak, aby splňovaly minimální bezpečnostní standardy vydané Národním úřadem kybernetické a informační bezpečnosti.[37]

5.1 Školení zaměstnanců

V dnešní době je mnoho mallware a phishing útoků vedených přímo na uživatele, protože to je největší slabina každého zabezpečení firemní sítě. Zkoumaná firma uchovává důležitá data počínaje údajích o zaměstnancích až po výrobní plány a strategie. Vyzrazením těchto dokumentů by mohla firma přijít o svoji konkurenční výhodu. Proto se zaměřím na školení zaměstnanců. Cílem tedy bude zvýšit povědomí o bezpečnosti u všech zaměstnanců, aby nedocházelo k vyzrazení firemních údajů, úmyslnému či neúmyslnému změnění dat nebo dokonce ztráty či zničení dat.

5.1.1 Vytvoření programu školení

Vzhledem k tomu, že firma nikdy předtím svoje zaměstnance neškolila a tito zaměstnanci mají velmi nízké povědomí o bezpečnosti, musím stanovit rozsah, který toto školení bude dodržovat. Abych co nejvíce snížil riziko spojené s nedostatečným vyškolením zaměstnanců, musí se program týkat následujících částí:

- Problematika uzamykání zařízení
- Sociální inženýrství
- Důvěryhodná komunikace a škodlivé přípony
- Stahování neznámých souborů

5.1.2 Očekávané přínosy

Jak je obecně známo, největší slabinou každého zabezpečení firemní sítě jsou samotní uživatelé. Útočníci často využívají sociálního inženýrství, aby se dostali tam, kam potřebují a chtějí. Přínosem bude dobře vyškolený pracovník, který dokáže rozpoznat hrozbu a snížit riziko spojené s ní. Sníží se i riziko úniku, zničení nebo modifikace firemních dat. Zaměstnanec si bude vědom svých povinností a zodpovědností ve firemní síti, rozpoznat škodlivý email a různé způsoby útoků.

5.1.3 Role a odpovědnosti ve školícím programu

Zkoumaná firma je počtem zaměstnanců chápána jako střední podnik. Pro školení o povědomí o kybernetické bezpečnosti zvolím centralizovaný model. Veškerá odpovědnost a řízení bude záviset na jednom člověku – CISO, v našem případě to bude správce sítě. Tento člověk zajistí, že každý zaměstnanec splní svoji část školení a prokáže se certifikátem, kterým dokáže, že školení dokončil.

Zaměstnance rozdělím do skupin, podle kterých jim budu přiřazovat jednotlivá školení. Tato školení budou odpovídat jejich pracovní náplni a zodpovědnostem. Rozdělení provedu následovně:

Nejdříve vytvořím skupiny podle toho, jaké mají zodpovědnosti:

Skupina	Odpovědnost ve firmě
Skupina A	Žádná nebo minimální práce se zařízením.
Skupina B	Práce s nedůležitými daty.
Skupina C.1	Práce s firemními finančními daty.
Skupina C.2	Práce s firemními výrobními daty.
Skupina C.3	Práce s firemními obchodními daty.
Skupina D	Práce s daty zákazníků.
Skupina E	Práce s daty zaměstnanců.

Tabulka 6: Tabulka rozdělení skupin dle odpovědností

Skupina A – Zaměstnanec nepoužívá žádné zařízení připojené k síti nebo jeho pracovní náplň nespočívá v práci s daty.

Skupina B – Zaměstnanec má přístup k firemní síti, avšak data, se kterými pracuje, nejsou pro firmu nijak významná.

Skupina C.1 – Finanční data jsou data o finančních tocích firmy, bankovní účty a přístupy k nim a finanční plány na další období.

Skupina C.2 – Výrobní data jsou data, která slouží operátorům k výrobě jednotlivých polotovarů a výrobků.

Skupina C.3 – Obchodní data jsou ta data, která se prezentují zákazníkům a slouží jako portfolio firmy.

Skupina D – Zaměstnanec pracuje s údaji odběratelů a dodavatelů.

Skupina E – Zaměstnanec má přístup k citlivým údajům zaměstnanců.

Dále si dle hierarchického schématu (obr. 2) přiřadím jednotlivým pracovním pozicím ve firmě skupiny.

Pracovní pozice	Skupina A	Skupina B	Skupina C			Skupina D	Skupina E
			C.1	C.2	C.3		
Provoz	X						
Sklad	X	X		X			
Výroba	X	X		X			
Údržba	X						
Technická příprava výroby		X		X			
Projektoví manažeři		X		X	X	X	
Oddělení kvality		X		X		X	
Technolog		X		X			
Nástrojaři	X	X		X			
Nákup		X		X	X	X	
Zákaznický servis		X			X	X	
Doprava	X						
HR		X	X				X
Účetní		X	X			X	X
Finance		X	X				
CISO		X	X	X	X	X	X
Obchodní zástupce		X			X	X	
Vedoucí sekcí – manažeři		X	X	X	X	X	X
Ředitel		X	X	X	X	X	

Tabulka 7: Tabulka přiřazení skupin pracovním pozicím

5.1.4 Výběr školícího programu a zhodnocení nákladů

Výběrem kvalitního školícího programu je jednou z cest snížení rizika napadení škodlivým softwarem. Jednou z podmínek vedení je vybrat takové školení, které bude pro firmu představovat co možná nejnižší náklady, ideálně žádné. Na trhu je několik variant, v následující tabulce uvedu nějaké příklady. Kurzy jsem vybíral tak, aby zaměstnanci získali povědomí a byly splněny očekávané přínosy.

Platforma	Cena	Cena celkem (ročně)	Místo konání
Cybersec	120 Kč / osoba / rok	18 000 Kč	Online
Instructor	70 Kč / osoba / rok	10 500 Kč	Online
GOPAS	7800 Kč / workshop	7800 Kč	Praha
NÚKIB	Zadarmo	-	Online

Tabulka 8: Tabulka porovnání školení

Dle mého názoru je nejlepším řešením školení od Cybersec, jelikož obsah školení splňuje nad rámec našich očekávaných přínosů. Výhodou je i to, že školení je realizováno formou e-learningového kurzu a je možné jej udělat přímo v areálu firmy a není třeba jezdit na workshop.

Abych ale splnil požadavky firmy na minimalizaci nákladů, volím online kurzy od Národního úřadu kybernetické a informační bezpečnosti. Jejich kurzy jsou zadarmo a výstupem je závěrečný test, po kterém zaměstnanec získá certifikát, který jej osvědčuje o splnění školení. Tento certifikát má z důvodu aktuálnosti platnost pouze 2 roky a zaměstnanci jej budou muset pravidelně aktualizovat. Jednotlivé moduly tohoto školení splňují očekávané přínosy.[30,31,32,33]

5.1.5 Přidělení školících programů pracovním pozicím

Nyní na základě pracovní pozice přidělím školící program, který nabízí NÚKIB. Jeho studijní materiály začínají u doporučení formou plakátů s názvem Bezpečný pohyb v kybersvětě, až po školení pro manažery. Doporučení bude stačit pro ty zaměstnance, kteří nepracují s důležitými daty. Povědomí o kybernetické bezpečnosti bude stačit na minimální úrovni. Pro zaměstnance, kteří denně pracují s důležitými daty, vyberu program nazvaný „Dávej kyber“, díky kterému se dozví veškeré důležité informace, jak předejít potenciálním útokům na firemní síť. Pro manažerské pozice a ředitele, včetně CISO, je vhodný program „Šéfuj kyber“. Nyní vytvořím tabulku, kde přehledně zobrazím přidělené programy.

Pracovní pozice	Bezpečný pohyb v kybersvětě	„Dávej kyber“	„Šéfuj kyber“
Provoz	X		
Sklad	X	X	
Výroba	X	X	
Údržba	X		
Technická příprava výroby	X	X	
Projektoví manažeři	X	X	
Oddělení kvality	X	X	
Technolog	X	X	
Nástrojaři	X	X	
Nákup	X	X	
Zákaznický servis	X	X	
Doprava	X		
HR	X	X	
Účetní	X	X	
Finance	X	X	
CISO	X	X	X
Obchodní zástupce	X	X	
Vedoucí sekcí – manažeři	X	X	X
Ředitel	X	X	X

Tabulka 9: Tabulka přiřazení školících programů

5.1.6 Bezpečný pohyb v kybersvětě

Na stránkách jsou pro veřejnost volně ke stažení plakáty, které mají poskytnout základní přehled o nástrahách v kybersvětě. Tyto plakáty je možné rozeslat každému zaměstnanci v příloze e-mailu, nebo je vyvěsit ve společných prostorách firmy, aby je každý zaměstnanec měl na očích.[38]

BEZPEČNÝ POHYB V KYBERSVĚTĚ

JAK SI ZABEZPEČÍM POČÍTAČ NEBO SMARTPHONE?

OMEZÍM PŘÍSTUP DALŠÍCH OSOB K SOUKROMÝM I PRACOVNÍM ZAŘÍZENÍM.

CHRÁNÍM SVÁ DATA PRO PŘÍPAD ODCIZENÍ ČI ZTRÁTY ZAŘÍZENÍ.
Využívám silné heslo, číselný kód, gesto nebo jiný způsob zabezpečení.

NIKDY SI NEUKLÁDÁM PŘIHLAŠOVACÍ ÚDAJE K ZAŘÍZENÍM A ÚČTŮM V JEJICH BLÍZKOSTI.
Pro uchování přihlašovacích údajů používám šifrovaného správce hesel.

UJISTÍM SE, ŽE PŘI ZADÁVÁNÍ PŘIHLAŠOVACÍCH ÚDAJŮ JE NIKDO CIZÍ NEVIDÍ, NAPŘÍKLAD POHLEDEM PŘES RAMENO.

ZAMKNU ZAŘÍZENÍ POKAŽDÉ, KDYŽ OD NĚJ ODCHÁZÍM.
U počítače s Windows je nejjednodušší způsob rychlého zamknutí klávesová zkratka WIN + L a u mobilního zařízení stisknutí vypínacího tlačítka na jeho boku. Pokud odcházím na delší dobu, ukončím správce hesel a všechny doposud používané aplikace a služby s citlivými údaji jako e-mail nebo internetové bankovnictví.

AKTUALIZUJI SOFTWARE A NEVYPÍNÁM PRAVIDELNÉ AUTOMATICKÉ AKTUALIZACE SYSTÉMU.
Díky tomu zajistím opravu známých zranitelností, které by mohly ohrozit mé zařízení.

POUŽÍVÁM AKTUALIZOVANÝ ANTIVIROVÝ SOFTWARE A FIREWALL.

ZAPÍNÁM WI-FI, BLUETOOTH, NFC A DALŠÍ BEZDRÁTOVÉ TECHNOLOGIE, JEN POKUD JE VYUŽÍVÁM.
Pro útočníka představují potenciální cestu do zařízení.

POKUD VYUŽÍVÁM NEZABEZPEČENOU WI-FI SÍŤ, VYUŽÍVÁM TZV. VPN (VIRTUAL PRIVATE NETWORK) NEBOLI VIRTUÁLNÍ SOUKROMOU SÍŤ, KTERÁ ZABEZPEČÍ MOU KOMUNIKACI NA POTENCIÁLNĚ NEBEZPEČNÉ SÍTI.

ŠIFRUJI CITLIVÁ DATA NA EXTERNÍM DISKU A DALŠÍCH PŘENOSNÝCH ZAŘÍZENÍCH.
Tak budou v případě ztráty nebo odcizení nečitelná.

PRAVIDELNĚ ZÁLOHUJI DATA.
Využít mohu například externí disk. Důležité je, aby záloha byla na jiném místě než v mém zařízení, byla šifrována a připojena pouze v okamžiku zálohování.

DO MÝCH ZAŘÍZENÍ NEPŘIPOJUJI NEZNÁMÉ USB FLASH DISKY, EXTERNÍ DISKY A JINÁ PAMĚŤOVÁ ZAŘÍZENÍ.
Mohou obsahovat malware. V případě nutnosti připojit neznámé médium provedu jeho antivirovou kontrolu. Zaměstnavatel může k tomuto účelu poskytnout tzv. antivirovou pračku, tedy počítač bez připojení k internetu, kde je nainstalovaný aktualizovaný antivirový program.

PŘI PROCHÁZENÍ WEBU PREFERUJI WEBOVÉ STRÁNKY ZABEZPEČENÉ POMOCÍ PROTOKOLU HTTPS.
Https protokol poznáme podle zámečku v adresním řádku:

Stránky zabezpečeně pomocí HTTPS

~~https://~~ Stránky s částečným šifrováním, nebo bez něj. Nedoporučeno pro odesílání citlivých dat.

DÁVÁM POZOR, NA KTERÉ ODKAZY KLIKÁM.
Je-li to technicky možné, zkontroluji, že odkaz nevede na pozdeřelou URL adresu. Pokud nemohu ověřit, kam odkaz vede, neklikám na něj.

VYPÍNÁM NEŽÁDOUCÍ SLUŽBY OPERAČNÍHO SYSTÉMU.
Například monitorování polohy, odesílání diagnostických dat, ovládání vzdáleného počítače na dálku, apod.

JAK MÁM SPRÁVNĚ A BEZPEČNĚ KOMUNIKOVAT?

K INFORMACÍM NA INTERNETU PŘISTUPUJI KRITICKY, NEMUSÍ BÝT PRAVDIVÉ.
Při práci s informacemi mohu využít rady, které sepsala iniciativa **ZVOLSLINFO** ve svém **Surfařově průvodci internetem**.

NEZVEŘEJŇUJI OSOBNÍ ANI CITLIVÉ INFORMACE O MNĚ, MÉ RODINĚ, PŘÁTELÍCH NEBO SPOLUPRACOVNÍCÍCH.
Data narození, náboženské vyznání nebo fotografie mohou být zneužity.

INTIMNÍ FOTOGRAFIE A VIDEA NEVYTVÁŘÍM, NEUMISŤUJI JE NA INTERNET ANI JE NIKOMU NEPOSÍLÁM.
Nikdy nevím, kdy může být takový materiál zneužit.

PŘI KOMUNIKACI SI VŽDY OVĚŘUJI IDENTITU PROTISTRANY.
Mohu se zeptat přátel nebo si dotyčného vyhledat na internetu. Pokud si nejsem jist, zda mi skutečně volají například z IT oddělení naší instituce, nebo mě po telefonu úkoluje nadřízený, kterého neznám, zavěsím a zavolám zpátky na telefonní číslo z oficiálního seznamu.

NIKDY NEOTEVÍRÁM PHISHINGOVÉ E-MAILY A PODEZŘELÉ PŘÍLOHY A INFORMUJI IT ODDĚLENÍ.
V práci podezřelý e-mail neotevírám a informuji o něm IT oddělení. Stejně tak neotevírám podezřelé přílohy. Pokud mi takový e-mail dorazí do mé osobní schránky, mohu to nahlásit provozovateli schránky.

JAK PHISHING POZNÁM?
"Phishing je podvodná technika, prostřednictvím které se útočníci snaží například získat mé osobní nebo citlivé informace (přihlašovací údaje, datum narození, číslo platební karty atd.), nasměrovat mě na podvodnou stránku, nebo mi zaslat závadnou přílohu. Phishing se nejčastěji šíří formou e-mailových zpráv, které vypadají jako odeslané z důvěryhodných institucí." Podvodník používá obecná oslovení typu „Vážený pane/i" bez uvedeného jména, v textu e-mailu mohou být gramatické, stylistické a grafické chyby, obsahuje podezřele vyhlížející odkazy typu https://www.xbamka.cz.

V KOMUNIKACI NEJSEM ZBYTEČNĚ SDÍLNÝ.
Vše, co na sebe prozradím, může být zneužito.

NENÍ OBĚD ZADARMO A TO ANI V ONLINE SVĚTĚ.
Zpozorním, jsou-li mi zdarma nabízeny jindy placené služby nebo produkty. Pokud za produkt neplatím, jde o má data.

RANSOMWARE JE PROGRAM, KTERÝ ZAŠIFRUJE DATA NEBO CELÝ OPERAČNÍ SYSTÉM A NABÍZÍ JEJICH ZPŘÍSTUPNĚNÍ AŽ PO ZAPLACENÍ VÝKUPNÉHO.
Do zařízení se mi může takový program dostat po otevření neznámé přílohy v e-mailu, z webového prohlížeče nebo tím, že navštívím infikovanou webovou stránku. Před známými druhy ransomware mě chrání aktualizovaný antivirový program. Svá data chráním také pravidelným zálohováním.

PŘI KOMUNIKACI NESPĚCHÁM A VŠE SI PROMYSLÍM.
Útočníci rádi pracují s časovou tísní - teď je třeba něco vykonat, napravit, sdělit. Klid! Škoda z prodlení bývá menší, než důsledky neuvážených činů.

JAK ZABEZPEČÍM MÉ ONLINE ÚČTY?

PŘÍSTUPY K PRACOVNÍM I OSOBNÍM ÚČTŮM SI CHRÁNÍM SILNÝM HESLEM.
Hesla nikdy nepíšu na papírky a nenechávám například na monitoru nebo pod klávesnicí. To platí jak v kanceláři, tak i doma.

U SILNÉHO HESLA ZADÁVÁM ALESPOŇ 12 ZNAKŮ A VÍCE.
Při jeho tvorbě jsem originální a kreativní. Využívám malá a velká písmena, číslice, speciální znaky a další symboly. Mohu si zvolit například unikátní větu nebo souvětí, které si lze snadno zapamatovat.

PRO KAŽDOU SLUŽBU POUŽÍVÁM JINÉ UNIKÁTNÍ HESLO.
To platí u pracovních účtů a zařízení bez výjimky. V soukromí se této zásady držím u služeb, které mohou obsahovat osobní a citlivé informace.

NEVYUŽÍVÁM ONLINE NÁSTROJE ČI SLUŽBY PRO KONTROLU SÍLY HESLA.
Výsledkem může být to, že heslo předám útočníkovi, který si díky tomu doplní vlastní databázi používaných hesel.

PROTOŽE JE OBTÍŽNÉ ZAPAMATOVAT SI VŠECHNA HESLA, VYUŽÍVÁM PRO TA MÉNĚ VÝZNAMNÁ SPRÁVCE HESEL.
Ten mi umožňuje bezpečně uložit a spravovat velké množství hesel. Přístup do něj je chráněn jedním silným zastřešujícím heslem ideálně v kombinaci s vícefaktorovým ověřením.

NESDÍLÍM PŘIHLAŠOVACÍ ÚDAJE K VLASTNÍM ÚČTŮM A SLUŽBÁM.
V případě pracovního e-mailu, pracovního intranetu, docházkového systému nebo hesla do počítače může mít takové jednání závažné následky.

U KRITICKÝCH SLUŽEB JAKO ELEKTRONICKÉ BANKOVNICTVÍ, PRACOVNÍ NEBO SOUKROMÝ E-MAIL VŽDY VYUŽÍVÁM VÍCEFAKTOROVOU AUTENTIZACI.
Příkladem může být elektronické bankovnictví, kdy musím přihlášení v prohlížeči potvrdit zadáním kontrolní SMS nebo potvrzením výzvy v mém mobilním telefonu. Pokud se do služby přihlašuji z mobilního telefonu, nechám si potvrzovací SMS zaslat na jiné zařízení.

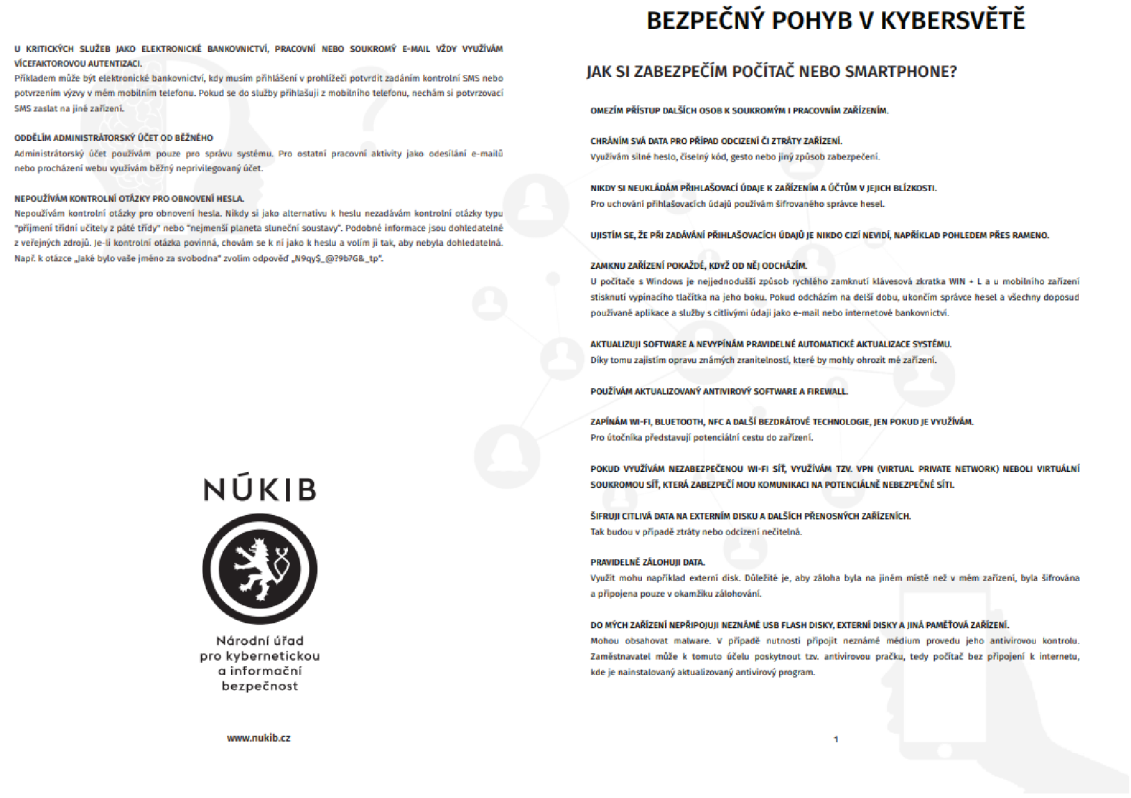
ODDĚLÍM ADMINISTRÁTORSKÝ ÚČET OD BĚŽNÉHO
Administrátorský účet používám pouze pro správu systému. Pro ostatní pracovní aktivity jako odesílání e-mailů nebo procházení webu využívám běžný neprivilegovaný účet.

NEPOUŽÍVÁM KONTROLNÍ OTÁZKY PRO OBNOVENÍ HESLA.
Nepoužívám kontrolní otázky pro obnovení hesla. Nikdy si jako alternativu k heslu nezadávám kontrolní otázky typu "příjmení třídní učitelky z páté třídy" nebo "nejmenší planeta sluneční soustavy". Podobně informace jsou dohledatelné z veřejných zdrojů. Je-li kontrolní otázka povinná, chovám se k ní jako k heslu a volím ji tak, aby nebyla dohledatelná. Např. k otázce „Jaké bylo vaše jméno za svobodna" zvolím odpověď „N9qy$_@?9b7G&_tp".

www.nukib.cz

Národní úřad pro kybernetickou a informační bezpečnost

Obrázek 4: Ukázka plakátu Bezpečný pohyb v kybersvětě 1



U KRITICKÝCH SLUŽEB JAKO ELEKTRONICKÉ BANKOVNICTVÍ, PRACOVNÍ NEBO SOUKROMÝ E-MAIL VŽDY VYUŽÍVÁM VÍCEFAKTOROVOU AUTENTIZACI.
Příkladem může být elektronické bankovnictví, kdy musím přihlášení v prohlížeči potvrdit zadáním kontrolní SMS nebo potvrzením výzvy v mém mobilním telefonu. Pokud se do služby přihlašuji z mobilního telefonu, nechám si potvrzovací SMS zaslat na jiné zařízení.

ODDĚLÍM ADMINISTRÁTORSKÝ ÚČET OD BĚŽNÉHO
Administrátorský účet používám pouze pro správu systému. Pro ostatní pracovní aktivity jako odesílání e-mailů nebo procházení webu využívám běžný nepriviegovaný účet.

NEPOUŽÍVÁM KONTROLNÍ OTÁZKY PRO OBNOVENÍ HESLA.
Nepoužívám kontrolní otázky pro obnovení hesla. Nikdy si jako alternativu k heslu nezadávám kontrolní otázky typu "příjmení třídní učitelky z páté třídy" nebo "nejmenší planeta sluneční soustavy". Podobné informace jsou dohledatelné z veřejných zdrojů. Je-li kontrolní otázka povinná, chovám se k ní jako k heslu a volím ji tak, aby nebyla dohledatelná. Např. k otázce „Jaké bylo vaše jméno za svobodna" zvolím odpověď „N9qyS_@79bPG&_tp".

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

www.nukib.cz

BEZPEČNÝ POHYB V KYBERSVĚTĚ

JAK SI ZABEZPEČÍM POČÍTAČ NEBO SMARTPHONE?

OMEZÍM PŘÍSTUP DALŠÍCH OSOB K SOUKROMÝM I PRACOVNÍM ZAŘÍZENÍM.

CHRÁNÍM SVÁ DATA PRO PŘÍPAD ODCIZENÍ ČI ZTRÁTY ZAŘÍZENÍ.
Využívám silné heslo, číselný kód, gesto nebo jiný způsob zabezpečení.

NIKDY SI NEUKLÁDÁM PŘIHLAŠOVACÍ ÚDAJE K ZAŘÍZENÍM A ÚČTŮM V JEJICH BLÍZKOSTI.
Pro uchování přihlašovacích údajů používám šifrovaného správce hesel.

UJISTÍM SE, ŽE PŘI ZADÁVÁNÍ PŘIHLAŠOVACÍCH ÚDAJŮ JE NIKDO CIZÍ NEVIDÍ, NAPŘÍKLAD POHLEDEM PŘES RAMENO.

ZAMKNU ZAŘÍZENÍ POKAŽDÉ, KDYŽ OD NĚJ ODCHÁZÍM.
U počítače s Windows je nejjednodušší způsob rychlého zamknutí klávesová zkratka WIN + L a u mobilního zařízení stisknutí vypínacího tlačítka na jeho boku. Pokud odcházím na delší dobu, ukončím správce hesel a všechny doposud používané aplikace a služby s citlivými údaji jako e-mail nebo internetové bankovnictví.

AKTUALIZUJI SOFTWARE A NEVYPÍNÁM PRAVIDELNÉ AUTOMATICKÉ AKTUALIZACE SYSTÉMU.
Díky tomu zajistím opravu známých zranitelností, které by mohly ohrozit mé zařízení.

POUŽÍVÁM AKTUALIZOVANÝ ANTIVIROVÝ SOFTWARE A FIREWALL.

ZAPÍNÁM WI-FI, BLUETOOTH, NFC A DALŠÍ BEZDRÁTOVÉ TECHNOLOGIE, JEN POKUD JE VYUŽÍVÁM.
Pro útočníka představují potenciální cestu do zařízení.

POKUD VYUŽÍVÁM NEZABEZPEČENOU WI-FI SÍŤ, VYUŽÍVÁM TZV. VPN (VIRTUAL PRIVATE NETWORK) NEBOLI VIRTUÁLNÍ SOUKROMOU SÍŤ, KTERÁ ZABEZPEČÍ MOU KOMUNIKACI NA POTENCIÁLNĚ NEBEZPEČNÉ SÍTI.

ŠIFRUJI CITLIVÁ DATA NA EXTERNÍM DISKU A DALŠÍCH PŘENOSNÝCH ZAŘÍZENÍCH.
Tak budou v případě ztráty nebo odcizení nečitelná.

PRAVIDELNĚ ZÁLOHUJI DATA.
Využít mohu například externí disk. Důležité je, aby záloha byla na jiném místě než v mém zařízení, byla šifrována a připojena pouze v okamžiku zálohování.

DO MÝCH ZAŘÍZENÍ NEPŘIPOJUJI NEZNÁMÉ USB FLASH DISKY, EXTERNÍ DISKY A JINÁ PAMĚŤOVÁ ZAŘÍZENÍ.
Mohou obsahovat malware. V případě nutnosti připojit neznámé médium provedu jeho antivirovou kontrolu. Zaměstnavatel může k tomuto účelu poskytnout tzv. antivirovou pračku, tedy počítač bez připojení k internetu, kde je nainstalovaný aktualizovaný antivirový program.

1

Obrázek 5: Ukázka plakátu Bezpečný pohyb v kybersvětě 2

PŘI PROCHÁZENÍ WEBU PREFERUJI WEBOVÉ STRÁNKY ZABEZPEČENÉ POMOCÍ PROTOKOLU HTTPS.
Https protokol poznáme podle zámečku v adresním řádku:

Stránky zabezpečené pomocí HTTPS

~~https://~~ Stránky s částečným šifrováním, nebo bez něj. Nedoporučeno pro odesílání citlivých dat.

DÁVÁM POZOR, NA KTERÉ ODKAZY KLIKÁM.
Je-li to technicky možné, zkontroluji, že odkaz nevede na pozdeřelou URL adresu. Pokud nemohu ověřit, kam odkaz vede, neklikám na něj.

VYPÍNÁM NEŽÁDOUCÍ SLUŽBY OPERAČNÍHO SYSTÉMU.
Například monitorování polohy, odesílání diagnostických dat, ovládání vzdáleného počítače na dálku, apod.

JAK MÁM SPRÁVNĚ A BEZPEČNĚ KOMUNIKOVAT?

K INFORMACÍM NA INTERNETU PŘISTUPUJI KRITICKY, NEMUSÍ BÝT PRAVDIVÉ.
Při práci s informacemi mohu využít rady, které sepsala iniciativa ZVOLSI.INFO ve svém Surfařově průvodci internetem.

NEZVEŘEJŇUJI OSOBNÍ ANI CITLIVÉ INFORMACE O MNĚ, MÉ RODINĚ, PŘÁTELÍCH NEBO SPOLUPRACOVNÍCÍCH.
Data narození, náboženské vyznání nebo fotografie mohou být zneužity.

INTIMNÍ FOTOGRAFIE A VIDEA NEVYTVÁŘÍM, NEUMISŤUJI JE NA INTERNET ANI JE NIKOMU NEPOSÍLÁM.
Nikdy nevím, kdy může být takový materiál zneužit.

PŘI KOMUNIKACI SI VŽDY OVĚŘUJI IDENTITU PROTISTRANY.
Mohu se zeptat přátel nebo si dotyčného vyhledat na internetu. Pokud si nejsem jist, zda mi skutečně volají například z IT oddělení naší instituce, nebo mě po telefonu úkoluje nadřízený, kterého neznám, zavěsím a zavolám zpátky na telefonní číslo z oficiálního seznamu.

NIKDY NEOTEVÍRÁM PHISHINGOVÉ E-MAILY A PODEZŘELÉ PŘÍLOHY A INFORMUJI IT ODDĚLENÍ.
V práci podezřelý e-mail neotevírám a informuji o něm IT oddělení. Stejně tak neotevírám podezřelé přílohy. Pokud mi takový e-mail dorazí do mé osobní schránky, mohu to nahlásit provozovateli schránky.

JAK PHISHING POZNÁM?
"Phishing je podvodná technika, prostřednictvím které se útočníci snaží například získat mé osobní nebo citlivé informace (přihlašovací údaje, datum narození, číslo platební karty atd.), nasměrovat mě na podvodnou stránku, nebo mi zaslat závadnou přílohu. Phishing se nejčastěji šíří formou e-mailových zpráv, které vypadají jako odeslané z důvěryhodných institucí." Podvodník používá obecná oslovení typu „Vážený pane/i" bez uvedeného jména, v textu e-mailu mohou být gramatické, stylistické a grafické chyby, obsahuje podezřelé vyhlížející odkazy typu https://www.xbamka.cz.

V KOMUNIKACI NEJSEM ZBYTEČNĚ SDÍLNÝ.
Vše, co na sebe prozradím, může být zneužito.

NENÍ OBĚD ZADARMO A TO ANI V ONLINE SVĚTĚ.
Zpozorním, jsou-li mi zdarma nabízeny jindy placené služby nebo produkty. Pokud za produkt neplatím, jde o má data.

RANSOMWARE JE PROGRAM, KTERÝ ZAŠIFRUJE DATA NEBO CELÝ OPERAČNÍ SYSTÉM A NABÍZÍ JEJICH ZPŘÍSTUPNĚNÍ AŽ PO ZAPLACENÍ VÝKUPNÉHO.
Do zařízení se mi může takový program dostat po otevření neznámé přílohy v e-mailu, z webového prohlížeče nebo tím, že navštívím infikovanou webovou stránku. Před známými druhy ransomware mě chrání aktualizovaný antivirový program. Svá data chráním také pravidelným zálohováním.

PŘI KOMUNIKACI NESPĚCHÁM A VŠE SI PROMYSLÍM.
Útočníci rádi pracují s časovou tísní – teď je třeba něco vykonat, napravit, sdělit. Klid! Škoda z prodlení bývá menší, než důsledky neuvážených činů.

JAK ZABEZPEČÍM MÉ ONLINE ÚČTY?

PŘÍSTUPY K PRACOVNÍM I OSOBNÍM ÚČTŮM SI CHRÁNÍM SILNÝM HESLEM.
Hesla nikdy nepíšu na papírky a nenechávám například na monitoru nebo pod klávesnicí. To platí jak v kanceláři, tak i doma.

U SILNÉHO HESLA ZADÁVÁM ALESPOŇ 12 ZNAKŮ A VÍCE.
Při jeho tvorbě jsem originální a kreativní. Využívám malá a velká písmena, číslice, speciální znaky a další symboly. Mohu si zvolit například unikátní větu nebo souvětí, které si lze snadno zapamatovat.

PRO KAŽDOU SLUŽBU POUŽÍVÁM JINÉ UNIKÁTNÍ HESLO.
To platí u pracovních účtů a zařízení bez výjimky. V soukromí se této zásady držím u služeb, které mohou obsahovat osobní a citlivé informace.

NEVYUŽÍVÁM ONLINE NÁSTROJE ČI SLUŽBY PRO KONTROLU SÍLY HESLA.
Výsledkem může být to, že heslo předám útočníkovi, který si díky tomu doplní vlastní databázi používaných hesel.

PROTOŽE JE OBTÍŽNÉ ZAPAMATOVAT SI VŠECHNA HESLA, VYUŽÍVÁM PRO TA MÉNĚ VÝZNAMNÁ SPRÁVCE HESEL.
Ten mi umožňuje bezpečně uložit a spravovat velké množství hesel. Přístup do něj je chráněn jedním silným zastřešujícím heslem ideálně v kombinaci s vícefaktorovým ověřením.

NESDÍLÍM PŘIHLAŠOVACÍ ÚDAJE K VLASTNÍM ÚČTŮM A SLUŽBÁM.
V případě pracovního e-mailu, pracovního intranetu, docházkového systému nebo hesla do počítače může mít takové jednání závažné následky.

Obrázek 6: Ukázka plakátu Bezpečný pohyb v kybersvětě 3

5.2 Segmentace stě

Pro zlepšení bezpečnosti sítě samotné je doporučeno provést rozdělení sítě, tzv. segmentaci. V případě útoku na kancelářské zařízení bude výroba dál schopna pokračovat v provozu bez omezení a obráceně. Segmentaci je možné realizovat fyzickou segmentací v místě, kde na router, který je připojen na vnější internet, připojíme další novou sít. Jednu síť pro kancelář a jednu pro sklad a výrobu. Toto řešení je jednoduché, ale podniku vzniknou další výdaje a je potřeba fyzicky změnit zapojení v samotné organizaci.

V našem případě volím možnost druhou, a to vytvoření nových logických podsítí. Je to z důvodu minimalizace nákladů a co nejmenšího zásahu do fyzického zapojení.

5.2.1 Identifikace switchů

Pro pochopení segmentace sítě jsem rozdělil jednotlivé switche podle toho, kde se nacházejí a pro jakou část firmy slouží. Oblasti firmy rozdělím podle funkce na kancelář a sklad/výrobu. Switche v kanceláři bereme ty switche, na které se napojují další switche a zařízení, které se nacházejí v administrativní budově. Switche pro sklad/výrobu jsou ve skladu a výrobních halách včetně prostor pro jejich správu.

Switch	Oblast
Klikarna	Kancelář
Autobus2	Kancelář
Skrinvlevo	Kancelář
Skrinvpravo	Kancelář
Switch TP LINK	Kancelář
Server	Kancelář
Dílna	Výroba/sklad
Dílna2-26	Výroba/sklad
Hala-Vyroba	Výroba/sklad
Mistri	Výroba/sklad
Dilna1-18 mistri	Výroba/sklad
Sklad	Výroba/sklad
Nova-hala	Výroba/sklad

Tabulka 10: Tabulka rozdělení switchů

5.2.2 Logické rozdělení sítě

Správce sítě používá v rámci celého zapojení 4 podsítě VLAN. Tyto sítě mají za úkol oddělit malé části firmy. Rozdělení je následovné:

VLAN	Funkce
Vlan 10 - guest	Oddělení připojení hostů k internetu přes wifi.
Vlan30_UnifiMGMT	Podsíť vytvořená pro správu UNIFI APOD.
Vlan36_Wifisklad	Přístup k internetu pro zařízení v rámci celé firmy.
Vlan60_EsetProtection	Podsíť určená pro server.

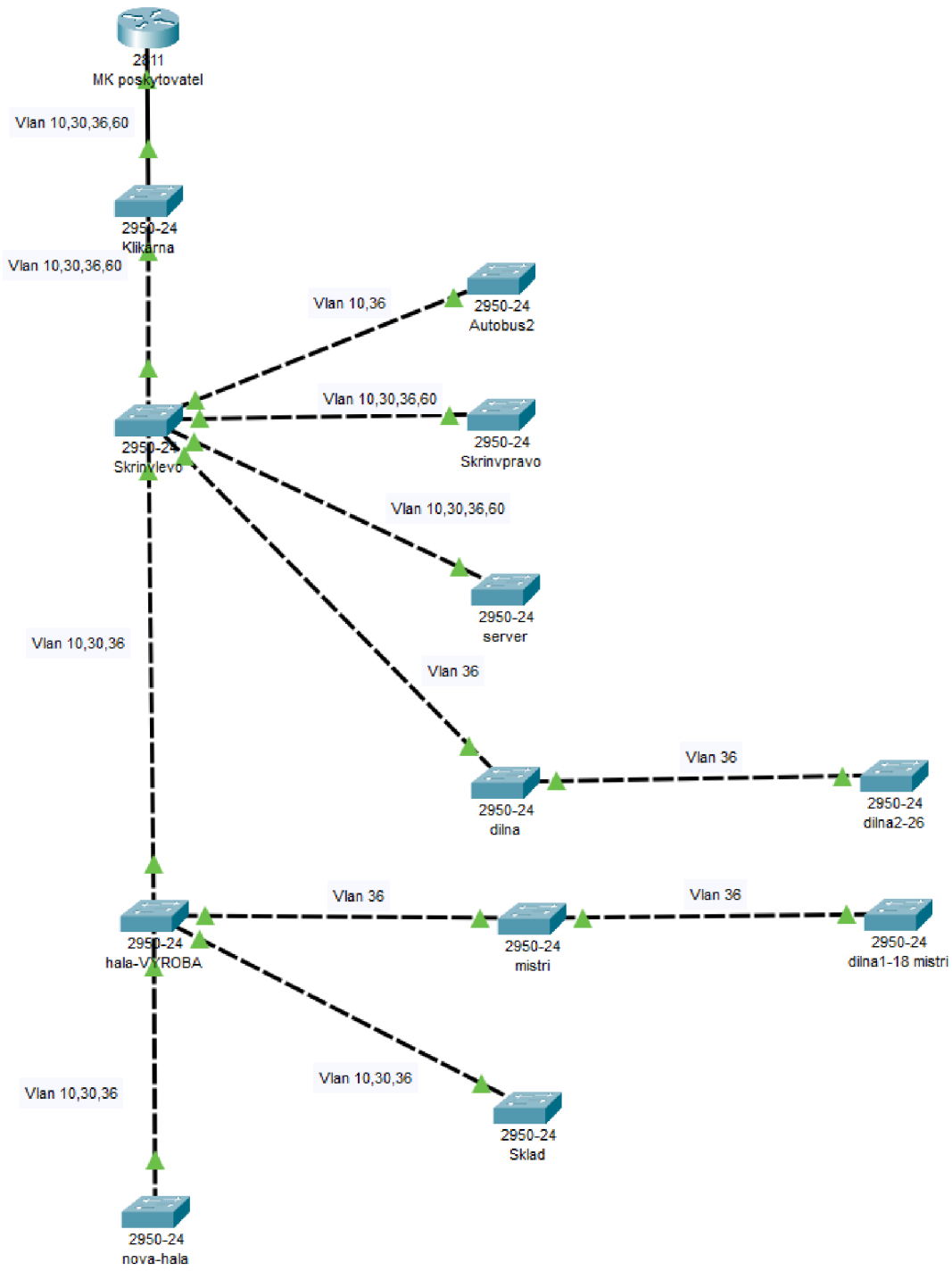
Tabulka 11: Tabulka logického rozdělení VLAN

Zařízení připojené v kanceláři ale mají přístup k zařízením ve skladu nebo ve výrobě. V případu napadení skrze počítače, například oddělení HR, hrozí zastavení celé výroby a firma bude přicházet o potenciální zisky. Proto vytvořím další 2 VLAN, které tyto sektory od sebe logicky oddělí. Pro navrhnutí řešení v aplikaci Cisco Packet Tracer vytvořím přesně dle schématu model sítě.[29]

5.2.3 Navrhované opatření

Pro sklad a výrobní haly vytvořím novou podsíť **Vlan2_Vyrobasklad** a pro kanceláře vytvořím podsíť **Vlan65_kancelare**. Tak dosáhnu toho, že jednotlivé tyto části pořád budou mít přístup k routeru, tudíž na „venkovní“ internet, ale zároveň budou pro sebe navzájem nedosažitelné. Na funkčnost samotné sítě to tedy nebude mít vliv a zároveň zvýšíme její celkové zabezpečení.

5.2.4 Současné nastavení sítě v programu Cisco Packet Tracer



Obrázek 7: Současné nastavení sítě v CISCO Packet Tracer

5.2.5 Nastavení switchů

V této části navrhnu jednotlivé nastavení komunikace mezi switchi a nastavení portů pro připojená zařízení v oddělených oblastech. Jako první nastavím switche pro přenos dat v modu trunk.

```
Switch#enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fa0/5
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

Switch(config-if)#switchport trunk allowed vlan 1-65
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#exit
```

Obrázek 8: Nastavení komunikace pro switch

Tímto krokem zajistím, že skrze tento port je povolena komunikace pro VLAN s číslem 1-65. Pro jednotlivé switche toto číslo bude jiné.

Následující tabulka rozepisuje jednotlivé spojení a jaké VLAN na nich povolím.

Komunikace	Povolené VLANy
MK poskytovatel - Klikarna	Switchport trunk allowed vlan 1-65
Klikarna - Skrinvlevo	Switchport trunk allowed vlan 1-65
Skrinvlevo – Autobus2	Switchport trunk allowed vlan 10, 36, 65
Skrinvlevo – Skrinvpravo	Switchport trunk allowed vlan 10, 30, 36, 60, 65
Skrinvlevo – server	Switchport trunk allowed vlan 10, 30, 36, 30, 65
Skrinvlevo – dilna	Switchport trunk allowed vlan 2, 36
Dilna – dilna2-26	Switchport trunk allowed vlan 2, 36
Skrinvlevo – hala-VYROBA	Switchport trunk allowed vlan 2, 10, 30, 36
Hala-VYROBA – nova-hala	Switchport trunk allowed vlan 2, 10, 30, 36
Hala-VYROBA – Sklad	Switchport trunk allowed vlan 2, 10, 30, 36
Hala-VYROBA – mistri	Switchport trunk allowed vlan 2, 36
Mistri - dilna1-18 mistri	Switchport trunk allowed vlan 2, 36

Tabulka 12: Tabulka zobrazující komunikace v síti

Tímto krokem se vytvořilo základní rozdělení firemní sítě. Nastavením povolených VLAN na switchích se omezí komunikaci mezi uzly, přes které by se v případě napadení mohli útočníci dostat do celé sítě přes jedno zařízení.

Následně je nutno podívat se na nastavení jednotlivých portů pro připojení koncových zařízení a přiřazuji jim tak VLAN, díky které budou komunikovat se zařízeními stejných skupin. Zároveň je potřeba nastavit námi vytvořené VLAN. Jako příklad nastavím porty pro switch Autobus2, u kterého bude každé další zařízení přiřazeno k Vlan65_kancelare.

```
Switch#enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 65
Switch(config-vlan)#name Vlan65_kancelare
Switch(config-vlan)#exit
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 65
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#exit
```

Obrázek 9: Nastavení VLAN pro kanceláře

Další switch, Sklad, upravím pro komunikaci koncových uzlů ve skupině Vlan2_Vyrobasklad.

```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

Switch(config-vlan)#name Vlan2_Vyrobasklad
Switch(config-vlan)#exit
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#exit
```

Obrázek 10: Nastavení VLAN pro sklad a výrobu

Switchům, které slouží jako „křižovatka“, musím inicializovat veškeré jeho používané VLAN. Pro příklad nastavím VLAN na switchi Skrinvlevo.

```
Switch#enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name Vlan2_Vyrobasklad
Switch(config-vlan)#exit
Switch(config)#vlan 65
Switch(config-vlan)#name Vlan65_kancelare
Switch(config-vlan)#exit
Switch(config)#exit
```

Obrázek 11: Nastavení trunk pro nové VLAN

5.2.6 Nastavení routeru

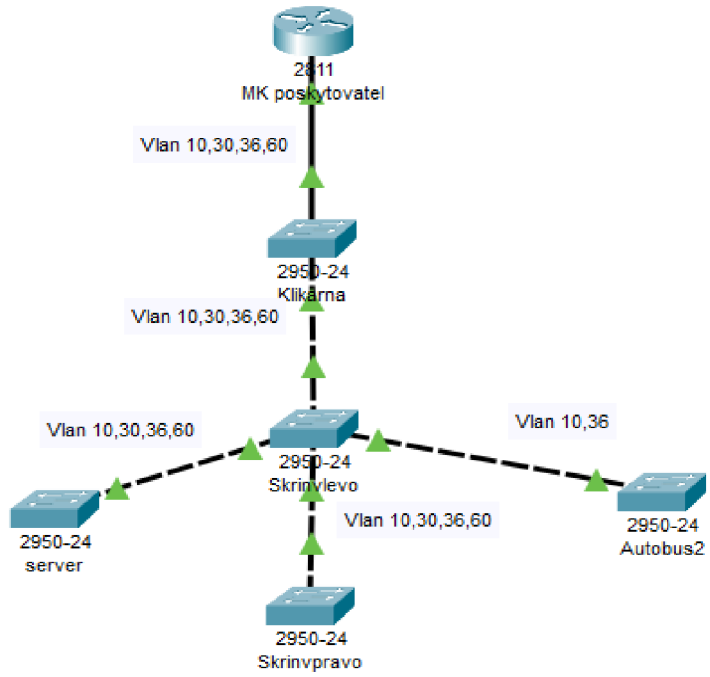
Aby všechna zařízení v síti dokázala komunikovat i s okolním světem, je potřeba nastavit na routeru veškeré VLAN, které jsou v síti. Tím dosáhnu toho, že ačkoliv se uzly z jiných podsítí nevidí, router bude pro všechny stejnou branou. Nastavení vytvořím takto:

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0.2
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state to up

Router(config-subif)#encapsulation dot1q 2
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#no shut
Router(config-subif)#exit
Router(config)#int fa0/0.65
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.65, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.65, changed state to up

Router(config-subif)#encapsulation dot1q 65
Router(config-subif)#ip address 192.168.65.1 255.255.255.0
Router(config-subif)#no shut
Router(config-subif)#exit
Router(config)#exit
```

Obrázek 12: Nastavení routeru pro komunikaci

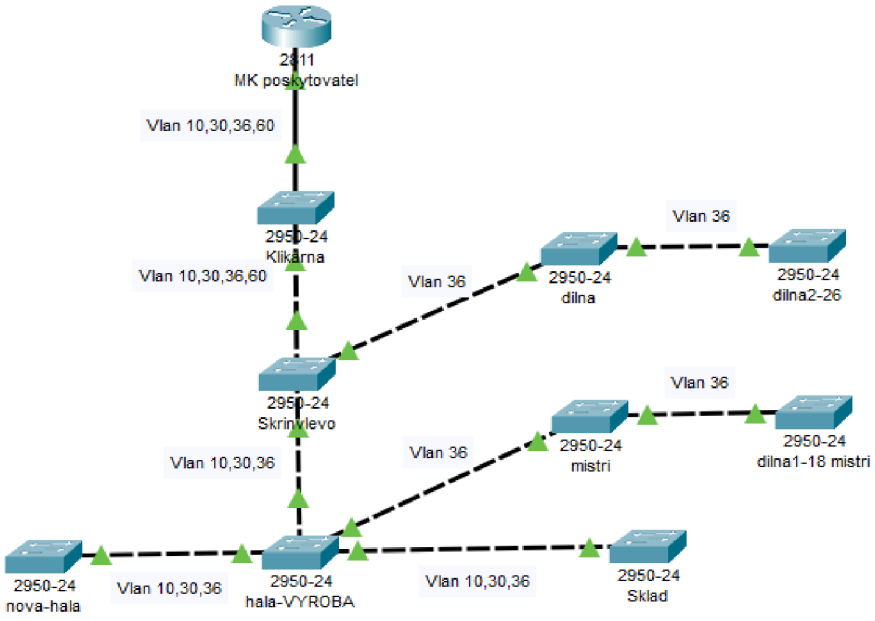
Takto nastavený router bude schopný směrovat komunikaci k jednotlivým podsítím v naší firemní síti.

5.2.7 Logické schéma zapojení pro kanceláře



Obrázek 13: Logické schéma zapojení pro kanceláře

5.2.8 Logické schéma zapojení pro sklad a výrobu



Obrázek 14: Logické schéma zapojení pro sklad a výrobu

5.3 Další navrhované řešení

5.3.1 Klasifikace dat

Veškerá firemní data je potřeba nějak kategorizovat a rozdělit podle jejich důležitosti a účelu. Firma doposud nijak konkrétně nedělí svoje data. Podle jejich významu jim přiřadím důležitost z logiky věci. V této části vytvořím konkrétní stupnici s ohodnocením a významem jednotlivých stupňů.

Stupeň	Význam
Interní personální	Tato data obsahují informace o zaměstnancích nebo zákaznících.
Interní výrobní	Tato data jsou důležitá pro výrobu, obsahují důležité návrhy součástek.
Interní veřejné	Veřejnými daty rozumíme informace, které firma prezentuje veřejnosti jako svoje portfolio.
Běžné	Data, která nemají žádný podstatný význam.

Tabulka 13: Tabulka klasifikace dat

5.3.2 Evidence bezpečnostních incidentů

Bezpečnostní incident je situace taková, kdy došlo k narušení zabezpečení firemní sítě. Evidence těchto skutečností může sloužit pro správce sítě. Jakmile nastane bezpečnostní událost, je důležité zaznamenat vše, co se odehrálo. Pro naše potřeby bude stačit formulář, který je volně dostupný na webu NÚKIB. Informace o události se předají správci sítě, ten formulář vyplní a založí. Tyto formuláře pomůžou v budoucnu pro rychlejší reakci a identifikaci událostí. V ideálním případě je potřeba tuto událost nahlásit na Národní úřad kybernetické a informační bezpečnosti a ten se jím bude zabývat dále. Tady je jeho ukázka:[35]

Formulář hlášení kybernetického bezpečnostního incidentu

Míra ochrany informace *: Neomezeno (veřejné)

Kontaktní údaje

Orgán a osoba uvedená v § 3 písm. c) a e) zákona *:

Identifikátor ****:

E-mail *:

Telefon *:

Pokračování *: Iniciační oznámení CERT/CSIRT týmu **ID **:**

Detaily kybernetického bezpečnostního incidentu / kybernetické bezpečnostní události

Jedná se o hlášení: INCIDENTU

Datum a čas zjištění *: YYYY MM DD hh : mm **Časová zóna*:** +- hh

Datum a čas výskytu incidentu: YYYY MM DD hh : mm Časová zóna: +- hh

Kategorie incidentu *: Kategorie I – méně závažný kybernetický bezpečnostní incident

Typ incidentu *:

Kybernetický bezpečnostní incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do sy

Upřesnění podle standardu ENISA/eCSIRT.net - "Incident Classification" ***:

- Abusive Content (např. spam, kyberšikana, nevhodný obsah)
- Malicious Code (např. virus, červ, trojský kůň, dialer, spyware)
- Information Gathering (např. skenování, sniffing, sociální inženýrství)
- Intrusion Attempts (např. zneužití zranitelnosti, kompromitace aktiva, "0-day" útok)
- Intrusions (např. kompromitace aplikace nebo uživatelského účtu)
- Availability (např. narušení dostupnosti způsobené DoS/DDoS útokem nebo sabotáží)
- Information Security (např. neautorizovaný přístup nebo neautorizovaná změna informace, ...)
- Fraud (např. neoprávněné využití ICT - porušení licenčních práv, krádež identity aj.)
- ostatní

Současný stav zvládání kybernetického bezpečnostního incidentu *:

Probíhá analýza a šetření kybernetického incidentu

Počet zasažených systémů (odhad) *:

Odhad počtu dotčených uživatelů *:

1/2

Obrázek 15: Formulář hlášení incidentu 1/2

Popis incidentu *:

Rozsah škod:

Jaká opatření již byla přijata?:

Systémové detaily - cíl útoku (kompromitovaný systém)	
Host nebo IP *:	
Funkce hosta *:	
Port:	
Protokol:	
OS / jiný systém + verze:	
Umístění systému v architektuře:	

Systémové detaily - zdroj útoku (je-li znám)	
Host / IP nebo jiné (zařízení/uživatel):	
Port:	
Protokol:	

** Povinné pole*
*** Povinné pole v případě, že je vybrána volba "Pokračování dříve oznámeného incidentu", jedná se o ID dříve oznámeného incidentu / události, na které chcete navázat nové hlášení*
**** zdroj: http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html*
***** Identifikátor zadávejte jen tehdy, pokud Vám byl sdělen ze strany GovCERTu (jde o jednoznačný identifikátor orgánu nebo osoby)*

UPOZORNĚNÍ:
Právo změny dokumentu vyhrazeno.
Orgány a osoby podle § 3 zákona o kybernetické bezpečnosti, písm. b) (orgány nebo osoby zajišťující významnou síť) hlásí kybernetické bezpečnostní incidenty národnímu CERT týmu (NIC.CZ) prostřednictvím formuláře, zveřejněného na: www.csirt.cz/stateincidentreport

2/2

Obrázek 16: Formulář hlášení incidentu 2/2

5.3.3 Audit zabezpečení sítě

Firma provádí penetrační testy své sítě. Ty zajišťuje firma MComputers. Tyto testy jsou ale nepravidelné, jen pokud na ně zůstanou finanční prostředky. Pro dobré fungování sítě a ověření její bezpečnosti je lepší provádět pravidelné audity zabezpečení takové sítě. Mohou nám odhalit vážné nedostatky upozornit na potenciální díry. Tento audit by se neměl provádět osobou zaměstnanou ve firmě, protože by mohlo dojít k neobjektivnímu hodnocení nebo k úmyslnému přehlédnutí problému v zájmu zachování dobrého jména. Tuto funkci by měl provádět nezaujatý člověk z vnějšku firmy. Jedna z firem, která nabízí tyto služby je PricewaterhouseCoopers (PwC). Specialista provede audit a zhodnotí rizika včetně řešení pro odstranění nebo alespoň snížení úrovně těchto rizik.

5.3.4 Záložní zdroj elektřiny

V případě výpadku elektřiny, ať už z důvodu poškození v elektrické rozvodně přírodními vlivy nebo mechanickými, dojde k ohrožení celé sítě. V této kapitole se budu bavit pouze o záložních zdrojích pro kanceláře. Vytvořená segmentace sítě by byla ohrožena, jelikož bez elektřiny není možné toto rozdělení udržet. Stejně tak i server a všechny jeho funkce budou v ohrožení. Je potřeba mít v záloze dostatečný zdroj energie, díky kterému budeme schopni rychle obnovit nejdůležitější funkce celého systému.

5.3.5 Dvoufázové ověřování

Zaměstnanci mají pro přístup do firemní sítě svoje uživatelské jméno a heslo. Řada zaměstnanců ale používá jen velmi jednoduché heslo a je tedy jednoduché pro útočníka zkoušet jedny z nejčastěji používaných hesel. Pokud ale zavedu dvoufaktorové ověřování při přihlašování, může se toto riziko snížit. Jedna z variant je používat SMS kód, který bude zaslaný na firemní nebo osobní telefon, během přihlašování. Tento kód bude mít omezenou životnost jen na dobu nezbytnou pro přihlášení a pro každé další přihlášení se bude generovat další.

Další varianta, která zlepší zabezpečení přihlašování, je použití jednorázového přihlašovacího kódu. Zaměstnanec nebude potřebovat heslo, které by si musel pamatovat, ale bude mu stačit jen potvrzovací kód, který se mu vygeneruje na žádost při přihlášení. Po zadání kódu se přihlášení ověří a hned poté se tento přidělený kód smaže. Na každé další přihlášení se vygeneruje nový kód a potenciálnímu útočníkovi se tak ztíží napadnutí sítě.[17]

5.3.6 Disaster recovery plan

V případě, že se útočník dostal do firemní sítě a působí škody v naší síti je důležité vytvořit postup, který nám pomůže minimalizovat škody. Bez žádného scénáře mohou nastat zbytečné zmatky, které budou prodlužovat reakční dobu, a tím způsobovat další škody. Je proto důležité nastavit kroky, kterými se bude firma řídit.

- Vytvořit seznam všech kritických zařízení, která jsou důležitá pro chod firmy.
- Sepsat všechny důležité procesy, které musí v případě nouze pracovat dále:
    - VLAN rozdělení sítě
    - Zabezpečení dveří na čip
    - Server
- Sepsat ty procesy, které mohou být během útoku narušeny.
- Vytvořit schéma zodpovědností. Určit, kdo má jaké povinnosti a o co se musí starat. Založit tým, který bude mít absolutní práva v rozhodujících situacích. V případě naší firmy to bude správce sítě, manažer bezpečnosti a ředitel. V případě absence jednoho nebo obou členů takového týmu je důležité jmenovat náhradníky.
- Ustanovit maximální objem dat, které nebude pro firmu likvidační.
- Vytvořit časový plán, kdy bude nebezpečná situace zažehnána a jaký maximální časový úsek je firma schopna přežít.
- Náhradní záloha dat. Firma vytváří pravidelné zálohy firemních dat, ale tato záloha je umístěna uvnitř firemní sítě. Je vhodně, aby firma zálohovala data i na cloudové úložiště. Díky tomu budou data v případě útoku na firemní síť v bezpeční a bude možné se k nim dostat vzdáleně a kdykoliv.
- Tento vytvořený plán je důležitý mít přehledně sepsaný, snadno dostupný a srozumitelný pro každého. Jeho funkci je dobré pravidelně testovat a aktualizovat s přibývajícím množstvím nových firemních dat.

Po vyřešení nastalé situace je dobré vše sepsat, aby při potenciálním budoucím útoku bylo možné díky archivaci předešlých incidentů stejného charakteru proti němu nasadit obranu dříve a reagovat efektivněji.[34]

5.3.7 Manažer bezpečnosti ICT

Pro správné fungování zabezpečení firemní sítě je velmi důležité, aby ve firmě byla oddělena povinnosti správce sítě. Ten totiž zastává funkci správy sítě a zároveň i manažera bezpečnosti ve firmě. Tady by mohlo docházet ke střetu zájmů a promlčování problémů a chyb. Tento manažer kybernetické bezpečnosti musí být nezávisle postavený v hierarchii organizace a být na stejné úrovni jako ředitel. Takové schéma by mělo vypadat takto:

Obrázek 17: Zjednodušené schéma organizace s novou pozicí manažera bezpečnosti

Tak bude manažer nezávislý ve své funkci a správce sítě bude mít na starosti pouze provoz informačního systému. Ten se bude zodpovídat přímo řediteli firmy. Tito tři budou zároveň tvořit kritický tým v případě kybernetického útoku.

Roli manažera kybernetické bezpečnosti lze vyřešit dvěma způsoby. Jednou z variant je vytvořit pracovní pozici ve firmě a zahájit výběrové řízení na tuto pozici. Tento zaměstnanec projde potřebnými školeními a bude dokonale zasvěcen do procesů ve firmě, aby dokázal efektivně nasadit, kontrolovat a zhodnotit nastavená pravidla. Toto řešení je vhodné, jelikož tento zaměstnanec bude přímo ve firmě a bude mít o důležitých věcech dokonalý přehled.

Druhá varianta je tuto pozici outsourcovat. Na trhu jsou firmy, které se tímto zabývají. Velmi důležité je dostatečně a vhodně sepsaná smlouva, která bude určovat práva a povinnosti tohoto externího zaměstnance. Nevýhodou je pak to, že takový externista nezná veškeré procesy nastavené uvnitř firmy. Bude se muset dokonale seznámit s fungováním a existuje zde riziko, že se obě strany nepochopí dokonale.

Jako řešení vybírám outsourcing, jelikož je na trhu nedostatek těchto odborníků, a je to tak jediné řešení. Pro splnění minimalizace nákladů jsem vybral firmu Sevitech CZ.[39]

5.3.8 Šifrování dat na disku

Je důležité pravidelně zálohovat data, ale stejně podstatné je i tato data šifrovat. V případě, že by se útočník dostal k důležitým souborům a informacím, mohl by bez sebemenší námahy tyto informace přečíst, a dostat se tak k případnému firemnímu know-how. V tomto případě se podívám na doporučované programy, které vybral NÚKIB. Preferované symetrické blokové šifrovací algoritmy jsou tyto:

Algoritmus	Délka klíče v bitech
Advanced Encryption Standard	128, 192, 256
Camellia	128, 192, 256
Serpent	128, 192, 256

Tabulka 14: Tabulka šifrovacích algoritmů

Nejen samotné použití algoritmu, ale i výběr vhodného módu jsou velmi důležité. Doporučení schvaluje následující módy XTS a EME. To nám zajistí, že útočník nebude schopný přečíst firemní data bez klíče.

Pro naše potřeby volím Advanced Encrypion Standard (AES), jelikož je na prvním místě v žebříčku preferovaných algoritmů vydaném NÚKIBem.[36]

5.3.9 Zabezpečení serveru proti vnějším vlivům

V serverovně by kromě samotného hasícího přístroje měl být i požární hlásič, který včas upozorní na první známky vznikajícího kouře. Proto vyberu takový požární hlásič, který bude splňovat požadavky firmy.

Místnost je v patře a celá firma není v záplavové oblasti. Chlazení zajišťuje nezávislá klimatizace.

5.3.10 Aplikační bezpečnost

Firma provádí penetrační testy, které zajišťuje firma M Computers. Problém je, že testy nejsou pravidelné. Navrhuji, aby se testy prováděly pravidelně každého půlroku, nebo pokud dojde k výrazné změně v infrastruktuře. Tyto testy a jejich výsledky včetně průběhu je vhodné evidovat. Tento soupis by měl obsahovat alespoň následující položky:

1. Datum provedení penetračního testu
2. Určení rozsahu
3. Použitá metodika testování
4. Název nástroje pro testování
5. Průzkum prostředí
6. Testovaná část sítě
7. Výsledek
8. Závěrečná zpráva a shrnutí testu[40]

5.4 Závěrečná kalkulace výdajů

Položka	Cena	Platební model	Poznámka
Školení zaměstnanců.	Zadarmo	-	Školení proběhne pomocí moodle kurzů na stránkách NÚKIB.
Vytvoření rozdělení sítě pomocí VLAN.	Zadarmo	-	Rozdělení bude pouze logické, fyzické zapojení tedy zůstane stejné a žádný další přístroj se nemusí pořizovat.
Audit zabezpečení sítě.	Nabídka vytvořená na míru.	Pravidelný výdaj	Externí auditor na základě jím vybraných kritérií zhodnotí zabezpečení a nastaví cenu.
Záložní zdroj energie.	126 799 Kč	Jednorázová investice	Hahn&Sohn dieslový generátor HDE12STAi zajistí dostatečný zdroj energie pro kritické zařízení v síti a zabezpečení dveří.
Outsourcing manažera kybernetické bezpečnosti.	30 000 Kč	Pravidelný měsíční výdaj	Tuto službu bude zajišťovat firma Sevitech CZ.
Šifrování dat na disku.	1100 Kč	Jednorázová investice	Platba za licenci šifrovacího algoritmu
Požární hlásič.	549 Kč	Jednorázová investice	Hlásič bude schopen varovat zaměstnance zvukovou signalizací a upozorní správce zprávou přes aplikaci.

Tabulka 15: Tabulka závěrečné kalkulace

6 Výstupní analýza po zavedení navrhovaných opatření

6.1 Oblast technická

Oblast	Čím plněna	Poznámka	Hodnocení
Záloha dat.	Záloha se provádí na konci každého pracovního týdne.		**Splňuje**
Segmentace sítě.	Firemní síť je nyní logicky rozdělena pomocí VLAN podsítí.	Síť je rozdělena část kancelářskou a výrobní.	**Splňuje**
Antiviry.	Na zařízeních je nainstalovaný antivir.		**Splňuje**
Aplikační bezpečnost.	Nyní se provádí testy penetrační s pravidelností.	Evidence prohlášení o provedení testů.	**Splňuje**
Šifrování dat.	Šifrování dat na disku je nyní zajištěno díky algoritmu Advanced Encrypion Standard.	Výběr vychází z preferovaných algoritmů NÚKIBem.	**Splňuje**
Omezení přístupu na internet.	Filtrace nelegálních témat a noční omezení přístupu na internet.	Pro noční směny je omezen přístup pouze na nezbytné procesy pro výrobu.	**Splňuje**
Aktivní blokování nežádoucí komunikace.	Zajištěno firewallem.	Nastavený antispam.	**Splňuje**
Použití dvoufázového ověření.	Zaměstnanci nyní pro přihlášení budou využívat generované kódy.	Pro přihlášení se kromě hesla bude využívat časově omezený číselný kód.	**Splňuje**
Záložní zdroj elektřiny.	Firma disponuje záložním zdrojem energie.	Dieslový generátor zajistí elektřinu pro kritické zařízení ve firmě.	**Splňuje**
Fyzické zabezpečení serveru.	Uzamykatelné dveře i samotná skříň.		**Splňuje**
Zabezpečení serveru proti vnějším vlivům.	Nezávislá klimatizace bez požárního hlásiče.	V místnosti je nyní i požární hlásič, který včas upozorní na vzniklé nebezpečí.	**Splňuje**

Tabulka 16: Tabulka zachycující navrhovaná opatření v oblasti technické

6.2 Oblast řízení

Oblast	Čím plněna	Poznámka	Hodnocení
Klasifikace informací.	Data jsou nyní klasifikována podle jejich citlivosti a důležitosti pro firmu.	Rozdělení do kategorií.	**Splňuje**
Školení zaměstnanců o bezpečnostním povědomí.	Školení bude probíhat na webu NÚKIBu, které je zcela zadarmo.	Proškolený zaměstnanec získá certifikát, kterým se prokáže.	**Splňuje**
Udělování přístupů zaměstnancům.	Role v systému odpovídají pracovním pozicím.		**Splňuje**
Disaster recovery plan.	Firma nyní má plán obnovy.	Vytvoření plánu, díky kterému může firma postupovat.	**Splňuje**
Audit bezpečnosti ICT.	Audit nyní zajišťuje firma PricewaterhouseCoopers.	Audity budou probíhat pravidelně dle dohody s odborníkem.	**Splňuje**
Fyzické zabezpečení.	Důležité místnosti pro chod sítě a celý areál firmy je pro veřejnost nedostupný.	Pro pohyb je potřeba klíče nebo čipu.	**Splňuje**
Evidence bezpečnostních incidentů.	Díky formuláři, který je volně dostupný na webu NÚKIBu, bude probíhat evidence bezpečnostních incidentů.	Tyto události budou hlášeny NÚKIBu pro jejich zpracování.	**Splňuje**
Bring your own device.	Používání vlastních zařízení firma nepodporuje.	Firma poskytuje svým zaměstnancům zařízení.	**Splňuje**
Oddělení povinností správce.	Firma má novou pracovní pozici manažera bezpečnosti ICT.	Správce sítě bude řešit správu sítě samotné a manažer bezpečnosti bude řešit bezpečností rizika a opatření.	**Splňuje**
Evidence pohybu zaměstnanců.	Firma používá docházkový systém	Zaměstnanec pro příchod a odchod používá čip.	**Splňuje**
Evidence hesel.	Hesla jsou uložena v Keypass.	Hesla se ale nemění pravidelně.	**Splňuje**

Tabulka 17: Tabulka zachycující navrhovaná opatření v oblasti řízení

6.3 Vyhodnocení navrhovaných opatření a jejich přínos

Navrhovaná opatření nyní splňují minimální bezpečnostní standardy vydané Národním úřadem pro kybernetickou a informační bezpečnost ve všech bodech. Firma zavedením těchto opatření vyřeší svoje trhliny v zabezpečení a ta mohou přispět svým dílem při vytváření bezpečnostních politik.

Opatření jsem se snažil dělat co nejefektivnější a zároveň za co nejnižší cenu, abych splnil požadavky vedení a správce sítě. Správce sítě firmy zareagoval na moje návrhy a některé z nich plánuje nasadit nebo dokonce již nasadil.

Školení zaměstnanců o bezpečnostním povědomí vnímá jako pozitivní vliv a je velmi reálné, že v blízké budoucnosti tento návrh zrealizuje.

Rozdělení sítě již zrealizoval a jeho zpětná vazba je, že se zvýšilo zatížení routeru. To je očekávaný výsledek, jelikož se vytvořili 2 nové VLAN podsítě. Výkon je nyní na 60% - 70%. Hodnota není tedy kritická, ale řešením tohoto problému by bylo zakoupení výkonnějšího modelu routeru.

7 Závěr

Hlavním cílem této bakalářské práce bylo zhodnotit zabezpečení firemní sítě středního podniku a implementovat navrhovaná opatření. Vycházel jsem z analýzy současného stavu a ten jsem porovnával s minimálními standardy vydané Národním ústavem kybernetické a informační bezpečnosti. Současný stav jsem získal díky konzultacím se správcem sítě dané firmy. Konzultace probíhaly osobně, po telefonu nebo přes e-mail, díky kterým jsem získal všechny potřebné informace.

Na základě těchto informaci jsem vytvořil GAP analýzu, ve které jsem v jednotlivých oblastech zabezpečení hodnotil, zda je firma splňuje. V oblastech, kde firma zaostávala, jsem navrhl opatření tak, aby splňovala standardy. Zároveň jsem dodržoval minimalizování nákladů, jakožto jeden z požadavků správce sítě. To ovlivnilo moje rozhodování při výběru opatření.

Výsledkem těchto opatření je nový stav zabezpečení, který již ve všech oblastech vyhovuje minimálním standardům.

Přínosem této práce je příprava firmy v zabezpečení její firemní sítě do budoucna. V příštích letech se očekává, že organizace budou muset tyto standardy zavést i ve svých sítích. Firma, díky které jsem mohl toto téma zpracovat, má nyní podklady pro zavedení těchto opatření a ulehčení práce do budoucna, až bude povinné splňovat podmínky NIS2.

Pro mě byl hlavním přínosem osobní rozvoj. Tato problematika mě zajímá a díky tomuto tématu jsem se dostal k zajímavým informacím a získal nové zkušenosti. V rámci kapitoly 5.1.4 jsem si sám splnil mnou navrhované školení a získal všechny certifikáty, které jsou níže v příloze.

Použité zdroje

[1] Ing. Lukáš Pavlík, Ph.D., Počítačové sítě, základní druhy sítí, síťové prvky [online]. Olomouc, 2021 [cit. 2023-04-23]. Dostupné z: https://is.mvso.cz/el/mvso/zima2021/XIN/233265/Prednaska_c._4_-_Pocitacove_site__zakladni_druhy_siti__sitove_prvky.pdf?. Prezentace. Moravská vysoká škola Olomouc.

[2] Towards automated cyber decision support: A case study on network segmentation for security | IEEE Conference Publication | IEEE Xplore. 301 Moved Permanently [online]. Copyright © Copyright 2023 IEEE [cit. 22.04.2023]. Dostupné z: https://ieeexplore.ieee.org/abstract/document/7849908

[3] Recenze: APC Back-UPS 950VA – když dojde | Geek Magazín. CZC.cz - rozumíme vám i elektronice [online]. Dostupné z: https://www.czc.cz/geek/recenze-apc-back-ups-950va-kdyz-dojde-stava/clanek

[4] Ing ŠPATENKA, Jan a Ing NOVÁK, Lukáš Ph.D., Podnikové informační systémy: Podnikové IS a řízení podnikové informatiky [online]. Brno, 2021 [cit. 2023-04-23]. Dostupné z: https://moodle.vut.cz/course/view.php?id=260060. Prezentace. Vysoké učení v Brně, Fakulta podnikatelská.

[5] Systém QI - Centrální mozek firmy - QI.cz. Informační systém QI, ERP systém - QI.cz [online]. Copyright © 2023 QI GROUP a. s. Páteřní 7, 635 00 Brno [cit. 22.04.2023]. Dostupné z: https://www.qi.cz/system-qi/?gclid=CjwKCAjwrdmhBhBBEiwA4Hx5gxUeua2bHXk-LTiXxPe8vso8oIed3cLtQPtZWIcuZxKDU1xO45e_ohoCxg0QAvD_BwE

[6] KUTINA, Michal. Operační systémy počítačů. Praha, 2007. Bakalářská práce. Vysoká škola ekonomická v Praze, Fakulta managementu v Jindřichově Hradci. Vedoucí práce Ing. Pavel Pokorný.

[7] Co je to antivirus a antivirový program? | ESET. Malware Protection & Internet Security | ESET [online]. Copyright © 1992 [cit. 22.04.2023]. Dostupné z: https://www.eset.com/cz/antivirus-software/

[8] Co je firewall? | ESET. Malware Protection & Internet Security | ESET [online]. Copyright © 1992 [cit. 22.04.2023]. Dostupné z: https://www.eset.com/cz/firewall/

[9] MIČAN, Jiří. Zálohování dat. Praha, 2015. Bakalářská práce. Bankovní institut vysoká škola Praha, Katedra informatiky a kvantitativních metod. Vedoucí práce Ing. Bohuslav Růžička, CSc.

[10] MŮČKA, Jan. RAID disková pole: Jaké jsou základní typy a v čem se liší. Master.cz [online]. Brno: MasterDC, 2021 [cit. 2023-04-23]. Dostupné z: https://www.master.cz/blog/raid-diskova-pole-jake-jsou-zakladni-typy-a-v-cem-se-lisi/

[11] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti ve znění pozdějších předpisů.

[12] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti [online]. Praha, 2012 [cit. 2023-04-23]. Dostupné z: https://afcea.cz/wp-content/uploads/2015/03/Slovnik_V1_5_El.pdf. Výkladový slovník. Policejní akademie ČR v Praze a Česká pobočka AFCEA.

[13] Ing. Viktor ONDRÁK PH.D. Management informační bezpečnosti. Brno. Skripta. Vysoké učení technické v Brně, Fakulta podnikatelská.

[14] AFREEN SIDDIQUI, Rahat. Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges [online]. In: . Deogiri Institute of Engineering and Management Studies, India, 2014 [cit. 2023-04-23]. Dostupné z: https://www.researchgate.net/publication/261136229_Bring_Your_Own_Device_BYOD_in_Higher_Education_Opportunities_and_Challenges

[15] KANTNER, Ondřej. Analýza konkurence na vybraném B2B trhu. Praha, 2021. Bakalářská práce. AMBIS Vysoká škola, a.s., Katedra ekonomie a managementu. Vedoucí práce Ing. Helena Cetlová.

[16] MILOŠ, Jiří. Kryptografické metody zabezpečení dat. Brno, 2008. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. Vedoucí práce Ing. Petra Lambertová.

[17] KLUČKA, Petr. Kyberkriminalita. Zlín: Univerzita Tomáše Bati ve Zlíně, 2018, 73 s. Dostupné také z: http://hdl.handle.net/10563/43720. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav počítačových a komunikačních systémů. Vedoucí práce Doc. Ing. Vojtěšek, Jiří Ph.D.

[18] OMAR, Adnan, David ALIJANI a Roosevelt MASON. Information Technology disaster recovery plan: Case study [online]. Texas, USA: Allied Business Academies, 2011 [cit. 2023-04-23]. ISSN 1939-6104. Dostupné z: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=1bb16aea09e38440d984cbe135da07c906fedf16

[19] PODDANÁ, Hana. Bezpečnostní audit podniku. Pardubice, 2017. Bakalářská práce. Univerzita Pardubice, Fakulta ekonomicko-správní. Vedoucí práce Doc. Ing. Radim Roudný, CSc.

[20] Co je malware? Jak se zbavit malwaru? | ESET. Malware Protection & Internet Security | ESET [online]. Copyright © 1992 [cit. 22.04.2023]. Dostupné z: https://www.eset.com/cz/malware/

[21] Co je phishing? | ESET. Malware Protection & Internet Security | ESET [online]. Copyright © 1992 [cit. 22.04.2023]. Dostupné z: https://www.eset.com/cz/phishing/

[22] POMYKAL, Martin. Sociální inženýrství. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012, 49 s. (53 355 znaků). Dostupné také z: http://hdl.handle.net/10563/22795. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav bezpečnostního inženýrství. Vedoucí práce Ing Vojtěšek, Jiří Ph.D.

[23] Ing. Viktor ONDRÁK PH.D. Management informační bezpečnosti. Brno. Skripta. Vysoké učení technické v Brně, Fakulta podnikatelská.

[24] Nová definice malých a středních podniků: Uživatelská příručka a vzor prohlášení [online]. In: . Evropská společenství, 2006, s. 50 [cit. 2023-04-23]. Dostupné z: https://www.dotaceeu.cz/getmedia/7bd6ab99-01ea-4940-8247-cba566022d14/MSP_7bd6ab99-01ea-4940-8247-cba566022d14.pdf

[25] VAGUNDA, Vojtěch. Návrh bezdrátové sítě v budově základní školy Kunovice. Zlín: Univerzita Tomáše Bati ve Zlíně, 2018, 77 s. Dostupné také z: http://hdl.handle.net/10563/43256. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav automatizace a řídicí techniky. Vedoucí práce Ing. Matýsek, Miroslav Ph.D.

[26] Bc. ZITTA, Stanislav. Penetrační testování. Pardubice, 2013. Diplomová práce. Univerzita Pardubice, Fakulta elektrotechniky a informatiky. Vedoucí práce Mgr. Josef Horálek.

[27] Ing. BERÁNKOVA, Eva. Základy Facility managementu. TZB-info [online]. 2013, 7 [cit. 2023-04-23]. Dostupné z: https://www.tzb-info.cz/facility-management/10072-zaklady-facility-managementu / Bc. ZELENKOVÁ, Stanislava. Analýza outsourcingu ve vybrané společnosti. Olomouc, 2020. Diplomová práce. Moravská vysoká škola Olomouc, Ústav managementu a marketingu. Vedoucí práce RNDr. Ing. Miroslav Rössler, CSc., MBA.

[28] SEDLÁK Petr, Martin KONEČNÝ a kolektiv. Kybernetická (ne)bezpečnost. CERM, Akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

[29] CISCO. Packet Tracer and Alternative Lab Solutions: Packet Tracer [online]. Cisco, 2023 [cit. 2023-05-08]. Dostupné z: https://learningnetwork.cisco.com/s/packet-tracer-alternative-lab-solutions

[30] NUKIB [online]. Copyright © 2023 PragoData Consulting, s.r.o. [cit. 08.05.2023]. Dostupné z: https://osveta.nukib.cz/local/dashboard/

[31] CYBERSEC. *Online školení kybernetické bezpečnosti* [online]. [cit. 2023-05-08]. Dostupné z: https://www.cybersec.cz/

[32] INSTRUCTOR. *Online školení BOZP a PO* [online]. [cit. 2023-05-08]. Dostupné z: https://www.cybersec.cz/

[33] Počítačová škola GOPAS [online]. [cit. 2023-05-08]. Dostupné z https://www.gopas.cz/

[34] EDITORIAL TEAM, Indeed. *How to create an effective IT disaster recovery plan* [online]. 2022 [cit. 2023-05-14]. Dostupné z: https://www.indeed.com/career-advice/career-development/how-to-create-disaster-recovery-plan

[35] *Formulář hlášení kybernetického bezpečnostního incidentu* [online]. 2023 [cit. 2023-05-14]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/formulare/

[36] NÚKIB, NAKIT a MVČR. *Minimální bezpečnostní standardy* [online]. In: . 2023 [cit. 2023-05-14]. Dostupné z: https://nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[37] NÚKIB, NAKIT a MVČR. *Minimální bezpečnostní standard* [online]. In: . 2023 [cit. 2023-05-14]. Dostupné z: https://nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

[38] NÚKIB. *Bezpečný pohyb v kybersvětě* [online]. 2019 [cit. 2023-05-14]. Dostupné z: https://www.nukib.cz/cs/infoservis/doporuceni/1508-doporuceni-pro-bezpecny-pohyb-v-kybersvete/

[39] Sevitech CZ. *Bezpečnost a GDPR software* [online]. 2023 [cit. 2023-05-14]. Dostupné z: https://www.sevitech.cz/bezpecnost-a-gdpr-software/

[40] NEUDERT, Lukáš. *Penetrační testování z pohledu NIS2* [Prezentace]. 2023 [cit. 2023-05-14].

Seznam obrázků

Obrázek 1: Schéma logického zapojení 25
Obrázek 2: Organizační hierarchie 33
Obrázek 3: Graf analýzy současného stavu 36
Obrázek 4: Ukázka plakátu Bezpečný pohyb v kybersvětě 1 44
Obrázek 5: Ukázka plakátu Bezpečný pohyb v kybersvětě 2 45
Obrázek 6: Ukázka plakátu Bezpečný pohyb v kybersvětě 3 45
Obrázek 7: Současné nastavení sítě v CISCO Packet Tracer 48
Obrázek 8: Nastavení komunikace pro switch 49
Obrázek 9: Nastavení VLAN pro kanceláře 50
Obrázek 10: Nastavení VLAN pro sklad a výrobu 51
Obrázek 11: Nastavení trunk pro nové VLAN 51
Obrázek 12: Nastavení routeru pro komunikaci 52
Obrázek 13: Logické schéma zapojení pro kanceláře 53
Obrázek 14: Logické schéma zapojení pro sklad a výrobu 53
Obrázek 15: Formulář hlášení incidentu 1/2 55
Obrázek 16: Formulář hlášení incidentu 2/2 56
Obrázek 17: Zjednodušené schéma organizace s novou pozicí manažera bezpečnosti . 60
Obrázek 18: Certifikát 1 76
Obrázek 19: Certifikát 2 77
Obrázek 20: Certifikát 3 78

Seznam tabulek

Tabulka 1: Tabulka síťových prvků 26
Tabulka 2: Tabulka prvků připojených v serveru 27
Tabulka 3: Tabulka využívaných SW 27
Tabulka 4: Tabulka současného stavu oblasti technické 34
Tabulka 5: Tabulka současného stavu oblasti řízení 35
Tabulka 6: Tabulka rozdělení skupin dle odpovědností 39
Tabulka 7: Tabulka přiřazení skupin pracovním pozicím 41
Tabulka 8: Tabulka porovnání školení 42
Tabulka 9: Tabulka přiřazení školících programů 43
Tabulka 10: Tabulka rozdělení switchů 46
Tabulka 11: Tabulka logického rozdělení VLAN 47
Tabulka 12: Tabulka zobrazující komunikace v síti 50
Tabulka 13: Tabulka klasifikace dat 54
Tabulka 14: Tabulka šifrovacích algoritmů 62
Tabulka 15: Tabulka závěrečné kalkulace 64
Tabulka 16: Tabulka zachycující navrhovaná opatření v oblasti technické 65
Tabulka 17: Tabulka zachycující navrhovaná opatření v oblasti řízení 66

Přílohy

Příloha 1: Certifikát Bvk! – Základní verze

Obrázek 18: Certifikát 1

Příloha 2: Základy kybernetické bezpečnosti

Obrázek 19: Certifikát 2

Příloha 3: Kurz pro manažery kybernetické bezpečnosti

Obrázek 20: Certifikát 3