POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

Katedra managementu a informatiky

Analýza a komparace zabezpečených páteřních krajských a lokálních datových sítí pro potřeby zajištění krizové komunikace státní správy, samosprávy a složek integrovaného záchranného systému

Bakalářská práce

Analysis and Comparison of Secured Regional and Local Backbone Data Networks for the Needs of Securing Crisis Communication of State Administration, Local Government and Integrated Rescue System Units

Bachelor thesis

VEDOUCÍ PRÁCE

Ing. Bc. Hana DŮBRAVOVÁ

AUTOR PRÁCE

Jakub TRČKA

PRAHA

2024

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 15.3.2024

Jakub TRČKA

Poděkování

Mé poděkování patří Ing. Bc. Haně Důbravové za odborné vedení, trpělivost a ochotu, kterou mi v průběhu zpracování bakalářské práce věnovala. Dále bych rád poděkoval zástupcům IZS z úseku KOPIS a IT za spolupráci při získávání informací pro výzkumnou část práce.

Anotace

V této bakalářské práci se zabývám analýzou a komparací páteřních krajských a lokálních datových sítí pro potřeby zajištění krizové komunikace státní správy, samosprávy a složek IZS a poskytnu ucelený pohled na jejich důležitost, integritu a bezpečnost datových sítí v oblasti krizové komunikace. V první části práce se zabývám pohledem na danou problematiku v teoretické rovině, charakterizuji jednotlivé sítě, jejich prvky a možné hrozby. Dále je charakterizován pohled na organizaci a fungování jednotlivých složek integrovaného záchranného systému. V druhé části můžeme vidět kvalitativní výzkum, jehož součástí jsou pohledy a názory odborníků z úseku základních složek IZS, jež byly získány za účelem analýzy a komparace dané problematiky.

Klíčová slova

Datové sítě * Integrovaný záchranný systém * krizová komunikace * kritická infrastruktura * prvky sítě * hrozba * kybernetická bezpečnost * Policie České republiky * Hasičský záchranný sbor České republiky * poskytovatelé zdravotnické záchranné služby

Annotation

In this bachelor thesis, I am focused on analysis and comparison of backbone regional and local data networks for needs of procuration of crisis communication within state administration, self-government and units of integrated rescue system and providing a complete view regarding its importance, integrity and security of data networks in the field of crisis communication. In the first part of my bachelor thesis I am going to define the stated issues in theoretical perception, characterize the network and its parts and possible threats. I continue with the characterization of the view regarding the organisation and functioning of the particular units of integrated rescue system. In the second part there is provided a qualitative research, which are the opinions and views of the specialists of the integrated rescue systém part of and that were obtained to be used within the analysis and the comparison of the stated issues.

Keywords

Data networks * integrated rescue systém * crisis communication * critical infrastucture * parts of the network * threat * cybersecurity * Police of the Czech republic * Fire rescue brigade of the Czech republic * Ambulance

Obsah

Úvod 1

1. Cíl práce 2

2. Metodika práce, metody zkoumání dané problematiky a stanovení hypotézy 2

3. Datové sítě 3

3.1. Rozdělení sítí 3

3.1.1. Páteřní sítě – MAN a WAN 3

3.1.2. Lokální sítě – LAN 4

4. Aktivní prvky sítě 5

4.1. Repeater (opakovač) 5

4.2. Switch 5

4.3. Router 5

4.4. Brána (gateway) 6

4.5. HUB (Rozbočovač) 6

4.6. IP telefonie 7

4.7. VoIP telefonie 8

5. Pasivní síťové prvky 9

5.1. PoE (Power over Ethernet) 9

6. Bezpečnost 9

6.1. Zabezpečení datových sítí 9

6.1.1. Brána firewall 10

6.1.2. Proxy server 10

6.1.3. DHCP protokol 10
6.1.4. DNS 10
6.1.5. Security Information and Event Management (SIEM) 11
6.1.6. Systém prevence průniku (IPS) 11
6.1.7. Systém detekce průniku (IDS) 12
6.1.8. Antivir 12
6.2. Ochrana dat 12
6.2.1. Šifrování 13
6.2.2. Elektronický podpis 13
6.2.3. VPN (Virtual Private Network) 14
6.3. Zranitelnost 14
6.4. Kybernetická bezpečnost a bezpečnost informačních systémů 15
6.4.1. Kybernetické hrozby 16
6.5. Příčiny a typy útoků na datové sítě 16
6.5.1. Malware 16
6.5.2. Phishing 18
6.5.3. Spoofing 18
6.6. Systém řízení bezpečnosti informací 18
6.7. ITIL 4 20
7. Kritická infrastruktura 20
7.1. Prvek kritické infrastruktury 21
8. Legislativní prameny 21
8.1. Zákon o Integrovaném záchranném systému 21
8.2. Zákon o kybernetické bezpečnosti a související předpisy 21
8.2.1. Vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích 22
8.2.2. Vyhláška č. 437/2017 Sb. o kritériích pro určení provozovatele základní služby 23

8.2.3. Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti 23
8.3. Krizový zákon a související předpisy 23
8.3.1. Ústavní zákon č. 110/1998 Sb. o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb. 23
8.3.2. Nařízení vlády ČR č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury 24
8.4. Další právní předpisy k řešené problematice 24
8.4.1. Zákon o zpracování osobních údajů 24
8.4.2. Zákon o utajovaných informací 24
8.4.3. Zákon o ochraně oznamovatelů 25
9. Krizová komunikace 26
9.1. Komunikace složek IZS 26
10. Krizové plánování 27
11. Integrovaný záchranný systém 28
11.1. Základní složky IZS 28
11.1.1. Hasičský záchranný sbor České republiky 28
11.1.2. Jednotky požární ochrany zařazené do plošného pokrytí kraje jednotkami požární ochrany 31
11.1.3. Poskytovatelé zdravotnické záchranné služby 32
11.1.4. Policie České republiky 33
11.2. Vedlejší složky IZS 35
11.3. Operační středisko integrovaného záchranného systému 36
11.3.1. NIS IZS 37
11.3.2. Krajské standardizované projekty HZS krajů 38
11.3.3. Možné vývojové trendy 38
12. Pohled zástupců složek IZS 38
13. Výsledek, návrh a doporučení 43

Závěr 45

Seznam použitých zdrojů 46

Seznam zkratek

AI	Umělá inteligence
CNP	Civilní nouzové plánování
HZS	Hasičský záchranný sbor
IP	Internet Protocol
IPL	Informační platforma, součást Národního informačního systému
ITIL	Information Technology Infrastructure Library
IZS	Integrovaný záchranný systém
KI	Kritická infrastruktura
KII	Kritická informační infrastruktura
KOPIS	Krajské operační a informační středisko
KŘ	Krizové řízení
KS	Krizová situace
MU	Mimořádná událost
MV	Ministerstvo vnitra
NIS	Národní Informační Systém
OO	Ochrana obyvatelstva
OPIS	Operační a informační středisko
PČR	Policie české republiky
PO	Požární ochrana
PoE	Power over Ethernet
Sb.	Sbírka zákonů a mezinárodních smluv
TCTV 112	Telefonní Centrum Tísňového Volání 112
VoIP	Voice over Internet Protocol
ZZS	Zdravotní záchranná služba

Úvod

V dnešní době je spolehlivá a bezpečná komunikace pro instituce ve veřejné správě, včetně státní správy, samosprávy a složek integrovaného záchranného systému, nezbytnou pro zajištění rychlé a efektivní reakce na různé krizové situace a mimořádné události. Páteřní krajské a lokální datové sítě představují základní infrastrukturní prvky pro tyto organizace, poskytující prostředky pro výměnu dat a informací v reálném čase. V kontextu různých krizových scénářů je nezbytné zajistit, aby tyto sítě byly řádně zabezpečeny, byla zachována integrita, dostupnost a důvěrnost přenášených informací.

Tato bakalářská práce se zaměřuje na analýzu a komparaci zabezpečených páteřních krajských a lokálních datových sítí, které slouží pro potřeby zajištění krizové komunikace státní správy, samosprávy a složek IZS. Cílem práce je poskytnout ucelený pohled na současný stav těchto sítí, analyzovat jejich zabezpečení a identifikovat případné nedostatky či slabiny. Dále práce zkoumá možnosti jejich optimalizace a zlepšení s ohledem na aktuální potřeby a požadavky na krizovou komunikaci.

V rámci této práce budou použity metody analýzy dat a informací získaných z odborné literatury, legislativy a praxe v oblasti informačních technologií a krizového řízení. Důraz bude kladen na porovnání různých přístupů a technologií v oblasti zabezpečených datových sítí a jejich aplikovatelnost v kontextu veřejné správy a IZS.

Závěry této práce by měly přispět k lepšímu porozumění problematiky zabezpečených páteřních sítí pro krizovou komunikaci a poskytnout doporučení pro efektivní využití a optimalizaci těchto infrastrukturních prostředků v rámci státní správy, samosprávy a složek IZS.

1. Cíl práce

Cílem bakalářské práce je porozumění faktorů, ovlivňujících zabezpečení páteřních krajských a lokálních datových sítí v kontextu potřeb krizové komunikace státní správy, samosprávy a složek Integrovaného záchranného systému, analýza organizačních, technologických a legislativních aspektů zabezpečení datových sítí prostřednictvím rozhovorů s IT odborníky a zaměstnanci z oblasti veřejné správy, informačních technologií a bezpečnosti, identifikace podstatných nedostatků a potenciálních oblastí zlepšení, které by mohly vést k efektivnějšímu využití páteřních datových sítí pro zajištění krizové komunikace v rámci státní správy, samosprávy a složek IZS.

2. Metodika práce, metody zkoumání dané problematiky a stanovení hypotézy

V bakalářské práci je použita metoda kvalitativního výzkumu, přičemž jsem se dotazoval odborníků v oblasti IT datových sítí a jejich zabezpečení u jednotlivých základních složek integrovaného záchranného systému formou osobního rozhovoru. Při rozhovorech byl všem odborníkům kladen stejný seznam otázek, přitom byly na mé straně očekávané víceméně stejné odpovědi, z důvodu využívání stejných či velice obdobných systémů a datových sítí. U mnou stanovené hypotézy se předpokládalo, že funkčnost, bezpečnost, kapacita a využívání datových sítí je uspokojivá pro všechny složky IZS, které byly tázány, jelikož jsou uživatelé stejných nebo obdobných systémů. Důvodem k vytvoření této hypotézy bylo mé přesvědčení, že v oblasti krizové komunikace není prostor pro chyby a je naprosto nezbytné, aby datové sítě a jejich bezpečnost korespondovala zabezpečení sítí a informačních systémů jiných subjektů, které též nakládají s utajovanými informacemi. Těmito subjekty jsou míněny společnosti jak veřejného, tak soukromého sektoru. Dalším důvodem shledávám fakt, že v případě datových sítí pro krizovou komunikaci se jedná o kritickou infrastrukturu státu, a tedy v případě jejího narušení může dojít k narušení bezpečnosti státu v rámci ochrany obyvatelstva, civilního nouzového plánování,

požární ochrany, ochrany zdraví osob, majetku a životního prostředí, a krizového řízení.

3. Datové sítě

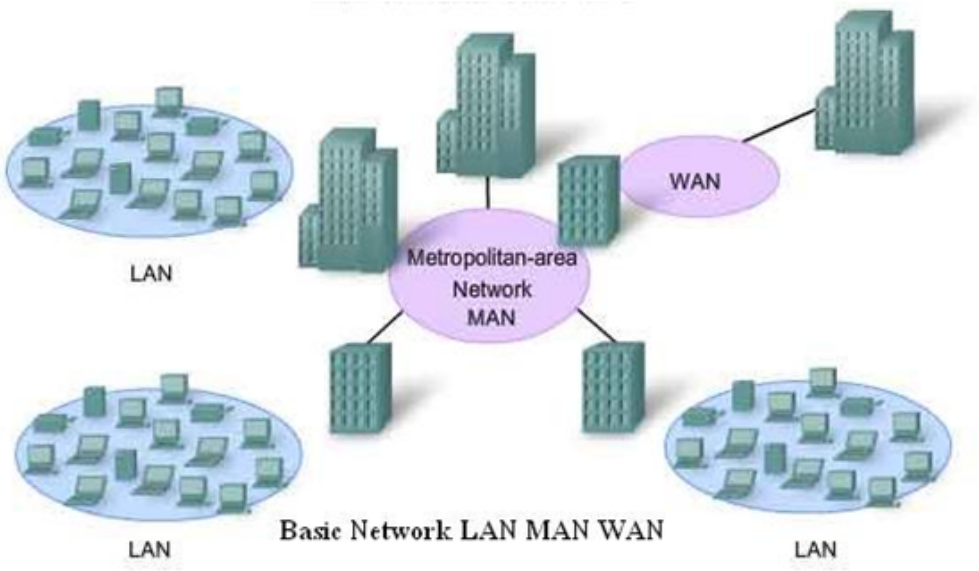
Datové sítě v dnešním světě představují nejrozsáhlejší komunikační metodu se schopností přenášet, vyměňovat nebo sdílet data a prostředky. Je tedy možné je vnímat jako systém zaručující přepojení jednotlivých uzlů sítě (z angl. *nodes*). Těmito uzly se rozumí přepojovací zařízení (z angl. *intermediary devices*) například směrovače (z angl. *routers*), přepínače (z angl. *switches*), rozbočovače (z angl. *hubs*) a mosty (z angl. *bridges*) a koncové zařízení (z angl. *end devices*), jakými jsou počítače nebo mobilní telefony. K přepojování uzlů se používají přenosová média, která se dělí dle způsobu přenosu dat. Mohou být tedy drátová či bezdrátová. Mezi neznámější datové sítě patří počítačové sítě, telekomunikační sítě a internet obecně. Dále lze rozdělit drátové sítě na optické a metalické. Bezdrátové sítě používají k přenosu dat rádiové, nebo jiné elektromagnetické záření.

3.1. Rozdělení sítí

Dle pokrytí lze datové sítě rozdělit na sítě na blízko (NFC – near-field communication) na vzdálenost do 4 cm. Ty zabezpečují pomalou komunikaci zařízení, jsou nejčastěji využívány na bezkontaktní platbu či autentifikaci. Osobní datové sítě neboli personal area network (PAN) slouží k zabezpečení komunikace zařízení v prostoru jednotlivce. Nejčastěji jsou využívané na připojení chytrých telefonů s chytrými doplňky.

3.1.1. Páteřní sítě – MAN a WAN

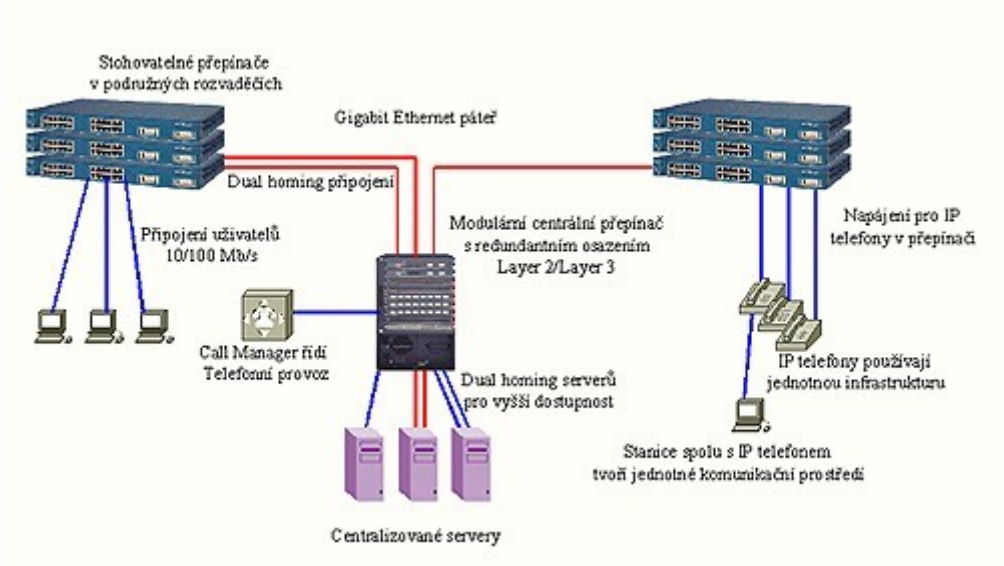
Páteřními sítěmi můžeme rozumět rozsáhlé sítě (WAN – wide area network) a metropolitní sítě (MAN – metropolitan area network), které jsou si ve skutečnosti docela podobné. Jedná se o sítě spojující více sítí LAN. Rozdíl mezi nimi nalezneme v rozsahu pokrytí. Zatímco MAN pojí sítě LAN prostřednictvím vysokorychlostních sítí v rámci území města do jedné velké sítě, WAN je tvořena více LAN sítěmi, které ale zahrnují a zabezpečují komunikaci na rozsáhlejším geografickém území, například regiony, kraje, státy a kontinenty.



Obrázek č. 1 – *rozdíly sítí LAN*. MAN, WAN APPOSITE TECHNOLOGIES, *What's The Difference Between A Local Area Network (LAN), Metropolitan Area Network (MAN), & Wide Area Network (WAN)?* [online]. Dostupné z: https://www.apposite-tech.com/whats-difference-metropolitan-area-network-man-wide-area-network-wan/

3.1.2. Lokální sítě – LAN

Lokální sítě neboli LAN (local area network) jsou datové sítě běžně omezené na malé oblasti, většinou se jedná o jednu budovu, například domov nebo malou firmu a mohou obsahovat několik zařízení. LAN je tedy síť pojící zařízení v jedné vymezené oblasti. Výhodou používání sítí LAN je, že všechna zařízení jsou propojena do sítě. Mohou tak sdílet jedno připojení k internetu, sdílet mezi sebou soubory, tisknout prostřednictvím sdílených tiskových zařízení.



Obrázek č. 2 – *struktura sítě LAN*. EUROSPOJ. *Rozdělení sítí LAN, MAN, WAN* [online] Dostupné z: https://eurospoj.cz/datove-site/

4. Aktivní prvky sítě

4.1. Repeater (opakovač)

Patří k nejjednodušším prvkům sítě, protože slouží k zesílení jím procházejícího signálu. Jedná se o zařízení se dvěma stejnými konektory, používá se v případech, kde síťový kabel není tak dlouhý a mohlo by dojít k zeslabení signálu na jeho konci.

4.2. Switch

Switch je aktivní prvek sítě, který pojí její jednotlivé části. Slouží jako centrální prvek v sítích hvězdicové typologie. V porovnání s hubem je switch inteligentnější, na základě MAC adresy dokáže rozpoznat, kam mají být data doručena, snížit tok zbytečných dat na síti a zefektivnit tak svoji funkčnost.

4.3. Router

Síťové zařízení, jež zprostředkovává přenos dat mezi dvěma nebo více sítěmi v procesu zvaném „routing“. Router propojuje sítě na úrovni vrstvy modelu osy. Je osazen dvěma, nebo více síťovými rozhraními, které mohou být stejného typu, ale není to potřeba. Router analyzuje adresu každého datagramu, který přichází

od jiného síťového zařízení na jedno ze svých síťových rozhraní a na základě stavu sítě na jiných rozhraních rozhoduje, kterému dalšímu zařízení má datagram zaslat, aby se dostal do bodu určení. Routery navzájem komunikují a podávají si informace o stavu sítě a směrování prostřednictvím zvláštních komunikačních protokolů ICMP.

4.4. Brána (gateway)

Gateway je uzel v sítích pojící dvě sítě používající odlišné protokoly. Brána tak vykonává i funkci routeru, a proto je nadřazena v hierarchii síťových zařízení. Tento prvek například přijímá z internetu pomocí webové stránky zprávu, kterou odesílá do mobilní GSM sítě jako SMS zprávu.

Funkce brány

Prvním typem brány je brána, která pracuje na aplikační úrovni. Brána přijme celou zprávu z mnoha menších částí, například datagramů. Zprávu pak převede do formátu určeného pro cílovou síť a odešle. Brána je tvořena speciálním programem spuštěným na PC, které je připojené do obou různých sítí, například do internetu za použití síťové karty a do GSM sítě pomocí mobilního telefonu, který je připojený přes sériový port.

Druhým typem brány je brána, která pracuje na transportní, nebo síťové vrstvě. Tyto brány pracují na nižší síťové vrstvě, například přímo s datagramy. V tomto případě brána zprávu nedekóduje, ale jenom transformuje datagramy jedné sítě do datagramů druhé sítě. Příkladem je tzv. SOCKS, kde dochází k přenosu dat TCP/IP přes síť, která TCP/IP nepodporuje. V takovém případě TCP/IP pomocí jiného protokolu například IPX/SPX a v bráně tak probíhá zpětný převod do protokolu TCP/IP a odeslání do cílového místa v internetu.

4.5. HUB (Rozbočovač)

Podstata hubu spočívá v tom, že funguje jako multiportový opakovač, který spojuje různé větve vodičů, například v topologii hvězda, a propojuje různá zařízení. Huby nedisponují schopností filtrovat data, takže všechny datové pakety jsou vysílány na všechna připojená zařízení. To znamená, že veškerá komunikace

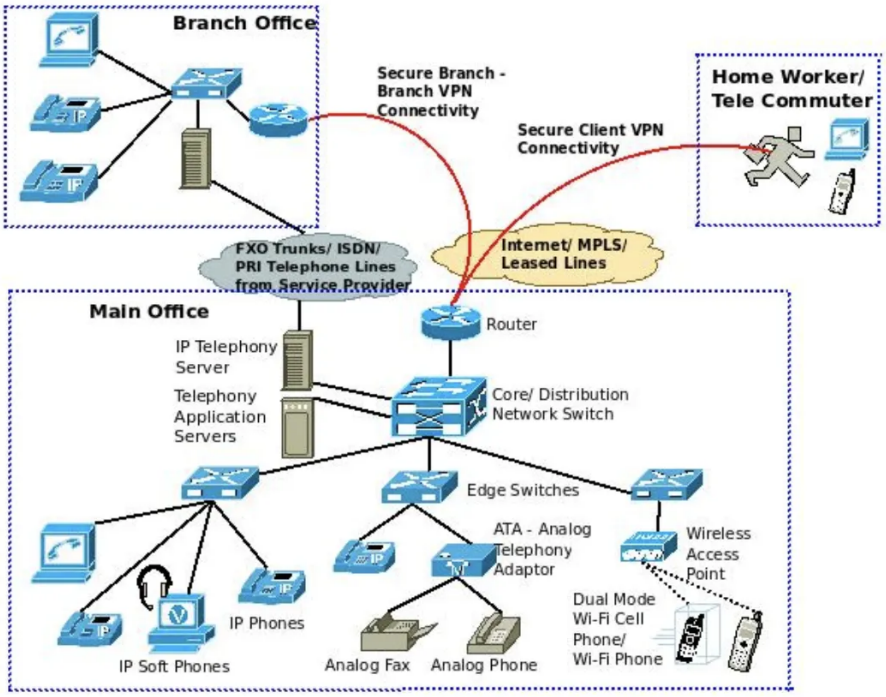
přes hub sdílí stejnou kolizní doménu. Hub nepoužívá směrovací tabulku pro přesměrování dat na specifické porty.

4.6. IP telefonie

Telefonní služby přenášené pomocí IP sítí využívají Internet Protocol (IP) k přenosu hlasových informací po datových sítích. Tento protokol, původně navržený pro přenos dat, umožňuje přenášet hlas společně s dalšími daty přes komunikační sítě. IP protokol funguje na základě přenosu datových paketů od odesílatele k příjemci bez preferování jednoho před ostatními. Princip IP telefonie spočívá v nahrazení tradičních telefonních ústředen za zařízení, která zajišťují převod hlasu na IP pakety a řízení komunikace v rámci sítě. IP telefonie využívá principu přepínání paketů, což využívá přenos hlasu ve formě číselníkových dat. Pokud data nedosáhnou cílového příjemce, mohou být dočasně zadržena v síti nebo dokonce vrácena odesílateli. Tím se odlišuje od tradiční telefonie, kde je potřeba stejného typu koncových zařízení pro komunikaci. IP telefonie je napájena za pomocí standardu Power over Ethernet přímo z infrastruktury. Z mého pohledu bylo vynalezení IP telefonie velikým milníkem v IT odvětví.

4.7. VoIP telefonie

VoIP neboli Voice over Internet Protocol, umožňuje uživatelům provádět hovory, vést videokonference a posílat multimediální zprávy prostřednictvím internetového připojení. Tento termín můžeme chápat jako širší koncept, který zahrnuje přenos hlasových dat přes IP sítě. VoIP je specifický aspektem IP telefonie, který se zaměřuje převážně na hovory prováděné přes internet. IP telefonie představuje rozsáhlejší myšlenku, která zahrnuje různé formy komunikace, včetně hlasových hovorů, videohovorů a zasílání zpráv, vše integrované do jednoho systému. Někdy jsou termíny VoIP a IP telefonie zaměňovány, ale jejich význam se může lišit v závislosti na kontextu, ve kterém jsou použity.



Obrázek č. 3 – *architektura VoIP/IP telefonie*. NGUYEN, Kevin. *VoIP Architecture Diagram,* [online]. Dostupné z: https://www.8x8.com/blog/voip-architecture-diagram

5. Pasivní síťové prvky

Pasivní síťový prvek je prvek sítě, jež data přenáší data v síti bez jakékoliv modifikace nebo zásahu. Mezi pasivní síťové prvky řadíme kabely, jejich spojky, koncovky, zásuvky či rozvaděče.

5.1. PoE (Power over Ethernet)

Možnost přívodu energie do zařízení za použití ethernetového kabelu, kde není potřeba přivést k zařízení přívod energie z externího zdroje. Použití PoE usnadňuje kabelovou infrastrukturu, jelikož není potřeba po budově rozvádět více typů kabelů. Je nutno rozvést jen kabeláž pro počítačovou síť, která napájí zařízení přímo z ní. Aby zařízení, která jsou připojena prostřednictvím PoE fungovala, je nutno použití síťového prvku, který tento standard podporuje.

6. Bezpečnost

Narušení síťové bezpečnosti je v dnešním světě běžným a každodenním jevem. Některé je možno považovat za malé s malými datovými či finančními ztrátami, velké množství je ale možné označit za vážné nebo i katastrofální. Vzhledem k tomu, že v sítích se často pracuje s citlivými daty, je otázka síťové bezpečnosti důležitá. Dle institutu SANS je síťová bezpečnost procesem, během kterého dochází k vykonávání preventivních opatření na ochranu základní síťové infrastruktury před neoprávněným přístupem, zneužitím, poruchou, modifikací, zničením dat, nebo jejich nepovoleným zveřejněním. Implementace těchto bezpečnostních opatření umožňuje počítačům, uživatelům programů vykonávat jejich povolené kritické funkce v rámci bezpečného prostředí.

6.1. Zabezpečení datových sítí

Zabezpečení sítě vyžaduje komplexní využití hardwaru, jako například směrovače, firewally, IPS, IDS a protimalwarové softwarové aplikace. V posledních letech narostla poptávka po bezpečnostních analyticích, jelikož se v průběhu let vyvíjejí nejen technologie zabezpečení, ale i typy a způsoby kybernetických útoků. Jejich prací je implementace bezpečnostních opatření a také sledování reakcí a efektivity těchto implementací.

6.1.1. Brána firewall

Síťová bezpečnostní brána, také známá pod pojem firewall, se používá na analýzu příchozích a odchozích datových toků na základě předem stanovených pravidel a filtruje komunikaci z nedostatečně zabezpečených nebo neověřených zdrojů s cílem zabránit útokům. Pravidla například omezují skupiny IP adres přistupovat do určitých částí sítě, nebo k určitým portům. Tímto způsobem se dá síť segregovat a zabezpečit její části proti nepovolenému přístupu. Brány firewall mohou být jak hardwarové, tak i softwarové, obecně je doporučeno použití obou typů. Softwarový firewall je nainstalovaný program na každém koncovém zařízení regulující komunikaci pomocí portů a aplikací, hardwarový firewall je fyzické zařízení zapojené do sítě před koncová zařízení na jejich ochranu.

6.1.2. Proxy server

Server Proxy je server počítačové sítě umožňující klientům nepřímé připojení k jinému serveru. Proxy server funguje jako zprostředkovatel mezi klientem a cílovým serverem. Předkládá požadavky klienta a oproti cílovému serveru vystupuje jako klient. Přijatý požadavek pak odesílá zpátky klientovi.

6.1.3. DHCP protokol

Je protokol sloužící ke správě sítě. Používá se v sítích internetového protokolu (IP) k automatickému přidělování IP adres a jiných parametrů za použití zařízení, které je připojené k síti na základě architektury klient – server.

6.1.4. DNS

DNS (z angl. Domain Name Systém) je hierarchický a distribuovaný systém pojmenování pro počítače, služby nebo další zdroje v internetu a jiných sítích internetového protokolu (IP). Slouží ke sdružování různých informací s názvy domén za pomocí identifikačních řetězců, jež jsou přiřazeny ke každé z přidružených entit. Nejvýrazněji překládá snadno zapamatovatelné názvy domén na číselné IP adresy, které jsou potřebné k lokalizaci a identifikaci PC služeb a zařízení za pomoci základních síťových protokolů.

6.1.5. Security Information and Event Management (SIEM)

SIEM je obor počítačové bezpečnosti, kde softwarové produkty a služby kombinují správu bezpečnostních informací a správu bezpečnostních událostí. SIEM je typickou složkou každého security operation center, což je tým odpovědný za řešení bezpečnostních problémů v rámci organizace.

6.1.6. Systém prevence průniku (IPS)

Systém prevence průniku (z angl. Intrusion Prevention System) je používaný jako nástroj k zabezpečení sítě a k prevenci hrozeb. Cílem tohoto systému je rychle a hlavně správně identifikovat a zastavit potenciální hrozby, které můžou způsobit škody. IPS se tedy používá na průzkum toku dat v síťovém provozu a k nalezení škodlivého softwaru a zabránění zneužití zranitelnosti sítě. Tyto systémy jsou obvykle implementovány za bránou firewall a to tak, že IPS slouží jako průchod veškeré síťové komunikace. Na tomto místě vystupují jako další vrstva ochrany, snažící se odhalit škodlivý obsah.

Podle detekčních metod dělíme IPS na: detekce na základě podpisu – IPS zde používá k detekci hrozeb a vykonávání akce podpisy útoků (informace, které identifikují typ útoků), detekce na základě anomálie – IPS hledá neočekávané chování v síti a blokuje přístup k zařízením po zjištění anomálie. Mezi výhody použití IPS můžeme zařadit zabránění útoků, jako například hrozby útoku nultého dne (útok nebo hrozba snažící se využít zranitelnosti používaného softwaru, pro který ještě neexistuje obrana) [15], DOS (z angl. Denial-Of-Service), DDOS (z angl. Distributed-Denail-of-Service) a brute – force útoky.

DOS (klasické odepření služby) útoky jsou útoky na internetové služby nebo stránky, jejichž záměrem je cílovou službu znefunkčnit a znepřístupnit ostatním uživatelům. DDOS (distribuované odepření služby) je podkategorií DOS, která se zaměřuje na zneškodnění a zahlcení cílové služby využitím velkého množství zařízení z různých geografických lokalit. Brute-force attack (útok hrubou silou) popisuje jev, při kterém útočník zkouší různé kombinace hesel, nebo číselných kombinací ve víře, že zkoušením dosáhne správné kombinace.

6.1.7. Systém detekce průniku (IDS)

Systém detekce průniku (z angl. Intrusion Detection System) je systém, který na rozdíl od IPS nezabraňuje jednotlivým útokům, ale snaží se útoky detekovat a informovat o nich jiné zařízení nebo administrátora. Systém IDS na vytvoření těchto upozornění využívá sledování aktivit za použití jeho vědomostí (databáze, statistiky, AI (umělé inteligence), atd.). Jelikož je jeho úloha pouze monitorovací, není oprávněn systém IDS vykonávat akce k zablokování podezřelých aktivit, ale potřebují administrátora ke zpracování upozornění. Tato zařízení jsou do sítě zapojena paralelně, z čehož vyplývá, že síťová komunikace prochází přímo přes IDS.

Systémy detekce průniku můžeme rozdělit obdobně jako IPS, a to tedy na: detekce na základě podpisu (stejná jako IPS), IDS využívá k detekci hrozeb již známé vzory útoků a dalším detekce na základě anomálie – touto metodou je možné odhalit dosud neznámé útoky, jelikož útoky se vyvíjejí rychle. Pro tuto metodu je použité strojové učení k vytvoření účinného modelu, který vyhodnocuje, zda se jedná o útočnou aktivitu, nebo běžnou síťovou komunikaci. Metody založené na strojovém učení jsou z pohledu generalizace lepší s porovnáním metodiky na základě podpisu, jelikož tyto modely mohou být naučeny na základě našich požadavků, aplikací nebo prostředí.

6.1.8. Antivir

Je znám také pod názvem antimalware, jedná se o počítačový program používaný k prevenci, detekci a odstranění malwaru. Antivir byl původně vyvinut k detekci a odstranění virů. S rozšířením dalšího malwaru však antivir začal chránit před dalšími počítačovými hrozbami. Některé produkty také obsahují ochranu před škodlivými URL adresami a phishingem.

6.2. Ochrana dat

Mezi tři hlavní zásady bezpečnosti datových sítí patří důvěrnost, integrita a dostupnost. Věda, která se zabývá zabezpečením informací, se nazývá kryptologie, dále se dělí na dvě vědní disciplíny, a to kryptografii a kryptoanalýzu. Kryptografie se zabývá návrhem zabezpečení na ochranu informací

a kryptoanalýza zkoumá možnosti útoků při různých typech zabezpečení. Možnosti, jak chránit informaci během její výměny v počítačové síti nám poskytuje také tato věda.

6.2.1. Šifrování

Pojmem šifrování se rozumí proces modifikace informací před jejím odesláním. Cílem zmíněné modifikace je utajit obsah dané informace. I kdyby byla nekompetentní osoba schopna zašifrovanou informaci zachytit, neměla by být schopna zjistit, respektive dešifrovat obsah informace. K šifrování kromě šifrovacího algoritmu je potřebná ještě dodatečná informace. Tuto informaci nazýváme „klíč“. To znamená, že hlavním záměrem šifrování je znemožnění dešifrování informace bez znalosti klíče. Šifrovací systémy dělíme na symetrické a asymetrické. Symetrické využívají k šifrování jeden utajený klíč sloužící na šifrování a dešifrování informace a zabezpečení informace je zde závislé na kryptografické síle klíče a jeho utajení. Asymetrické šifrování je založeno na existenci dvou kryptografických klíčů, které označujeme jako soukromý a veřejný. Při asymetrickém šifrování je soukromý klíč použitý na dešifrování obsahu zprávy a je utajen, zatímco veřejný klíč je veřejně přístupný a slouží k zašifrování obsahu zprávy. Výhodou asymetrického šifrování je snazší správa klíčů, ale nevýhodou je nezanedbatelně vyšší výpočtová náročnost, právě proto se v praxi využívá hybridní šifrování, což je kombinace symetrického a asymetrického šifrování. Principem tohoto typu šifrování je, že se zpráva zašifruje pomocí náhodně zvoleného klíče asymetrické šifry. Tento náhodný klíč je následně zašifrován využitím asymetrického šifrování za pomoci veřejného klíče příjemce. Příjemce po přijetí zprávy nejdříve dešifruje zašifrovaný náhodný klíč použitím svého soukromého klíče a dešifrovaný náhodný klíč pak použije k dešifrování zprávy.

6.2.2. Elektronický podpis

Při použití symetrického a asymetrického šifrování se vytváří podstatný nedostatek a tím je autentizace šifrovaných údajů. Jako řešení vidíme elektronický podpis. Je realizovaný za pomoci asymetrických šifrovacích systémů. Základním principem fungování elektronického podpisu je, že z dokumentu,

který podepisujeme, je za pomocí hashovací funkce vypočítaný otisk dokumentu tzv. hashovací kód. Algoritmus výpočtu nám zaručuje, že pro každý dokument je výsledkem rozdílná číselná hodnota hashovacího kódu.

6.2.3. VPN (Virtual Private Network)

VPN je mechanismus sloužící k vytvoření připojení zabezpečeného vzdáleného přístupu přes zprostředkovatelskou síť. Tato privátní síť využívá šifrování a autentifikaci s cílem poskytnout důvěrnost, integritu a ochranu soukromí pro síťovou komunikaci. Technologie VPN může fungovat přes standardní internetové připojení, nebo formou dedikovaných komerčních komunikačních obvodů například ATM, nebo Frame Relay. Jedná se o jeden z nejúčinnějších a nákladově efektivních prostředků k zabezpečení bezpečného vzdáleného připojení.

6.3. Zranitelnost

Zranitelnost můžeme chápat jako chybu v programu nebo systému, která má za důsledek snížení úrovně zabezpečení. Vyskytují se v operačních systémech (OS), serverových aplikacích, uživatelských programech, ale i v OS routerů, switchů a jiných. Z praktického hlediska se dá zranitelnost rozdělit do dvou kategorií:

- Zranitelnosti, pro něž ještě nebyly vydány opravné záplaty – nazýváme je jinak zranitelnosti nultého dne a jelikož pro tyto zranitelnosti neexistují záplaty, jsou pro útočníka nejvíce cenné a získává značnou výhodu. Jedná se například o software, jež vyžaduje aktualizaci.
- Zranitelnosti, pro které již byly záplaty vydány – navzdory dostupnosti záplat existuje určité množství systémů, nebo aplikací, kde nebyly implementovány. Důvodů může být několik, počínaje důvody racionálními až po obyčejnou lenost, pohodlnost, nebo selhání lidského faktoru.

6.4. Kybernetická bezpečnost a bezpečnost informačních systémů

Bezpečnost informačních systémů je oblast zajišťující ochranu informací a dat uložených, zpracovávaných a přenášených v rámci informačních systémů. Zahrnuje opatření a procedury, které mají za cíl chránit integritu, dostupnost a důvěrnost těchto informací před neoprávněným přístupem, pozměněním, zničením nebo ztrátou. Bezpečnost informačních systémů zahrnuje technologická opatření, jako jsou šifrování, firewall, antivirová ochrana, ale také procesy, politiky a pravidla pro řízení přístupu, zálohování dat, školení zaměstnanců a monitorování aktivit pro detekci možných hrozeb a útoků.

Zásadními rozdíly mezi kybernetickou bezpečností a bezpečností informačních systémů je prostředí, kde jsou data zpracovávaná a kde existuje možnost útoků na IS/IT nebo jejich části. Za posledních 50 let jsme postupovali od izolovaných počítačů a minipočítačů přes osobní počítače a počítačové sítě LAN či WAN až k virtuálnímu kyberprostoru. V současnosti probíhají útoky v kyberprostoru, který tvoří nejen počítačové sítě a jejich jednotlivé prvky, což jsou jiné sítě, podsítě atd. ale i jakákoli zařízení, kterým byla přidělena IP adresa. Kyberprostor tedy netvoří pouze počítače, ale cokoliv, co je schopno prostřednictvím protokolu TCP/IP, nebo jiného protokolu komunikovat s jinými prvky kyberprostoru. Na základě nárůstu počtu potenciálních hrozeb v rámci kybernetické bezpečnosti vydala Evropská unie Směrnici NIS. Tento předpis má za úkol sjednotit legislativu v oboru bezpečnosti sítí a informačních systémů a zavést kongruentní standard úrovně kybernetické bezpečnosti. V České republice byla směrnice NIS aplikována do českého právního řádu novelou zákona o kybernetické bezpečnosti.

6.4.1. Kybernetické hrozby

Jednou z nejvíce zřejmých vnějších hrozeb je internet. Pod pojem internet rozumíme celosvětovou síť, která spojuje lidi a zdroje za pomocí vysokorychlostní komunikace v reálném čase. Tato infrastruktura naneštěstí také umožňuje zneužívání v o mnoho větší míře. Díky vývoji internetu a bezdrátové technologie, tak jakýkoliv hacker kdekoliv může iniciovat snahu o narušení bezpečnosti sítě. Mezi nejlepší obranu proti internetovým hrozbám řadíme řádně přezkoumané písemné bezpečnostní politiky, důkladně vyškolený personál v ohledu na kybernetickou bezpečnost, použití firewallu, použití šifrované komunikace (například VPN) a důkladný audit a monitoring činnosti všech uživatelů.

6.5. Příčiny a typy útoků na datové sítě

Je známo, že k útokům dochází denně, ale i tak jsou lidé nezodpovědní a přistupují k problematice kybernetické bezpečnosti lhostejně. Jsou přesvědčeni, že je firewall ochrání. Častým důvodem, díky kterému dochází k narušení bezpečnosti je fakt, že uživatel nemá v oblasti bezpečnosti dostatečnou znalost a tím pádem není schopný rozeznat to, co je pro útočníka zajímavé a co ne. Jiná skupina lidí problematiku potenciální hrozby zná, ale tím veškerý zájem o bezpečnost a potenciální hrozbu končí. Jsou přesvědčeni, že přes firewall žádná hrozba není schopna proniknout. I když je firewall v otázce bezpečnosti přínosem, již mnohokrát jsme byli svědky, kdy firewallové produkty měli v softwaru bezpečnostní chybu, kterou útočníci neprodleně zneužili.

6.5.1. Malware

Slovo malware pochází spojením anglických slov malicious a software, což v překladu znamená škodlivý software. Jedná se o souhrnné pojmenování pro následující typy programů a nástrojů.

Počítačové viry

Jedná se o programy, jejichž vlastnost spočívá v tom, že jsou schopny se připojit k jinému souboru případně programu, čímž soubor infikují a vykonávají

nežádoucí efekty. K jejich šíření je potřeba jiných souborů, které jsou schopny modifikovat tak, že budou obsahovat repliku daného viru.

Počítačový červ

Jedná se o škodlivý software, který ke svému šíření nepotřebuje hostitelský soubor. Je šířen aktivně přes síť, což znamená, že je schopen se šířit z jednoho systému na druhý. Šíření je podmíněno propojením těchto systémů datovou sítí.

Ransomware

Ransomware je druh škodlivého softwaru, jehož úlohou je únos dat. Útočník data zakóduje a požaduje platbu za poskytnutí klíče, který data oběti dešifruje. Ransomwarem lze počítačový systém infikovat při prohlížení webové stránky, určené k infikování počítačového systému škodlivým kódem, otevřením infikované emailové přílohy nebo spuštěním programu, jehož obsahem je ransomware.

Trojský kůň

Pojem trojský kůň popisuje program nebo jeho část, která se nazývá spustitelný kód, prezentující se jako bezvýznamný program. Cílem trojského koně je infikovat počítač a otevřít porty pro útočníka, čímž získá přístup k infikovanému počítači. Trojský kůň se primárně ukrývá ve formě spustitelného souboru .exe, případně .bin, .zip a podobně.

Spyware

Spyware je ve své podstatě špionážní software, jehož úlohou je zachycení citlivých údajů z počítače bez vědomí jeho uživatele. Získaná data se pak snaží odeslat třetí straně. Ve většině případů se informace, které takto předává, týkají hesel, souborů nacházejících se v počítači, aktivit uživatele, nebo programů nainstalovaných na počítači. Spyware není zvykem programovat jako samostatný program. Obvykle se tváří jako užitečná aplikace, případně je do užitečné aplikace přidán, a tak si uživatel svou nedostatečnou obezřetností, nebo neznalostí daný program nainstaluje, čímž počítač infikuje.

Keylogger

Keylogger je software, jehož úlohou je zaznamenávat stisknuté klávesy na počítači. Tyto údaje pak zapisuje do souborů a odesílá osobě, která keylogger (hardwarový nebo softwarový) na počítač nainstalovala. Pomocí tohoto nástroje se odcizí přihlašovací údaje, nebo celková komunikace na počítači, jelikož keylogger zaznamená každou stisknutou klávesu. Moderní softwarové keyloggery umožňují uložit i obraz celé obrazovky, čímž usnadní identifikování aplikace, které přihlašovací údaje patří.

6.5.2. Phishing

Phishing je primitivní metoda na způsob odesílání falšovaného emailu příjemci, který klamavým způsobem napodobuje legální instituci s úmyslem získat důvěrné informace od oběti, například číslo platební karty nebo heslo k internetovému bankovnictví. Email s tímto obsahem navádí uživatele k návštěvě různých webových stránek a zadávání důvěrných informací. Tyto stránky mají stejný vzhled jako stránky instituce, za které je phisher vydává, aby získal důvěru oběti.

6.5.3. Spoofing

Spoofing je založen na principu, při kterém se uživatel sítě nebo program vydává za někoho jiného, respektive krade identitu osobě, za kterou se vydává. Tento typ narušení bezpečnosti spočívá v tom, že si spoofer vybere nějaké koncové zařízení a snaží se získat co nejvíce informací, aby věděl, která zařízení mají jaká práva v síti. Toto zařízení pak vyřadí z provozu, aby jej mohl nahradit, odpovídat místo něj a využívat jeho funkce pro svou potřebu.

6.6. Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací (Information Security Management System (ISMS) dále jen SŘBI) je charakterizován v §2 písm. j) vyhlášky totožně jako v normě ČSN ISO/IEC 27001 jako *„část systému řízení povinné osoby založené na přístupu k rizikům informačního a komunikačního systému, která*

stanoví způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat".[1]

Informační systémy vykonávají důležité úkoly během každodenního provozu v organizacích bez ohledu na jejich velikost. K podpoře svých procesů využívá IS již každá organizace. Během let a díky rozvoji informačních technologií se mění i typy informačních systémů, s čímž úzce souvisí i pojetí řízení bezpečnosti u zpracovávaných přenášených a uchovávaných informací. Během posledních let v minulosti, kdy lidstvo využívalo sálové počítače, bylo cíleno na dodržování kontrol v rámci fyzické bezpečnosti a řízení informačních technologií se vykonávalo v rámci bezpečnostního perimetru. V současné době jsou možnosti informačních a komunikačních technologií velice odlišné. Namísto uzavřeného výpočetního prostředí, které bylo využívané jako součást automatizovaného systému řízení (ASŘ), technologie dospěly až ke globální architektuře informačních systémů spjaté s modely ICT služeb. ICT služby dodávají potřebné funkčnosti a informace nezbytné k realizaci procesů v rámci organizace. Parametry těchto služeb, kvantitativní i kvalitativní, musí být v souladu s aktivitami a činnostmi organizace. V porovnání se systémem ASŘ se dostupnost systém ICT značně rozšířila. Nyní jsou poskytovány v různých lokalitách v online režimu při komunikaci přes veřejné sítě. Pro nynější IS je nutno splňovat požadavky kvalitní podpory procesů, s čímž souvisí i zabezpečení požadavků pro zajištění bezpečnosti, aktuálnosti, věcné správnosti a důvěryhodnosti konkrétních funkcí a procesů. Z hlediska bezpečnosti IS se s touto problematikou pojí zabezpečení zpracovávaných dat proti neoprávněnému přístupu, jejich odcizení či zničení. Je nezbytné, aby funkce a procesy informačních systémů byly v souladu s legislativou České republiky. Co se týče řízení bezpečnosti informací a jejich zpracovávaných dat je nedílnou součástí ekonomické hledisko návrhu realizovaných opatření.

[1] (Vyhláška č. 82/2018 Sb., 2018)

6.7. ITIL 4

Metodika ITIL 4 je rámcem poskytujícím komplexní, praktické a osvědčené postupy pro správu IT služeb po celou dobu jejich životního cyklu. Důraz je kladen na dodanou hodnotu jak produktů, tak služeb. Metodika je navržena jako systém hodnot služeb, zahrnující hlavní principy správy, hodnotový řetězec a procesy s cílem neustálého zlepšování. Poskytuje komplexní operační model pokrývající dodávky produktů a služeb založených na technologii a řídí prostředí ICT s rozšířením na obchodní strategii. ITIL 4 je postaven na systému hodnot služeb SVS, který zdůrazňuje spolupráci všech komponent a činností organizace jako systém, umožňující vytváření hodnoty pro organizace, zákazníky a další zúčastněné strany. Obsahuje vedení ekonomiky služeb a komplexní postupy pro využití nových metod řízení, jako je například DevOps. Pracovní model zahrnuje technické služby a produkty podle digitálního provozního modelu. K dosažení stanovených cílů je v této metodice nutné postupovat podle definovaného řetězce hodnot služeb. ITIL 4 definuje sedm hlavních principů, které jsou obecně formulovány a použitelné pro jakoukoli velikost organizace, a pomáhají upravit vztahy a formy spolupráce mezi jednotlivými pracovními skupinami.

7. Kritická infrastruktura

Pojem kritická infrastruktura je vymezen v zákoně č. 240/2000 Sb. o krizovém řízení a o změně některých jeho zákonů, ve znění pozdějších předpisů (dále jen krizový zákon), a dle §2 se jím rozumí: „*g) kritickou infrastrukturou prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu,“*[2]. S kritickou infrastrukturou úzce souvisí pojem evropská kritická infrastruktura. Tou je myšlena kritická infrastruktura nacházející se na území České republiky, která bude mít v případě výpadku vážný dopad na jiný členský stát Evropské unie.

[2] §2 písm. g) zákona č. 240/2000 Sb. Zákon o krizovém řízení a o změně některých zákonů (krizový zákon)

7.1. Prvek kritické infrastruktury

Vymezení pojmu prvek kritické infrastruktury nalezneme v zákoně č. 240/2000 Sb. Zákon o krizovém řízení a o změně některých zákonů v §2 odst. *„i) prvkem kritické infrastruktury zejména stavba, zařízení, prostředek nebo veřejná infrastruktura36), určené podle průřezových a odvětvových kritérií; je-li prvek kritické infrastruktury součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury“*[3]

8. Legislativní prameny

8.1. Zákon o Integrovaném záchranném systému

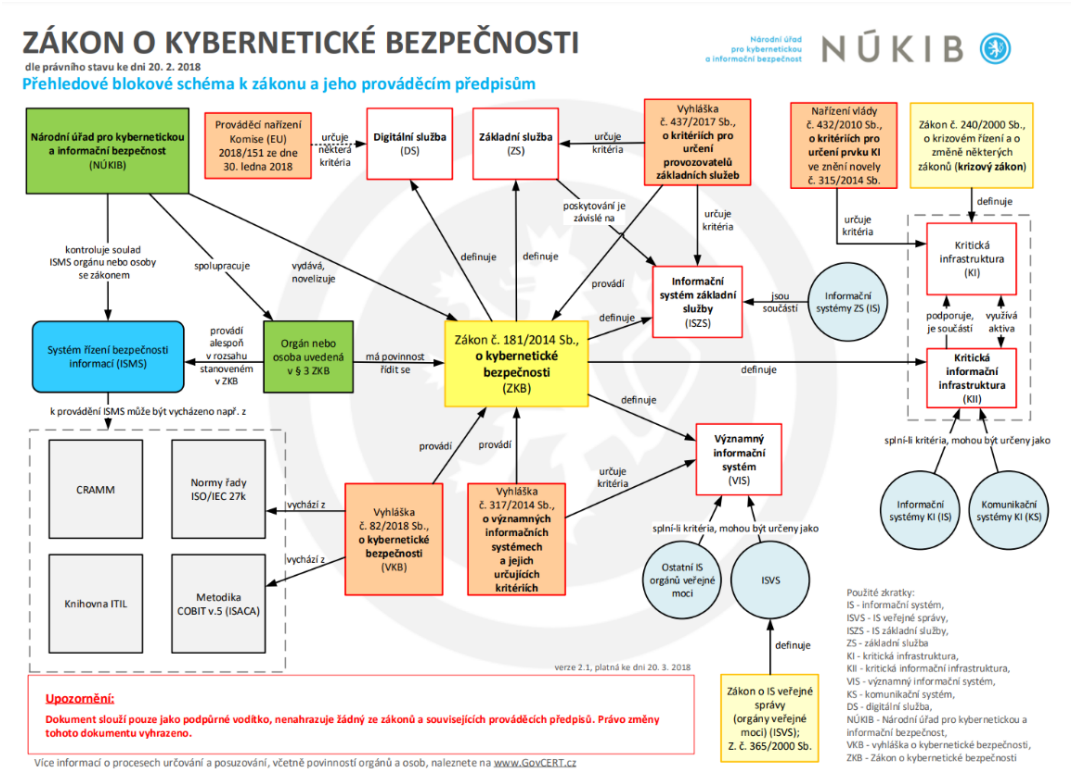
Zákon č. 239/2000 Sb. o integrovaném záchranném systému a o změně některých zákonů vymezuje pojem IZS, popisuje postup jeho složek při přípravě na MU a KS a při výkonu záchranných a likvidačních pracích. Dále obsahuje právní úpravu ochrany obyvatelstva, kde vymezuje pojmy jako evakuace, nouzové přežití, varování a podobně. Charakteristika těchto a dalších opatřeních na ochranu života, majetku a zdraví definuje jako úkoly civilní ochrany čl. 61 Dodatkového protokolu k Ženevským úmluvám z 12. srpna 1949 o ochraně obětí mezinárodních ozbrojených konfliktů.

8.2. Zákon o kybernetické bezpečnosti a související předpisy

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů pojednává o právech a povinnostech osob, působnosti a pravomocech orgánů veřejné moci v oblasti kybernetické bezpečnosti. Dodatečná právní úprava zákona o kybernetické bezpečnosti je charakterizovaná a novelizovaná ve vyhláškách č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích, č. 437/2017 Sb. o kritériích pro určení provozovatele základní služby a č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání

[3] §2 písm. i) zákona č. 240/2000 Sb. Zákon o krizovém řízení a o změně některých zákonů (krizový zákon)

v oblasti kybernetické bezpečnosti a likvidaci dat, která nahradila původní vyhlášku č. 316/2014 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti.



Obrázek č. 4 – *blokové schéma zákona o kybernetické bezpečnosti NÚKIB*. Blokové schéma zákona o KB, [online] dostupné z: https://www.govcert.cz/download/kii-vis/ZKB_blokove_schema.pdf

8.2.1. Vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích

Vstoupila v platnost 19. prosince 2014. Popisuje významné informační systémy a kritéria pro jejich určení. Nabyla účinnosti 1. ledna 2015 a přešla novelizací na vyhlášku č. 205/2016.

8.2.2. Vyhláška č. 437/2017 Sb. o kritériích pro určení provozovatele základní služby

Byla vydána 15. prosince 2017 ve sbírce zákonů České republiky a nabyla účinnosti 1. února 2018. Vyhláška aplikuje směrnici a její požadavky Evropského parlamentu a rady Evropské unie č. 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (směrnice NIS). Vyhláška stanovuje odvětvové a dopadové specifikace, které identifikují provozovatele klíčových služeb a stanovují důležitost poruch těchto služeb pro ochranu společenských a ekonomických aktivit podle příslušných ustanovení zákona o kybernetické bezpečnosti.

8.2.3. Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti

Reguluje předpisy týkající se Směrnice NIS a garantuje dodržování bezpečnostních norem v různých informačních systémech a sítích, včetně těch nejkritičtějších. Ta zahrnuje stanovení požadavků na dokumentaci, bezpečnostních opatření a postupů pro hlášení kybernetických incidentů a jejich řešení. Také stanovuje pravidla pro likvidaci dat a provozních informací.

8.3. Krizový zákon a související předpisy

Zákon č. 240/2000 Sb. O krizovém řízení a o změně některých zákonů (krizový zákon) popisuje pravomoci orgánů územních samosprávných celků a státních orgánů, jejich působnost, práva a povinnosti fyzických a právnických osob při přípravě na KS nesouvisející se zajišťováním obrany státu. Stanovuje řešení KS a podílí se na ochraně kritické infrastruktury. Definuje odpovědnost za porušení těchto povinností. Tento zákon vychází z článku č. 3 ústavního zákona
č. 110/1998 Sb.

8.3.1. Ústavní zákon č. 110/1998 Sb. o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb.

Dle tohoto ústavního zákona je zajištění svrchovanosti a územní celistvosti státu, ochrana demokratických základů, životů, zdraví a majetkových hodnot základní povinností státu. Zákon dále definuje orgány a osoby činné při zajišťování

bezpečnosti ČR, charakterizuje povinnosti státních orgánů, orgánů územních samosprávných celků a fyzických a právnických osob podílejících se na zajišťování bezpečnosti ČR. Ústavní zákon č. 110/1998 Sb. upravuje vyhlášení stavu ohrožení státu a nouzového stavu.

8.3.2. Nařízení vlády ČR č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury

Nařízení vlády stanovuje univerzální kritéria pro identifikaci kritické infrastruktury v různých odvětvích. V jeho příloze je specifikováno devět odvětví spolu s jejich individuálními kritérii pro určení prvků kritické infrastruktury. V rámci rozšíření působnosti kybernetické bezpečnosti na tato odvětví proběhla novelizace nařízením vlády č. 315/2014 Sb.

8.4. Další právní předpisy k řešené problematice

8.4.1. Zákon o zpracování osobních údajů

Tento zákon aplikuje právní předpisy a normy Evropské unie a upracuje práva a povinnosti při zpracování osobních údajů se zřetelem na ochrany soukromí. Zákon č. 110/2019 Sb. o zpracování osobních údajů dále upravuje osobní údaje příslušnými orgány, které slouží k předcházení, odhalování trestné činnosti, stíhání trestných činů, výkonu trestu, nebo ochranných opatření či zajišťování veřejného pořádku, vnitřní bezpečnosti, obranných či bezpečnostních zájmů ČR.

8.4.2. Zákon o utajovaných informací

Zákon č. 412/2005 Sb. o ochraně utajovaných informací a bezpečnostní způsobilosti. Zákon byl mnohokrát novelizován, upravuje a definuje aspekty, které slouží ke stanovení informací, jako informací utajovaných. Stanovuje podmínky pro přístup k daným informacím a další specifické požadavky na jejich ochranu. Definuje jejich citlivé činnosti a podmínky pro jejich vykonávání a s tím spojený výkon státní správy. Hlava VI. definuje bezpečnost informačních a komunikačních systémů, kde udává, že podmínkou k provozu IS je certifikace Národním úřadem pro kybernetickou bezpečnost (NÚKIB).

8.4.3. Zákon o ochraně oznamovatelů

„(1) Ochrana podle tohoto zákona náleží oznamovateli, který oznámení

a) podal prostřednictvím vnitřního oznamovacího systému,

b) podal ministerstvu, nebo

c) uveřejnil, pokud

1. podal oznámení prostřednictvím vnitřního oznamovacího systému a ministerstvu nebo pouze ministerstvu a ve lhůtách stanovených tímto zákonem nebylo přijato vhodné opatření, zejména příslušná osoba neposoudila důvodnost oznámení podle § 12 odst. 3, povinný subjekt nepřijal k předejití nebo nápravě protiprávního stavu jiné vhodné opatření podle § 12 odst. 5, nebo státní zaměstnanec podle § 13 neposoudil oznámení podle § 17 odst. 1,

2. má oprávněný důvod se domnívat, že protiprávní jednání uvedené v oznámení může vést k bezprostřednímu nebo zjevnému ohrožení vnitřního pořádku nebo bezpečnosti, života nebo zdraví, životního prostředí nebo jiného veřejného zájmu nebo ke vzniku nenapravitelné újmy, nebo

3. má oprávněný důvod se domnívat, že v případě podání oznámení ministerstvu existuje vzhledem k okolnostem případu zvýšené riziko, že budou on nebo osoba podle § 4 odst. 2 písm. a) až h) vystaveni odvetným opatřením nebo že je ohrožen postup podle hlavy III.

(2) Ochrana před odvetným opatřením podle tohoto zákona náleží rovněž osobě, která oznámení podala orgánu veřejné moci příslušnému podle jiného právního předpisu nebo přímo použitelného předpisu Evropské unie.

(3) Ochrana před odvetným opatřením nenáleží osobě, která učinila oznámení, aniž měla oprávněné důvody se domnívat, že se zakládá na pravdivých informacích (dále jen „vědomě nepravdivé oznámení“).“[4]

[4] §7 zákona č. 171/2023 Sb. Zákon o ochraně oznamovatelů

9. Krizová komunikace

Předmětem krizové komunikace je účinně a transparentně informovat orgány krizového řízení, veřejnost, zúčastněné strany (fyzické a právnické osoby) a pracovníky v oblasti krizového řízení o současné situaci, rizicích, opatřeních a dalších důležitých informacích. Tento druh komunikace je nezbytný pro správný průběh krizového řízení. Efektivní krizová komunikace přispívá k lepšímu zvládání krizových situací, minimalizaci škod a ochraně životů a majetku.

9.1. Komunikace složek IZS

Systém krizové komunikace je významným aspektem sloužícím ke koordinaci integrovaného záchranného systému, jak ve fázi příprav, tak ve fázi vykonávání záchranných a likvidačních prací (Z a L prací). K prostředku hlasového i datového přenosu informací sloužícím ke krizové komunikaci řadíme:

- Sítě ministerstva vnitra, jež slouží k hlasové a datové komunikaci a připojení hromadné sítě IZS na bázi radiokomunikace.
- Hromadné radiokomunikační sítě pod názvem PEGAS, které jsou využity jako jediný radiokomunikační prostředek v případě ukončení přechodu z radiokomunikačních technologií do hromadné sítě sloužící pro běžný provoz všech složek IZS.
- Pevné telekomunikační sítě dostupné veřejnosti, kde je spojení zabezpečeno regulačními opatřeními, díky uplatnění přednostního spojení.
- Mobilní telekomunikační sítě, kde spojení zabezpečují regulační opatření na základě aplikace (krizové telefony).
- Prostředky telekomunikační sítě sloužící pouze k zajištění spojení orgánů KŘ a obcí.
- Rádiové sítě v záloze, jež fungují v přímém režimu a na určeném kmitočtu.
- Vytvořené rádiové sítě, nebo propojení, jež slouží k přenosu zpráv, při selhání všech technologií.

- Telekomunikační sítě, nebo zařízení, kde o jejich nasazení rozhoduje velitel zásahu (VZ), nebo příslušné operační a informační středisko (OPIS) IZS, zdali došlo k nedostatečné kapacitě běžně používaných prostředků spojení.

10. Krizové plánování

Krizové situace jsou takové události, které lidé považují za nebezpečné tak, že mohou ohrozit jejich zdraví, majetek a v nejhorším i jejich životy. V zákonu o IZS je krizová situace popsána jako „škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také havárie, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací, narušení kritické infrastruktury nebo jiné nebezpečí, při nichž je vyhlášen stav nebezpečí, nouzový stav nebo stav ohrožení státu“[5]. Krizové situace mohou být způsobeny činností člověka (např. havárie, požáry) nebo přírodními živly (povodeň, tornádo).

Pro řešení krizových situací se zpracovávají krizové plány, které obsahují opatření a postupy k řešení takových situací. Krizové plány musí mít zpracovány státní orgány (ministerstva a další ústřední správní orgány) a Česká národní banka. Krizový zákon ukládá povinnost mít vypracovaný krizový plán vyjmenovaným státním orgánům, krajům a obcím s rozšířenou působností. Způsob zpracování a obsah krizových plánů obsahuje nařízení vlády č. 462/2000 Sb. a navazující „Metodika zpracování krizových plánů“. Dokument obsahuje veškeré náležitosti pro zpracování konkrétního krizového plánu. Náležitosti a způsob zpracování je uveden v §15 tohoto nařízení.

Krizový plán se skládá ze základní části, která stanovuje např. kdo má povinnost zpracovat krizový plán, výčet a hodnocení možných krizových rizik a jejich dopady, zásady pro používání přílohové části. Přílohovou část tvoří například typové plány, manuál krizových opatření, operační plány a postupy řešení krizových situací, plán k provádění záchranných a likvidačních prací.

[5] §2 zákona č. 239/2000 Sb. Zákon o integrovaném záchranném systému (zákon o IZS)

11. Integrovaný záchranný systém

„Integrovaný záchranný systém (IZS) je efektivní systém vazeb, pravidel spolupráce a koordinace záchranných složek orgánů státní správy a samosprávy, fyzických a právnických osob při společném provádění záchranných a likvidačních prací a přípravě na mimořádné události.“[6]

Integrovaný záchranný systém ČR vznikl z důvodu potřeby vzájemné koordinace a spolupráce hasičů, záchranářů, policie a dalších složek při řešení mimořádných událostí. Základy IZS byly položeny v roce 1993, legislativně byly však zakotveny později v zákoně č. 239/2000 Sb. O Integrovaném záchranném systému. Složky IZS realizují za pomoci sil a prostředků záchranné a likvidační práce včetně ochrany obyvatel. Smyslem je integrita všech, kdo může být zapojen v rámci poskytnutí sil a prostředků při likvidaci následků mimořádných událostí.

Hlavním koordinátorem a páteří integrovaného záchranného systému je Hasičský záchranný sbor České republiky. V praxi tento pojem znamená, že operačním a informačním střediskem IZS (OPIS IZS) je operační a informační středisko Hasičského záchranného sboru ČR (KOPIS HZS ČR).

Integrovaný záchranný systém dělíme na dvě kategorie, a to jsou hlavní složky IZS a vedlejší složky IZS.

11.1. Základní složky IZS

11.1.1. Hasičský záchranný sbor České republiky

V rámci organizace veřejné správy můžeme hasičský záchranný sbor České republiky (HZS ČR) považovat za jediný veřejný neozbrojený bezpečnostní sbor, která je pod přímou státní správou a současně správním orgánem na úseku požární ochrany (PO). HZS ČR vznikl zákonem 238/200 Sb. o HZS ČR, tento zákon byl však zrušen a následně nahrazen zákone č. 320/2015 Sb. o HZS ČR.

---

[6] HZS ČR. *Co je to IZS?* Online. Dostupné z: https://www.hzscr.cz/clanek/co-je-to-izs.aspx#:~:text=Integrovan%C3%BD%20z%C3%A1chrann%C3%BD%20syst%C3%A9m%20(IZS)%20je,a%20p%C5%99%C3%ADprav%C4%9B%20na%20mimo%C5%99%C3%A1dn%C3%A9%20ud%C3%A1losti. [citováno 2025-01-13].

Zákon č. 320/2015 Sb. o HZS ČR popisuje sbor jako ucelený bezpečnostní sbor a charakterizuje jeho úkoly. K jeho základním úkolům patří ochrana životů a zdraví obyvatel, životního protřídí, majetku a zvířat před požáry, mimořádnými událostmi (MU) a krizovými situacemi. Dále je součinný při zajišťování bezpečnosti České republiky plněním úkolů na úseku PO, ochrany obyvatelstva (OO), civilního nouzového plánování (CNP), krizového řízení (KŘ) v rozsahu a za podmínek stanovených zákonem 320/2015.

Organizace a struktura

HZS ČR se skládá z:

- Generální ředitelství HZS ČR
- Hasičské záchranné sbory krajů
- Záchranný útvar HZS ČR
- SOŠ PO a VOŠ PO

Zvláštností této struktury je právě Generální ředitelství (GŘ), které je součástí Ministerstva vnitra (MV), jehož působnost vykonává všude tam, kde mu to zákon ukládá. To znamená, že MV plní svoji působnost vůči HZS ČR za použití GŘ.

GŘ HZS ČR

GŘ HZS ČR je z hlediska hierarchie organizační struktury na jejím vrcholu. Je součástí Ministerstva vnitra, z čehož vyplývá, že není organizační složkou státu, ale plní úlohy MV na úseku PO, OO, CNP, KŘ a IZS. V čele Generálního ředitelství je generální ředitel Hasičského záchranného sboru České republiky, v současné době je v této funkci Generálporučík Ing. Vladimír Vlček, Ph.D., MBA. Tento post může zastávat pouze příslušník Hasičského záchranného sboru České republiky. Generálního ředitele jmenuje do funkce ministr vnitra. Generálnímu ředitelství jsou podřízeny HZS krajů, Záchranný útvar a škola. Dle zákona o HZS ČR MV zřídilo prostřednictvím GŘ HZS ČR Hasičský útvar ochrany Pražského hradu, který je v rámci organizace součástí HZS.

HZS krajů

Působnost HZS krajů je shodná s územní působností vyšších samosprávných celků – krajů. Na základě této územní působnosti v ČR 13 HZS kraje a HZS hl. m. Prahy. Vnitřní členění HZS kraje je:

- Ředitelství HZS kraje
- Územní odbory HZS kraje
- Jednotky HZS kraje

V čele HZS kraje je ředitel, jehož náplní práce je výkon státní správy v rámci územního obvodu ve věcech PO, OO, CNP, IZS a KŘ s výjimkou veřejného pořádku a vnitřní bezpečnosti. Krajský ředitel stojí za zřízením krajského operačního a informačního střediska (KOPIS), které vykonává svou činnost na úseku operačního řízení. Operační řízení KOPIS je proces zahrnující přijímání a vyhodnocování tísňových zpráv, vysílání sil a prostředků a jejich řízení, vyžadování pomoci od jiných osob, nebo subjektů a poskytování informací veliteli zásahu, nebo dalším subjektům. Územním odborem HZS kraje je myšleno území okresu, které má svého ředitele přímo podřízeného řediteli krajskému, dále pak jednotky PO a zastání OO a požární prevence.

Záchranný útvar HZS ČR

Záchranný útvar HZS ČR (ZÚ HZS ČR) má dislokace v Hlučíně, Zbirohu a Jihlavě. Sídlo ZÚ HZS ČR je v Hlučíně, který je centrálně řízenou zálohovou jednotkou Generálního ředitelství HZS ČR se vznikem 1.1.2009. V jejím čele je velitel útvaru. Hlavní činností ZÚ je záchranná činnost, plnění úkolů jednotek PO při řešení MU nebo KS většího rozsahu a úkoly při obnově území, rozhodne-li tak GŘ. ZÚ HZS ČR se v rámci vnitřní organizační struktury dělí na 4 záchranné roty a oddělení přípravy a řízení jednotek.

SOŠ a VOŠ PO

SOŠ a VOŠ PO sídlí ve Frýdku Místku. Je organizační součástí HZS ČR a organizační složkou státu. V roce 1967 vznikla za účelem vzdělávání v oboru požární ochrany. Účelem školy je vzdělávání a poskytování středoškolského a vyššího odborného zdělání potřebného k výkonu zaměstnání na úseku požární ochrany, ochrany obyvatelstva a krizového řízení. Vede rekvalifikační kurzy

a přípravy na získání odborné způsobilosti, která je potřebná k výkonu služby příslušníků u HZS ČR. Ředitel školy je jmenován generálním ředitelem HZS ČR a zároveň je statutárním orkánem školy.

Hasičský útvar ochrany Pražského hradu

Tento útvar vznikl přijetím nového zákona o HZS ČR (320/2015 Sb.) jež nabyl účinnosti 1.1.2016 a je součástí GŘ HZS ČR. V čele útvaru je velitel útvaru, který je přímo podřízen generálnímu řediteli HZS ČR. Činnost útvaru spočívá v zajištění PO a bezpečnosti Pražského hradu a plnění úkolů v běžné hasičské činnosti ve vlastním zásahovém obvodu, jímž je Pražský hrad.

11.1.2. Jednotky požární ochrany zařazené do plošného pokrytí kraje jednotkami požární ochrany

„Jednotkou požární ochrany (dále jen „jednotka PO“) se rozumí organizovaný systém tvořený odborně vyškolenými osobami (hasiči), požární technikou (automobily) a věcnými prostředky požární ochrany (výbava automobilů, agregáty apod.). Základním posláním jednotek PO je chránit životy a zdraví obyvatel a majetek před požáry a poskytovat účinnou pomoc při mimořádných událostech, které ohrožují život a zdraví obyvatel, majetek nebo životní prostředí a které vyžadují provedení záchranných, resp. likvidačních prací.“[7]

Plošné pokrytí území kraje a hlavního města Prahy jednotkami požární ochrany označuje strategii, při které jsou jednotky požární ochrany umístěny tak, aby co nejlépe pokrývaly celé území daného kraje a hlavního města Prahy.

[7] („Jednotky PO”, online, dostupné z: https://www.hzscr.cz/clanek/jednotky-po-961839.aspx?q=Y2hudW09MQ%3d%3d)

	Kategorie jednotek PO pro účely plošného pokrytí					
	JPO – I	JPO – II	JPO – III	JPO – IV	JPO – V	JPO – VI
Doba výjezdu	2	5	10	2	10	10
Územní působnost	20	10	10	Není	Není	Není
Druh jednotky PO	HZS	JSDHO	JSDHO	HZSP	JSDHO	JSDHP

Tab. č. 1 – operační hodnoty kategorií jednotek PO, HANUŠKA, Zdeněk; ADAMEC, Vilém; ŠENOVSKÝ, Michail a BREJZOVÁ, Iva. *Integrovaný záchranný systém*. Vyd. 2. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2022, ISBN 978-80-7385-262-7

Jednotky požární ochrany jsou začleněny do bezpečnostního systému České republiky. Jejich začlenění do plošného pokrytí území kraje je důležité pro plnění základních úkolů dle Zákona o požární ochraně (č. 133/1985 Sb.), což zahrnuje provádění požárních zásahů a poskytování pomoci při živelných katastrofách a jiných MU. Organizační struktura, požadavky na akceschopnost a procedury výjezdů jednotek jsou stanoveny příslušnou vyhláškou Ministerstva vnitra. Důležitým bodem akceschopnosti jednotek požární ochrany je plnění požadavků na odbornou kvalifikaci všech hasičů podle jejich přidělených funkcí v rámci jednotek, což je definováno jak v zákoně o požární ochraně, tak ve vyhlášce č. 247/2001 Sb., o organizaci a činnosti jednotek požární ochrany.

11.1.3. Poskytovatelé zdravotnické záchranné služby

Dle zákona č. 374/2011 Sb. o zdravotnické záchranné službě se zdravotnickou záchrannou službou rozumí služba, v jejímž rámci je na základě tísňové výzvy není-li dále stanoveno jinak poskytována zejména přednemocniční neodkladná péče osobám s postižením zdraví, nebo přímém ohrožení života. Poskytovatelem zdravotnické záchranné služby (ZZS) je organizace zřízená krajem, jež je vlastníkem oprávnění k poskytování zdravotnické záchranné služby. ZZS je základní složkou IZS. Dle §8 zákona č. 374/2011Sb. je její poskytovatel povinen ji poskytovat nepřetržitě.

V rámci organizační struktury se zařízení ZZS dělí na:

- ředitelství
- zdravotnické operační středisko
- výjezdové základny s výjezdovými skupinami
- pracoviště krizové připravenosti
- vzdělávací a výcvikové středisko

Ředitelství ZZS

Je řídícím orgánem pro poskytování ZZS a pro její činnosti sloužící k řešením MU a KS na území kraje.

Zdravotnické operační středisko

Zdravotnické středisko je pracovištěm operačního řízení pracující v nepřetržitém režimu. Dále je centrem tísňové komunikace na tísňové číslo 155.

Výjezdové základny s výjezdovými skupinami, pracoviště krizové připravenosti

Výjezdovou základnou se rozumí místo, ze kterého na pokyn operátora je zpravidla vyslána výjezdová skupina. Ta je tvořena pracovníky ZZS, má minimálně 2 členy a dělí se na dva druhy. Na výjezdové skupiny rychlé lékařské pomoci (RLP), jejíž členem je lékař, dále pak výjezdové skupiny rychlé zdravotnické pomoci (RZP), jejímiž členy jsou zdravotníci nelékařského charakteru.

Pracoviště krizové připravenosti (PKP)

Slouží ke koordinaci úkolů, které jsou určeny poskytovateli ZZS z krizového plánu dokumentace integrovaného záchranného systému a havarijního plánování, vzdělávání a výcviku pro usnadnění plnění úkolů poskytovatele ZZS v oblasti urgentní medicíny, medicíny katastrof a krizového řízení. Pracoviště KP vypracovává návrh traumatologického plánu a jeho změny

11.1.4. Policie České republiky

Policie České republiky (PČR) je ucelený ozbrojený bezpečnostní sbor zřízený zákonem č. 283/1991 Sb. o policii České republiky. Policie je podřízena

policejnímu prezidentovi dle zákona č. 361/2003 Sb. o služebním poměru příslušníků bezpečnostních sborů. PČR z ekonomického hlediska není samostatná, jelikož její příjmy a výdaje jsou nedílnou součástí rozpočtové kapitoly MV. Současné postavení PČR je upraveno v zákoně č. 273/2008 Sb. o policii České republiky, jehož znění popisuje činnost policie a její pravomoci. Při plnění úkolů policie reprezentuje právnickou osobu, jíž je stát. Základními prvky organizační struktury PČR, jež jsou vymezeny v hlavě II. zákona o policii jsou:

- Policejní prezidium (PPČR)
- Útvary s celostátní působností
- Krajská ředitelství
- Útvary zřízené v rámci kraje

PČR je řízena civilním orgánem, jímž je ministerstvo vnitra ČR v čele s ministrem vnitra, jehož pravomocí je jmenování a odvolávání policejního prezidenta.

Policejní prezidium

V čele hierarchie organizační struktury policie je policejní prezídium. Jeho postavení souvisí s vrcholným řízení výkonu policejní činnosti. Prezidium sídlí v hl. m. Praze. Organizace prezidia je stanovena rozkazem policejního prezidenta, jímž se vydává i organizační řád PPČR. Policejní prezidium má strategickou, metodickou, kontrolní a řídící funkci. V rámci organizačního řádu PPČR jsou uvedena i jednotlivá ředitelství související s organizačním členěním policie. Jsou jimi úřad služby kriminální policie a vyšetřování, ředitelství služby pořádkové policie, ředitelství služby dopravní policie, ředitelství služby pro zbraně a bezpečnostní materiál, ale také i odbor vnitřní kontroly a operační odbor, jež spadají přímo pod policejního prezidenta. Mezi služby patří kriminální policie a vyšetřování, železniční policie, dopravní policie, cizinecká policie, pořádková policie, útvar rychlého nasazení, ochranná služba policie a letecký útvar.

Útvary s celostátní působností

Jedná se o specializované útvary zřízené ministerstvem vnitra na návrh policejního prezidenta na základně nařízení vlády č. 67/2008. Jedná se o útvary:

Národní centrála proti organizovanému zločinu služby kriminální policie a vyšetřování, Národní protidrogová centrála služby kriminální policie a vyšetřování, Útvar zvláštních činností služby kriminální policie a vyšetřování, Útvar speciálních činností služby kriminální policie a vyšetřování, Úřad dokumentace a vyšetřování zločinu komunismu služby kriminální policie a vyšetřování, Kriminalistický ústav, Útvar rychlého nasazení, Ochranná služba (ochrana ústavních činitelů), Útvar pro ochranu prezidenta republiky, Letecká služba, Ředitelství služby cizinecké policie, Pyrotechnická služba, Útvar policejního vzdělávání a služební přípravy.

Krajská ředitelství PČR

Krajská ředitelství (KŘP ČR) jsou útvary s územně vymezenou působností zřízené policejním prezidentem na návrh krajského ředitele. V čele krajského ředitelství stojí krajský ředitel, jenž je přímo podřízen policejnímu prezidentovi. V rámci KŘ jsou zřízeny územní odbory, které vykonávají působnost policie na daném území.

Útvary zřízené v rámci kraje

Útvary zřízené v rámci krajských ředitelství jsou zřízeny na návrh ředitele KŘ policejním prezidentem. V čele těchto útvarů jsou ředitelé.

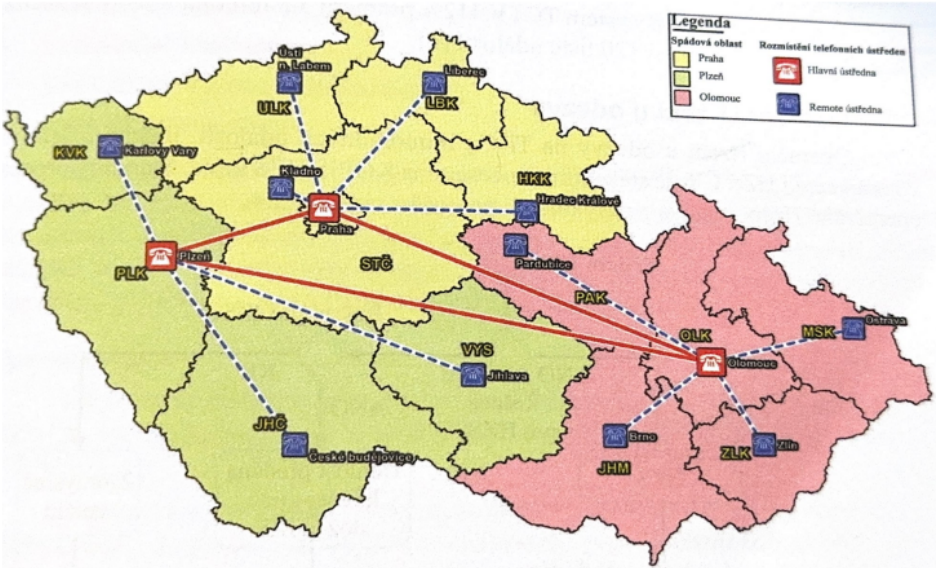
11.2. Vedlejší složky IZS

- Vyčleněné síly a prostředky ozbrojených sil
- Ostatní ozbrojené bezpečnostní sbory
- Ostatní záchranné sbory
- Orgány ochrany veřejného zdraví
- Havarijní, pohotovostní a odborné jiné služby
- Zařízení civilní ochrany
- Neziskové organizace a sdružení občanů, která lze využít k záchranným a likvidačním pracím

11.3. Operační středisko integrovaného záchranného systému

Právní úprava sdílená operačními středisky složek IZS je zákon 239/2000 o IZS. Zákon určuje, že základní složky IZS jsou povinné zajistit nepřetržitou pohotovost sloužící na příjem ohlášení vzniku mimořádných událostí (dále jen MU), neodkladný zásah v místě MU a zpracování obsahu ohlášení. Výkon těchto činností nazýváme také operační činnosti.

Zákon o HZS ČR (320/2015 Sb.) stanovuje zřízení operačního a informačního střediska MV – generálního ředitelství HZS ČR (OPIS MV-GŘ HZS ČR) a krajská operační a informační střediska HZS krajů (KOPIS HZS kraje). KOPIS HZS krajů jsou střediska pro příjem nejen volání na národní číslo tísňového volání – 150, ale i na jednotné evropské číslo tísňového volání – 112. KOPIS rovněž vykonává úkoly svěřené operačním a informačním střediskům IZS a další povinnosti, pokud je to stanoveno jinými právními předpisy.



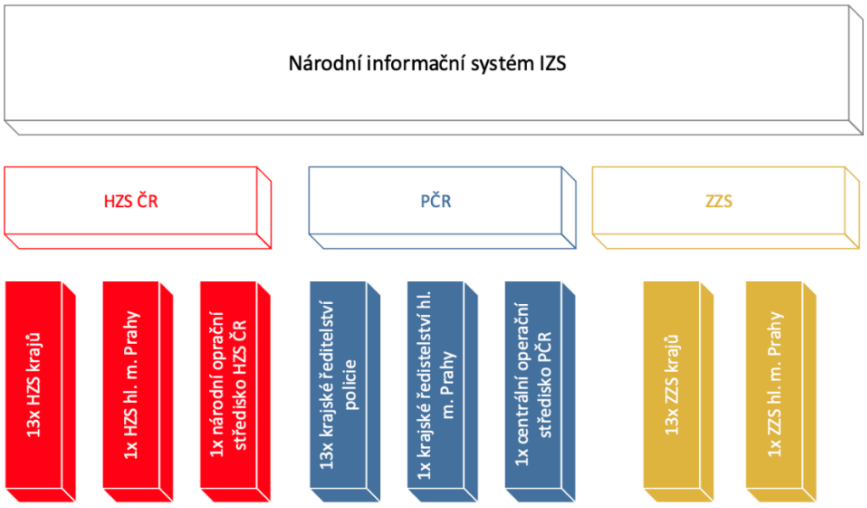
Obrázek č. 5 – organizační struktura TCTV 112 ADAMEC, Vilém; BERGLOWIEC, Petr; VÁLEK, Dušan; ŠENOVSKÝ, Pavel a ADAMEC, Martin.: *Operační střediska v integrovaném záchranném systému*. Vyd. 1. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2019, ISBN 978-80-7385-225-2

„Z procesního hlediska rozlišujeme na KOPIS HZS kraje procesy probíhající v rámci telefonního centra tísňového volání 112, činnosti operační úrovně řízení při zdolávání mimořádných událostí v kompetenci HZS ČR a ostatních činností.

Jednotlivá operátorská pracoviště mohou realizovat všechny výše zmíněné procesní součásti nebo jen některé.“[8]

11.3.1. NIS IZS

Projekt NIS IZS vznikl z důvodu integrace datové komunikace základních složek integrovaného záchranného systému. Realizace projektu systému probíhala mezi roky 2008–2015 a schválené výdaje byly 333 mil. korun. Systém přinesl rychlejší komunikaci mezi operačními středisky základních složek IZS pomocí datových vět. Tato společná platforma osahuje IPL (Informační platforma, součást Národního informačního systému IZS), což je sběrnice předávající data mezi jednotlivými systémy. Při vzniku události ji každá složka ve svém systému datově vkládá do IPL, kde pomocí určených parametrů předá informace dál. Komunikace zahrnuje nejen datové prvky jednotlivých událostí, ale také stav jednotlivých složek IZS v kontextu řešené situace. Stav složek IZS v rámci řešené události jsou interpretovány operátorům za pomocí jednotlivých mandatorních systémů (Geografický informační systém GIS a vizualizace).



. Obrázek č. 6 – *grafické zobrazení NIS IZS,* Zdroj: Vlastní zpracování

[8] (Operační střediska v integrovaném záchranném systému, 2019)

11.3.2. Krajské standardizované projekty HZS krajů

Při nasazování NIS IZS se GŘ HZS ČR rozhodlo standardizovat vybavenost operačních středisek. Na projekt standardizace byl schválen rozpočet 489 mil. korun. Realizační fáze probíhala shodně s realizací NIS IZS, tedy konkrétně v letech 2008–11/2015. Standardizace KOPIS měla veliký přínos pro vyšší informační vybavenost, dále pak pro lepší zajištění propojenosti a akceschopnosti složek při společném zásahu bez ohledu na geografickou polohu jednotlivých OPIS HZS krajů.

11.3.3. Možné vývojové trendy

S vývojem technologií v průběhu posledních let se modernizují i zařízení a systémy využívané OPIS. Operační střediska poslední generace se tak stávají vysoce optimalizovanými a specializovanými řídícími centry. Vize jejich dalšího rozvoje je spojena s možnostmi i potřebami v rámci prostředí I4 (průmysl 4.0), které popisuje informatizaci a robotizaci života v rámci společnosti. Rozvoj operačních středisek počítá s využitím podpory analýz velkých objemů dat, nebo nástrojů umělé inteligence (AI), jež se stává čím dál více populárním prostředkem k plně automatizovanému procesu.

12. Pohled zástupců složek IZS

Otázka č. 1 *(Zhodnocení dostupné páteřní datové sítě na úrovni krajů a lokálních samospráv)*

Zdravotnická záchranná služba – zástupce zdravotnické záchranné služby odpovídající na naše otázky v rámci bakalářské práce uvedl, že datová síť pro hlasovou komunikaci IZS je ve správě Ministerstva vnitra, a tak je možné hodnocení provést z pohledu koncového uživatele. Koncový uživatel, jehož zástupcem byl náš respondent, není spokojen s neexistencí redundantního připojení, jež je právě v řešení. Spokojený ale je s celkovou stabilitou, redundancí a servisním zajištěním provozu. Datovou síť pro datovou komunikaci IZS vnímá v koncovém bodě jako zcela bezproblémovou.

Hasičský záchranný sbor České republiky – respondent zastupující HZS ČR konstatoval, že je datová síť ve vysoké dostupnosti.

Policie České republiky – odborník zastupující policii prohlásil, že dostupnost páteřní datové sítě z pohledu koncového uživatele je vyhovující a neustále se navyšuje její kapacita a redundance.

Otázka č. 2 *(Posouzení šířky pásma, stabilita a odolnost proti výpadkům)*
Zdravotnická záchranná služba – při položení této otázky se respondent odkazoval na předešlou odpověď, kde konstatuje, že je šířka pásma a její stabilita vyhovující, ale odolnost proti výpadkům pro hlasovou komunikaci v koncovém bodě vyhodnotil jako nedostatečnou.

Hasičský záchranný sbor České republiky – příslušník hasičského záchranného sboru pouze konstatoval, že je datová síť stabilní

Policie České republiky – z pohledu policie není posouzení šířky pásma koncový uživatel schopen posoudit. Stabilita a odolnost proti výpadkům je adekvátní.

Otázka č. 3 *(Posouzení aktuální kapacity sítě a schopnosti přenášet velké objemy dat v krizových situacích)*
Zdravotnická záchranná služba – tázaný odpověděl, že datová síť pro hlasovou i datovou komunikaci nepřenáší z pohledu koncového vodu velké objemy dat, její kapacitu však hodnotil jako dostatečnou.

Hasičský záchranný sbor České republiky – na danou otázku mi bylo odpovězeno, že se datová síť postupně modernizuje, a právě kvůli této skutečnosti není tázanému známo, zda bude schopna zvládnout zvýšené toky dat, které souvisí s přenosem videozáznamů ze zásahů.

Policie České republiky – příslušník policie zhodnotil aktuální kapacitu sítě tak, že se dle jeho názoru nachází na hranici své kapacity a mírně naznačil potřebu modernizace a navýšení přenosových kapacit. Zároveň však zmínil, že přenášení velkého objemu dat policie v krizových situacích není schopna hodnotit, jelikož tato skutečnost neprošla řádným testováním.

Otázka č. 4 *(Stanovení specifických požadavků na komunikaci v krizových situacích pro státní správu, samosprávu a složky IZS)*

Zdravotnická záchranná služba – požadavky, jež stanovila zdravotnická záchranná služba jsou stabilita služby, dostupnost služby, dostupnost rychlého servisního zásahu

Hasičský záchranný sbor České republiky – zástupce HZS ČR jako požadavek definoval potřebu schopnosti sítě se přepnout do stavu „nouzový režim“, kdy se omezí toky méně důležitých dat v případě krizových situací. Nedůležitá data blíže však nedefinoval, dle jeho názoru je nutno provést analýzu a tyto „nedůležité přenosy“ identifikovat.

Policie České republiky – v otázce specifických požadavků stanovil příslušník police obdobné požadavky, jež byly stanoveny zástupcem ZZS.

Otázka č. 5 *(Zhodnocení bezpečnostních opatření implementovaných na úrovni datových sítí)*

Zdravotnická záchranná služba – ZZS v tomto případě nebyla schopna bezpečnostní opatření z pohledu koncového bodu zhodnotit

Hasičský záchranný sbor České republiky – odborník v oblasti IT zastupující HZS ČR zhodnotil bezpečnostní opatření sítě jako dostatečné k jejímu využívání, dále poukázal na potřebu ochrany sítě v rámci jednotlivých organizací a přistupovat k společné síti jako k síti nedůvěryhodné

Policie České republiky – z pohledu PČR je vždy prostor na zlepšení s ohledem na vývoj a sofistikovanost útoků v kyberprostoru za poslední dobu

Otázka č. 6 *(Hrozby a rizika spojená s bezpečností dat a komunikací)*

Zdravotnická záchranná služba – jako hrozby a rizika spojené s bezpečností dat a komunikací bylo zástupcem ZZS uvedeno vyřazení služeb sloužících ke komunikaci z provozu nebo jejich možné zneužití

Hasičský záchranný sbor České republiky – příslušník HZS ČR uvedl, že jako složka, jež je součástí IZS, musí myslet na reálnou možnost útoků cizí moci. Útočníka vnímal jako člověka s neomezenými zdroji lidí, financí a technologií. Za největší hrozbu definoval neautorizovanou změnu dat, jež může zkomplikovat a znemožnit zásah jednotek HZS, které spoléhají na data a informace sdělené operačními středisky, a na základě kterých se rozhodují, jak během zásahu postupovat. Kdyby dostaly špatná data a informace, rozhodnutí založené na těchto datech by mohlo mít i fatální následky a důsledky na životy a zdraví obyvatel.

Policie České republiky – za největší hrozbu PČR v rámci bezpečnosti dat a komunikace definovala kyberútok na integritu dat, hrozbu jejich zneužití nebo jejich úpravu z pro útočníka zištného důvodu.

Otázka č. 7 *(Posouzení interoperability s dalšími systémy a komunikačními kanály v rámci integrovaného záchranného systému (spolupráce několika systémů))*

Zdravotnická záchranná služba – v rámci otázky Posouzení interoperability s dalšími systémy a komunikačními kanály v rámci integrovaného záchranného systému respondent uvedl, že v rámci základních složek je k dispozici unifikované řešení pro hlasovou a datovou komunikaci. Interoperabilita je řešena na úrovni organizačních opatření.

Hasičský záchranný sbor České republiky – v tomto případě se odpovídající zaměřil na Národní Informační Systém (NIS), jež popsal jako funkční, ale zároveň poukázal na skutečnost, že jeho implementace proběhla v roce 2015 a tedy technologie odpovídají trendům tohoto roku, čímž naznačil, že nevyhovují dnešním požadavkům. NIS je i dnes ve stejné podobě jako v době jeho uvedení do provozu.

Policie České republiky – základní složky IZS používají sjednocené řešení pro hlasovou komunikaci a je k dispozici modulární řešení pro datovou komunikaci. Řešení interoperability uvedl jako na úrovni lidských zdrojů.

Otázka č. 8 *(Posouzení dostupné technologie pro rychlou a efektivní komunikaci během krizových událostí)*

Zdravotnická záchranná služba – popsáno jako spolehlivé a naplňující veškeré potřeby uživatelů

Hasičský záchranný sbor České republiky – zhodnocení technologie bylo popsáno jako absolutně nevyhovující pro dnešní požadavky. Dle názoru odborníka IT se složky IZS s touto skutečností vypořádávají tak, že požadavky dnešní doby transformují do podoby, se kterou je používaná technologie schopna vypořádat. Bylo zde poukázáno na potřeby zavedení zcela nové technologie, jež se bude schopna přizpůsobit aktuálním trendům a požadavkům.

Policie České republiky – na rozdíl od HZS byl příslušník méně kritický a jeho pohled na dostupnost technologií byl spíše pozitivní. Jejich dostupnost zhodnotil jako vyhovující, za nedostatečnou však označil informovanost koncových uživatelů o jejím plném využití.

Otázka č. 9 *(Zjištění protokolů šifrování, firewall, monitoring a dalších bezpečnostních prvků)*

Zdravotnická záchranná služba – dle ZZS není možné zjištění protokolů šifrování, firewall, monitoring a jiné bezpečnostní prvky hodnotit, jelikož jsou úkolem vlastníka a provozovatele.

Hasičský záchranný sbor České republiky – zástupce hasičů evaluoval kybernetickou bezpečnost a její úroveň obecně jako velmi nízkou.

Policie České republiky – daná problematika byla PČR popsána v kontextu bezpečnostních incidentů jako vyhovující.

Otázka č. 10 *(Posouzení struktury správy a údržby datových sítí)*

Zdravotnická záchranná služba – ZZS opětovně poukázala na fakt, že struktura zprávy a údržby není hodnotitelná z pohledu koncového bodu, jelikož je definována vlastníkem a provozovatelem této sítě.

Hasičský záchranný sbor České republiky – na tuto otázku bylo od HZS odpovězeno velice obdobně jako na otázku předchozí.

Policie České republiky – správa struktury a údržba sítí byly charakterizovány jako závislé na finančních prostředcích, o kterých se příslušník PČR domnívá, že jsou nedostatečné.

Otázka č. 11 *(Zhodnocení finančních nákladů spojených s provozem, údržbou a rozvojem těchto sítí)*

Zdravotnická záchranná služba – opět z pohledu ZZS nelze hodnotit danou problematiku, jelikož finanční náklady jsou v gesci vlastníka a provozovatele.

Hasičský záchranný sbor České republiky – respondent zastupující HZS kritizoval obnos dostupných finančních prostředků, považuje je za zcela nedostatečné a podotýká, že za dostupné finanční zdroje není možno provozovat a udržovat dostupné ICT.

Policie České republiky – „nelze hodnotit“

Otázka č. 12 *(Návrh plánu na aktualizace a modernizaci sítí v rámci technologického rozvoje)*

Zdravotnická záchranná služba – koncový uživatel, kterého respondent zastupuje nemá žádné požadavky na aktualizaci a modernizaci využívaných sítí s výjimkou požadavků na zvýšení odolnosti proti výpadkům u datové sítě, zajišťující hlasovou komunikaci.

Hasičský záchranný sbor České republiky – tázaný ocenil existenci programu s názvem Kybernetická bezpečnost HZS ČR, jež obsahuje komplexní řadu technických opatření sloužících k modernizaci a zabezpečení technologií.

Policie České republiky – příslušník policie České republiky se k dané problematice pouze stroze vyjádřil: „nejsou peníze, zbytečné hodnotit“.

13. Výsledek, návrh a doporučení

V mnou výše stanovené hypotéze bylo konstatováno, že funkčnost, bezpečnost, kapacita a využívání datových sítí je uspokojivá pro všechny složky IZS. Ačkoli jsem se domníval, že tato hypotéza bude rozhodně verifikovaná, můj kvalitativní výzkum však hypotézu falsifikoval. Všechny tři z tázaných základních složek IZS poukazovaly na značné nedostatky v rámci bezpečnosti informaci,

jednak v oblasti finančních nedostatků, nedostatečné informovanosti ohledně dané problematiky anebo zastaralosti systémů. Popis těchto problémů můžeme pozorovat na výše zodpovězených otázkách viz otázka č. 4. Při komparaci odpovědí složek pozorujeme rozdílnost odpovědí a názorů jednotlivých složek IZS, z čeho vyplývá, že každá složka klade důraz na jiné odvětví a oblasti v rámci bezpečnosti informací a informačních systémů. Například policie klade důraz na ochranu dat před hrozbou jejich zneužití, nebo úpravy, zatímco HZS považuje za důležitou správnost a přesnost dat.

V rámci mnou doporučených řešení bych chtěl uvést důležitost doposud neexistujícího testování datových systémů, kterými v případě MU, nebo KS může docházet ke zvýšenému toku dat a informací, jež by mohly mít za následek fatální výpadek zmíněných sítí. Dalším doporučeným návrhem je uvolnění vyšších finančních prostředků do oblasti zabezpečení datových sítí a komunikací. Důvodem tohoto návrhu je fakt, že i samotné složky si jsou vědomy finanční nedostatečnosti v tomto ohledu. S tímto návrhem úzce souvisí aktualizace systémů a sledování aktuálních trendů v oblasti zabezpečení proti útokům, jelikož oblast IT je oblastí budoucnosti s nezastavitelným vývojem, z čehož vyvstává potřeba „držet krok“ s vývojem ICT. Dle mého názoru je důležité investovat vyšší finanční částky do aktualizací nových technologií a snažit se držet krok s pravidelnými aktualizacemi a aktuálními trendy na trhu, jelikož jenom tak jsme schopni zabránit historicky se opakujících nedostatků, které vedly k nynější zastaralosti NIS. Problematika ohledně aktuálnosti technologie NIS je uvedena výše. Posledním doporučením z mé strany je lepší proškolení koncových uživatelů, protože v mnoha odpovědích uvedených výše můžeme sledovat, jak koncoví uživatelé nejsou schopni danou problematiku zhodnotit.

Závěr

V průběhu této bakalářské práce jsem provedl analýzu a komparaci zabezpečených páteřních krajských a lokálních datových sítí, které slouží pro potřeby zajištění krizové komunikace státní správy, samosprávy a složek Integrovaného záchranného systému. V rámci provedené analýzy jsem zjistil, že existuje řada faktorů ovlivňujících bezpečnost těchto sítí, včetně technologických, organizačních a legislativních aspektů. Zabezpečení datových sítí se stává stále důležitějším tématem v souvislosti s rostoucím počtem kybernetických hrozeb a rizik. Při komparaci různých přístupů k zabezpečení datových sítí bylo zjištěno, že existují různé technologické a organizační postupy, které lze aplikovat pro zlepšení bezpečnosti komunikace v rámci státní správy, samosprávy a složek IZS. Mezi tyto postupy patří implementace moderních šifrovacích technologií, síťových firewallů, monitorování provozu a řízení přístupu k datům. Závěry této práce naznačují, že je nezbytné neustále sledovat a aktualizovat zabezpečení datových sítí v souladu s nejnovějšími technologickými a legislativními požadavky. Pouze tak lze zajistit spolehlivou a bezpečnou datovou síť a komunikaci. Na závěr mohu konstatovat, že analýza a komparace zabezpečených páteřních krajských a lokálních datových sítí představuje důležitý krok směrem k efektivnímu využití informačních technologií pro potřeby krizového řízení a komunikace ve veřejné správě.

Seznam použitých zdrojů

Bibliografické zdroje

ADAMEC, Vilém; BERGLOWIEC, Petr; VÁLEK, Dušan; ŠENOVSKÝ, Pavel a ADAMEC, Martin.: *Operační střediska v integrovaném záchranném systému*. Vyd. 1. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2019, ISBN 978-80-7385-225-2

HANUŠKA, Zdeněk; ADAMEC, Vilém; ŠENOVSKÝ, Michail a BREJZOVÁ, Iva. *Integrovaný záchranný systém*. Vyd. 2. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2022, ISBN 978-80-7385-262-7

HORÁK, Jaroslav a KERŠLÁGER, Milan. *Počítačové sítě pro začínající správce*. Vyd. 5. Brno: Computer Press a.s., 2011, ISBN 978-80-251-3176-3

JAMES, Lance. *Phishing bez záhad.* Vyd. 1. Praha: Grada Publishing, 2007, ISBN 978-80-247-1766-1

KOLOUCH, Jan; BAŠTA, Pavel a kol.: *CyberSecurity*. Vyd. 1. Praha: Edice CZ.NIC, 2019, ISBN 978-80-88168-31-7

NEMATI, Hamid R. a YANG Li. *Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering*. Vyd. 1. Pennsylvania, USA: IGI Global, 2011, ISBN 978-1615207831

SOUKUPOVÁ, Veronika. *ISO a ESG pro udržitelný růst organizace*. Vyd. 1. Praha: Wolters Kluwer, 2023, ISBN 978-80-7676-796-6

SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Vyd. 1. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk s.r.o., 2019, ISBN 978-80-7380-765-8

STEWART, J. Michael. *Network Security: Firewalls and VPNs*. Vyd. 2. Sudbury: Jones and Bartlet Publishers, 2014, ISBN 978-1-284-03167-6

Legislativa

Nařízení vlády ČR č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury

Nařízení vlády č. 315/2014 Sb., kterým se mění nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury

Směrnice Evropské unie č. 2016/1148 Sb. o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii

Ústavní zákon č. 110/1998 Sb. o bezpečnosti České republiky

Ústavní zákon č. 300/2000 Sb., kterým se mění ústavní zákon č. 110/1998 Sb. o bezpečnosti ČR

Vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích

Vyhlášku č. 205/2016 Sb. o významných informačních systémech a jejich určujících kritériích

Vyhláška č. 437/2017 Sb. o kritériích pro určení provozovatele základní služby

Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti

Zákon č. 239/2000 Sb. o integrovaném záchranném systému a o změně některých zákonů

Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon)

Zákon č. 412/2005 Sb. o ochraně utajovaných informací a bezpečnostní způsobilosti

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů

Zákon č. 110/2019 Sb. o zpracování osobních údajů

Zákon č. 171/2023 Sb. o ochraně oznamovatelů

Elektronické zdroje

ANDREA, Harris. *Comparison and Differences Between IPS vs IDS vs Firewall vs WAF* [online] Dostupné z: https://www.networkstraining.com/firewall-vs-ips-vs-ids-vs-waf/

Apcaglobal, co je to LAN, [online] Dostupné z: https://apcaglobal.com/cs/2949-what-is-a-local-area-network-lan.html

APPOSITE TECHNOLOGIES, *What's The Difference Between A Local Area Network (LAN), Metropolitan Area Network (MAN), & Wide Area Network (WAN)?* [online]. Dostupné z: https://www.apposite-tech.com/whats-difference-metropolitan-area-network-man-wide-area-network-wan/

BROCK, Thomas. *Zero Day Attack* [online]. Dostupné z: https://www.investopedia.com/terms/z/zero-day-attack.asp

EUROSPOJ. *Rozdělení sítí LAN, MAN, WAN* [online] Dostupné z: https://eurospoj.cz/datove-site/

GEEKS FOR GEEKS. *Intrusion Detection System (IDS)* [online]. Dostupné z: https://www.geeksforgeeks.org/intrusion-detection-system-ids/

GEEKS FOR GEEKS. *What is Network Hub and How it Works?* [online]. Dostupné z: https://www.geeksforgeeks.org/what-is-network-hub-and-how-it-works/

GILLIS, Alexander S. *Intrusion prevention system (IPS)* – [online]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/intrusion-prevention

GILLIS, Alexander S. *What is DHCP (Dynamic Host Configuration Protocol)* [online]. Dostupné z: https://www.techtarget.com/searchnetworking/definition/DHCP

HOSKOVA, Katka. *IP telefonie,* [online]. Dostupné z: https://wiki.knihovna.cz/index.php/IP_telefonie

HZS ČR, *„Hasičský útvar ochrany Pražského hradu“* [online]. Dostupné z: https://www.hzscr.cz/clanek/hasicsky-utvar-ochrany-prazskeho-hradu-menu-o-nas-zakladni-informace.aspx

HZS ČR, *„SOŠ a VOŠ PO“* [online]. Dostupné z: https://www.hzscr.cz/clanek/o-nas-zakladni-informace-zakladni-informace.aspx

IBM Cloud Education [online] dostupné z: https://www.ibm.com/topics/networking

IBM, *What is SIEM,* [online]. Dostupné z: https://www.ibm.com/topics/siem

INTERNET A JEHO SLUŽBY, *Aktivní síťové prvky,* [online]. Dostupné z: https://ijs2.8u.cz/index.php?option=com_content&view=article&id=18&Itemid=123

LaBOUNTY, Chris. *What is Network Security and Why is it Important?* [online] dostupné z: https://www.herzing.edu/blog/what-network-security-and-why-it-important

LUOTONEN, Ari a ALTIS, Kevin. *World – Wide Web Proxies,* [online]. Dostupné z:https://web.archive.org/web/20161009061935/http://courses.cs.vt.edu/~cs4244/spring.09/documents/Proxies.pdf

MANAGEMENT MANIA, *Pasivní síťové prvky,* [online]. Dostupné z: https://managementmania.com/cs/pasivni-sitove-prvky

Microsoft Corporation, *What is antivirus software,* [online]. Dostupné z: https://www.microsoft.com/en-us/surface/do-more-with-surface/what-is-antivirus-software

MIN, Donghyun; KO, Yungwoo; WALKER, Ryan; LEE, Junghee a KIM, Youngjae. *A Content-Based Ransomware Detection and Backup Solid-State Drive for Ransomware Defense* [online]. Dostupné z: https://ieeexplore.ieee.org/document/9493745

NGUYEN, Kevin. *VoIP Architecture Diagram,* [online]. Dostupné z: https://www.8x8.com/blog/voip-architecture-diagram

NÚKIB, Blokové schéma zákona o KB, [online] dostupné z: https://www.govcert.cz/download/kii-vis/ZKB_blokove_schema.pdf

Papouch store, *PoE,* [online]. Dostupné z: https://papouch.com/zdroje/poe/#

VMWARE. *Network security* [online]. Dostupné z: https://www.vmware.com/topics/glossary/content/network-security.html

WU, Hao; DANG, Xianglei; WANG, Lidong a HE, Longtao. *Information fusion-based method for distributed domain name system cache poisoning attack detection and identification.* Dostupné z: https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/iet-ifs.2014.0386