Jihočeská univerzita v Českých Budějovicích
Zdravotně sociální fakulta

ZABEZPEČENÍ A OCHRANA DAT PŘI ČINNOSTI HASIČSKÉHO ZÁCHRANNÉHO SBORU JIHOČESKÉHO KRAJE

diplomová práce

Autor práce: **Bc. František Remiáš**
Studijní program: **Ochrana obyvatelstva**
Studijní obor: **Civilní nouzová připravenost**

Vedoucí práce: **prof. Ing. Gustav Šafr, DrSc.**
Konzultant: **Ing. Lubomír Bureš**
Datum odevzdání práce: **22. května 2012**

ABSTRAKT

REMIÁŠ, F. Zabezpečení a ochrana dat při činnosti Hasičského záchranného sboru Jihočeského kraje: diplomová práce. České Budějovice: Jihočeská univerzita v Českých Budějovicích, 2012. 133 s. Vedoucí diplomové práce prof. Ing. Gustav Šafr, DrSc.

Diplomová práce je zaměřena na práci s daty a informacemi u Hasičského záchranného sboru Jihočeského kraje a jejím cílem zjistit, zda je s daty a informacemi, se kterými se setkávají příslušníci a zaměstnanci Hasičského záchranného sboru při své práci, nakládáno v souladu platnou legislativou, a zda jsou tyto dostatečně zabezpečeny a chráněny proti zneužití a ztrátě.

Na základě organizační struktury je kvalitativním výzkumem podrobně zmapováno zabezpečení a ochrana dat na jednotlivých odděleních a pracovištích. Z těchto informací jsou sestaveny rizikové oblasti pro různé druhy dat a zpracována mapa rizik pro tyto oblasti. Na základě zjištěných výsledků jsou navržena konkrétní opatření ke zmírnění rizik pro některé oblasti práce s daty a informacemi.

V první části práce jsou vysvětleny základní pojmy a definice slov data, informace a znalosti. V další části jsou zmapovány historické souvislosti s uchováváním dat a nakládání s daty v papírové a elektronické podobě včetně vývoje informačních systémů a technologií. Dále jsou popsána možná ohrožení těchto dat nejrůznějšími vlivy. Další kapitola je zaměřena na popis současného stavu práce s daty a popis technologií používaných k tomu u Hasičského záchranného sboru. Poté je rozpracována organizační struktura se zaměřením na práci s daty.

V další části práce je vypracována mapa rizik pro jednotlivé oblasti a navrženo několik konkrétních řešení a opatření pro zmenšení největších výsledných rizik.

Přínosem práce je realizace několika konkrétních řešení pro eliminaci a snížení hrozby rizik při práci s daty u HZS JčK, a návrh několika dalších opatření a postupů pro další zabezpečení a ochranu dat.

Klíčová slova: data, informace, Hasičský záchranný sbor, záloha dat, ukládání dat, míra rizika, mapa rizik, dokumenty, bezpečnost

ABSTRACT

REMIÁŠ, F. Security and Data Protection in the activities of the Fire and Rescue Service of South Bohemia Region: Thesis. České Budějovice: University of South Bohemia České Budějovice, 2012 133 s Thesis Supervisor prof. Ing. Gustav Šafr, MD.

The thesis is focused on work with the data and information for the Fire and Rescue Service of South Bohemia Region, and its goal is to determine whether the data and information faced by members and employees of Fire and Rescue Service in their work are treated in accordance with applicable legislation, and whether they are adequately secured and protected against misuse and loss.

Based on the organizational structure of qualitative research are mapped in detail the security and protection of data on individual departments and workplaces. These information compile risk areas for different types of data and due to this is prepared the risk map for these areas. Due to the findings the specific measures are designed to mitigate the risks for certain fields of work with data and information.

The first part explains the basic concepts and definitions of words data, information and knowledge. The next section discusses the historical context of the mapped datastorage and handling of data in paper and electronic form, including the development of information systemsand technologies. Further are described the possible threats by varius effects on these data. Another chapter focuseson describing the current state ofwork with data and description oftechnologies used to it at the Fire and Rescue Service. Afterwards is elaborated an organizational structure focused on work with data.

In following part the risk map is prepared for each area and proposesseveral solutions and particular measures to reducethe greatest of the resultingrisks.

The benefit of this work is the implementation of several specific solutions to eliminate and reduce the threat of risks when working with dataat Fire and Rescue Service of South Bohemia Region, and several otherproposal measures and stepsfor additional security and data protection.

Keywords: data, information, Fire and Rescue Service, data backup, data storage, the degree of risk, risk map, documents, safety.

Prohlášení

Prohlašuji, že svoji diplomovou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své diplomové práce, a to – v nezkrácené podobě – v úpravě vzniklé vypuštěním vyznačených částí archivovaných fakultou – elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejich internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne .....

Bc. František Remiáš

Poděkování

Touto cestou bych velice rád poděkoval panu prof. Ing. Gustavu Šafrovi**,** Dr.Sc a panu plk. Ing. Lubomíru Burešovi za odborné vedení, vstřícnost, praktickou pomoc, cenné připomínky a rady při zpracování diplomové práce.

Bc. František Remiáš

OBSAH

SEZNAM POUŽITYCH ZKRATEK

ACTA – Anonymus – svoboda internetu

AMDS - Automated Message Delivery System

CD RW - Compact Disk ReWritable - medium

CO - Civilní obrana

ČVUT – České vysoké učení technické

DDoS - Denial of Service – odmítnutí služby

DoS – Denial of Service

ENICAC - Electronic Numerical Integrator And Computer

FBI – Federální úřad pro vyšetřování

FIDO – Firemní doprava

HZS ČR – Hasičský záchranný sbor ČR

HDD - Hard disk drive

HW - Hardware – technické vybavení počítače

ICT - Integrovaný záchranný systém

IT – Informační technologie

JETE – Jaderná elektrárna Temelín

JSEP – Jednotný systém elektronických počítačů

KISKAN – informační nástroj pro podporu systému Krizkom

KRIZKOM – nástroj informační podpory pro orgány krizového řízení

LAN - Local Area Network

OSN – Organizace spojených národů

PAL - phase alternating line – jeden ze standardů kódování

PC –computer - počítač

PIN - Personal identification number

PO – Požární ochrana

RVHP – Rada vzájemné hospodářské pomoci

SIAŘ – Sbírka interních aktů ředitele

SMEP- Systém malých elektronických počítačů

SOPA – návrh amerického zákona k omezení počítačového pirátství

SW - Software

TCTV - Telefonní centrum tísňového volání

UPN - United Paramount Network – televizní síť

USA - United states of america

USB - Universal Serial Bus Sériová sběrnice

VEMA – Informační systém pro řízení ekonomiky a logistiky

WWW - World wide web

ÚVOD

Dost často se dozvídáme z médií o nejrůznějších únicích a zneužívání dat, proto jsem se rozhodl ve své práci na téma „Zabezpečení a ochrana dat při činnosti Hasičského záchranného sboru Jihočeského kraje“, analyzovat tuto problematiku v organizaci, u níž jsem zaměstnán od roku 1984 a navrhnout řešení pro případnou nápravu současného stavu.

Vycházím z předpokladu, že technika zneužití a ztráta dat je tím pravděpodobnější, čím jednodušší je možnost pořízení jejich kopií. Zároveň také možnost ztráty dat je tím větší, čím je jejich objem větší a čím je složitější technologie, které slouží k jejich uchovávání. Proto proti stále se zdokonalujícím technologiím a k zabránění jejich zneužití a ztrátě dat musí být vyvíjeny efektivnější nástroje. Tím myslím jak technické nástroje, tak k podpoře zmírnění možných rizik a zabránění úniku také legislativní nástroje.

Práci jsem se rozhodl začít kapitolou výkladů pojmů data, informace, znalosti, protože při získávání podkladů pro práci jsem zjistil, že velké procento lidí a to i IT odborníků nezná jejich pravý význam, nebo alespoň nemá vymezeny pevné hranice mezi nimi. Tento fakt by mohl být jistě zajímavým námětem k samostatné práci, ale v mé práci přesahuje rámec cílů a hypotéz, které jsem si stanovil. Cílem mé práce bylo zjistit, jestli je při práci s daty a informacemi u Hasičského záchranného sboru Jihočeského kraje dodržovaná platná legislativa a posoudit úroveň zabezpečení a ochrany nejrůznějších dat v celé organizaci.

Vzhledem k tomu, že riziko ohrožení dat nemůže mít nikdy nulovou hodnotu a nelze jednoznačně konstatovat dva mezní stavy, rozhodl jsem se pro dosažení výsledků, řešit tuto úlohu metodou kvalitativního výzkumu s následným vypracováním mapy rizik.

Aby měla má práce ucelenou formu a obsahovala co největší množství informací, a nemusel si je zájemce, o tuto práci dodatečně vyhledávat, věnoval jsem část práce historii ukládání dat a informačních technologií, na níž je vidět, jak se tyto v čase vyvíjely a čím přispívaly k prohlubování a vytváření této problematiky. Vždyť bez těchto technologií bychom otázky nastolené v této práci řešit nemuseli. Zároveň může tato kapitola případného čtenáře zaujmout, stejně jako mne zaujala práce

na vyhledávání a shromažďování podkladů při cestách do minulosti informačních technologií.

1 SOUČASNÝ STAV

1.1 Definice pojmů: data, informace, znalosti

Pojmy data a informace jsou hojně rozšířené, ale jejich užívání je velmi volné a intuitivní. Tvoří běžnou součást slovní zásoby každého z nás. Termíny data, informace a znalosti lze v běžném hovoru považovat za synonymní. Pro pochopení podstaty stojí za to zamyslet se nad jejich odlišnostmi. Odlišnost mezi daty, informacemi a znalostmi se projeví, začneme-li uvažovat nad jejich účelem.

Data jsou základním stavebním prvkem všeho vědění. Ta mohou být vyjádřena a zaznamenána různými způsoby, avšak abychom z nich mohli získat informace, musí tato data splňovat dva předpoklady. Musí nějaké informace obsahovat a musí být zaznamenána takovým kódem, který jsme schopni přečíst.

Pojem informace je spojen až s nějakým konkrétním významem. Lze říci, že z dat se stávají informace teprve tehdy, pokud jsme z nich schopni získat nějaké poznatky a vědomosti. Pokud tedy rozumíme významu v datech ukrytém, znamenají pro nás data také nějakou informaci. Je nutné si ale uvědomit, že ne všechna data musí nést nějakou informaci.

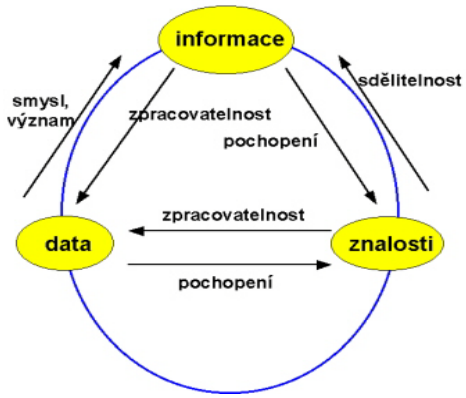
Pro správné pochopení uvedu příklad. Uvažujeme o dvou řetězcích znaků, první například „UDBRVA“ a druhý “BUDVAR“. Z první posloupnosti nejsme schopni žádný konkrétní význam získat, nejedná se tedy pro nás o nic jiného, než o data. Druhá posloupnost ale pro určitou skupinu lidí již konkrétní význam má. Název světoznámého piva. Ve druhém případě se jedná pro nějakou množinu lidí o informaci, v prvním nikoli. Jiná situace nastane například použitím dat ve spojení s informačním systémem, kupříkladu internetu. A tak zatímco například řetězec znaků neboli data „MC8790V“ převážné většině lidí nic neřekne, při dosazení řetězce do informačního systému dostaneme konkrétní informaci o tom, že se jedná o 3G modem konkrétního výrobce s konkrétními parametry a to s celosvětovým dopadem, neboli pro všechny osoby mající přístup k tomuto informačnímu systému.

Informace, které některá data obsahují, samy o sobě nejsou ničím významné. Je třeba zapojit znalosti, abychom na základě těchto informací mohli něco vykonat, odvodit nebo se rozhodnout.

Zjednodušeně lze data charakterizovat jako libovolnou posloupnost znaků a nemusí se jednat pouze o bity či bajty. Pod posloupností se mohou skrývat libovolné znaky. Samo o sobě jsou znaky této posloupnosti jen jakási "suchá" data, která nám mohou, ale nemusí něco říkat. Pojmy, data, informace a znalosti jsou často používány k překrývání pojmů. Hlavní rozdíl je v míře uvažování abstrakce. Data jsou na nejnižší úrovni abstrakce, na druhém místě jsou informace a znalosti jsou na nejvyšší úrovni. Např. údaje o výšce nemají samy o sobě žádný význam. V případě aby se z těchto údajů stala informace, musí jim být přiřazen nějaký význam. Výška Mount. Everestu je obecně považována za data. Geologickou charakteristiku v knize o Mount. Everestu lze považovat za informace a zprávu, která obsahuje praktické informace o nejlepším způsobu, jak dosáhnout tohoto vrcholu lze považovat za poznání neboli znalosti. Znalosti, které během svého života získáme, nám umožňují vstupní informace transformovat na rozhodnutí. Schází-li nám v oboru, jehož se informace týká znalosti, pak pro nás nebude mít takový význam. Alespoň v tom smyslu, abychom na jejím základě mohli učinit nějaká kvalitní rozhodnutí.

Data jsou vyjádřením neboli reprezentací skutečnosti, jsou schopné přenosu, interpretace či zpracování. Účelem dat je přenášet a dále zpracovávat odraz skutečnosti. Jsou to jakékoli zaznamenané poznatky či fakta. Informace je definována pomocí dat a znalostí. Jsou to data, která mají smysl neboli význam. Znalost je to, co jednotlivec vlastní neboli ví po osvojení dat a informací a po začlenění do souvislostí. Účelem znalostí je schopnost porozumět skutečnosti. Jako média pro uchování znalostí slouží lidská paměť, organizace, dokument nebo počítač. /12/

V rozhodovacím procesu vyjádříme tuto myšlenku takto. Vlastníme-li data, ale nechápeme jejich smysl, ztrácí pro nás význam, jsou nepoužitelná. Pokud nám ale dávají smysl, představují pro nás informace. Pokud správně pochopíme informace, informace se pro nás stávají znalostmi, které můžeme zpracovat opět do dat.



Obr. č. 1: Schéma rozhodovacího procesu

Zdroj: http://books.google.cz/books?id=UJh-gLdTH8IC&printsec=frontcover&hl=cs#v=onepage&q&f=false

Člověk oproti ostatním živočichům na zemi získal své dominantní postavení díky tomu, že si dokáže předávat informace a znalosti. Každý tak veškeré znalosti nemusí objevovat sám. Na rozdíl od ostatních živočichů nepostupuje cestou pouze vrozenými instinkty, jejichž přidávání do genetického kódu postupuje velmi pomalým tempem zhruba „jeden bit za rok“, ale znalosti předků mu jsou předány procesem učení už po jeho narození. On poté na těchto znalostech může stavět, vytvářet tak znalosti nové a předávat je dál.

Sdílení nepřeberného množství znalostí na celosvětové síti internet je dnes již běžnou realitou a není problémem z kteréhokoli místa na světě zjistit téměř cokoli. Díky této skutečnosti, okamžité, levné, veřejně přístupné komunikaci současný výzkum ve všech oblastech vědy může pokračovat stále rychlejším tempem.

V současné době v oblasti znalostních systémů převládá spíše interní využívání v rámci jednotlivých organizací. Každá z nich pak vytváří svůj vlastní znalostní systém v oboru své činnosti, do kterého zachycuje své know-how, tedy vlastní zkušenosti, postupy a znalosti.

Do budoucna se předpokládá postupný vznik centrálního globálního znalostního systému, obdařeného určitým stupněm umělé inteligence, který bude teoreticky schopen na základě dostatečně velké databáze znalostí zodpovědět jakoukoli otázku, na kterou bude existovat odpověď. Dalším krokem, který člověk učinil na této ose je možnost šíření „hmotných“ statků a to za pomocí internetu ve spojení s 3D tiskárnami.

1.1.1 Zabezpečení a ochrana dat

V dřívějších dobách se naši předkové snažili prostřednictvím kreseb, později písmem zaznamenávat informace, které považovali za důležité. V současnosti se na tomto poli uplatňují moderní informační technologie, které využívají stále výkonnější počítače a informační systémy.

Již od pradávna informace byly výhodou před soupeřem. V časech dob lovců mamutů kmen, který znal dobré loviště a uměl rozdělávat oheň, mohl přežít, a proto se snažil toto tajemství strážit. Časem se utajované informace zaměřily např. na zpracování železa nebo výrobu zbraní. V současné době stejně tak jako dříve, informace opět znamenají náskok před ostatními a znamenají moc. Cílem každé firmy je proto chránit svá tajemství před konkurencí. Pro úspěšnou implementaci bezpečnostní politiky firmy je nutné, aby byla podporována managementem z nejvyššího vedení. Ochrana dat rozhodně není jen záležitost lidí, kteří s nimi pracují, ale zahrnuje každého zaměstnance firmy.

Ochranu dat můžeme rozdělit z několika hledisek. Prvním hlediskem je ochrana přístupu a zabezpečení vstupů fyzických osob. Bude nás tedy zajímat pověření osob, které mají na pracoviště přístup, dále jejich prověření z hlediska důvěryhodnosti, tzn. pokud to situace vyžaduje, zaměříme se na osobní koníčky, finanční situaci a majetkovou situaci v rodině, osobní styky mimo zaměstnání. A to nejen pracovníků podílejících se na monitorované činnosti, ale všech osob s přístupem na pracoviště jako jsou ostatní technici nebo uklízečky.

Druhé hledisko ochrany přístupu je z pohledu kontroly. Např. kontrola na vrátnici, kontrola před vstupem do budovy, kanceláře a to fyzická, ale i softwarová. Použití PIN přístupu, čipových karet, biometrická identifikace, otisky prstů, hlasové a visuelní kontroly či sítnicového potvrzení. Zabezpečení budov proti možnému monitoringu. Toto jsou základní možná rizika úniku informací z pohledu fyzické osoby a fyzické bezpečnosti.

Další kapitolou je ochrana dat z hlediska výpočetní techniky. Zabezpečení vlastních počítačů z pohledu používaného softwaru, šifrování informací, antivirových programů, firewallů, bezpečnost připojení konkrétního počítače do sítě, pouze intranet nebo on-line připojení. Bezpečnost síťového připojení počítače a jeho hlavních

datových uzlů, využití, zapojení a zabezpečení wi-fi. Dále je potřeba se zaměřit na využití dalších bezpečnostních prvků hardware a software. Např. do zabezpečení opět spadá složka řízení přístupů a vstupů do areálů a kontrola vstupních dat pro možné odemknutí přístupu. Při práci využíváme určitého softwaru, kdy vytvořený produkt musíme uložit, buď k pokračování v práci, nebo dalšímu zpracování dat. Uložení můžeme provádět přímo na pracovním počítači, přes síť na server či datový nosič, a to buď bez úprav, jako šifrované zprávy či fragmentární ukládání dat. K využívání přenosných datových nosičů můžeme použít celou řadu, od magnetických nosičů jako jsou diskety různých velikostí, pevné disky, magnetooptické disky, magnetické pásky, audiokazety, videokazety, přes optická media jako jsou CD a DVD nosiče, Blu-ray, HD DVD až k elektronickým flash pamětem jako např. Secure Digital, Multimedia memory Card, Memory Stick, Flash card, xDcard, USB flash paměť aj. Je tedy mít na paměti, že informace z počítače se dají odnést velmi jednoduše. Z toho důvodu je důležité mít zabezpečený systém proti uložení dat mimo daný systém, mít uzamčené USB nebo povolení CD/DVD mechaniky pouze ke čtení.

S ukládáním dat souvisí i problematika telefonní linky a mobilních telefonů. Mobilní telefon se dá relativně jednoduše odposlouchávat, i když je vypnutý, ale má v sobě baterii. Tím souvisí i oprávnění mít na pracovišti mobilní telefon a vnitřní předpisy kdy a kde ho mít zapnutý, proti možnému zabránění odposlechu. Nehledě na to, že mobilní telefony dnes už většinou obsahují paměťové karty, na které je možné opět přenést uložené informace.

Velmi opomíjeným velkým nebezpečím úniku dat je uložení fyzické podoby informací, tj. v papírové formě např. archív, ale i hotový prototyp nebo jeho vývoj. Ožehavější je však likvidace dat. A to skartace papíru. Nejefektivnější jsou drtičky, ze kterých nelze vůbec nic obnovit, vzniká pouze velmi jemná papírová drť. Skartovat stejným způsobem bychom měli i informace obsažené na datových nosičích. Velmi často se zapomíná při likvidaci počítačů nebo jejich obměny na novější a výkonnější, kdy např. dochází k prodeji starých modelů na HDD, které jsou smazány a nahrán nový operační systém. Průměrný technik však dovede bez větších problémů obnovit všechny data, která se na pevném disku nacházela před tím. Doporučuje se tedy při prodeji starých počítačů úplně odstranit HDD a nahradit novými. V obecné rovině jsou toto

hlavní zásady, které bychom si měli ohlídat, pokud nechceme přijít o námi střežené informace.

Nacházíme se ve světě, který se díky počítačům a internetu neustále modernizuje a sbližuje. S tímto fenoménem se objevují také různá nebezpečí, která nás mohou poškodit. Počítač je úložiště různých druhů informací. Obyčejná data, profesní data, ale i soukromá a osobní data mohou být v ohrožení ihned, jakmile se připojíme na internet, do sítě nebo když si nedáme pozor na přístup k počítači. Proto se musíme chránit před vniknutím do PC a před způsobením jakékoliv škody. Pokud by naše ochrana nebyla dostatečná, pak tyto informace mohou být zničeny nebo odcizeny. Vznikají tedy mnohá nebezpečí, jimž se musíme vyhnout.

V dnešní době se veškerá data digitalizují, a proto se instituce zaměřují hlavně na ochranu proti hackerům. Nicméně papírová ochrana dat existuje již mnoho let, protože jiný způsob uchovávání informací do vzniku počítačů nebyl. Papírové listiny, tedy spíše pergamenové listiny, se uchovávaly a strážily už ve starověkém Římě. Od té doby se neustále vymýšlí 100% způsob ochrany listinné formy dokumentů. Dnes se ve firmách stále používají papírové formy dokumentů jako např. faktury, dodací listy, zaměstnanecké smlouvy, osobní spisy apod. Firma je musí chránit před vlivy z nitra firmy. Problémem jsou veřejné kopírky na chodbách firem, šanony plné smluv apod. Mnohá bezpečnostní rizika se již daří úspěšně ošetřovat ve většině firem. Veřejné kopírky jsou dnes buď chráněné pin kódem, nebo speciální identifikační kartou. Šanony jsou uzamčené ve skříních a mohou se k nim dostat pouze lidé s klíčem. Velmi důležité dokumenty jsou v trezorech a servery jsou bezpečně uzamčeny ve speciální místnosti. Firma má za povinnost veškeré písemnosti archivovat.

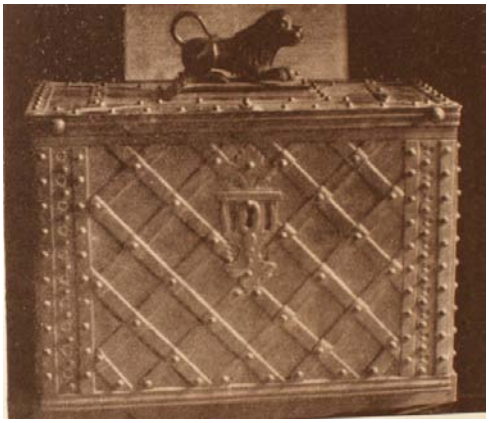
Ochrana dat v papírové formě

Již od pradávna se člověk pokoušel nějakým způsobem zaznamenávat důležité informace. Pravěcí lidé pomalovávali stěny svých obydlí, později ve starověku bylo vynalezeno písmo. Nejstarší druh písma je obrázkové, kdy jeden znak vyjadřuje pojem nebo slovo. Další stádia představují slovní, slabičná a hlásková písma. Tehdy se objevila první média, protože písmena bylo potřeba někam umístit. Zprvu byl jediný způsob množení knih opisování. Po stovky let se šíření informací věnovaly tisíce

mnichů a kláštery se staly centry vzdělanosti. Z těchto informací vyplývá, že ochrana proti kopírování takovýchto dat nebo informací nepředstavovala prakticky žádné riziko. Problémem bylo samozřejmě uchránit papírové dokumenty a knihy proti tehdy poměrně častým požárům. Mezi nejznámější a nejničivější určitě patří vypálení Alexandrijské knihovny.

Obr. č. 2: Požár Alexandrijské knihovny (malba)
Zdroj: http://jolie.blog.cz/1007/alexandrijska-knihovna

Historii této události pro dokreslení podrobněji popisuji v příloze č.1 této práce. Nejstarší přímé zmínky o ochraně důležitých dokumentů v českých zemích pocházejí z 15. století. Například v „Právech“ města Kamenice nad Lipou z roku 1462 jsou obsažena ustanovení o městské truhlici, do níž se ukládají pečetidla a městské knihy. Podobným způsobem se dokumenty uchovávaly i v dalších městech, u cechů nebo na farách.



Obr. č. 3: Truhla z 18. Století
Zdroj: http://www.mza.cz/pelhrimov/historie.php

Docenění historického významu písemných dokumentů se začalo prosazovat až ve druhé polovině 19. a na počátku 20. století. Důsledkem snahy zachránit nejcennější dokumenty byla zpočátku skutečnost, že řada archiválií se tehdy dostala do fondů a sbírek centrálních institucí, do Národního muzea nebo do Zemského archivu v Praze.

Spisovny nových státních úřadů vzniklých po roce 1850 byly pod obecným dohledem velkých státních archivů, což v některých případech nezabránilo unáhleným skartacím. Výraznou změnu situace znamenalo vydání zákona o archivnictví č. 29/1954 Sb., jemuž o rok předcházela vyhláška ministerstva vnitra č. 62/1953 Sb. o zásadách pro vyřazování (skartaci) písemností. Tyto normy, vytvořené v návaznosti na některé představy archivních odborníků z doby meziválečné republiky, položily základy k systému jednotně organizované archivní služby.

Vedle okresních archivů působily v průběhu 50. let rovněž archivy při některých místních národních výborech. Tyto archivy zanikly v roce 1958. Oddělení archivů a muzeí mělo význam především proto, že oblast odborné péče o archiválie zahrnovala nyní nejenom cenné historické soubory, ale rozšířila se také na novodobé úřední registratury. Nově vzniklé archivy byly prvními specializovanými archivními institucemi s všeobecnou působností.

Všeobecná působnost okresních archivů vyplynula ze změn ve správní struktuře státu, při níž došlo k odstranění dosavadního oddělení státní správy a samosprávy a ke vzniku místních a okresních národních výborů. Okresní archivy začaly provádět skartační řízení a výběr archiválií a převzaly do archivní péče řadu fondů velkých institucí.

V roce 1960 byly v souvislosti se správní reformou tyto okresní archivy zrušeny a jejich fondy byly soustředěny do Okresního archivu Pelhřimov. Současně zanikl i Státní archiv v Telči a dohled nad archivem převzal v rámci nově zřízeného Jihočeského kraje Státní archiv v Třeboni. Zřízení společného archivu pro celé území okresu Pelhřimov posílilo centralizaci archivní péče zahájenou na počátku 50. let. /1/

A jaké hrozí nebezpečí při archivaci? Životnost archiválií bývá negativně ovlivněna různými riziky, jako jsou havárie, technické závady, živelní pohromy nebo jiné nenadálé události, které mohou ohrozit chráněnou dokumentaci.

Živelní pohromy jako např. požáry, povodně, zemětřesení, vichřice, kalamitní výskyt sněhových srážek, technické závady na vodovodním řádu nebo havárie způsobené stavebními závadami na archivních budovách jsou riziky, se kterými je nutné počítat. Při požáru může dojít k poškození archiválií ohněm, sazemi a kouřem, ale také hasebními prostředky. Nenapravitelné škody na svěřených archivních písemnostech může způsobit havárie vodovodního řádu nebo topného systému, stejně tak jako povodně. Silný vítr, vichřice, kalamitní výskyt sněhových srážek může poničit špatně zabezpečenou budovu archivu, kde jsou archiválie uchovávány.

Neméně důležitá je také ochrana před vandalismem či poškození písemností nevhodnou manipulací či nevhodným uložením. Vzhledem k tomu, že se mnohdy jedná o dokumentaci značné historické hodnoty, je třeba zabezpečit archiválie proti krádeži nebo terorismu.

I když máme budovy dostatečně zabezpečené, ke zničení archiválií může dojít působením času, vzduchu, tepla nebo zimy. Jedná se o přirozené stárnutí archiválií, které je nutné odstranit, oddálit či zmírnit.

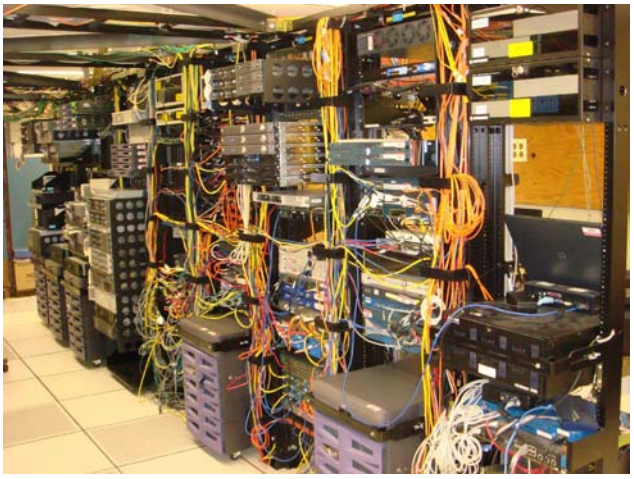
Vedle nebezpečí ztráty papírových dat, je samozřejmě neméně nebezpečné jejich zneužití. Toto riziko je tím vyšší, čím jsou k dispozici vyspělejší technologie. A tak je již běžné, že v bezpečnostní politice nejrůznějších firem a institucí jsou zakotveny zákazy používání mobilních telefonů, vybavených fotoaparáty, kartových systémů přístupu ke skenovacím a kopírovacím zařízením.

Ochrana dat v elektronické podobě

Ještě před několika desítkami let žádná ochrana elektronických dat v rámci počítačů a počítačových sítí nebyla zapotřebí, neboť žádné počítače ani internet nebyly. Historie počítačů započala až ve 40. letech minulého století. Navazovala na éru mechanických strojů, které byly vymýšleny a sestrojovány pro zjednodušení práce při matematických a výpočetních operacích. První počítač sestrojil roku 1652 francouzský filozof a matematik Blais Pascal. O téměř 150 let později, v roce 1801, známý průmyslník Jacquard poprvé v praxi použil programové řízení, když zvolil děrné štítky s naprogramovaným vzorem látky pro řízení tkalcovského stavu. V roce 1890 byly pak děrné štítky poprvé použity pro hromadné strojové zpracování dat při sčítání

lidu v USA. Roku 1834 navrhl anglický matematik Charles Babbage programově řízený mechanický číslicový počítač, který nazval Analitical Engine. Stroj již měl být vybaven aritmetickou jednotkou, pamětí pro 1000 padesáticiferných čísel, vstupem z děrných štítků a výstupem na primitivní tiskárnu. Programování se mělo provádět pomocí Jacquardouých děrných štítků. Návrhem Analytical Engine ovšem Babbage předběhl svou dobu natolik, že tehdejší dostupná technologie na tak složitou konstrukci nestačila. Vývoj nejrůznějších technologií probíhal ještě více než století a v létě 1946 bylo sestrojeno a uvedeno do provozu elektronkové monstrum chlazené dvěma leteckými motory a nazvané ENIAC. Byl to pradědeček všech počítačů dneška. Geniální vynález integrovaného obvodu neboli čipu, v roce 1958 umožnil nástup nové generace počítačů. V konstrukci počítače byl čip poprvé využit firmou IBM a to v dubnu 1964. IBM zahájila třetí generaci a současně novověk počítačové éry.

Tím byla započata revoluce v pořizování, uchovávání a práci s daty a informacemi. Začala se psát historie elektronických informačních technologií.



Obr. č. 4: Informační technologie

Zdroj: http://wikibon.org/w/images/5/5e/CSUOldServers.jpg

Sítě – přítel a zároveň největší nepřítel elektronických dat

V roce 1939 badatel George Stibitz dokončil v Bellových telefonních laboratořích vývoj kalkulačky komplexního čísla (CNC) a v následujícím roce na American Mathematical Society konferenci na Dartmouth College, ohromil přihlížející při provádění výpočtů na CNC s použitím Teletype, připojením přes

speciální telefonní linky. Tato demonstrace je považována za první vzdálený přístup k počítači. Nikoho v té době nenapadlo, že tím položil základy vzniku počítačových sítí. Sítě tak umožnily dostat se k datům a informacím bez nutnosti fyzické návštěvy datového úložiště.

Obr. č. 5: Kalkulačka komplexního čísla
Zdroj: http://www.computerhistory.org/timeline/?year=1940

Vznik a vývoj počítačových sítí je pak úzce spjat s rozvojem počítačů a výpočetní techniky. K jejímu vývoji došlo již v 50. letech. Tehdejší počítače se velmi složitě programovaly v tzv. strojovém kódu. V 60. letech převažoval tzv. dávkový způsob zadávání úloh. Uživatel vytvořil program a zapsal jej na speciální formulář, na jehož základě se vyděrovala sada děrných štítků a ty se předaly do výpočetního střediska ke zpracování. Doba mezi zadáním úlohy a získáním výsledků činila několik hodin i dní. Oprava chyby v programu či znovuvytvoření chybně vyděrovaných štítků obvykle znamenaly nejméně další dny zdržení.

Uživatelé sálových počítačů proto volali po jednodušším a rychlejším způsobu komunikace s počítačem. Objevily se první terminály, tj. zařízení, která sloužila k zadávání údajů do počítače a zobrazování výsledků jeho činnosti. Tím začala éra propojování velkých počítačů.

První testovací síť na světě byla instalována počátkem roku 1968 v Národní výzkumné laboratoři ve Velké Británii. Tato síť však neopustila hranice jedné budovy. Přišel požadavek na vybudování podobné počítačové sítě a zároveň i potřebné finanční prostředky z resortu obrany, konkrétně od ministerstva obrany USA. Nová experimentální síť, která vznikla v roce 1969 byla pojmenována ARPANET. Síť

americké armády, v jejímž rámci byla vyvinuta i protokolová sada TCP/IP, kterou dnes používá internet. Další sítě byly DECnet firmy Digital, síť univerzity na Havaji ALOHA, z níž čerpala technologie Ethernet, a řada dalších. Koncem 70. let začalo docházet i ke vzájemnému propojování dílčích sítí, zejména akademických – vznikl internet. /24/

Internet – „síť sítí“

Internet vznikl zákonitým evolučním vývojem počítačových sítí. Touha po celosvětové síti spolu se zdokonalováním technologií vytvořily dva základní předpoklady pro vznik internetu.

Internet je celosvětová počítačová síť, která dnes nemá vzhledem ke své rozsáhlosti žádného vlastníka. Počátky internetu sahají až do roku 1945, kdy v červencovém čísle amerického časopisu The Atlantic Monthly publikoval Vannevar Bush svůj světoznámý As We May Think, jenž bývá považován za jeden ze základních kamenů informační vědy. Tento článek, který se týkal využití počítačů pro komunikaci je zajímavý tím, že byl napsán mnoho let před tím, než byly pro tuto úlohu skutečně poprvé počítače použity.

První experimentální síť vznikla v roce 1969 a byla pojmenována jako ARPANET, podle názvu grantové agentury ministerstva obrany USA s názvem ARPA. Až do poloviny 80. let se internet nijak zvlášť nerozvíjel, byl omezen především na vládní a vojenské organizace.

V roce 1984 bylo k internetu připojeno pouhých 1000 počítačů. Velký rozvoj nenastával ani v nejbližších několika letech, kdy v roce 1992 bylo k internetu připojeno více než jeden milion počítačů. Teprve vývojem standartu WWW začíná rokem 1993 internet v USA prožívat nebývalý rozmach. K internetu je připojen i Bílý dům.

Na celém světě bylo odhadováno v roce 1995 na 20 miliónů uživatelů internetu, v roce 2000 již přes 300 miliónů./24/

V roce 2010 dle telekomunikační agentury OSN, Hamadoun Toure dosáhl počet uživatelů internetu 2 miliardy. /2/

Internet v ČR

První experimentální připojení do internetu se uskutečnilo v listopadu 1991 mezi počítačem umístěným na ČVUT v Praze a počítačem Univerzity Jana Keplera v rakouském Linci. 13. února 1992 se na Fakultě elektrotechnické ČVUT v Praze uspořádalo slavnostní setkání, na němž se oficiálně oznámilo připojení tehdejšího Československa k internetu a pozvaným odborníkům se předvádělo, jak toto připojení funguje. Tento den je proto označován za okamžik, kdy se naše země oficiálně připojila k internetu. /15/

Dnes je v České republice více než 7 milionů uživatelů internetu. Vedle nesporných výhod, které přináší internet pro informační technologie, představuje zároveň i jejich největší hrozbu, neboť vytváří jednu z cest, jak zpřístupnit data potencionálním útočníkům odkudkoli na zemi. I přesto, že dochází ke stále většímu zdokonalování internetových technologií, včetně nejrůznějšího zabezpečení, nelze internet považovat za bezpečný. Proto se téměř nevyužívá pro kritické technologie, tedy takové, při jejichž výpadku by mohly vzniknout nenahraditelné ztráty a nebo ztráty většího finančního rozsahu. /23/

Ohrožení elektronických dat

Elektronická data jsou mnohem více zranitelná než jejich papírová obdoba. Neohrožují je jenom živelní katastrofy jako je tomu u dat papírových, ale i samotné selhání technologií, které slouží pro jejich uchovávání. Není výjimkou selhání magnetických médií, optických disků, pevných disků případně flash disků. S poměrně snadným způsobem kopírování elektronických dat je snadnější způsob zneužití, než tomu je u písemných dat. Zatímco tyto hrozby lze poměrně dobře eliminovat, mnohem větší hrozbou je napadení informačních technologií a v nich uchovaných dat prostřednictvím počítačových sítí, kterými jsou tyto propojeny. Tyto útoky jsou o to nebezpečnější, že mohou být uskutečněny nepozorovaně kdykoli 24h denně, 365dní v roce a navíc téměř anonymně.

Metody útoků na Informační technologie

Techniky pro vloupání do systému můžou zahrnovat pokročilé programovací schopnosti a sociální inženýrství, ale častěji se jednoduše použije poloautomatických software.

DoS, DDoS útoky. DoS (Denial of Service), je jeden z nejčastějších typů útoků. Dochází při něm k zahlcení programů, počítače či celých počítačových systémů a sítí a dojde tak k vyčerpání zdrojů, které jsou určeny k běžnému chodu. DoS se od DDoS (Distributed Denial of Service) liší tím, že napadá pouze jeden počítač, jedná se tedy o primitivnější útok, který lze poměrně snadno zastavit tím, že napadený systém odstaví napadenou část. DDoS útok je sofistikovanější, využívá při útoku soustavu mnoha počítačů a počítačových sítí, kdy každý z počítačů má svoji roli a útok je koordinován.

Útoky přes WWW. Tyto útoky využívají především databáze, kdy přes SQL Injection hacker vloží přes nechráněný vstup do databáze svůj vlastní kód. Jakmile je kód do databáze vložen, může data jakkoliv upravovat, mazat či vynášet. Tento způsob útoku využívá chyby programátora databáze.

Trojský kůň je typ malware, který se dostane do počítače a po jeho spuštění odstaví firewall, antivirové programy, rezidentní štíty, anti-spyware programy a podobně. Po odstavení ochran počítače posílá přes internet zprávu hackerovi či dalším virům, kde pak dojde ke specifickému útoku.

Spyware. Tento typ programu, infiltrace do počítače (velmi často po napadení trojským koněm) shromažďuje osobní data či hesla a odesílá je pomocí internetu pryč.

Viry jsou široká skupina programů, které škodí operačnímu systému, mažou data, upravují je, mohou dokonce ničit hardware, například pomocí přepětí nebo nestandardními příkazy pro ovládání například pevných disků či optických mechanik. Jsou primárním nebezpečím, které bezprostředně ohrožuje data každého uživatele PC. Každý uživatel počítače by měl dbát na co nejlepší ochranu svých dat pomocí specifických programů - antivirů. V praxi bývá tato situace mnohdy podceňována především z důvodů nízké počítačové gramotnosti většinových uživatelů. V organizaci je situace o mnoho lepší, neboť se o tuto problematiku starají IT odborníci.

Nové hrozby

Informační technologie a zejména pak právě počítačové sítě umožnily vzniknout novým hrozbám, o kterých jsme neměli před několika desítkami let ani tušení. Vedle nejrůznějších forem kriminality, kterou zejména celosvětová síť internet umožňuje páchat, je to přímé ohrožení dat a technologií a technologických procesů.

Možné dopady na HZS? Přesto, že tato problematika zdánlivě přímo nesouvisí s ochranou dat u HZS, představuje nezanedbatelnou hrozbu pro všechny informační technologie připojené do celosvětové sítě internet. Je jen otázka času a záleží na vůli hackerských skupin, na které organizace a orgány zaměří svoji pozornost, aby prosadily své více či méně oprávněné požadavky. A právě s přibývajícími technologiemi závislými na bezchybném fungování sítí se stává toto riziko více než aktuální.

V příloze č. 4 jsem tuto problematiku rozebral podrobněji, včetně aktuálních událostí, které se odehrály během zpracovávání mé práce.

1.2 Bezpečnost ochrany dat HZS Jihočeského kraje

1.2.1 Ochrana objektů

Pod pojmem objektová bezpečnost se skrývá soustava opatření, která pomáhají chránit fyzické ohrožení daného objektu. Patří sem jak mechanické zábrany, tak elektronické sledovací a vyhodnocovací systémy.

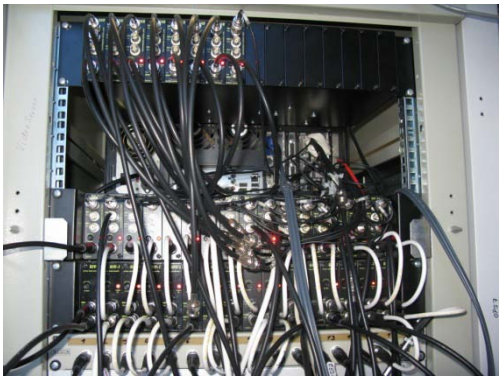
Celý areál krajského ředitelství HZS Jihočeského kraje v Českých Budějovicích tvoří uzavřený celek, chráněný zvenčí plášti budov, zdmi a smíšenými ploty (betonové profily, trapézový plech). Přístup do areálu je možný dvěma vjezdovými a přístupovými branami, z nichž zadní, která ústí do Nádražní ulice, je elektricky otevíraná a slouží pouze pro průjezd těžké požární techniky. Hlavní brána, která slouží i ke vstupu osob je dozorována fyzickou ostrahou.

Obr. č. 6: Areál HZS JčK

Zdroj: Vlastní

Kamerový systém

Kamery pro monitorování areálu jsou u Hasičského záchranného sboru Jihočeského kraje používány od roku 2002. Nejprve to bylo 6 kamer napojených na analogový monitor umístěný na operačním středisku HZS. Tento systém umožňoval on line sledování a neumožňoval žádný záznam. Byl primárně využíván pro podporu operačního řízení při odbavování výjezdu jednotek k zásahům. Bylo možné sledovat průjezdní křižovatky a popřípadě řídit jejich provoz. Kamerový systému s možností záznamu a archivace byl následně pořízen v roce 2006. Videoserver Axemax DVRX1600 byl vystavěn na platformě PC s procesorem Intel Pentium a osazen grabovacími kartami s 24 analogovými vstupy. Instalovaný systém je Windows XP, aplikační SW iGuard.



Obr. č. 7: Video server

Zdroj: Vlastní

Obr. č. 8: Videoserver

Zdroj: Vlastní

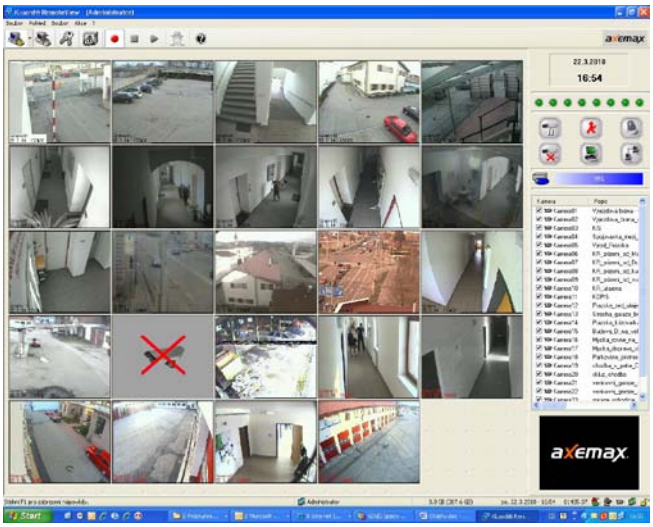
Technická data video serveru:

- Plně triplexní provoz - živý obraz/záznam/přehrávání
- Hybridní systém – připojení analogových i LAN kamer
- 16-32 kamerových vstupů
- Rychlost záznamu 100/50 fps v rozlišení PAL
- Propracovaná detekce pohybu
- Vzdálený dohled a prohlížení záznamů přes LAN a internet
- Archivace všech událostí do deníku
- Možnost využití poplachových vstupů a výstupů
- Upozornění na poplach přes email, příp. SMS
- Export a tisk snímků, export videosekvencí do AVI souboru
- Integrovaná CD-RW mechanika (volitelně DVD-RW)
- Standardně 200GB pevný disk rozšiřitelný vnitřně až na 2,4TB!
- Síťové rozhraní 10/100 Mbps RJ5
- Výstup VGA monitor + kompozitní
- USB 2.0 pro snadné připojení dalších periférií
- Robustní provedení s možností uzamknutí celohliníkového čelního panelu
- Možnost montáže do 19" rozvaděče
- Možnost virtuální klávesnice

Ukládání záznamu probíhá na interní pevný disk. Vlastní videoserver je zapojen do lokální počítačové sítě. Pro vlastní monitoring a přehrávání záznamů je používán SW iGuard instalovaný na uživatelských PC. Ke spuštění monitoringu je třeba znalost uživatelského hesla. Pro konfiguraci pak heslo administrátorské.

V systému jsou využity stávající instalované kamery, následně rozšířeny do současného počtu 27 ks. Kamery jsou analogové s rozlišením 380 televizních řádků, což již na dnešní podmínky nepřináší příliš velkou kvalitu obrazu. Ke zhoršené kvalitě přispívá i vlastní napojení jednotlivých kamer, které je realizováno vedeními z koaxiálních kabelů s velkým počtem spojů s nepříliš kvalitními konektory typu F, velkým množstvím konektorů a propojovacích kablíků u rozbočení signálu umístěného před vstupy do vlastního videoserveru. Pro vzdálenější připojení jsou používány převodníky coax/twistpeer. To by samo o sobě nebylo tak špatné řešení, ale kabeláž,

která je pro toto propojení k dispozici, je použita ze staré elektroinstalace, provedené syky kabely, u kterých není zachováno požadované spletení „kroucení“ párů, jež je pro přenos kvalitního signálu nezbytné.



Obr. č. 9: Aplikace iGuard

Zdroj: Vlastní

Elektronická kontrola vstupu

Zabezpečení jednotlivých objektů areálu krajského ředitelství HZS Jihočeského kraje je realizováno čipovými kartami standartu Wiegand a systémem elektronicky řízených elektrických zámků ABLOY. Wiegand je standardní rozhraní, používané jako výstup ze čteček bezkontaktních karet. Komunikace je pouze jednosměrná a to ze čtečky do připojeného zařízení (Wie 232). Fyzickou vrstvou Wiegandu jsou tři vodiče GND, DATA0 a DATA1. Přenášená data se mírně liší v závislosti na typu protokolu Wiegand. Nejčastěji je možné se setkat s protokoly Wiegand 26 a Wiegand 30. Protokol je zabezpečen paritou. Výhodou rozhraní Wiegand je hlavně možnost připojení čtečky na poměrně velkou vzdálenost. Vlastní zpracovávání přijatých kódů provádí procesorové jednotky NS2 výrobce Honeywell (obr. č. 10). Ke každé této jednotce lze připojit dvě čtečky karet. Vlastní jednotky lze řadit do kaskády přes rozhraní RS485 a tím vytvořit kompaktní systém. Vlastní konfigurace systému se provádí pomocí SW NStar.

Obr. č. 10: Zařízení kontroly vstupu
Zdroj: Vlastní

Obr. č. 11: Zámek Aboy
Zdroj: Vlastní

Čipové karty vlastní každý příslušník a zaměstnanec organizace. V systému je mu pak přiřazeno oprávnění, které dveře má ten či onen zaměstnanec právo otevřít. Tento systém je nadále využit k řízení vstupu, co se týče bezpečnosti organizace, do důležitých místností. Tak jsou těmito zámky vybaveny třeba i dveře na OPIS, dveře do technologických místností a také vstup na oddělení informačních systémů.

Nadstavba elektronické kontroly vstupu - docházkový systém

Docházkový systém je jedinou aplikací, která se využívá u HZS Jihočeského kraje jako nadstavba kartového systému. V jednotlivých objektech jsou instalovány terminály se čtečkami karet, které se ovládají klávesnicí s několika symboly, pomocí nichž si jednotliví zaměstnanci a příslušníci zvolí příznak, neboli důvod průchodu, jež je znázorněn na obr. č. 13 a slouží k následnému načtení čipové karty.

Obr. č. 12: Inteligentní čtečky karet
Zdroj: Vlastní

Obr. č. 13: Čtečka karet s vysvětlivkama
Zdroj: Vlastní

Důvody průchodu, které lze zadat, jsou patrny s interaktivních návodů, které jsou umístěny v místech instalace inteligentních čteček karet.

1.2.2 Ochrana písemností

Do roku konce 80. let byly písemné dokumenty jedinou formou uchování dat. Dnes 20 let po nástupu informačních systémů, tvoří na některých odděleních, zejména ekonomickém a personálním, převažující médium při práci s daty a informacemi. Právě proto, že je tu papírové médium od nepaměti, je systém manipulace s papírovými informacemi poměrně dobře propracovaný a zažitý. Pro písemné dokumenty platí spisový a skartační řád, kde je přesně vymezena práce s nimi. Jak pracovníci mohou nebo musí s nimi zacházet. A zatímco písemné dokumenty v minulosti ohrožovaly spíše přírodní živly, dnes se zvyšující se váhou, která je přisuzována zejména osobním datům, ohrožují práci s informacemi faxy, kopírky a mobilní telefony. U mobilních telefonů jsou to také stále dokonalejší kamery.

Jednotlivá pracoviště, na kterých se manipuluje s papírovými dokumenty jsou vybavena uzamykatelnými, převážně dřevěnými skříněmi pro jejich uskladnění (obr. č. 16). Pro dlouhodobou archivaci jsou pro jednotlivá oddělení zřízeny Archivy v půdních prostorách objektů HZS Jihočeského kraje (obr. č. 14, 15).

Pro manipulaci s papírovými dokumenty organizace vůči vnějším subjektům slouží spisovna HZS JčK. Pohyb a uchování papírových písemností uvnitř organizace se řídí spisovým řádem.



Obr. č. 14, 15, 16: Archiv HZS JčK
Zdroj: Vlastní

1.2.3 Informační technologie

Počítače

PMD 85 – počátky informačních technologií u HZS. První počítač, který se objevil u Hasičského záchranného sboru, byl PMD 85. (obr. č. 18). Byl to 8 bitový osobní počítač vyráběný od roku 1985 společností Tesla Piešťany a Tesla Bratislava v bývalém Československu.

Obr. č. 17: 8 bit počítač PMD 85

Zdroj: http://www.root.cz/clanky/ceskoslovenske-osmibitove-pocitace-2-ndash-pmd-85/

Tento počítač byl vyráběn v tuzemsku, a z důvodu nedostatku devizových prostředků a embarga na vyspělé technologie byl vyráběn výhradně z tuzemských součástek. Autorem tohoto „počítače pro školy i průmysl“ byl ing. Roman Kišš a ing. Štefan Tóth z Tesly Piešťany. Jeho představení bylo na výstavě Elektronizace a automatizace 83. Výroba PMD 85 byla zastavena v roce 1989.

Tyto počítače bylo možné využít maximálně pro jednoúčelové aplikace a sloužily převážně k experimentům v této dosud neznámé oblasti. Jedinou známou aplikací, která našla využití u HZS v Jihočeském kraji, byla elektronická časomíra, kterou vyrobil, sestrojil a naprogramoval v programovacím jazyku Basic jeden nadšený zaměstnanec.

Další snahou pokusit se dohonit vlak v tomto novém odvětví, byl nákup počítačů ze Slušovic. Počítače řady TNS vyrábělo zemědělské družstvo Agrokombinát Slušovice od roku 1985. Zkratka TNS znamenala Ten Náš Systém. Počítač byl původně navržen pro zemědělské podniky, později však pronikl i do škol a státních institucí. Typ TNS HC 8 (obr. č. 19) byl 8-bitový. Byl osazen procesorem Z80 a pamětí RAM 256 kB.

Obr. č. 18: 8bitový počítač TNS Slušovice HC8

Zdroj: http://www.root.cz/clanky/ceskoslovenske-osmibitove-pocitace-2-ndash-pmd-85/

Klávesnice měla národní abecedu a tlačítka pro ovládání kurzoru, výstup na obrazovku byl možný až v 16 barvách. Počítače bylo možné jako terminál připojit k počítačům SMEP nebo JSEP. Přítomný byl akustický modem pro přenos po telefonních linkách. Na obalu byl prolis pro telefonní sluchátko. Bylo možné připojit myš, joystick a další měřící zařízení. Operační systém TNS-DOS dovoloval použít programy Wordstar a Supercalc a programovat ve vyšších programovacích jazycích jako Fortran, Cobol, C, Prolog, Fort nebo Turbo-Pascal. Pořizovací cena byla 25 000,- Kč.

Teprve v roce 1981 do hry vstoupila firma IBM se svým prvním komerčním mikropočítačem IBM PC. Osobní počítač IBM nebyl ve skutečnosti úplný počítač, ale pouze jakési výpočetní jádro, které bylo možné pomocí standardní sběrnice vyvedené na konektory doplňovat o další HW prvky. Byl tak vytvořen otevřený výpočetní systém s neomezenou variabilitou a rozšiřitelností. Dalším přínosem bylo použití softwarové mezivrstvy, označované jako BIOS. To umožnilo odstranit závislost prováděných programů na technických prostředcích počítače.

Vstup IBM PC na trh vyvolal řetězovou reakci. Výrobci tehdejších mikropočítačů byli nuceni přehodnotit svou strategii, a ti prozíravější opustili firemní architektury a začali vyrábět počítače používající architekturu IBM PC a označované jako počítače kompatibilní s IBM PC. Především díky tomu, že společnost IBM zveřejnila architekturu svého osobního počítače a firma Microsoft zase uvolnila definici rozhraní pro uživatelské programy, vzniklo během mimořádně krátké doby pro IBM PC nepřeberné množství programů a doslova během několika let se PC rozšířilo tak, že byly vytlačeny sálové počítače a nastupující minipočítače. Každý úředník,

výzkumník či manažer měl na stole osobní počítač, na němž si udržoval svá data a prováděl svoje výpočty.

Počítač se tak stal dostupným pro každého, odpadla také pracná příprava programů a dat. I v rámci nevelkého podniku či pracovní skupiny byly postupně značné objemy různorodých dat rozprostřeny po několika počítačích a začaly vznikat problémy s jejich vyhledáváním a přenosem. Přišla druhá vlna, a tou bylo propojování osobních počítačů do lokálních sítí. Trochu trnitější cesta zavádění těchto kompatibilních IBM počítačů byla v tehdejším Československu, neboť vlivem embarga vůči socialistickým zemím ve spojení s nedostatkem devizových prostředků nebyly tyto PC dostupné. Toho využil tehdejší Agrokombinát Slušovice, který jako jediný směl v tehdejším Československu vyrábět PC z dovezených komponent mnohdy vyřazených z výrobních linek pro sníženou jakost. /24/

A tak první PC nakupovaná pro Hasičské záchranné sbory byly právě PC od tohoto dodavatele. Cena v té době byla 300 000,- Kč.

K masivnímu nákupu počítačů docházelo postupně s jejich rychle klesající cenou a samozřejmě s postupně vznikající potřebou v souvislosti se zaváděním nejrůznějších informačních technologií na administrativní činnosti organizace. Dnes má pro svou práci k dispozici počítač každý zaměstnanec a příslušník denní směny. Obměna výpočetní techniky u HZS Jihočeského kraje probíhá v souladu s celosvětovým trendem, a tak se ve stále větší míře obměňují stolní pracovní stanice, které nahrazují notebooky spolu s dokovacími stanicemi. Toto řešení sice přináší větší mobilitu jednotlivých zaměstnanců a příslušníků, ale zároveň však zvýšené bezpečnostní riziko pro data obsažená na lokálních discích jednotlivých notebooků.

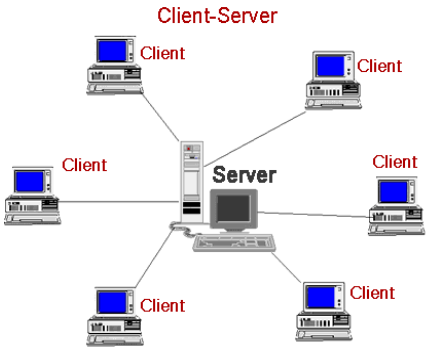
Počítačové sítě HZS

Z hlediska ochrany dat zaznamenal právě tento segment největší rozvoj a nákup technologií a investice do personálního obsazení právě IT oddělení představuje nezanedbatelnou položku rozpočtu HZS.

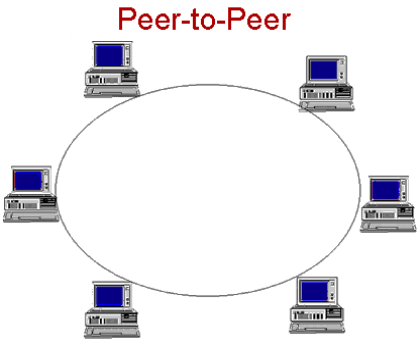
V roce 1993 došlo k osazení několika PC síťovými adaptéry s následně sériovým pospojováním prostřednictvím koaxiálního kabelu. Toto řešení bylo rychlé, poměrně levné ale značně nespolehlivé, a jakýkoli přerušený spoj kdekoli v síti měl za následek

výpadek komunikace v celé síti. Síť byla provozována na síťovém operačním systému Lantastic a její rychlost byla 10 MB/s. V této síti bylo možné propojit počítače se systémem DOS 5.0 (nebo vyšší) a Windows 3.x nebo vyšší (včetně Windows XP).

Síť TCP/IP



Obr. č. 19: Síť topologie klient server
Zdroj: Vlastní



Obr. č. 20: Topologie peer to peer
Zdroj: Vlastní

Ve 2. polovině 90. let se začaly informační technologie uplatňovat přímo v operačním řízení. Pro zabezpečení potřebné spolehlivosti bylo potřeba přejít na nové síťové technologie a změnit topologii počítačové sítě. Byla zvolena síť server-klient na bázi ethernetu ve hvězdicovém uspořádání topologie.

Přesto, že na základě zkušeností a již odzkoušených vlastností byla technologie ethernet nejhorší z nově vzniklých technologií, orientovaných právě na lokální sítě, zvítězila díky masivnímu marketingu a rozsáhlé podpoře výrobců integrovaných obvodů. Síťový operační systém Lantastic byl v roce 1999 nahrazen sítí na bázi protokolu TCP/IP se serverem, umístěným v technologické místnosti s klimatizací.

Velkou výhodou byla implementace přenosových protokolů přímo v operačních systémech Windows. Koaxiální kabel nahradily kabely twist pair a později byla vybudována strukturovaná kabeláž. V dalších letech byla síť nadále rozšiřována a zkvalitňována. Došlo k několika generačním obměnám aktivních síťových prvků od hubů po dnes již plně managovatelné switche Cisco. Rychlost sítě z původních 10 Mbit/s dosahuje nynější 1 Gbit/s. /32/

Internet u HZS Jihočeského kraje

Internet při řešení krizových událostí nabývá stále většího významu, ať už jako nevyčerpatelný zdroj informací, zejména jako nezbytná informační podpora OPIS, ale ve stále větší míře jako platforma pro propojování nejrůznějších technologií. HZS JčK se k internetu zpočátku připojoval telefonním vedením „vytáčenou linkou“, teprve koncem 90. let byly za pomocí tzv. „poslední míle“ budována bezdrátová připojení za pomocí mikrovlnných technologií v nelicencovaném pásmu 2,4 GHz. Ty jsou nyní nahrazovány spolehlivější mikrovlnou technologií v licencovaném pásmu 18 GHz a technologií DSL. Touto technologií je vybudována privátní síť všech požárních stanic Jihočeského kraje a tyto stanice jsou propojeny se sítí KŘ HZS JčK. V současné době je síť KŘ HZS Jihočeského kraje propojena se sítí internet dvěma nezávislými mikrovlnnými spoji 10 Mb/s a 25 Mb/s. Jednotlivé další lokality HZS jsou na Internet připojeny právě přes síť KŘ, což přináší lepší možnost kontroly a zabezpečení.

Konvergovaná telekomunikační síť HZS ČR

První komunikační infrastruktura WAN u složek HZS byla síť Frame Relay vytvořena pronajatými linkami Frame Relay Českého Telecomu a.s., zapojenými do hvězdicové topologie po linii GŘ HZS ČR - HZS kraje a HZS kraje - ÚO HZS kraje. Tuto síť delimitoval HZS JčK při slučování se složkami civilní obrany na základě zákona 239/2000 Sb., o IZS. Do té doby sloužila k provozování systému JSVV a elektronické pošty. Pro Jihočeský kraj byl vytvořen pilotní projekt a síť byla rozšířena o 13 linek až do úrovně požárních stanic. Dále byla síť propojena pomocí technologie Vanguard do ITS Ministerstva vnitra. Na straně HZS byly, opět přes technologii Vanguard připojeny komunikační prostředky - telefonní ústředny, telefony.

Základní nevýhodou výše uvedené komunikace však byla především nehomogenita komunikačního prostředí, nízké přenosové rychlosti (64-128 kb/s) a nižší kvalita služby (bez QoS). Proto byl v březnu 2005, na poradě generálního ředitele HZS ČR s řediteli HZS krajů předložen návrh na přechod do jednotného komunikačního prostředí IP MPLS, tedy sloučení komunikací HZS ČR (síť Frame Relay) a sítě IP MPLS služby TCTV 112. Návrh byl podrobně rozpracován a posouzen jak z technického, tak finančního hlediska a následně schválen.

Cílem nového řešení komunikačního prostředí bylo:

- integrovat existující technická řešení (intranet HZS ČR, síť TCTV 112) do jednotné a jediné komunikační infrastruktury,
- připojit do systému všechny součásti HZS ČR,
- zvýšit přenosové šířky pásem tak, aby byly pokryty všechny potřeby HZS ČR v rámci datových komunikací,
- umožnit základní služby GOVNetu a Centrální podporu uživatelů (CPU),
- v případě potřeby vyčlenit i pásmo na přístup do sítě TESTA II,
- zlepšit ekonomiku provozu spolu se zvýšením standardní úrovně QoS.

V rámci zavedené služby byly vytvořeny jednotlivé virtuální privátní sítě, ve kterých

- VPN1 slouží pro potřebu TCTV 112,
- VPN2 slouží jako vlastní intranet HZS ČR s možností IP telefonie, se zabezpečeným přístupem do internetu a dalších sítí (TESTA II, GovNET).

Přístup k výše uvedeným VPN a přenosové rychlosti jsou umožněny dle následujícího schématu: *GŘ HZS ČR (celkem 10 Mbit/s)*

VPN 1 … multisite TCTV (2 Mbit/s),

VPN 2 … datová síť HZS s možností IP telefonie.

HZS kraje (až 10 Mbit/s)

VPN 1 … služby TCTV (xMbit/s - dle charakteru TCTV),

VPN 2 … datová síť HZS s možností IP telefonie.

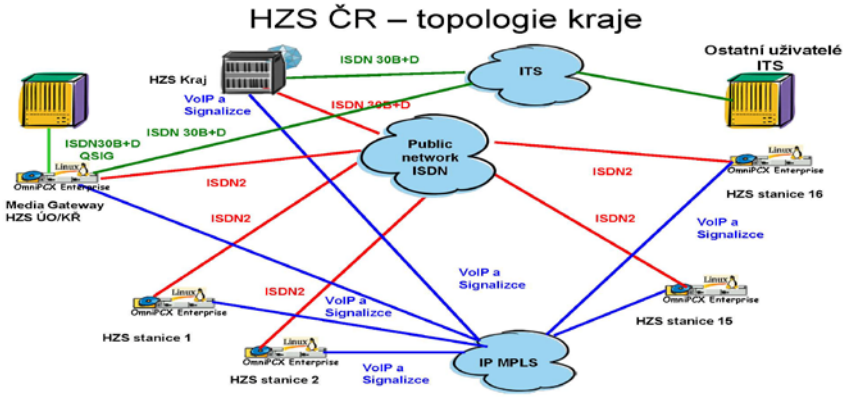
Územní odbor HZS (typicky 384 kbit/s)

VPN 1 … služby TCTV (+ 128 kbit/s),

VPN 2 … datová síť HZS s možností IP telefonie.

Požární stanice (128 kbit/s)

VPN 2… datová síť HZS s možností IP telefonie. /24/



Obr.č. 21: - Schéma konvergované telekomunikační sítě HZS

Zdroj: Vlastní

Ochrana sítí

Zatímco cílem útočníka při napadení počítače či serveru je získat přístup do tohoto terminálu přes nějaký nechráněný otevřený port a nadále zde páchat datové škody, či získávat z něj data pro svou potřebu, tak útok na počítačovou síť je zaměřen na datovou komunikaci. To znamená, že útočník se snaží data proudící v síti takzvaně odposlouchávat a nadále je zneužívat pro svou potřebu. Ve sdílených sítích ethernet realizovaných pomocí habů (rozbočovačů), jsou rizika útoku vysoká. Zejména odposlech dat je velmi jednoduchý, protože data se šíří ke všem terminálům (stanicím) v daném segmentu. V takzvaných přepínaných ethernetových sítích realizovaných pomocí switchů a routerů je bezpečnost vyšší než u předtím uvedených ethernetových sítí sdílených. Přesto jsou i přepínané sítě zranitelné řadou útoků. I zde lze odposlouchávat data na LAN síti, odesílat falešná data do sítě, přistoupit bez oprávnění do sítě a realizovat útok proti službám LAN sítě. Vhodným výběrem switchů a routerů, jejich správnou konfigurací je možné rizika v přepínaných sítích výrazně omezit.

V současné době jsou sítě HZS vystavěny výhradně pomocí síťových prvků od firmy Cisco. Vedle vysoké spolehlivosti těchto síťových prvků, je nově zaváděna bezpečnostní politika při připojování uživatelů do sítě pomocí protokolu 802.1X, přepínači Cisco Catalyst 2900/350 a RADIUS serveru.

Standtard IEEE 802.1X definuje protokol typu klient-server pro řízení přístupu, který zabraňuje přístupu neautorizovaných klientů do sítě přes veřejně přístupné porty. Autentizační server ověří každého klienta připojujícího se k portu přepínače dříve, než zpřístupní jakékoliv služby nabízené přepínačem. Dokud není klient autorizován, 802.1X dovolí přístup pouze pomocí protokolu Extensible Authentication Protocol over LAN (EAPOL) přes port ke kterému je klient připojen. Až po úspěšném ověření prochází přes port normální provoz.

Ochrana sítí proti neoprávněnému přístupu z internetu

V každém počítačovém uzlu, kde je lokální počítačová síť HZS připojena do sítě internet, je umístěn firewall.

Obr. č. 22: Grafické znázornění firewallu

Zdroj: Vlastní

Firewall definuje konkrétní pravidla, podle kterých musí být komunikace mezi počítačovými sítěmi vedena. Každý příchozí paket zkontroluje podle zdroje a cíle dat včetně zdrojového a cílového portu. K ideálnímu zabezpečení je potřeba, aby se mohl firewall opřít i o znalosti používaného protokolu a informace o stavu spojení.

V rámci své činnosti firewall odhaluje pokusy o průnik do lokální sítě, definuje překlady adres NAT nebo instrukce pro vytváření šifrovaných spojů. Souhrnně jsou tyto procesy nazývány bezpečnostní politikou sítě.

Firewally používané u HZS jsou opět od firmy Cisco. Starší typy PIX jsou postupně nahrazovány generačně novějšími typy ASA.

Obr. č. 23: Firewall Cisco ASA

Obr. č. 24: Firewall Cisco PIX

Zdroje: http://www.ovh.cz/dedikovane_servery/firewall_dedikovane_servery.xml
http://www.infracom.com.sg/products.php?product=CISCO851%252dK9-%252d-Ethernet-SOHO-Security-Router

Servery z pohledu ochrany dat

Společně se zaváděním informačních technologií, výstavbou lokálních počítačových sítí a hlavně nutností pracovat se stále se zvětšujícím se objemem dat a informací, bylo nutné přistoupit k implementování serverů. Zpočátku to byly zejména souborové servery pro sdílené ukládání souborů a servery pro práci s elektronickou poštou. Později byly implementovány databázové servery, nejrůznější technologické servery pro ovládání zvyšujícího se počtu technologií, audioservery, videoservery a komunikační servery. U HZS JčK je v současnosti implementováno 50 ks serverů. Již téměř každý server obsahuje diskové RAID pole.

Obr. č. 25: Servery HZS JčK

Zdroj: Vlastní

Obr. č. 26: Servery HZS JčK

Zdroj: Vlastní

Nejdůležitější Servery HZS s pohledu ochrany dat jsou

- Doménový server ntscb01 – operační systém Windows server 2003 (provoz personálního a ekonomického SW např. VEMA, účetnictví, EKOS, ASPI)

Instalováno diskové pole RAID-5 se čtyřmi disky o kapacitě 136GB.

- Doménový server ntscb02 – operační systém Windows server 2003 (souborový server, politika active directory)

Instalováno diskové pole RAID-5 se třemi disky 136GB. Dále je instalován jeden disk 136GB jako Hotspare.

- Data Storage – operační systém Windows server 2003 (krajské datové úložiště)

Instalována dvě disková pole

RAID-1 se dvěma disky 500GB na nichž je instalovaný operační systém.

RAID-5 se šesti disky 1TB pro ukládání dat a zároveň záloh z doménových serverů.

- 2 ks databázové servery ORACLE, obsahující veškeré databáze, potřebné po činnost technologií a informačních systémů OPIS

Tyto servety pracují ve dvojici, přičemž vždy jeden je v „ostrém“ provozu a jeden ve standby režimu. Data se na obou serverech synchronizují, aby byla stále aktuální. Instalována disková pole RAID-10 s osmi disky.

- AMDS – komunikační server – operační systém Windows WP

Diskové pole RAID-1 se dvěma disky.

- Video server – Windows XP (SW iGuard) je součástí kamerového systému
- Web server – na tomto serveru je provozován Intranet HZS JčK
- Terminál server – provozování terminálových aplikací (GINIS)

Diskové pole RAID-1 se dvěma disky.

- OmniVista – Windows XP (SW OmniVista) nadstavba pro management a dohled komunikačního systému Alcatel)

Diskové pole RAID-1 se dvěma disky.

- Exchange – poštovní server

Diskové pole RAID-1 se dvěma disky.

- Mail server – Linux – ubuntu (smtp server, squid)

Diskové pole RAID-1 se dvěma disky.

- LUPUS – zpracování dat z mobilních navigačních systémů

Diskové pole RAID-1 se dvěma disky.

- Centrum – ovládání systému JSVV
- Dohled – monitorování technologií a sítí HZS JčK

Diskové pole RAID-1 se dvěma disky.

Raid pole – ochrana dat

Vzhledem k tomu, že pevný disk je složité zařízení kombinující elektroniku a jemnou mechaniku, je již ze svého principu náchylný k poruše. Toto je nepříjemné zejména u serverů, kde jednak cena uložených dat může představovat mnohamilionové částky, jednak - i při pravidelném zálohování - jen odstávka serveru spojená s opravou a obnovou dat představuje značnou ztrátu na prostojích mnoha uživatelů. Proto byla zkonstruována disková pole, kde se pomocí speciálního řadiče více disků fyzických navenek jeví, jako jeden disk logický. Pole se ve zkratce nazývají RAID.

Odlišné způsoby ukládání dat jsou realizovány buď softwarově nebo hardwarově. V softwarovém řešení obsluhuje zápis do pole RAID operační systém (resp. speciální mezivrstva nebo přímo ovladač zařízení), a proto se jedná o nejlevnější řešení, které však trpí některými nedostatky jako např. snížení rychlosti. Hardwarové řešení tyto nedostatky odstraňuje pomocí speciálního zařízení, který se nazývá řadič, jež obstarává obsluhu RAID sám a hlavní procesor počítače tak není zatěžován. Problémem je, že většina lacinějších RAID řadičů na trhu je ve skutečnosti softwarově řízena, takže se o hardwarové řešení nejedná.

Pokud dojde při provozu RAID pole k výpadku některého z disků respektive členu pole, dostane se pole do tzv. *degradovaného stavu*, ve kterém je jeho výkon typicky nižší, avšak stále jsou všechna uložená data k dispozici. Správce počítače vymění havarovaný disk za nový a ten začlení zpět do pole, čímž začne tzv. *rekonstrukce* pole, při které jsou dopočítány chybějící údaje a zapsány na nový disk. Data jsou typicky během rekonstrukce stále přístupná. Po dokončení rekonstrukce je RAID pole opět tzv. *synchronizováno*. Někdy je v poli trvale k dispozici rezervní disk, takže rekonstrukce pole může být zahájena zcela automaticky.

Častou chybou je považování RAID pole za zálohování dat. Skutečná záloha však vyžaduje doplňující operace. Tj. uložení dat na bezpečné místo, jejich fyzické

zabezpečení, šifrování zálohy, možnost návratu ke starší verzi dat apod. Proto není možné při používání RAID pole samotné zálohování vyloučit.

Nejčastěji používaná RAID pole jsou typu RAID-0, RAID-1, RAID-5 a RAID-6. poskytují plnou ochranu dat před výpadkem libovolného disku v diskovém poli. Dále pak RAID-10, které vzniká kombinací RAID-0 a RAID-1. Nestandardní pole typů RAID-2, RAID-3, RAID-4 a RAID-7 se používají velmi sporadicky. Technický popis RAID polí včetně jejich specifikací je v příloze č. 5 této práce.

Hotspare disk

Je disk, který je zapojen v diskovém poli, ale není součástí diskového pole RAID. Pokud dojde k výpadku disku, hotspare disk se automaticky do pole začlení a po jeho synchronizaci bez ohrožení datové integrity může opět dojít k výpadku libovolného disku, třeba nově začleněného. Hotspare disk je ideálním řešením pro instalace, kde není 24 hodinový dohled, ovšem je třeba udržet vyšší úroveň zabezpečení dat i v případech, kdy není přítomen vyškolený personál. Také poskytuje možnost překlenout období, kdy je sice vadný disk, ovšem není možné znepřístupnit data kvůli výměně disku.

Páskové mechaniky – záloha dat

Nezbytnou součástí technologických místností, kde jsou umístěny servery, jsou zálohovací technologie pro zálohu elektronických dat. Vzhledem k objemům dat v řádech stovek GB se upustilo od zálohování na optické disky CD a DVD a přešlo se na dnešní páskové technologie.

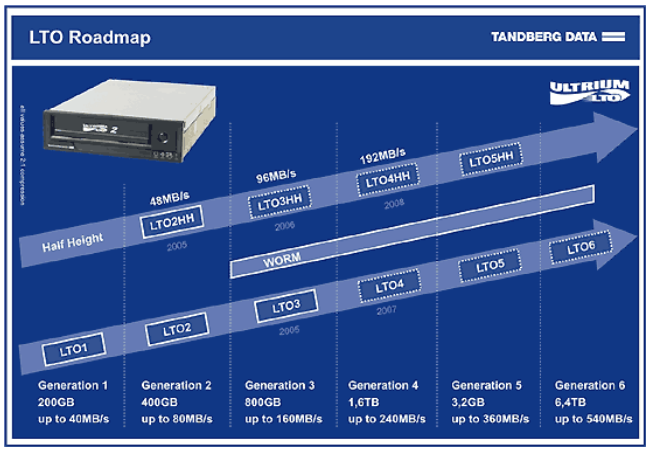
Existuje řada zálohovacích technologií. Díky spolehlivosti a bezpečnosti uložených dat zvítězila lineární technologie zápisu do podélných stop (SLR, DLT, SDLT, LTO) nad technologií helical scan – tedy zápisem rotační hlavou (DAT, AIT).

Jednoznačně zvolit nejlepší z lineárních technologií záznamu dat asi není možné, protože vždy budeme muset nahlížet na volbu zálohovacího zařízení jak z finančního, tak technologického hlediska. Proto v současné době souběžně žijí tyto lineární technologie, o kterých se budu nyní zmiňovat.

Historicky nejstarší technologie QIC byla zásluhou Tandberg Data zdokonalena v technologii SLR (Scalable Linear Recording). Dnes nejvyšší dosažená kapacita 140 GB (s kompresí) je současně nejvyšší v této třídě zařízení. Kazeta se vyznačuje robustní mechanickou konstrukcí, která zajišťuje nejen přesné usazení v mechanice, ale znamená i lepší odvádění tepla. Je minimalizována možnost zničení záznamového média, páska zůstává stále uvnitř kazety.

Do skupiny zálohovacích mechanik s kapacitou pod 100 GB náleží i odlehčená verze nové generace DLT (SDLT) v podobě typu VS. DLT (SDLT) technologie patří do početné rodiny s lineárním zápisem. Používá pásek s půlpalcovým formátem. Kazety mají jen jednu cívku, ta druhá je pevnou součástí streameru. V roce 2001 byl představen formát SDLT220, který prolomil nativní 100 GB kapacitní bariéru, druhá generace SDLT320 přinesla 160 GB na médium, a zatím poslední v řadě, je mechanika třetí generace SDLT600. Dosahuje nejen nativních rychlostí zálohování vyšších než 2 GB/min, ale také přináší nativní kapacitu 300 GB.

Seagate, ve spolupráci s partnery Hewlett-Packard a IBM vytvořil Linear Tape-Open, nebo LTO technologie, nová, výkonná, škálovatelná a otevřená pásková architektura, která bude následovat roustoucí požadavky na ukládání od středně velkých po prvotřídní servery a dosahujících kapacit až 800 GB na jednu cartrige v generaci 3 Ultrium formatů. Jde o otevřený formát a díky tomu je zde patrný konkurenční tlak na cenu. V současnosti jde o nejpesrpektivnější formát. /8/



Obr. č. 27: LTO Roadmap

Zdroj: http://www.storage.cz/775-lto-dlt-slr-co-je-lepsi

U HZS Jihočeského kraje jsou pro vytváření záloh použity mechaniky LTO technologie ve dvojím provedení.

- Typ VC 160 o kapacitě páskové cartridge 200GB (1. generace)
- Typ LTO2 o kapacitě páskové cartridge 400GB (2. generace)

Obr. č. 28: Zálohovací mechaniky HZS JčK

Zdroj: Vlastní

Ochrana proti virům, spamu

Na ochranu pracovních stanic a serverů HZS JčK proti virům je 8 let využíván produkt ESET NOD32 Antivirus. Tento antivirový program využívá nejmodernějších detekčních metod a poskytuje vyváženou ochranu před všemi druhy počítačových hrozeb.

Centrální správa síťové bezpečnosti – ESET Remote Administrator představuje ucelenou koncepci vzdálené instalace a správy klientských stanic z jediného místa. Což představuje významnou úsporu času pro oddělení IT.

Ochrana elektronické pošty HZS

ClamAV je open-source (GPL) antivirový program určený pro detekci trojských koní, virů, malware a jiných nebezpečných hrozeb. Je to de facto standard pro skenování emailové brány. Nabízí vysoký výkon skenování Mutli-threaded daemon a utility příkazové řádky pro skenování souborů na vyžádání.

Kerio Connect používá několik technologií pro boj s nevyžádanou poštou, tzv. spamem. Základním stavebním prvkem v boji proti spamu v Kerio Connect je SpamAssassin. Jedná se o parametrický filtr, který analyzuje zprávy a na základě nalezených příznaků přidělí dané emailové zprávě bodové hodnocení. Na základě tohoto bodového hodnocení se určí, zda je zpráva nevyžádaná nebo se jedná o korektní email.

Tato technologie je dále upřesněna tzv. Bayes filtrem, který zajišťuje zpřesnění výsledků získaných základní analýzou emailové zprávy. Funkce Bayes filtru by se dala přirovnat k "učení" spamového filtru. Tato metoda je založena na označování emailů jako Spam, případně Ham (korektní emailová zpráva). Takto označené zprávy se dále analyzují tak, že se v základním režimu rozeberou na jednotlivé příznaky. Jednotlivým příznakům jsou pak přiřazeny pravděpodobnostní hodnoty, které udávají s jakou pravděpodobností může nevyžádaný email obsahovat daný příznak.

Součet těchto pravděpodobností pak určí výslednou pravděpodobnost, zda je email Spam či Ham. Jelikož se jedná pouze o upřesňující informaci, je tato pravděpodobnost přepočtena na určité bodové ohodnocení, které je přičteno k celkové hodnotě získané z předchozích testů. V emailové zprávě najdete tuto hodnotu pod označením BAYES_xx v hlavičce X-Spam-Status. Příklad takovéto hlavičky je uveden na obr. č. 29.

```
X-Spam-Status: Yes, hits=10.0 required=5.0 tests=AWL: -1.138,BAYES_99:
4.07,DATE_IN_PAST_06_12: 0.918, HTML_50_60: 0.539,HTML_FONT_TINY:
0.521,HTML_MESSAGE: 0.001, HTML_TAG_BALANCE_BODY: 0.096,HTML_WEB_BUGS:
0.311,MIME_HTML_ONLY: 1.156, SARE_HEAD_SPAM: 2.222,SARE_HTML_FSIZE_1ALL:
1.666,SARE_HTML_USL_1CHAR2: 0.2, SARE_SUB_MISC_1: 1.272
```

Obr. č. 29: Bayes filtr

Zdroj: https://kb.kerio.com/article/jak-pracuje-bayes-filtr-a-spamassassin-560.html

Jak je z příkladu patrné, Bayes filtr může významně ovlivnit výsledné hodnocení Spamového filtru a tudíž je velice důležité, aby byl korektně natrénován. Kerio MailServer umožňuje trénovat Bayes filtr dvěma způsoby:

- Email je "spam" - nevyžádaná pošta
- Email je tzv. "ham" - korektní email.

Uživatel má k dispozici rozhraní (tlačítka "Spam" a "Not Spam"), kterými může Bayes filtr určit. V případě obecného IMAPového klienta, je možné provést určení prostým přesunutím zprávy do složky „nevyžádaná pošta“ nebo naopak vyjmutí emailu z této složky.

Dobře naučený Bayes filtr je nutný k efektivnímu hodnocení emailových zpráv, jak je patrné z předchozího popisu. Aby mohly být spočteny počáteční pravděpodobnosti a filtr tak mohl začít správně pracovat, je zapotřebí získat alespoň 200 označených spamových zpráv a 200 korektních emailových zpráv. Spam Assassin poskytuje technologii samoučení. Automatické trénování funguje tedy dle následujícího schématu: Má-li emailová zpráva vysoké hodnocení, zpráva se použije pro naučení Bayes filtru. Taková zpráva musí dosáhnout hodnocení 3 bodů za testy týkající se hlavičky emailové zprávy a 3 bodů za tělo emailové zprávy. Zároveň musí celkové bodové hodnocení zprávy překročit hodnotu 12 bodů. Je-li hodnocení velmi nízké, použije se zpráva v učícím mechanismu jako korektní (ham). Nesplňuje-li zpráva žádné z výše uvedených kritérií, zpráva není využita pro další učení Bayes filtru, zprávu může označit uživatel.

Uživatelé mohou též určit Bayes filtr a tím zpřesňovat výsledné hodnocení Spam Assassinu. Učením dochází k zvyšování/snižování hodnot pravděpodobností jednotlivých příznaků a tím i k zvyšování/snižování pravděpodobnosti, že zpráva bude označena jako spam/ham. Neznamená to tedy, že nevyžádanou zprávu již uživatel neobdrží, ale že pravděpodnost obdržení obdobné zprávy bude vyšší nebo nižší. /22/

Tyto dva produkty jsou nainstalovány a provozovány na email serveru, přes který probíhá komunikace veškeré email komunikace z a do organizace a také v rámci organizace. Aplikováním tohoto SW se poměrně zdárně daří čelit hrozbám elektronické pošty.

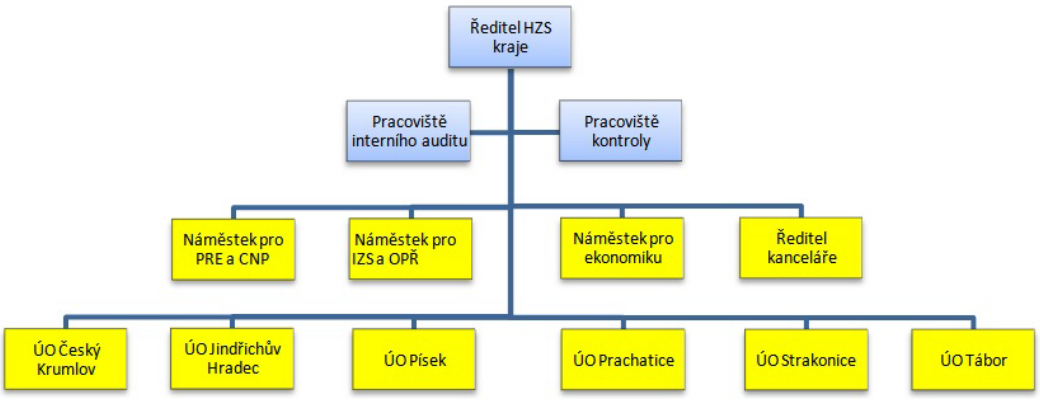
Rozvoj informačních technologií v 80. letech nabral na dynamičnosti a po roce 1989 se tyto technologie rychle začleňovaly do všech odvětví lidské činnosti. A tak došlo i na organizace, jejichž činnost se zdánlivě s novými technologiemi neslučovala. Naštěstí se v této době našlo pár nadšenců, kteří včas rozpoznali potenciál a budoucnost informačních technologií pro podporu činnosti HZS. V době zavádění informačních technologií u HZS nebylo žádné specializované programové vybavení a počítače

sloužily především jako lepší psací stroje, později k vedení ekonomických agend a statistiky událostí bylo zřízeno u HZS oddělení ASŘ - automatizovaný systém řízení, které se v počtu dvou příslušníků staralo o zavádění těchto nových technologií.

Začátkem 90. let pak vzniklo oddělení informačních systémů, které má dnes sedm příslušníků, kteří se v rámci HZS JčK starají o více než 390 počítačů a 50 serverů.

1.3 Organizační struktura HZS JčK z pohledu přístupu k informacím

V této kapitole se zaměřuji na popis vlastního výzkumu pro analyzování nebezpečí a ochrany dat na jednotlivých odděleních. K tomu jsem zvolil metodu kvalitativního výzkumu. Osobními pohovory s vedoucími příslušníky a zaměstnanci jsem zjišťoval s jakými daty a informacemi přicházejí do styku při své práci. Ptal jsem se, s jakými zákony, vyhláškami a obecně závaznými předpisy se při své práci s daty a informacemi řídí. Zjišťoval jsem, jak provádějí nejrůznější bezpečnostní politiky při práci s daty a informacemi a zároveň je nechal posoudit a ohodnotit míru rizika při práci s daty na svém oddělení metodou, kterou popisuji v následujících kapitolách.



Obr č. 30: Organizační struktura

Zdroj: Vlastní

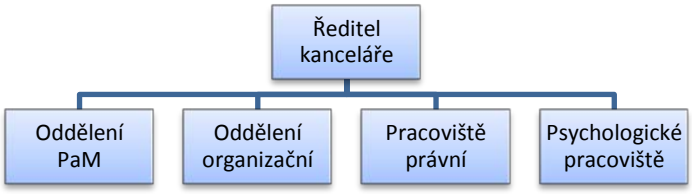
Krajský ředitel - odpovídá za chod HZS Jihočeského kraje a jeho úkoly. Přichází do styku s veškerými daty a informacemi, které vznikají a s nimiž pracují příslušníci a zaměstnanci celé organizace. Má přístup téměř do všech úrovní informačního systému HZS JčK. Má prověrku na stupeň D.

Pracoviště interního auditu - příslušník tohoto pracoviště vykonává následnou veřejnoprávní kontrolu ve smyslu ustanovení zákona o finanční kontrole, zajišťuje vykonání auditů, plán interního auditu vyhodnocuje a vykonává mimořádné interní audity na základě pověření ředitele HZS kraje.

Příslušník tohoto pracoviště přichází do styku téměř se všemi informacemi u HZS, kromě informací označených stupněm tajné. Nemá přístup do všech úrovní informačního systému HZS, ale data a informace pro svou práci má právo si vyžádat na základě pověření ředitele HZS od vedoucích pracovníků kontrolovaných oddělení.

Pracoviště kontroly - příslušník tohoto oddělení vykonává kontroly v rámci plánu kontrolní činnosti a mimořádné kontroly na základě pověření ředitele HZS kraje podle zákona o státní kontrole a zákona o finanční kontrole. Vykonává následnou veřejnoprávní kontrolu ve smyslu ustanovení zákona o finanční kontrole, vede agendu stížností a petic adresovaných krajskému řediteli.

Přichází do styku téměř se všemi informacemi, kromě informací označených stupněm tajné. Do všech úrovní informačního systému HZS přístup nemá, ale data a informace pro svou práci si může vyžádat na základě pověření ředitele HZS JčK od vedoucích pracovníků kontrolovaných oddělení.



Obr. č. 31: Organizační struktura – ředitel kanceláře

Zdroj: Vlastní

Ředitel kanceláře - kancelář zabezpečuje organizaci a koordinaci činnosti krajského ředitelství, včetně agend v oblasti právní, organizační, styků s veřejností, informací, zahraniční spolupráce, utajovaných informací, personální práce, vzdělávání, práce a mezd a oblasti sociální. Kancelář se člení na oddělení organizační, oddělení personální a PaM (personální a mzdové), psychologické pracoviště a pracoviště právní.

Ředitel kanceláře přichází do styku s osobními daty zaměstnanců, příslušníků a žadatelů o zaměstnání. Zajišťuje systemizaci služebních míst a její obsazenost. Tuto

agendu zpracovává na PC, jež je připojen do lokální sítě. Organizační schéma zveřejňuje na Intranetu HZS JčK. Má přístup do informačního systému HZS pro oblast personální a mzdové práce (VEMA). Na základě vyžádání má přístup do osobních spisů příslušníků. K elektronické komunikaci využívá systém GINIS.

Oddělení PaM (personální a mzdové) - příslušníci a zaměstnanci tohoto oddělení zajišťují personální agendu HZS kraje, zajišťují vzdělávání a odbornou přípravu zaměstnanců HZS kraje ve spolupráci s odbornými pracovišti HZS kraje, zpracovávají mzdovou agendu a agendu sociálního zabezpečení zaměstnanců HZS kraje, zabezpečují realizaci platové politiky. Shromažďují a prověřují podklady pro výplaty náležitostí a sociálních dávek zaměstnancům HZS kraje.

Přichází do styku s osobními daty zaměstnanců, příslušníků a žadatelů o zaměstnání. Mají kdykoliv přístup do osobních spisů příslušníků. Osobní spisy jsou vedeny v papírové formě a uchovávány jsou na tomto oddělení v uzamykatelných kovových skříních. Některá data z činnosti oddělení se zadávají do systému VEMA. Žádosti žadatelů o zaměstnání včetně životopisů a osobních dat, se na tomto oddělení uchovávají v papírové podobě 2 roky. Poté dochází ke skartaci těchto dokumentů a to na skartovacím stroji přímo na oddělení, bez záznamu o tomto úkonu. Žádosti o kurzy a školení příslušníků a zaměstnanců zadávají do informačního systému CEP, který je veřejně přístupný na internetu. Osobní spisy zaměstnanců a příslušníků jsou na tomto oddělení uloženy po celou dobu trvání jejich pracovního poměru. Po jejich odchodu ze zaměstnání a služebního poměru se přesouvají do archivu, kde jsou archivovány po dobu 50 let. Po této době jsou skartovány ve sběrných surovinách za dohledu příslušníka HZS a je o tomto proveden písemný záznam. Na oddělení se rovněž zpracovávají mzdy příslušníků a zaměstnanců, včetně veškerých k tomu potřebných informací (rodinné poměry, půjčky, studia, nemocnost atd.) Tyto údaje jsou zpracovány rovněž za pomocí systému VEMA. Údaje jsou vedeny na mzdových listech, ty jsou stejně jako osobní spisy, uchovávány 50 let v archivu po ukončení pracovního poměru. K elektronické komunikaci je využívají systém GINIS (zasílání nejrůznějších hlášení nadřízeným orgánům). Pro potřebu komunikace s pojišťovnami přistupují zaměstnanci a příslušníci ze svých PC přes internet šifrovaným protokolem pomocí certifikátů na společný portál zdravotních pojišťoven. Vyjímku tvoří všeobecná zdravotní

pojišťovna, která má svůj vlastní a portál České správy sociálního zabezpečení. Výplatní lístky jsou jednotlivým příslušníkům a zaměstnancům zasílány na pracovní email a těm co jej nemají zřízen, což jsou hasiči ve výkonu služby, dostávají výplatní lístek v papírové podobě zalepený v certifikované obálce.

Oddělení organizační - příslušníci a zaměstnanci tohoto oddělení odpovídají za organizaci a koordinaci činností spojených s postavením krajského ředitele. Realizují jeho rozhodnutí včetně příslušných administrativních úkonů, zabezpečují ochranu utajovaných informací a ochranu areálů, zajišťují styk s veřejností a získávání potřebných informací, zabezpečují agendu mezinárodních styků a zabezpečují chod podatelny a spisovny.

Přicházejí do styku s osobními daty příslušníků a zaměstnanců při zpracovávání žádostí na vydání dokladu o bezpečnostní způsobilosti. Osoby, u kterých se provádí bezpečnostní prověrky, jsou určeny platnou systemizací s ohledem na vykonávanou funkci. Z ní vychází i jednotlivé stupně bezpečnostní způsobilosti. Stupeň „Důvěrné“ je určen pro ředitele, náměstky ředitele a pracovníky kanceláře ředitele. Mimo systemizaci pak ještě musí splnit tento bezpečnostní stupeň ředitel OPŘ a KIS a vedoucí OPIS. Stupeň „Vyhrazené“ mají určen ředitelé odborů a vedoucí oddělení, kromě odboru ekonomiky.

Pracovníci organizačního oddělení zabezpečují provoz v „zabezpečené oblasti“. Přístup do tohoto prostoru má jeden příslušník oddělení organizačního (heslo EZS+klíče), jeden příslušník oddělení IS (heslo EZS). Tito dva pracovníci zpracovávají návrhy z oblasti objektové bezpečnosti (ostraha, kamerové systémy, EZS).

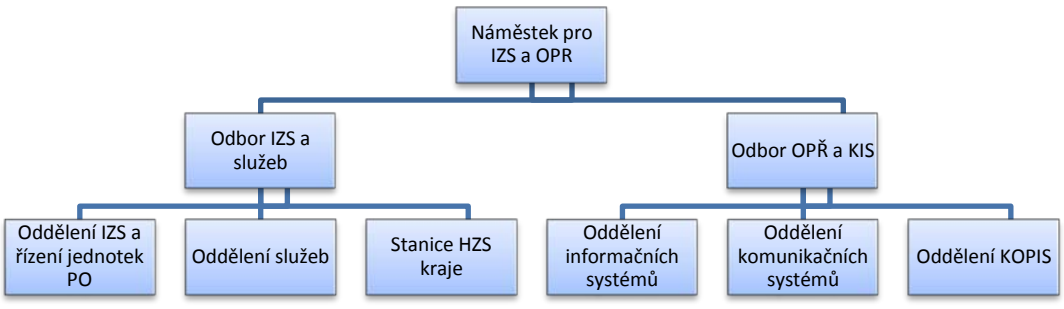
Psychologické pracoviště - příslušníci a zaměstnanci tohoto oddělení realizují posttraumatickou péči příslušníkům HZS ČR, připravují podklady pro personální práci (psychologická vyšetření při přijetí příslušníků).

Přichází do styku s osobními i jinými citlivými údaji o osobách a jejich rodinných příslušnících, které jsou uvedeny v ANAMNESTICKÉM DOTAZNÍKU. Tento dotazník vyplňuje každý uchazeč přicházející na psychologické vyšetření. Dotazník je v papírové podobě uložen na tomto oddělení v uzamykatelné skříni po dobu 5 let. Poté je skartován dle skartačního řádu. Vlastní psychologické testy se provádějí na lokálních PC, které jsou mimo síť HZS. K výsledkům tak mají přístup pouze

příslušníci psychologického oddělení, tj. 2 lidé. Doba uchování testů na těchto PC není řešena žádným předpisem, a proto jsou k dispozici výsledky testů od počátku vzniku tohoto pracoviště, tj. 8 let. Výsledky vyšetření jsou předávány v papírové formě na oddělení PaM. Pracoviště je zaregistrováno na úřadu pro ochranu osobních údajů. Přicházejí do styku s informacemi týkajícími se soukromého a osobního života příslušníků a zaměstnanců, kteří přicházejí na pracoviště, aby řešili psychologické problémy vznikající při výkonu povolání.

Pracoviště právní - příslušníci a zaměstnanci tohoto oddělení zabezpečují právní činnost HZS kraje, vedení agendy interních aktů řízení krajského ředitele, zpracovávají podklady k vydání právních předpisů pro příslušné správní orgány kraje v oblastech, které vymezuje zákon. Dále projednávají přestupky a správní delikty na úseku požární ochrany.

Přichází do styku s osobními daty příslušníků a zaměstnanců pouze v souvislosti s řešením konkrétních právnických případů. Osobní spisy mají k dispozici pouze na základě jednotlivých požadavků. Oprávněnost těchto prostředků není řešena. Přichází rovněž do styku s osobními údaji jiných zúčastněných osob vně organizace na základě řešení právnických případů souvisejících s činností HZS, např. záznamy výslechů svědků. Dokumenty při své práci vytváří na lokálním PC připojeném do lokální sítě, přičemž tyto jsou následně uloženy na file serveru. Pro elektronickou komunikaci s právnickými subjekty a subjekty státní správy využívají GINIS. Pro komunikaci s advokáty vně organizace využívají nešifrovanou email komunikaci.



Obr. č. 32: Organizační struktura – náměstek pro IZS a OPŘ

Zdroj: Vlastní

Náměstek pro IZS a OPŘ - stojí v čele úseku zastřešujícího odbor IZS a služeb a odboru operačního řízení a komunikačních a informačních služeb.

Odbor IZS a služeb - odpovídá za řešení problematiky IZS kraje, koordinaci záchranných prací a spolupráci složek IZS, za usměrňování, koordinaci a kontrolu činnosti jednotek PO, za organizaci a výkon služby v jednotkách HZS kraje. Odbor IZS a služeb řídí ředitel odboru.

Oddělení IZS a řízení jednotek PO - příslušníci a zaměstnanci tohoto oddělení předkládají podklady pro zpracování koncepce požární ochrany kraje, roční zprávy o stavu požární ochrany kraje, podílejí se na přípravě podkladů pro jednání bezpečnostní rady kraje, zpracovávají návrhy pro plošné rozmístění jednotek PO v kraji. V rámci své působnosti vedou přehled jednotek PO, jejich činností, početních stavů a jejich vybavení. Vedou přehledy o ostatních složkách IZS na základě dohod o součinnosti, dohod o plánované pomoci na vyžádání, vedou a využívají stanovenou dokumentaci požární ochrany a IZS. Vyjadřují se k dokumentům, které se svým obsahem dotýkají složek IZS.

Mají přístup do informačního systému ISV Admin, kde získávají osobní data zaměstnanců a příslušníků, osobní data příslušníků jednotek SDH, data členů státní správy a samosprávy a členů havarijních komisí v rozsahu identity, data narození a kontaktů. Mají přístup k datům, která jsou součástí uzavíraných dohod o spolupráci mezi HZS a právnickými subjekty. Tyto jsou zpracovávány na PC, zapojeních do lokální sítě a následně uloženy na file serveru. Získaná data jsou také k dispozici OPIS HZS JčK. Zpracovávají výjimky z pojištění vozidel pro všechny složky IZS v souvislosti s činností IZS. K tomuto účelu mají k dispozici údaje o těchto vozidlech a jejich držitelích. Agenda je zpracovávána elektronicky na PS zapojeném do sítě.

Oddělení služeb - příslušníci a zaměstnanci tohoto oddělení zabezpečují akceschopnost požární techniky a dalších strojních věcných prostředků požární ochrany. Sledují a vyhodnocují nehodovost vozidel HZS kraje a jednotek PO v kraji.

Přicházejí do styku s osobními daty téměř všech příslušníků a zaměstnanců v souvislosti s pravidelnými obnovami profesních řidičských průkazů, svářečských listů, při školení jeřábníků a obsluh vysokozdvižných vozíků. Mají k dispozici podrobné informace o technice a technických prostředcích ve výbavě jednotek HZS. Setkávají se

s osobními daty při odprodejích požární techniky zejména obcím. Při dopravních nehodách, jejichž účastníky jsou příslušníci nebo zaměstnanci HZS mají přístup k příslušnému policejnímu spisu, kde jsou i osobní údaje všech zúčastněných osob. Hlášení o dopravních nehodách provádějí na hlasovou linku Policie ČR. Písemná komunikace probíhá přes spisovnu HZS JčK. Mají přístup do informačního systému IKIS HZS – moduly strojní a technická služba. Vyexportovaná data z tohoto systému zasílají na vyžádání nadřízených orgánů elektronickou poštou. Pro spisovou službu využívají systém GINIS.

Odbor operačního řízení a komunikačních a informačních systémů - odpovídá za plnění úkolů operačního řízení jednotek PO, za výstavbu a provoz informačních a komunikačních sítí, zřízení a zabezpečení systému varování a za krizovou komunikaci. Odbor OPŘ a KIS řídí ředitel odboru.

Operační a informační středisko - příslušníci a zaměstnanci tohoto oddělení zabezpečují výkon služby na krajském operačním a informačním středisku, zabezpečují součinnost operačních středisek jiných složek IZS a zajišťují součinnost složek IZS v operačním řízení, přijímají a vyhodnocují zprávy o požárech a jiných mimořádných událostech. Podílejí se na shromažďování a vyhodnocení statistických údajů o požárech a událostech řešených v rámci požární ochrany a IZS. Spolupracují s krizovými štáby při řešení mimořádných událostí a krizových situací. Provádějí varování a vyrozumění obyvatelstva, přijímají tísňová volání na linkách 150 a 112.

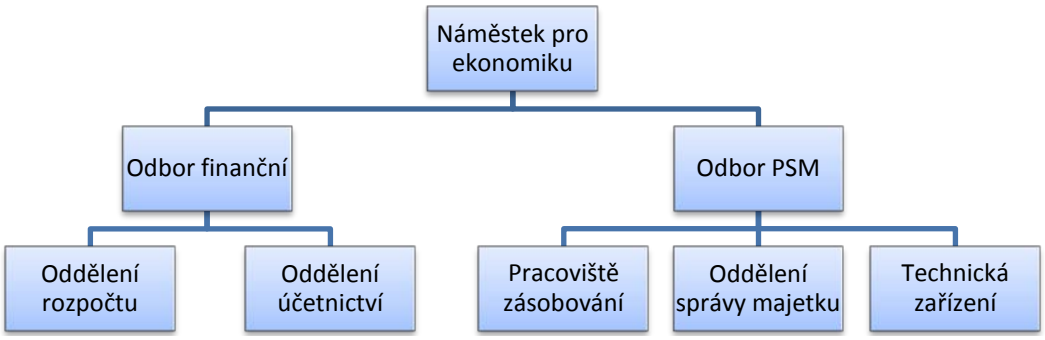
Příslušníci a zaměstnanci OPIS shromažďují a vyhodnocují největší množství dat a informací, zejména informace o všech mimořádných událostech na území kraje, činnosti jednotek IZS, činnosti krizových štábů, shromažďují a uchovávají kontaktní informace na příslušníky a zaměstnance HZS a členy krizových štábů. Dále mají přístup ke kontaktům na členy jednotek SDH obcí, kontaktům fyzických a právnických osob, zařazených do krizových a havarijních plánů kraje, a mnoho dalších citlivých dat. Mají přístup do informačního systému HZS pro oblast OPŘ. Mají přístup k informační podpoře, zejména ke krizovému a havarijnímu plánu kraje, k vnějšímu havarijnímu plánu JETE, ke krizovým a havarijním plánům zájmových objektů. Nemohou však na svých pracovních stanicích kopírovat data a všechny telefony OPIS jsou monitorovány

Oddělení informačních systémů - příslušníci a zaměstnanci tohoto oddělení zajišťují provoz informačních systémů a výpočetní techniky, aktualizaci jejího programového vybavení a používání programového vybavení v souladu s právními předpisy, provozují a vytvářejí informační systémy v oblasti požární ochrany, IZS, ochrany obyvatelstva a krizového řízení, zajišťují dohled a údržbu provozovaných informačních systémů. Zajišťují ochranu dat před jejich zneužitím, jejich archivaci a vnitřní i vnější bezpečnost lokálních sítí.

Vykonávají správu a dohled nad veškerými daty a informačními systémy HZS JčK, správu nad lokálními PC příslušníků a zaměstnanců, přičemž mají přístup k lokálním datům na těchto počítačích. Spravují informační systémy a PC OPIS HZS JčK, počítačové sítě HZS, včetně jejich zabezpečení. Mají přístup do všech informačních systémů HZS. Vedoucí oddělení se podílí na provozu utajovaného pracoviště.

Oddělení komunikačních systémů - příslušníci a zaměstnanci tohoto oddělení zabezpečují provoz v oblasti linkových a rádiových přenosových prostředků, podílejí se na zajišťování provozu počítačové sítě HZS, zabezpečuje rozvoj a provoz koncových prvků jednotného systému varování a vyrozumění, podílí se na zajištění objektové bezpečnosti.

Přichází do styku zejména informacemi týkajícími se telekomunikačního provozu, radiokomunikačních systémů a jednotlivými komunikacemi v nich. Mají přístup k podrobným přehledům o telekomunikačním provozu příslušníků a zaměstnanců HZS. Mají znalosti o topologiích komunikačních, radiových a počítačových sítí. Starají se o systém JSVV, včetně programování jednotlivých komponent. Mají přístup do informačního systému HZS, oblast komunikačních systémů a částečně informačních systémů. Starají se o dodržování Usnesení vlády ČR č. 624/2001 Sb. o užívání počítačových programů.



Obr. č. 33: Organizační struktura – náměstek pro ekonomiku

Zdroj: Vlastní

Náměstek pro ekonomiku - stojí v čele úseku zastřešujícího odbor finanční a odbor provozní a správy majetku.

Odbor finanční - odpovídá za přípravu rozpočtu HZS kraje a za rozpočtové hospodaření podle schváleného rozpočtu. Odbor se vnitřně člení na oddělení rozpočtu a oddělení účetnictví. Odbor finanční řídí ředitel finančního odboru.

Oddělení rozpočtu - příslušníci a zaměstnanci tohoto oddělení řídí a usměrňují hospodaření s rozpočtovými prostředky HZS kraje, řídí čerpání rozpočtu HZS kraje, provádí rozpočtová opatření, zpracovávají analytické zprávy plnění včetně podkladů pro státní závěrečný účet.

Přichází do styku zejména s informacemi týkajícími se rozpočtu organizace, což jsou informace veřejně přístupné na internetu, navíc s povinností podávání informací
na vyžádání dle Zákona č.106/1999 Sb. o svobodném přístupu k informacím. Pracují s informačním systémem VEMA – EKOS.

Oddělení účetnictví - příslušníci a zaměstnanci tohoto oddělení vykonávají funkci účtárny HZS kraje, vedou předepsanou účetní evidenci a zpracovávají předepsané doklady statistického výkaznictví. Provádějí účetní analýzu hospodaření s rozpočtovými prostředky HZS kraje v návaznosti na stanovený rozpočet.

Přicházejí do styku zejména informacemi týkajícími se finančního hospodaření organizace. Informace o hospodaření jsou na základě požadavků ministerstva financí zadávány na portál CSUIS, který je přístupný na webu tohoto ministerstva. Komunikace

s tímto portálem je šifrovaným protokolem. Likvidují a proplácejí faktury za nákup služeb a materiálu související s činností organizace. K zadávání jednotlivých příkazů je využíván portál České národní banky ABO-K, s přístupem pro 3 zaměstnance. Stejným způsobem dochází k zadávání příkazů k proplácení mezd příslušníkům a zaměstnancům. Mají přístup do informačního systému HZS, oblast personální a mzdová, do systému GINIS týkajícího se spisové pošty. Na vyžádání odesílají data ze systému VEMA nadřízenému orgánu - GŘ HZS ČR. Vyřizují agendu spojenou s půjčkami z fondu FKSP. Při této činnosti se setkávají s osobními údaji příslušníků a zaměstnanců, kteří o tyto půjčky žádají.

Odbor PSM (odbor provozní a správy majetku) - odpovídá za hospodaření s majetkem v působnosti HZS kraje. Zajišťuje veškerou majetkoprávní agendu související s předepsanými výstupy na resortní program a správu majetku. V jeho působnosti jsou také sklady materiálu a humanitární pomoci a rekreační objekty. Odbor se dělí na oddělení zásobování a oddělení správy majetku. Odbor provozní a správy majetku řídí ředitel odboru PSM.

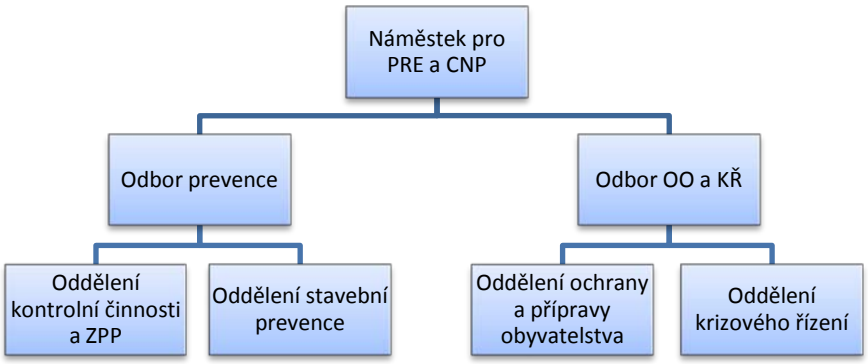
Pracoviště zásobování - příslušníci a zaměstnanci tohoto oddělení na základě podkladů odborných pracovišť zpracovávají plány materiálního a technického zabezpečení, pořizují movitý majetek, popřípadě převody práva hospodaření, zabezpečují stravování příslušníků HZS kraje u zásahu, zabezpečují plánování a nákup výstrojních součástek a ochranných pomůcek pro příslušníky HZS kraje, zabezpečují evidenci a účtování majetku HZS kraje, zabezpečují obměnu zásob věcných prostředků ve skladech HZS kraje.

Přichází do styku zejména informacemi týkajícími se movitého majetku a skladových zásob tohoto majetku. Mají přístup do informačního systému HZS – oblast zásobování.

Oddělení správy majetku - příslušníci a zaměstnanci tohoto oddělení zabezpečují evidenci, účtování a ochranu majetku. Realizují nové investiční a neinvestiční nákupy, od plánování, přes výběr podle zákona o veřejných zakázkách, zabezpečení finančních prostředků až po zařazení a evidenci nakoupeného majetku. Podle zákona o majetku vyřazují přebytečný a neupotřebitelný majetek HZS JčK. Starají se o movitý i nemovitý

majetek v kraji, o správu a ochranu budov. Řeší otázky ochrany životního prostředí, bezpečnosti práce, otázky vodohospodářské a energetické.

Přicházejí do styku zejména s informacemi o majetku HZS, o výběrových řízeních (zadávání, výběr, vyhodnocení) na nákup techniky a materiálu. S právními akty uzavíranými na nákupy, nájmy, výpůjčky (smlouvy). Informacemi o prodeji nepotřebného movitého a nemovitého majetku z majetku HZS (nabídková řízení a následný výběr zájemce). Mají přístup do informačního systému HZS – oblast VEMA. Pracují se SW KRIZKOM, KIS KAN, Isprofin SMWS.



Obr.č. 34: Organizační struktura – náměstek pro PRE a CNP

Zdroj: Vlastní

Náměstek pro PRE a CNP (prevence a civilní nouzové plánování) - stojí v čele úseku, zastřešujícího odbor prevence a odbor ochrany obyvatelstva a krizového řízení.

Odbor prevence - odpovídá za zabezpečení výkonu státní správy v oblasti požární ochrany, podílí se na odborné přípravě hasičů, na preventivně výchovné činnosti a organizuje v rámci své působnosti porady a metodická zaměstnání. Zabezpečuje kontrolní činnost na úseku požární ochrany, stavební prevenci a zjišťování příčin vzniku požárů. Koordinuje zabezpečování požární ochrany v kraji spolu s ostatními orgány veřejné správy. Odbor se vnitřně dělí na oddělení kontrolní činnosti a ZPP (zjišťování příčin požáru) a oddělení stavební prevence. Odbor prevence řídí ředitel odboru prevence.

Oddělení kontrolní činnosti a ZPP (zjišťování příčin požáru) - příslušníci a zaměstnanci tohoto oddělení vykonávají státní požární dozor formou kontroly dodržování povinností stanovených předpisy o požární ochraně. Vykonávají státní správu na úseku prevence závažných havárií. Schvalují posouzení požárního nebezpečí činností s vysokým požárním nebezpečím, provádějí zjišťování příčin vzniku požárů a okolností mající vliv na šíření požáru, zpracovávají předepsanou dokumentaci v oblasti ZPP.

Při provádění kontrolní činnosti uložené jim Zákonem č.133/1985 Sb. o požární ochraně ve znění pozdějších předpisů a Zákonem č. 238/2000 Sb. o HZS mají právo vstupu do kontrolovaných objektů. Pořizují kopie a fotodokumentace z dokumentace kontrolovaných subjektů, které si pro svou činnost ukládají na server HZS, do vyhrazené oblasti s právem přístupu příslušníkům a zaměstnancům oddělení. Zápisy z kontrol včetně veškeré dokumentace, jakožto i dokumentace o posouzení požárního nebezpečí, jsou uloženy v plechových uzamykatelných skříních na oddělení a v archivu HZS. Skartační znak pro tyto dokumentace se přiřazuje V10. Na úseku vyšetřování příčin požáru se setkávají s osobními údaji vyšetřovaných osob a právnických subjektů. Mají právo vstupu do objektů. Seznamují se detailně s postiženými objekty a jejich technologiemi a zpracovávají o tom spisy o požáru a ty archivují v archivu HZS. Pořizují fotodokumentaci z míst vyšetřování požáru, kterou ukládají na server HZS do oblasti, ke které mají kromě příslušníků a zaměstnanců odboru přístup i nadřízení pracovníci a tisková mluvčí HZS.

Oddělení stavební prevence - příslušníci a zaměstnanci tohoto oddělení posuzují podklady pro vydání územního rozhodnutí, projektovou dokumentaci stavby ke stavebnímu řízení. Ověřují, zda byly dodrženy podmínky požární bezpečnosti staveb vyplývající z posouzených podkladů a dokumentace. Vedou evidenci staveb CO a staveb dotčených požadavky CO, jsou dotčeným orgánem státní správy na úseku požární ochrany, zpracovávají podklady pro koncepci požární ochrany a roční zprávy o stavu požární ochrany v kraji. Při posuzování staveb a jejich požárního nebezpečí a následně při kolaudačních řízeních přicházejí do styku zejména s informacemi týkajícími se projektové dokumentace, včetně instalovaných technologií. Z těchto dokumentů mají

právo pořizování kopií. Součástí těchto schvalovacích řízení jsou osobní data účastníků řízení. Ke své práci využívají informační systém „prevence“ od společnosti PC Help.

Odbor OO a KŘ (ochrany obyvatelstva a krizového řízení) - odpovídá za řešení problematiky ochrany obyvatelstva včetně varování, evakuace, nouzového přežití a výchovy. Odpovídají za zpracování havarijních plánů a krizových plánů kraje a obcí s rozšířenou působností. Odbor se vnitřně dělí na oddělení ochrany a přípravy obyvatelstva a oddělení krizového řízení. Odbor prevence řídí ředitel odboru OO a KŘ.

Oddělení ochrany a přípravy obyvatelstva - příslušníci a zaměstnanci tohoto oddělení zabezpečují zpracování úkolů ochrany obyvatelstva do havarijních plánů a krizových plánů kraje, obcí s rozšířenou působností a do opatření při přechodu z mírového na válečný stav. Předávají Ministerstvu vnitra, hejtmanovi a starostovi obce s rozšířenou působností na jejich žádost údaje nezbytné k přípravě na krizové situace, vyžadují, shromažďují a evidují údaje nezbytné pro zpracování krizového plánu kraje pro přípravu a řešení krizových situací a koordinují pro účely krizového řízení sběr dat od územních správních úřadů.

Přicházejí do styku zejména informacemi z registrů právnických a fyzických subjektů, z registru obyvatel, informacemi týkajících se bezpečnostních složek a složek systému IZS. Pracují s informačním systémem ARGIS a KRIZKOM, kam zadávají informace o právnických subjektech a krizových situacích.

Oddělení krizového řízení - příslušníci a zaměstnanci tohoto oddělení zabezpečují zpracování krizového plánu kraje a krizového plánu obce s rozšířenou působností, zpracovávají havarijní plány kraje a vnější havarijní plány. Vyžadují, shromažďují a evidují údaje nezbytné pro zpracování krizových plánů, pro přípravu a řešení krizových situací v rozsahu § 15 odst. 3 krizového zákona.

Při zpracovávání analýzy rizik přicházejí do styku zejména s osobními daty právnických subjektů a s údaji z oblasti obchodního práva. Tyto informace mají k dispozici v elektronické formě prostřednictvím elektronické pošty. Při zpracovávání havarijního plánu kraje mají k dispozici údaje dotčených právnických subjektů, včetně plánů fyzické ostrahy objektů. Tyto informace jsou k dispozici na CD médiu. To se ukládá na oddělení, přičemž následná skartace není dosud řešena. Havarijní plán kraje ukládají na server HZS a mají k němu přístup příslušníci a zaměstnanci odboru a

oddělení OPIS. Složkám IZS je k dispozici na CD. Touto formou je rovněž předáván na Krajský úřad, který ho má k dispozici na svém intranetu. Staré havarijní plány jsou skartovány ve sběrných surovinách o čemž je pořizován záznam.

Územní odbory HZS JčK - v členění HZS Jihočeského kraje je dále 6 územních odborů. Příslušníci a zaměstnanci těchto ÚO zpravidla nemají přístup k datům a informacím, které se netýkají činnosti právě jejich ÚO a proto je toto riziko pro data HZS JčK z hlediska mé práce zanedbatelné a nebudu se jím dále zabývat.

1.4 Zabezpečení legislativou

Legislativu, která se bezprostředně týká tématu mé diplomové práce, bych mohl rozdělit do několika oblastí. Tou první jsou platné zákony, vyhlášky a nařízení vlády řešící především utajované skutečnosti, ochranu osobních údajů a v neposlední řadě ochranu duševního vlastnictví a legálnost používaného SW. Druhou oblastí jsou pak interní předpisy Hasičského záchranného sboru České republiky, které rozpracovávají platnost obecně právních předpisů do podmínek Hasičského záchranného sboru ČR a konečně další rovinou jsou obecné normativy a nepsané zákony, kterými je třeba se řídit při činnostech, při kterých se pracuje s daty a informacemi.

Zákony a nařízení vlády

- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti,
- Zákon č. 101/2000 Sb., o ochraně osobních údajů,
- Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon). Z tohoto zákona zejména § 2 odst. 2, který zní: „Za dílo se považuje též počítačový program, je-li původní v tom smyslu, že je autorovým vlastním duševním výtvorem. Za dílo souborné se považuje databáze, která je způsobem výběru nebo uspořádáním obsahu autorovým vlastním duševním výtvorem.“
- Zákon č. 361/2003 Sb., o služebním poměru příslušníků bezpečnostních sborů,
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě,

- Usnesení vlády ČR č. 624/2004 Sb., pravidla, zásady a způsob zabezpečování kontroly užívání počítačových programů uvedená v příloze tohoto usnesení (dále jen "Pravidla") jako závazný dokument pro orgány státní správy a jimi řízené organizace. Tento dokument řeší používání SW produktů od jejich pořizování, vedení si evidence a způsoby vedení dokumentace o SW, převody práv k užívání SW, kontroly přes inventarizace až po likvidaci SW po ukončení platnosti licencí.
- Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění nařízení vlády č. 240/2008 Sb.

Interní předpisy HZS

- SIAŘ GŘ č. 34/2002 Generálního ředitele Hasičského záchranného sboru České republiky ze dne 14. října 2010, kterým se stanoví pravidla elektronické pošty v rámci HZS ČR,
- SIAŘ GŘ č. 40/2009 Generálního ředitele Hasičského záchranného sboru České republiky ze dne 1. září 2009, o personální evidenci v Hasičském záchranném sboru České republiky a zpracovávání osobních údajů, které s ní souvisejí,
- SIAŘ č. 50/2003 Generálního ředitele Hasičského záchranného sboru ČR a náměstka ministra vnitra ze dne 20. listopadu 2003, kterým se stanoví osnova a obsah bezpečnostní politiky subjektů pro datové sítě Hasičského záchranného sboru České republiky,
- SIAŘ č. 75/2008 Ředitele Hasičského záchranného sboru Jihočeského kraje ze dne 30. října 2008, kterým se jmenují vedoucí objektů a jejich pomocníků Hasičského záchranného sboru Jihočeského kraje,
- SIAŘ č.67/2009 Ředitele Hasičského záchranného sboru Jihočeského kraje ze dne 21. prosince 2009, kterým se jmenuje ředitel areálů HZS JčK a zařazují objekty do skupin.
- SIAŘ č. 102/2004 Ředitele Hasičského záchranného sboru Jihočeského kraje ze dne 27. prosince 2004, kterým se stanoví pravidla Bezpečnostní politiky v oblasti informačních technologií Hasičského záchranného sboru Jihočeského kraje.

1.4.1 Utajované informace

Institut utajovaných skutečností, častěji nazývaný státní tajemství se v novodobé historii českého státu poprvé objevil v zákoně č. 50/1923 Sb., na ochranu republiky. Úprava v tomto zákoně, byť zdůvodňovaná existencí úkladů o republiku, představovala výrazný zásah do demokratických práv občanů nové republiky, zejména co se týkalo svobody projevu a ve znění novelizací z 30. let svobody tisku.

Zákon vedle toho postihoval i republice nebezpečné aktivity - vojenskou zradu, atentáty i ohrožení státního tajemství, nicméně ne vždy odpovídajícím způsobem.

Právní úprava pamatovala i na správně trestní ochranu tzv. úřední tajemství. To však byl odlišný institut, který naplňoval z Rakousko-Uherska převzatý princip diskrétnosti veřejné správy a utajoval tak podstatnou část administrativní činnosti. Z materiálního hlediska tyto skutečnosti obecně postrádaly znak újmy pro důležité zájmy státu, zejména vnitřní bezpečnost, svrchovanost a územní celistvost. Nelze je tedy považovat za totožný institut se státním tajemstvím či utajovanými skutečnostmi podle nové terminologie. Zákon o ochraně úředního tajemství obsahoval i způsob jeho vymezení. Stačilo k tomu, že jednání či informace byly prohlášeny za důvěrné rozhodnutí samotného úřadu podle § 5 odst. 1. výše uvedeného zákona. /9/

V současné době řeší problematiku utajovaných skutečností Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. V §4 tohoto zákona, jsou definovány čtyři stupně utajení:

a) Přísně tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům České republiky,

b) Tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky,

c) Důvěrné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům České republiky,

d) Vyhrazené, jestliže její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky.

V § 5 jsou vyjmenovány druhy zajištění ochrany utajovaných informací:

a) personální bezpečností, kterou tvoří výběr fyzických osob, které mají mít přístup k utajovaným informacím, ověřování podmínek pro jejich přístup k utajovaným informacím, jejich výchova a ochrana,

b) průmyslovou bezpečností, kterou tvoří systém opatření k zjišťování a ověřování podmínek pro přístup podnikatele k utajovaným informacím a k zajištění nakládání s utajovanou informací u podnikatele v souladu s tímto zákonem,

c) administrativní bezpečností, kterou tvoří systém opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými informacemi,

d) fyzickou bezpečností, kterou tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat,

e) bezpečností informačních nebo komunikačních systémů, kterou tvoří systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost utajovaných informací, s nimiž tyto systémy nakládají, a odpovědnost správy a uživatele za jejich činnost v informačním nebo komunikačním systému,

f) kryptografickou ochranou, kterou tvoří systém opatření na ochranu utajovaných informací použitím kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání utajovaných informací. /20/

S utajovanými informacemi a daty podle zákona č. 412/2005 Sb., přichází do styku pouze ředitel a 2 prověřené osoby, o kterých jsem se již zmiňoval v kapitole 1.4. , osoby z organizačního oddělení a oddělení informačních systémů.

Ochrana osobních dat

Zákon č. 101/2000 Sb. řeší ochranu osobních údajů. V Hlavě I. tohoto zákona došlo k jasnému vydefinování, co jsou osobní a citlivé údaje a co se naopak za ně nepovažuje. A dále pojmenování jednotlivých operací při manipulaci s informacemi.

- *osobní údaj je* jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více

prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.

- *citlivý údaj je* osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a jakýkoliv biometrický nebo genetický údaj subjektu údajů.
- *anonymní údaj je* takový údaj, který buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů.

Subjektem údajů je fyzická osoba, k níž se osobní údaje vztahují, z*pracováním osobních údajů* jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace. *Shromažďováním osobních údajů* je systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování, *uchovávání osobních údajů* znamená udržování údajů v takové podobě, která je umožňuje dále zpracovávat, *blokováním osobních údajů* je vytvoření takového stavu, při kterém je osobní údaj určitou dobu nepřístupný a nelze jej jinak zpracovávat, *likvidací osobních údajů* se rozumí fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování, *správcem* je každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak. *Zpracovatelem* je každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona, *zveřejněným osobním údajem* osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu, *evidencí nebo datovým souborem osobních údajů* (dále datový soubor) jakýkoliv soubor osobních údajů uspořádaný nebo zpřístupnitelný podle společných nebo zvláštních kritérií, *souhlasem subjektu údajů* svobodný a vědomý projev vůle

subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů, *příjemcem* každý subjekt, kterému jsou osobní údaje zpřístupněny; za příjemce se nepovažuje subjekt, který zpracovává osobní údaje podle § 3 odst. 6 písm. g) uvedeného zákona. /28/

2 CÍLE PRÁCE a HYPOTÉZY

Cílem mé práce je zjistit, zda je s daty u HZS Jihočeského kraje nakládáno v souladu s platnou legislativou a zda jsou dostatečně zabezpečeny a chráněny proti zneužití a ztrátě.

Pro svou práci jsem si stanovil dvě hypotézy:

1. Práce s daty a jejich zabezpečení je u HZS JčK v souladu s platnou legislativou
2. Data jsou dostatečně chráněna proti ztrátě a zneužití.

3 METODIKA

3.1 Metodika získávání informací

Pro získání co největšího množství relevantních údajů pro svou práci jsem si zvolil následující postup. Prostudoval jsem organizační strukturu HZS JčK a sestavil dílčí organizační schémata do úrovní jednotlivých oddělení a pracovišť v kapitole *Organizační struktura HZS JčK z pohledu práce s daty a informacemi*. Na základě náplně práce a úkolů, které jednotlivá oddělení vykonávají, jsem prostudoval platnou legislativu a vnitřní předpisy organizace, jimiž se mají tyto činnosti řídit. Abych mohl verifikovat popřípadě falzifikovat hypotézy, stanovené při zadání práce, potřeboval jsem získat ještě informace o skutečném stavu práce s daty v celé organizaci. Z časových důvodů jsem nemohl oslovit všechny příslušníky a zaměstnance, proto jsem se pro jejich získání rozhodl oslovit vedoucí příslušníky a zaměstnance. Z organizační struktury je patrné, že právě tito představují ten článek podniku, u kterého se setkávají informace jak od nadřízených tak od podřízených.

Záměrně jsem nezvolil dotazníkovou metodu, neboť jsem vycházel z předpokladu, že na jednotlivých odděleních a pracovištích pracují příslušníci a zaměstnanci profesně převážně jiného zaměření než je specializace na data a informace. Raději jsem proto zvolil formu kvalitativního výzkumu. Ten jsem rozdělil na dvě části.

V první části jsem formou moderovaného pohovoru zjišťoval objem dat a informací s jakými se na daném pracovišti či oddělení pracuje a jak je zabezpečována ochrana těchto dat a informací. Dále jsem zjišťoval informace, jak je zabezpečen přístup k dokumentům a jak jsou zabezpečeny pracovní postupy, tzn. zabezpečení počítačů, používání hesel a jak je řešen institut zastupování jednotlivých pracovníků na jednotlivých pracovištích v době nepřítomnosti. Dle těchto získaných informací jsem sestavil devět oblastí, které by charakterizovaly možná rizika pro data a informace.

Oblasti možných rizik:

- Ztráta a znehodnocení dat
- Zneužití dat kopírováním
- Zneužití přístupu k datům z lokální sítě
- Zneužití dat kamerového systému
- Únik dat utajovaného charakteru

- Zneužití přístupu do cizího PC
- Zneužití přístupu k datům z internetu
- Zneužití objektové bezpečnosti
- Odchod specializovaného odborníka.

Ve druhé části rozhovoru jsem vedoucí pracovníky stručně seznámil s první částí mé práce, aby získali možný přehled o nebezpečích, kterým čelí data a informace, se kterými pracují příslušníci a zaměstnanci na jejich odděleních nebo pracovištích.

Poté jsem jim předložil dvě hodnotící tabulky, které jsem si připravil, a požádal jsem dotazované pracovníky, aby každé z devíti oblastí přiřadili jednu hodnotu pro možný dopad rizika na činnost organizace. Tento dopad by odpovídal tomu, jak jej vnímají z pohledu, že by tato situace mohla vzniknout na jejich oddělení. Otázkou také bylo, jaký by měla vliv na činnost organizace. Druhá hodnota měla vyjádřit četnost rizika, neboli jak dotazovaní pracovníci vnímají pravděpodobnost toho, že daný dopad rizika může nastat.

Abych mohl verifikovat nebo falzifikovat hypotézu č.1 „Práce s daty a jejich zabezpečení je u HZS JčK v souladu s platnou legislativou“, musel jsem porovnat skutečnosti zjištěné při mém výzkumu s legislativou popsanou v kapitole 1.4. Zabezpečení legislativou. Uvedenými druhy legislativy se řídí činnost příslušníků a zaměstnanců na jednotlivých pracovištích HZS Jihočeského kraje a mým úkolem bylo zjistit případné rozdíly mezi skutečností a zákony. Využíval jsem též právní rozbory dostupné na internetu.

3.2 Zdroje informací

Jako zdroj informací jsem používal tištěné i elektronické dokumenty. Veškeré zdroje jsou uvedeny v seznamu použité literatury. Byla použita odborná literatura, manuály k jednotlivým zařízením, technologiím a systémům, zákony a vyhlášky, které upravují související legislativu. Dále zdrojem mých informací byly již zmiňované osobní konzultace a rozhovory. Významným zdrojem informací, zejména pro oblast informačních technologií a sítí byl internet. Tam jsem čerpal největší množství informací pro svou práci. Bylo to hlavně z důvodu toho, že dnešní moderní internetové prohlížeče nabízí jak textové vyhledávání, tak vyhledávání dle zadaných kritérií či

témat. Nezanedbatelnou výhodou takové metody jsou online webové překladače, čímž padají bariéry nejen jazykové, ale i geografické, neboť se tímto způsobem dostaneme k materiálům, které bychom v domácích zeměpisných šířkách hledali marně nebo bychom o jejich existenci neměli ani tušení. Tato metoda mi pomohla hlavně při sestavování historického vývoje technologií, když jsem čerpal informace z amerických webů například webu Computer History Museum California.

Na internetu jsem též vyhledával platnou legislativu včetně právních rozborů a výkladů. Místně závazné předpisy organizace jsem dostal k dispozici prostřednictvím sítě Intranet HZS ČR. Zde jsou k dispozici i předpisy nadřízeného orgánu GŘ HZS ČR.

Další náměty jsem čerpal při návštěvách knihovny Jihočeské university v Českých Budějovicích. Zde jsem se spíše seznamoval s formální podobou diplomových prací a jejich zpracováním. S pracemi obdobného tématu nebo zaměření jsem se zde nesetkal.

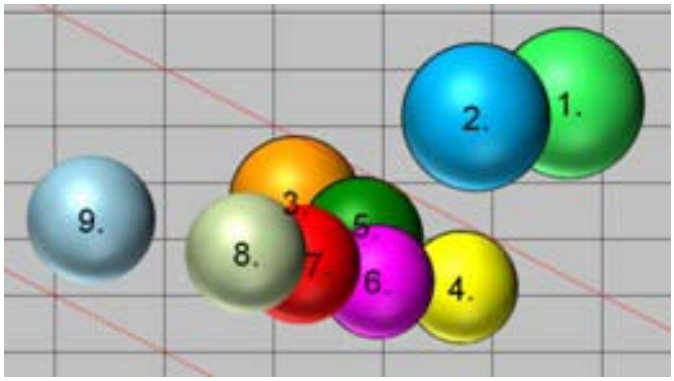
3.3 Členění práce

V první části jsem seznámil čitatele se základními pojmy, s daty a informacemi, se kterými se bude setkávat v celé práci. Mimo jiné krátce mapuji historii jednotlivých technologií, které se využívají při práci s daty a s informacemi. Popisuji také ohrožení technologií. Zaměřil jsem se také na implementaci těchto technologií u Hasičského záchranného sboru Jihočeského kraje. V úvodní části také představuji organizační strukturu HZS JčK, včetně popisu práce s daty a s informacemi na jednotlivých odděleních, které jsem zjistil kvalitativním výzkumem. Po vyhodnocení zjištěných dat a doplnění do vytvořené mapy rizik, popisuji ve druhé části práce způsob, jakým byla tato mapa vytvořena. V kapitole Výsledky mapuji výsledek mé práce, tzn. zjištěné nedostatky a navrhuji opatření, která jsou vhodná pro bezpečnější práci s daty a informacemi.

4 VÝSLEDKY

Provedeným průzkumem a následnou analýzou byly určeny oblasti, které z pohledu práce s daty nejvíce ohrožují činnost organizace. Pořadí tohoto rizika je následující:

1. Ztráta a znehodnocení dat
2. Zneužití dat kopírováním
3. Zneužití přístupu do cizího PC
4. Zneužití dat kamerového systému
5. Zneužití objektové bezpečnosti
6. Odchod specializovaného odborníka
7. Zneužití přístupu k datům z lokální sítě
8. Zneužití přístupu k datům z internetu
9. Únik dat utajovaného charakteru



Obr. č. 35: Mapa rizik – výsledná
Zdroj: Vlastní

Již v průběhu zpracovávání své práce jsem narazil na některé odchylky od bezpečnostních standardů týkajících se práce a nakládání s daty a informacemi. Jelikož jsem pravidelně práci konzultoval s vedoucím práce, zároveň jsem o postupu informoval ředitele organizace, ten se rozhodl některé výsledky řešit bezodkladně.

Návrhy, které byly využity před dokončením mé diplomové práce a které vzešly z mého průzkumu

1. Dát do souladu s platnou legislativou používání kamerového systému. Bylo nutné provést registraci k provozování kamerového systému u Úřadu

pro ochranu osobních údajů. Jelikož bylo potřeba provést tuto registraci neprodleně, aby nedošlo k porušování Zákona č. 101/2000 Sb. o ochraně osobních údajů.

2. Jelikož na některých odděleních některé důležité dokumenty v papírové podobě byly uchovávány v dřevěných skříních bez certifikátů pro ukládání dokumentů, bylo rozhodnuto o nákupu certifikovaných uzamykatelných skříní pro uskladnění osobních spisů. Jednalo se o oddělení personální a mzdové, dále oddělení kontrolní činnosti a stavební prevence.

Návrhy, které nebyly do současné doby realizovány a vyplývají z mého šetření

1. Pro zvýšení bezpečnosti elektronických dat a tím i snížení rizika jejich ztráty jsem navrhl několik opatření pro zvýšení spolehlivosti zařízení a jejich ukládání. S ohledem na finanční náročnost těchto řešení jejich realizace bude probíhat při pravidelné generační obměně zařízení. Pro nově nakupované servery na ukládání dat požadovat do technologické specifikace náhradu diskového pole RAID 5 diskovým polem s vyšší bezpečností RAID 6 a tyto osadit pevnými disky s URE 10 ^ 16.
2. Pro zvýšení spolehlivosti zálohování zavézt pravidelnou verifikaci uložených dat.
3. Pro snížení rizika úniku dat kopírováním jsem navrhl komplex opatření, jež budou zřejmě přijímána postupně v delším časovém horizontu. Jedná se o citlivou oblast a tato opatření dle vášnivých diskuzí, které jsem měl možnost studovat na internetu, se rozhodně nesetkává s vroucím přijetím zaměstnanců. Jedná se zejména o instalaci kamer na pracovištích a zákazy používání soukromých fotoaparátů a mobilních telefonů.

   Nicméně vzhledem k tomu, jak se na jedné straně zvětšuje množství nejrůznějších dat a na straně druhé exponenciální řadou roste zdokonalování technických parametrů mobilních telefonů, budou tato opatření k eliminaci vysoké hrozby rizik zneužití dat nezbytná. O tomto trendu svědčí množící se dotazy zaměstnanců v internetových právních poradnách. /26/

4. Pro adresný a zabezpečený přístup ke kopírovacím zařízením a pracovním stanicím (počítačům), jsem navrhl instalaci individuálních čteček čipových karet, které již vlastní každý příslušník a zaměstnanec organizace. Investice do těchto čteček je 800,- Kč až 900,- Kč na jedno zařízení.
5. Snadnou cestou jak zkopírovat jakákoli data vně organizaci se ukázalo využití cesty elektronické pošty. Jelikož elektronická pošta je jedním z elektronických médií, které se oficiálně využívá pro komunikaci s externími subjekty nelze toto nebezpečí eliminovat zákazy. Rovněž nelze zamezit přístupu na internet všem příslušníkům a zaměstnancům, jelikož jej využívají pro svou práci. Zde jsem navrhl využít některého nástroje pro monitorování přístupu počítačů na web, s možností filtrování například webových stránek, z kterých se dá odesílat elektronická pošta. Investice do plošného zavedení tohoto systému je nákladná záležitost a tak bude zřejmě probíhat rovněž postupně v delším časovém horizontu a to s ohledem na reálné potřeby nutné ochrany dat a informací. Zde bych snad jen zmínil nezanedbatelný přínos tohoto řešení, jehož přínos u některých firem převyšuje otázku bezpečnosti a to je zvýšení produktivity práce úředníků, jejichž internetová aktivita je monitorována.

Návrhy administrativní

V neposlední řadě ze zjištěných skutečností vyplývá potřeba novelizovat Sbírku interních aktů řízení krajského ředitele HZS JčK č. 102/2004 Bezpečnostní politika v oblasti informačních technologií HZS JčK, kterou se stanoví pravidla Bezpečnostní politiky v oblasti informačních technologií Hasičského záchranného sboru Jihočeského kraje.

Vzhledem k rychlému vývoji v oblasti informačních technologií citovaná Sbírka již v mnoha oblastech již neodpovídá současnosti a skutečná zabezpečení v některých oblastech informačních technologií HZS JčK, již předstihla opatření požadovaná v tomto dokumentu. Jelikož v době vzniku této sbírky nebyly naopak známy nové možné hrozby pro snížení míry rizik, bylo by třeba některá nová opatření realizovat.

Mimo jiné i toto bylo uloženo v textu výše uvedené Sbírky. „Bezpečnostní politika se mění v závislosti na vývoji bezpečnostních rizik a musí být průběžně aktualizována.“

Navržená administrativní opatření se z toho důvodu doporučuje zapracovat do platné legislativy HZS Jihočeského kraje.

5 DISKUSE

5.1 Zhotovení mapy rizik

5.1.1 Tabulka rizikových oblastí

Pro získání podkladů a výchozích parametrů k tomu, aby bylo možné navrhnout případná opatření ke snížení rizik při práci s daty u Hasičského záchranného sboru Jihočeského kraje jsem stanovil několik oblastí, dle charakteru možného zneužití dat a informací a sestavil jsem tabulku rizikových oblastí práce s daty.

Tab. č. 1: Rizikové oblasti práce s daty

Pořadí	Riziková oblast práce s daty	Dopad rizika	Četnost rizika
1.	Ztráta a znehodnocení dat	7,4	6,7
2.	Zneužití dat kopírováním	7,2	5,9
3.	Zneužití přístupu do cizího PC	5,7	4,2
4.	Zneužití dat kamerového systému	4,1	5,7
5.	Zneužití objektové bezpečnosti	5,0	4,8
6.	Odchod specializovaného odborníka	4,3	5,0
7.	Zneužití přístupu k datům z lokální sítě	4,6	4,3
8.	Zneužití přístupu k datům z internetu	4,8	3,8
9.	Únik dat utajovaného charakteru	5,3	2,3

Zdroj: Vlastní

5.1.2 Tabulky stupně dopadu a četnosti rizika

Při pohovorech s vedoucími příslušníky a zaměstnanci na jednotlivých odděleních jsem zjišťoval s jakou formou dat a informacemi pracují, jaký je počet dat se kterými přichází do styku a jak by jejich případná ztráta či zneužití ovlivnilo chod organizace. Rovněž jsem zjišťoval jaká je možnost, že by se k těmto datům a informacím mohl dostat někdo nepovolaný, ať už překonáním některého prvku objektového zabezpečení nebo jinou formou, např. přístupem po počítačové síti. Jelikož práce s daty a informacemi je na jednotlivých odděleních diametrálně odlišná, sestavil jsem ještě dvě pomocné tabulky č. 2 a č. 3, kde jsem přesně definoval stupně dopadu rizika a četnosti rizika. Tyto tabulky byly vodítkem jednotlivým funkcionářům k přesnějším odhadům a stanovením hodnot k jednotlivým rizikovým oblastem.

Tab. č. 2: Stupnice hodnot dopadu rizika

Dopad rizika = význam vlivu (významnost)		
Stupeň	**Popis**	**Následky**
10	Katastrofální	Zastavení chodu organizace jako celku, obrovské finanční ztráty
9	Rozsáhlý	Ohrožení chodu organizace, neplnění zákonných povinností
8	Velký	Výpadek chodu některé rozhodující činnosti, velké finanční ztráty
7	Závažný	Ohrožení plnění zákonných povinností, finanční ztráty
6	Značný	Poruchy mají dopad na veřejnost, finanční ztráty
5	Střední	Periodicky se opakující výpadky v činnostech, riziko finančních ztrát, velké množství pochybení musí řešit soudy a nadřízené orgány
4	Okrajový	Poruchy mají dopad na veřejnost bez finančních ztrát
3	Malý	Občasné výpadky v činnostech, nutné zásahy do režimu organizace, poruchy narušující vnitřní chod
2	Nepatrný	Výpadky v činnostech nemající vliv na chod organizace, nápravná opatření vyžadují spolupráci několika subjektů
1	Zanedbatelný	Výpadky v činnostech nemající vliv na chod organizace, běžná nápravná opatření

Zdroj: Vlastní

Tab. č. 3: Stupnice hodnot četnosti rizika

Četnost rizika = pravděpodobnost výskytu		
Stupeň	**Popis**	**Příklad a procentní vyjádření**
10	Téměř jistá	Vyskytuje se téměř vždy (91%-100%)
9	Velmi pravděpodobná	Vyskytuje se často (81%-90%)
8	Pravděpodobná	Vyskytuje se v rozsahu 3/4 (71%-80%)
7	Téměř pravděpodobná	Vyskytuje se (61%-70%)
6	Možná	Vyskytuje se ve větší části (51%-60%)
5	Téměř možná	Vyskytuje se občas (41%-50%)
4	Řídká	Vyskytuje se občas (31%-40%)
3	Neobyčejně řídká	Vyskytuje se maximálně v rozsahu 1/3 (21%-30%)
2	Nepatrná	Vyskytuje se za výjimečných okolností (11%-20%)
1	Zanedbatelná	Vyskytuje se v zanedbatelném rozsahu (0%-10%)

Zdroj: Vlastní

5.1.3 Tabulka výsledných hodnot

Na základě takto získaných informací jsem sestavil hodnotový žebříček dopadu rizika dle stanovené škály vlivu na činnost organizace. Druhým kritériem bylo posouzení četnosti těchto rizik, neboli předpokládané pravděpodobnosti, že by to které riziko mohlo nastat. Zatím co při dotazech na možný stupeň dopadu daného rizika byla tendence některých vedoucích funkcionářů o stanovení spíše vyššího stupně, tedy zvýšení významu svého oddělení na chod organizace, u druhého parametru to bylo právě naopak, tedy snížení stupně pravděpodobnosti četnosti rizika. Proto jsem následně provedl drobnou korekci, hodnot porovnáním práce s daty a informacemi napříč všemi odděleními. Z těchto hodnot jsem sestavil přehlednou tabulku (č.4 – Výsledné hodnoty rizikových oblastí), s hodnotami jednotlivých rizik a vypočítal jejich průměry. Ty jsem použil při sestavení mapy rizik.

Tab. č. 4: Výsledné hodnoty rizikových oblastí

	Oddělení	1		2		3		4		5		6		7		8		9	
		Dopad	Četnost	Dopad	Četnost	Dopad	Četnost	Dopad	Četnost	Dopad	Četnost	Dopad	Četnost	Dopad	Četnost	Dopad	Četnost	Dopad	Četnost
1	krajský ředitel	7	5	9	3	4	1	3	3	2	1	8	1	5	2	3	2	6	2
2	Interní kontrola a audit	7	5	6	4	5	3	-	-	-	-	3	5	5	6	-	-	-	-
3	kancelář ředitele	7	5	7	4	7	2	4	3	-	-	4	2	5	5	3	2	-	-
4	oddělení PaM	6	7	6	6	7	5	-	-	-	-	4	4	4	4	-	-	-	-
5	oddělení organizační	6	7	8	5	6	5	-	-	-	-	3	4	4	4	-	-	5	3
6	psychologické pracoviště	7	5	6	4	6	3	-	-	-	-	4	2	3	3	-	-		-
7	pracoviště právní	7	6	6	4	7	3	-	-	-	-	3	3	4	3	-	-		-
8	oddělení IZS a řízení jednotek PO	8	8	7	6	4	5	4	5	-	-	3	5	5	4	-	-	-	-
9	oddělení služeb	6	7	6	6	4	4	-	-	-	-	3	5	4	4	-	-	-	-
10	OPIS	9	9	9	9	5	6	5	8	5	7	7	9	5	7	-	-	-	-
11	oddělení informačních systémů	9	9	9	8	9	8	5	8	8	6	9	9	9	8	9	6	5	2
12	oddělení komunikačních systémů	8	8	8	7	3	6	5	6	6	5	3	8	8	6	4	5	-	-
13	oddělení rozpočtu	8	7	5	6	4	4	-	-	-	-	2	5	4	3	-	-	-	-
14	oddělení účetnictví	8	6	6	6	7	4	-	-	-	-	2	5	4	3	-	-	-	-
15	oddělení zásobování	7	7	5	6	4	3	-	-	-	-	2	4	3	3	-	-	-	-
16	oddělení provozní a správy majetku	7	6	8	7	6	4	3	7	4	5	3	4	4	4	-	-	-	-
17	oddělení kontrolní činnosti a ZPP	7	7	8	6	6	4	-	-	-	-	5	6	4	4	-	-	-	-
18	oddělení stavební prevence	8	6	8	7	6	5	-	-	-	-	5	6	4	4	-	-	-	-
19	oddělení ochrany a přípravy obyvatelstva	7	7	8	6	6	4	-	-	-	-	6	6	3	4	-	-	-	-
20	oddělení krizového řízení	9	7	8	7	7	5	-	-	-	-	6	6	4	4	-	-	-	-
	průměr	7,4	6,7	7,2	5,9	5,7	4,2	4,1	5,7	5,0	4,8	4,3	5,0	4,6	4,3	4,8	3,8	5,3	2,3

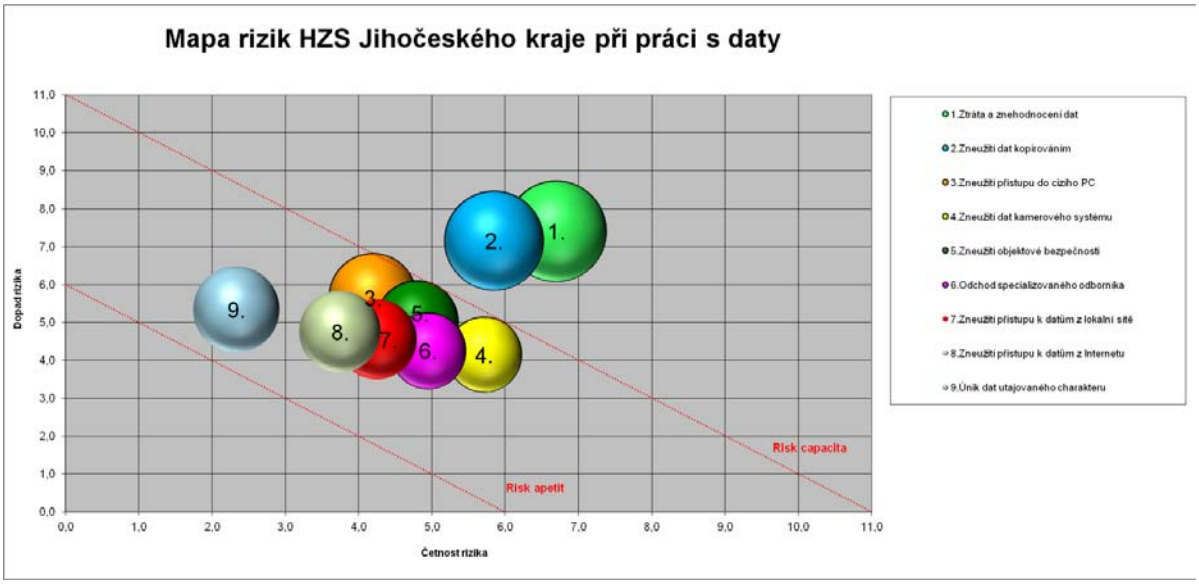
Zdroj: Vlastní

Čísla 1-5 určují sloupce pro posuzovanou oblast. V řádkách 1-20 jsou jednotlivá posuzovaná oddělení. Vynechané hodnoty v některých buňkách jsou proto, že se s uvedenou oblastí na daném oddělení příslušníci a zaměstnanci nesetkávají, nebo nemohou ovlivnit ani jednu sledovanou veličinu. Například příslušníci a zaměstnanci některých oddělení se vůbec nesetkají při své práci s utajovanými skutečnostmi nebo s daty z kamerového systému. Rovněž tak většina příslušníků a zaměstnanců nemůže ovlivnit přístup k datům HZS JčK z internetu oproti jiným, kteří tu možnost mají. U některých dokonce vyplývá z popisu služební činnosti povinnost chránit data proti této možnosti.

Po vyhodnocení těchto údajů jsem zjistil, že oblasti možného ohrožení dat různého typu zasahují do činnosti všech oddělení HZS JčK. Proto jsem se po konzultaci se svým vedoucím práce rozhodl ze získaných údajů vypracovat analýzu rizik a dle dosažených výsledků navrhnout opatření pro ty oblasti činností, které v souvislosti s daty a informacemi jsou pro činnost HZS nejvíce kritické a pro něž je potřeba snížit míru možného rizika.

5.1.4 Popis grafu

Na osu x jsem vynesl zprůměrované hodnoty dopadu rizika pro jednotlivé oblasti dle tabulky č.1, na osu y potom hodnoty četnosti rizika pro tyto oblasti. Úhlopříčkou jsem pro přehlednost vymezil fiktivní oblasti výsledné velikosti celkové míry rizika, abych oddělil oblasti s nejvyšší hodnotou rizika oproti ostatním oblastem, u kterých tato míra není tak vysoká.



Obr. č. 36: – Mapa rizik

Zdroj: Vlastní

5.2. Návrhy řešení

Při získávání informací a údajů při kvalitativním výzkumu na jednotlivých odděleních a pracovištích HZS Jihočeského kraje jsem si formoval představu nejrizikovějšího oddělení z pohledu práce s daty a informacemi a to z pohledu toho, jaké množství dat jednotlivá oddělení obhospodařují a jak mohou příslušníci a zaměstnanci ovlivnit jejich bezpečnost. Měl jsem tedy původně v úmyslu se zabývat jedním, popřípadě dvěma takovými odděleními. Ovšem s ohledem na výsledek provedeného výzkumu a následně provedené analýzy jsem se rozhodl prostudovat a následně navrhnout některá efektivní opatření, která by plošně přispěla ke snížení míry rizika pro některé oblasti práce s daty.

Dle výsledku průzkumu a analýzy rizik jsou nejrizikovější oblastí při práci s daty u HZS Jihočeského kraje oblast možné ztráty a znehodnocení dat a oblast možného zneužití dat kopírováním, ať už se jedná o data papírová nebo elektronická.

5.2.1 Oddělení informačních systémů

Toto oddělení je pro data organizace z hlediska jejich ochrany nejvíce klíčové. Je to z toho důvodu, že příslušníci tohoto oddělení se starají o veškeré informační systémy organizace, spravují počítačové sítě, kamerový systém a systém vstupů včetně správy čipových karet. Starají se o ukládání a zálohování elektronických dat a informací. Jednotliví příslušníci oddělení, jsou vzájemně zastupitelní, což zvyšuje četnost rizika případného zneužití. Vedle zneužití dat má práce příslušníků oproti jiným oddělením organizace jiný přímý vliv na ochranu elektronických dat organizace. Je to dáno právě tím, že nastavují pravidla ostatním příslušníkům a zaměstnancům pro přístup do informačních systémů, včetně souborových serverů, kam mohou dle těchto pravidel svá data zapisovat a mazat nebo jen číst. Příslušníci a zaměstnanci tohoto oddělení dále zpracovávají a plní postupy pro pravidelné zálohování všech elektronických dat organizace.

5.2.2 Ztráta a znehodnocení dat

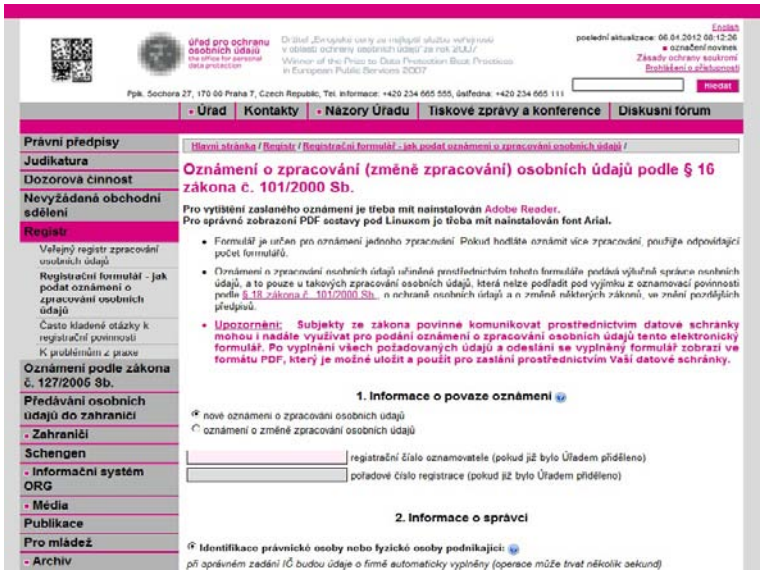
Velký dopad tohoto rizika je dán tím, že na datech a informacích, zejména elektronických je závislá činnost všech oddělení a pracovišť HZS JčK, a některé by v případě jejich ztráty nebo znehodnocení nemohla činnost vykonávat, čímž by byl přímo ohrožen chod organizace. Tímto oddělením je Operační a informační středisko HZS JčK. Při nedostupnosti dat a informací by nebylo možné účinné nasazení sil a prostředků k řešení mimořádných událostí. Neméně důležitým problémem by byla ztráta důležitých dat a informací, která by ohrozila mnoho dalších oddělení např. tím, že by nemohla plnit zákonité povinnosti organizace. Jedná se např. o oddělení krizového řízení při zpracovávání krizového plánu kraje, což vyplývá Hasičskému záchrannému sboru ze zákona 240/2000 Sb. Oddělení ekonomické nebo personální a mzdové by přišla o podklady pro proplácení faktur a vyplácení mezd.

5.2.3 Zneužití dat kopírováním

Další oblastí, která se umístila na druhém místě v analýze rizik, je možnost zneužití dat kopírováním. Tento stav je dán především v dostupnosti přístupu ke kopírovacím zařízením a neomezené možnosti pořizovat elektronické kopie na svých počítačích, kromě počítačů umístěných na OPIS.

S větším odstupem od těchto dvou oblastí se umísila oblast možného zneužití přístupu nebo manipulace s cizím počítačem a možné zneužití osobních dat kamerového systému.

Právě v posledně jmenované oblasti jsem při zpracovávání mé práci narazil na jediný problém v oblasti legislativy a to ten, že organizace neměla registraci k provozování kamerového systému od úřadu pro ochranu osobních údajů. Jelikož bylo potřeba provézt tuto registraci neprodleně tak, aby nedošlo k porušování zákona č. 101/2000 Sb., dohodl jsem se s vedoucím práce, že po provedené registraci, ke které došlo 1. března 2012, budeme z pohledu mé práce pohlížet na věc v souladu s platnou legislativou.



Obr. č. 37: PrtSc webu úřadu pro ochranu osobních údajů

Zdroj: http://www.uoou.cz/uoou.aspx

Tato registrace se provádí vyplněním elektronického formuláře přímo na webových stránkách úřadu na ochranu osobních údajů (obr č. 38).

5.2.4 Nutnost registrace kamerového systému

Provozování kamerového systému je považováno za zpracování osobních údajů, pokud je vedle kamerového sledování prováděn záznam pořizovaných záběrů nebo jsou-li v záznamovém zařízení uchovávány informace a je-li zároveň účelem pořizovaných záznamů, případně vybraných informací, jejich využití k identifikaci fyzických osob v souvislosti s určitým jednáním.

Samotné kamerové sledování fyzických osob není zpracováním osobních údajů podle zákona č. 101/2000 Sb., protože postrádá úroveň podmínek pro zpracování údajů ve smyslu § 4 písm. e) zákona č. 101/2000 Sb., „Zpracováním osobních údajů je jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.“ /28/

To však nevylučuje aplikaci jiných právních předpisů, zejména ustanovení občanského zákoníku upravujícího podmínky ochrany osobnosti. Údaje uchovávané v záznamovém zařízení, ať obrazové či zvukové, jsou osobními údaji za předpokladu, že na základě těchto záznamů lze přímo či nepřímo identifikovat konkrétní fyzickou osobu. Fyzická osoba je identifikovatelná, pokud ze snímku, na němž je zachycena, jsou patrné její charakteristické rozpoznávací znaky, což je zejména obličej a na základě propojení rozpoznávacích znaků s dalšími disponibilními údaji je možná plná identifikace osoby. Osobní údaj pak ve svém souhrnu tvoří ty identifikátory, které umožňují příslušnou osobu spojit s určitým, na snímku zachyceným, jednáním.

Zpracování osobních údajů provozováním kamerového systému je přípustné:

- v rámci plnění úkolů uložených zákonem (např. Policii ČR), ale v těchto případech je třeba dbát ustanovení příslušného zákona,
- dále je toto možné na základě řádného souhlasu subjektu údajů, to však je prakticky realizovatelné ve velmi omezených případech, kdy je možné jednoznačně vymezit okruh osob nacházejících se v dosahu kamery,

- užití kamerového systému však je možné i bez souhlasu subjektu údajů s využitím ustanovení § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. /31/

Povinnosti správce při provozování kamerového systému vybaveného záznamovým zařízením:

- Kamerové sledování nesmí nadměrně zasahovat do soukromí. Kamerový systém je možno použít zásadně v případě, kdy sledovaného účelu nelze účinně dosáhnout jinou cestou (např. majetek je možno chránit před odcizením uzamčením místnosti). Dále je vyloučeno užití kamerového systému v prostorách určených k ryze soukromým úkonům (např. toalety, sprchy).
- Je třeba předem jednoznačně stanovit účel pořizování záznamů, který musí korespondovat s důležitými, právem chráněnými zájmy správce např. ochranou majetku před krádeží. Záznamy tak mohou být využity pouze v souvislosti se zjištěním události, která poškozuje tyto důležité, právem chráněné zájmy správce.
- Přípustnost využití záznamů pro jiný účel musí být omezena na významný veřejný zájem, např. boj proti pouliční kriminalitě.
- Je třeba stanovit lhůtu pro uchovávání záznamů. Doba uchovávání dat by neměla přesáhnout časový limit maximálně přípustný pro naplnění účelu provozování kamerového systému. Uchovávaná data by měla být uchovávána v rámci časové smyčky např. 24 hodin a po uplynutí této doby vymazána. Pouze v případě existujícího bezpečnostního incidentu by měla být data zpřístupněna orgánům činným v trestním řízení, soudu nebo jinému oprávněnému subjektu.
- Je třeba řádně zajistit ochranu snímacích zařízení, přenosových cest a datových nosičů, na nichž jsou uloženy záznamy před neoprávněným nebo nahodilým přístupem, změnou, zničením či ztrátou nebo jiným neoprávněným zpracováním § 13 zákona č. 101/2000 Sb.
- Subjekt údajů musí být o užití kamerového systému vhodným způsobem informován (např. nápisem umístěným v monitorované místnosti), viz § 11 odst. 5 zákona č. 101/2000 Sb., nejde-li o uplatnění zvláštních práv a povinností vyplývajících ze zvláštního zákona.
- Je třeba garantovat další práva, zejména právo na přístup ke zpracovávaným datům a právo na námitku proti jejich zpracování, viz § 1 zákona č. 101/2000 Sb.

- Zpracování osobních údajů je třeba registrovat u Úřadu pro ochranu osobních údajů, nejde-li o uplatnění zvláštního práva či povinností vyplývajících ze zvláštního zákona, viz §18 odst. 1 písm. b) zákona č. 101/2000 Sb. /10/

5.2.5 Zabezpečení elektronických dat

Na rozdíl od ostatních oddělení, oddělení informačních systémů, má největší podíl na tom, jestli data ostatních uživatelů budou dostatečně zabezpečena a pravidelně zálohována. Je to dáno především tím, že většina dat, které vytváření a s nimiž pracují ostatní příslušníci a zaměstnanci není uložena na lokálních počítačích a noteboocích uživatelů, ale na serverech HZS. Z tohoto hlediska je nejdůležitější souborový server. V dnešní době již servery HZS JčK zpravidla obsahují více disků pro ukládání dat, které jsou zapojeny to tzv. Raid polí viz. příloha č. 5 – RAID pole.

Proč RAID 5 přestane fungovat

Přesto, že disky jsou neuvěřitelně spolehlivé zařízení, zpravidla selžou, když to nejméně čekáme. Data poruchovosti ukazují, že více než 3% disků selže každý rok v prvních třech letech života, a pak míra selhání začne rychle růst. Tomu odpovídá, že máme-li diskové pole sestavené ze sedmi nových disků, máme 20% šanci na selhání každý rok. Když k tomu vezmeme v úvahu rostoucí poruchovost s věkem tak po dobu 4 let, téměř jistě zažijeme výpadek disku během života tohoto diskového pole.

Máme chráněna data polem RAID-5? U SATA disků se obvykle uvádí střední doba neodstranitelné chyby (URE)10.^14. Což znamená, že jednou za 100,000,000,000,000 bitů se na disku objeví nečitelná data. Jedno sto bilionů bitů je asi 12 terabajtů. Což je použití 7ks disků s kapacitou 2TB v diskovém poli RAID-5. Tzn., že při selhání jednoho disku z tohoto pole bude ze zbývajících šesti zbývající 2 TB disků rekonstruovat data vadného disku, což by znamenalo téměř jistotu, že narazí na nečitelná data (URE).

Řešení pro oddálení této hrozby našli samotní výrobci disků. A začali vyrábět disky v edici enterprise u které zvýšily URE na 10 ^ 16, tedy o dva řády, čímž se značně zvýšila spolehlivost raid polí. Ceny těchto disků jsou přibližně o 50% vyšší než běžných disků. Těmito disky jsou osazovány nově nakupované servery HZS. /11/

Dalším řešením ke zvýšení spolehlivosti diskových polí a eliminování selhání, by bylo nahrazení RAID-5 diskovými poli RAID-6. V současné době žádné provozované servery HZS nemají řadiče diskových polí, které by uměly vytvořit RAID-6. Při generační obměně nebo nákupu dalších serverů by to však měl být požadovaný parametr.

5.2.6 Zálohování

Jak vyplývá s předchozích kapitol, čím složitější a zdánlivě dokonalejší technologie, tím důležitější je nepropadnout pocitu zabezpečení dat a věnovat pozornost zálohování. Problém v zálohování je především ve stále se zvětšujícím objemu dat, které samozřejmě z ekonomických důvodů nelze zálohovat všechny. Proto je třeba vydefinovat nejdůležitější data vzhledem ke kapacitě zálohovacího média, které máme k dispozici.

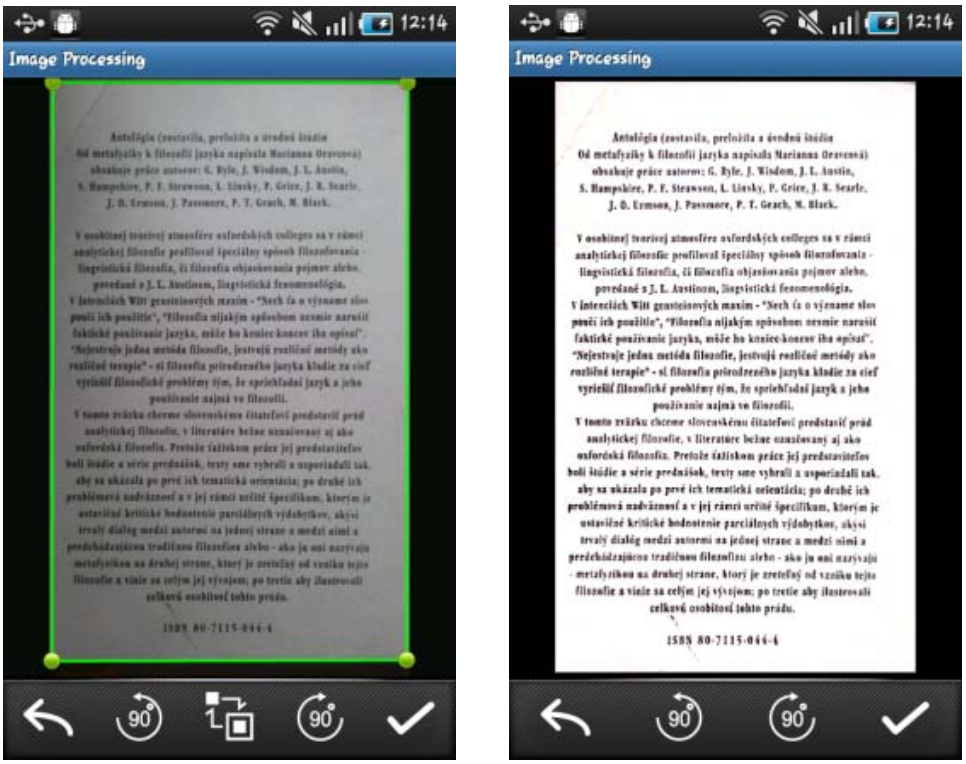
Zálohování dat se provádí tak, že se zálohy nejdříve ukládají na server pro ukládání dat (data storage) a následně zálohují na páskové mechaniky. Jak bylo zjištěno tato záloha se provádí jednou týdně bez následné verifikace uložených dat. Vzhledem
k vysoké pravděpodobnosti možného výskytu tohoto rizika a možným důsledkům po celou organizaci bych doporučil zavézt pravidelné kontroly jednotlivých záloh na páskách.

Těmito opatřeními by bylo možno docílit snížení míry rizika minimálně o dva stupně a tím se dostat do pásma přijatelného rizika.

5.2.7 Ochrana dat před optickým kopírováním dat

Dalším opatřením zabezpečujícím data v papírové podobě a foto scaning obrazovek monitorů, který se již v hojné míře uplatňuje u mnoha zahraničních firem, např. Accenture (http://www.accenture.com/cz-en), kde dochází ke zpracovávání i méně choulostivých osobních údajů a dat je zákaz používání mobilních telefonů, fotoaparátů vlastních notebooků a tabletů na pracovištích. Zejména telefony jsou s každou jejich generací stále dokonalejší a zejména ve spojení s čím dál dokonalejšími a většími fotočipy dokážou zaznamenat i ty nejmenší detaily. Ve spojení s nejrůznějším SW

přímo v telefonu například CamScanner pracujícím pod operačním systémem Android se smartphone promění v poměrně dokonalý scanner s možností úpravy konečných kopií, které lze navíc díky tomu, že se zároveň jedná o telefon, okamžitě odeslat.



Obr. č. 38 a 39: Aplikace CamScanner (vlevo před a vpravo po úpravě)
Zdroj: http://www.androidmarket.cz/aplikace/nastroje/camscanner-%E2%80%93-skenujte-cokoliv-a-kdekoliv/

Pracoviště, na kterých platí tato omezení jsou označována informačními tabulkami např. s nápisem „Production Area“ viz vzor obr. č. 41. Přesná podoba ani grafické znázornění neřeší žádný zákon ani vyhláška a každá firma si je řeší individuelně.

Obr. č. 40: Pracoviště označené production area
Zdroj: http://www.productionarea.com/

5.2.8 Zabezpečení dat OPIS

Pracoviště, které by si zasloužilo přijmout komplex bezpečnostních opatření na ochranu proti zneužití dat kopírováním je především OPIS. Je to pracoviště, kde je k dispozici veliké množství osobních a neveřejných údajů v písemné a elektronické podobě a zároveň se zde v nepřetržitém směnném provozu střídají tři desítky příslušníků a zaměstnanců.

Ti mají tyto informace k dispozici pro svou práci včetně další informační podpory. Tou je podpora GIS (geografický informační systém), krizový plán kraje, havarijní plán kraje a vnější havarijní plán JETE, havarijní plány podniků a další dokumentace. Jak už jsem zmínil, riziko zneužití dat na tomto oddělení tkví především ve velkém počtu zaměstnanců, což představuje zvýšené nebezpečí četnosti rizika.

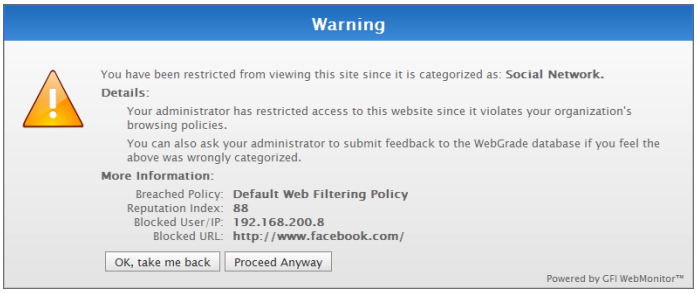
OPIS je vybaven 8 identickými pracovišti pro operační řízení jednotek HZS při řešení mimořádných událostí a 4 pracovišti příjmu a odbavení tísňového volání telefonních čísel 112 a 150.

Příslušníci a zaměstnanci mají na svých pracovištích přístup do sítě internet. Přesto, že je na pracovních počítačových stanicích systémem active directory, zamezeno nahrávání dat na externí záznamová média, není nikterak zamezeno odesílání dat elektronickou poštou (email) přes rozhraní web.

Jelikož přístup příslušníků a zaměstnanců OPIS k internetu nejde zakázat, ač by toto bylo jednoduché a nejlevnější řešení, popřelo by to jednu z úloh OPIS HZS JčK a to informační podporu při řešení mimořádných událostí. Z důvodu toho, že internet je pro zdroj informací nenahraditelným médiem.

Řešením by tedy bylo nasazení některého ze SW nástrojů pro skenování a filtraci webové aktivity jednotlivých uživatelů. Jedním z takových SW nástrojů je GFI WebMonitor™ 2012. Tento SW je samostatná proxy, jejíž instalací na některý server nebo PC přes nějž probíhá internetová komunikace, získáme následující vlastnosti:

- Účinné monitorování přístupu na internet využitím interaktivních reportů, kdy zjistíme, jaké weby ten který uživatel navštěvuje, kolik času na nich tráví a kolik dat stáhne. Jedná se o první krok ke stanovení efektivních pravidel využití internetu v organizaci. Každá organizace funguje jinak, každá organizace tedy musí stanovit taková pravidla, která odpovídají právě jejím potřebám.
- Filtrování přístupu na web s omezením na čas, objem dat i kategorie nastavení a vynucení pravidel přístupu na internet. Různým IP adresám a uživatelům můžeme povolit nebo zakázat přístup k různým kategoriím webů a omezit objem stažených dat nebo čas strávený na různých stránkách. Denně aktualizovaná databáze WebGrade obsahuje přes 205 000 000 domén tříděných do různých kategorií. Dokážeme tak velmi snadno stanovit, na které weby se uživatelé dostanou a na které weby přístup naopak zablokujeme, např. obsah pro dospělé, online hraní, soukromý email, P2P sítě nebo sociální sítě jako Facebook a Twitter.
- Monitorování vyhledávacích služeb, monitorování výrazů vyhledávaných uživateli na hlavních vyhledávacích portálech Google, Bing, Yahoo! pomůže včas rozpoznat potenciální hrozby, jako jsou například zaměstnanci rozhlížející se po nové práci, zaměstnanci hledající návody na výrobu výbušin nebo zaměstnanci vyvíjející jiné podezřelé aktivity. Pozorné monitorování vyhledávaných výrazů může sloužit jako dobrý indikátor nálady ve firmě.
- Varování založená na událostech dokáže upozornit na nastalé situace. Co to pro nás znamená? Jednoduše nastavíme konkrétní spouštěče, aktivační události např. někdo navštívil nevhodnou webovou stránku, někdo si příliš dlouho pročítá zpravodajské servery nebo si někdo aktivně hledá novou práci, na které chcete být upozorněni.
- Smart Dashboards usnadňuje přístup osob mimo IT oddělení k reportům a výstupům z nashromážděných dat. Smart Dashboards – inteligentní dashboard jsou rozděleny do tří skupin: Aktivity, Šířka pásma a internetový provoz v reálném čase.

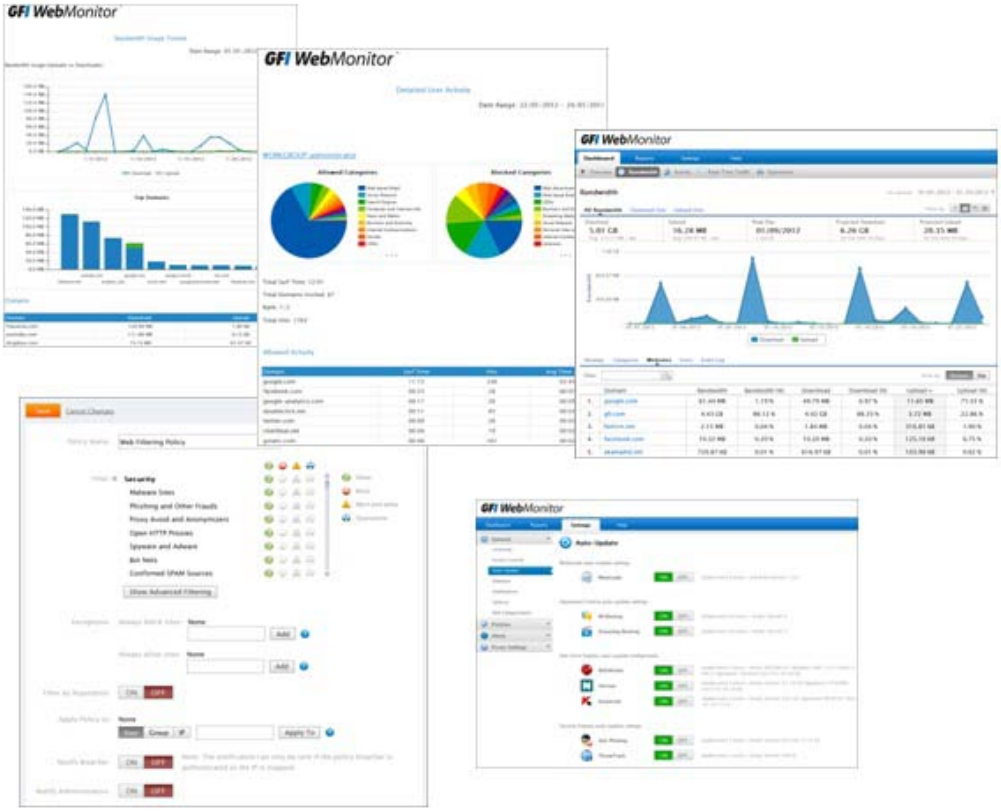


Obr. č. 41: Upozornění na nevhodné stránky

Zdroj: http://www.gfi.cz/webmon/webmonscreenshots.htm

- Monitorování nebo blokování spojení v reálném čase uživatelské rozhraní poskytuje pohled na stránky, po kterých uživatelé právě surfují, a soubory, které si stahují. Aktivní spojení, session nebo download snadno zablokujeme kliknutím na ikonku Block connection.
- Z reportů získáme veškeré informace o všech uživatelích, kterým GFI WebMonitor na základě narušení vašich pravidel přístupu na internet „zatrhl“ přístup. Mezi těmito narušeními nalezneme například pokusy o přístup na zakázané weby, stahování infikovaných souborů nebo stahování zakázaných typů souborů např. video a spustitelné soubory.
- Monitorování skrytých downloadů. Některé aplikace se automaticky připojují k jejich domovským serverům, odkud si pomocí HTTP tunelování stahují aktualizace. Sice to usnadňuje administraci, ale na druhou stranu se může jednat o bezpečnostní riziko. Stejným způsobem si neznámé aplikace mohou stáhnout škodlivý kód, včetně virů, spyware, adaware a pornware na uživatelovo PC. GFI WebMonitor vám dává kontrolu nad stránkami, ze kterých povolíte stahování aktualizací.
- Nastavení výjimek pomocí whitelistu a blacklistů. Na whitelist nebo blacklist můžetme přidat jakoukoli URL/uživatele/IP, a to dočasně nebo trvale. Obejdeme tak veškeré politiky pro web filtering i web security. Například můžeme uživateli povolit časově omezený přístup na jeho osobní web mail, řekněme v době oběda.
- Skenováním HTTPS provozu dokážeme rozšifrovat provoz probíhající přes SSL, proskenovat obsah na přítomnost malware a znovu jej zašifrovat. Tato funkce

rozšiřuje možnosti filtrování a kontroly stahovaného obsahu i na provoz zabezpečený šifrováním.



Obr. č. 42: Náhled SW GFI WebMonitor
Zdroj: Vlastní

Dalším opatřením, které by bezesporu přispělo ke zmírnění bezpečnostního rizika na tomto oddělení, by bylo instalování bezpečnostní kamery. Jelikož se jedná o pracoviště se zvláštním režimem, určením by tento krok byl i legislativně ospravedlnitelný. Zde by bylo třeba obhájit umístění tak, aby nedošlo k porušení zákona č. 262/2006 Sb., Zákoník práce, kde se v § 316 odst. 2 a 3 uvádí, že „Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci. Jestliže je u zaměstnavatele dán

závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení kontrolních mechanismů podle odstavce 2, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění.“ /29/

5.2.9 Pro ochranu zaměstnavatele

Jelikož zpřísnění monitoringu na pracovištích a instalace kamer zvlášť, téměř vždy vyvolává napětí mezi zaměstnanci a zaměstnavatelem, doporučuji před takovým krokem provézt následující postup:

- Zavedení kamer projednat s odborovou organizací, včetně důvodů jejich instalace.
- Vydat vnitřní předpis, obsahující účel zavedení systému, umístění kamer, dobu, po kterou bude fungovat, okruh osob, které záběry z kamery budou sledovat a za jakým účelem a dobu uchovávání záznamů.
- Všechny dotčené osoby s vnitřním předpisem seznámit (proti podpisu).
- Na místech sledovaných kamerou viditelně umístit informační cedule.

Obr. č. 43: Pohled z navrhované kamery na OPIS

Zdroj: Vlastní

Možnost kopírování jakýchkoli dat v písemné nebo elektronické formě není až na pár výjimek nikterak technicky omezováno. Zde platí pouze legislativní opatření ve formě platných zákonů a vnitřních předpisů. Přístup na kopírovací stroje je omezen číselnými kódy čímž je sice zajištěn přístup na kopírovací stroj, ale neřeší to

problematiku ochrany kopírovaných dokumentů. Na základě provedeného šetření je řediteli HZS JčK navrženo umístění monitorovacích kamer nad jednotlivé kopírky. Příkladem je pohled kamery na kopírku, jež ukazuje obrázek č. 44.

Obr. č. 44: Pohled z navrhované kamery na kopírovací zařízení
Zdroj: Vlastní

5.3. Další návrhy opatření

5.3.1 Čtečky karet

Dalším opatřením, které se nabízí pro snížení hodnot rizik je návrh vybavit zařízení, u nichž je vyžadována individuální forma přístupu namísto zabezpečení heslem, instalací čtečky čipových karet Wiegand. Jak je popsáno již v kapitole o elektronické kontrole vstupu, tyto karty vlastní každý příslušník a zaměstnanec organizace a proto se přímo nabízí jejich další využití ke zvýšení bezpečnosti nejen v objektové bezpečnosti, ale i dalších bezpečnostních politikách organizace. Mimo jiné využití navrhuji zabezpečený přístup ke kopírovacím zařízením a přístup na jednotlivé pracovní stanice (počítače). Vhodná čtečka karet s rozhraním USB je na obr č. 45.

Obr. č. 45: Čtečka čipových karet Wiegand
Zdroj: Vlastní

Změna v bezpečnostní politice při zabezpečení pracovních stanic vychází z filozofie chování uživatelů. Příliš časté změny hesel a jejich požadovaná skladba a délka s ohledem na bezpečnost nutí většinu uživatelů si tyto zapisovat v dosahu svých počítačů.

5.3.2. Výměna kamerového systému

Další oblastí, která byla z pohledu výše rizika problematická, je kamerový systém HZS. Na základě mého šetření je na letošní rok plánovaná jeho výměna. Podílel jsem se na výběru vhodného nového zařízení, které by mimo lepší technické parametry a zvýšenou spolehlivost, přineslo i lepší ošetření a kontrolu z pohledu ochrany osobních údajů. Velmi významným parametrem, který přímo souvisí s ochranou osobních dat a údajů v této sledované oblasti je možnost jednotlivým uživatelům selektivně nadefinovat soubor kamer, z nichž budou mít k dispozici zaznamenána data. Toto je důležité zejména, když by došlo na realizaci dalších mých navrhovaných opatření, instalováním kamer na některá režimová pracoviště. Jejich sledování by rozhodně nemělo být umožněno všem uživatelům kamerového systému a přístup k prohlížení a záznamům by musel být omezen pouze na velmi úzký okruh příslušníků nebo zaměstnanců. Pravděpodobně by se jednalo o vedoucího daného oddělení nebo pracoviště. Technicky to s novým systémem bude řešitelné.

Obr. č. 46: Hybridní záznamová zařízení (HVR) - řada MX 3. generace – MX3232 4000/900
Zdroj: https://www.cee.siemens.com/web/cz/cz/corporate/portal/home/infrastructure-cities/IBT/pozarni_a_bezpecnostni_systemy/cctv/hybridni_zz_hvr-rada_mx_3_generace/Pages/MX32324000900.aspx

SISTORE MX 3. generace je hybridní digitální záznamové a monitorovací zařízení umožňující REAL-TIME záznam v rozlišení až 4CIF a nabízející vzdálenou obsluhu pomocí LAN nebo ISDN. Uživatelsky příjemné grafické rozhraní, shodné s předchozími verzemi, umožňuje profesionální ale zároveň i snadné ovládání.

K rychlému prohledávání záznamů lze využít vyhledávací masku "Easy-search". Virtuální nebo CKA klávesnice umožňuje plně ovládat PTZ zařízení i IP, včetně prepozic a konfigurace.

Zařízení umožňuje přijímat a zaznamenávat i video stream až z 32 IP kamer. Je vybaveno dvěma hlavními monitorovými výstupy a dále čtyřmi analogovými monitory se základní funkcí matice včetně alarmového přepínání obrazů kamer.

Za normálních podmínek nevyžaduje systém SISTORE MX žádnou zvláštní údržbu. V zařízení je možné snadno rozšířit záznamovou kapacitu až na 4TB. Zařízení je dodáváno včetně programu pro vzdálenou správu RemoteView. /18/

6 ZÁVĚR

Cílem mé práce bylo zjistit, zda je s daty a informacemi, se kterými se setkávají příslušníci a zaměstnanci Hasičského záchranného sboru Jihočeského kraje při své práci, nakládáno v souladu s platnou legislativou, a zda jsou tyto dostatečně zabezpečeny a chráněny proti zneužití a ztrátě.

Byly stanoveny dvě hypotézy, které jsem měl za úkol na základě výsledků práce buď verifikovat, nebo falzifikovat. Výsledky zkoumání mě opravňují ke konstatování, že hypotéza č. 1: Práce s daty a jejich zabezpečení je u HZS JčK v souladu s platnou legislativou byla verifikována. Během svého výzkumu a zpracovávání práce jsem až na jedinou výjimku, chybějící registraci kamerového systému u úřadu pro ochranu osobních údajů, nenašel odchylku nakládání s daty a informacemi od platné legislativy. Tento jediný případ byl neprodleně napraven na počátku zpracovávání mé práce, a tudíž jsem se rozhodl jej považovat za odpovídající ustanovením příslušného zákona. Podrobně jsem o této události psal v kapitole Diskuse.

Hypotéza č. 2: Data jsou dostatečně chráněna proti ztrátě a zneužití byla falzifikována. Při svém výzkumu jsem dospěl k některým zjištěním, z nichž vyplývá poměrně veliké riziko možné ztráty nebo zneužití dat. Tento stav je dán tím, že množství nejrůznějších dat je opravdu obsáhlé a téměř všechna opatření na zabezpečení a ochranu dat vyžadují nemalé finanční náklady, kterých je ve státní správě citelný nedostatek. Přesto je vyšší ochrana dat průběžně zaváděna s ohledem na dostupnost finančních prostředků. Během řešení mé práce to bylo několik nových opatření, jako např. nákup nových bezpečnostních skříní nebo realizace malé zakázky na nový videoserver pro kamerový systém.

Pro další zvýšení zabezpečení dat jsem navrhl a popsal několik dalších řešení a opatření. Jejich případná realizace bude závislá na finančních prostředcích. Jedná se o rozšíření kamerového systému, nákup monitorovacího SW, obměna datových úložišť. Dále realizace mých návrhů bude záviset na přijetí některých většinou nepopulárních administrativních opatření. Jedná se o omezení používání vlastních zařízení, zejména mobilních telefonů na některých pracovištích.

Cíl, který byl vytyčen při zadání práce, zjistit, zda je s daty u HZS Jihočeského kraje nakládáno v souladu s platnou legislativou a zda jsou dostatečně zabezpečeny a

chráněny proti zneužití a ztrátě byl splněn a výsledky podrobně rozebrány a popsány spolu s návrhy konkrétních řešení.

Přínosem práce k řešené problematice je jednak zmapování a zpracování jednotlivých rizik, kterými jsou ohrožena data a informace na jednotlivých odděleních a pracovištích Hasičského záchranného sboru Jihočeského kraje a zároveň návrh opatření ke zmírnění těchto rizik, přičemž některá opatření byla realizována již v průběhu zpracovávání této práce. Využitelnost dalších navržených opatření budou do jisté míry záviset na budoucích finančních rozpočtech organizace.

7 SEZNAM INFORMAČNÍCH ZDROJU

7.1 Literatura a elektronické zdroje

1. Státní okresní archiv Pelhřimov. *Historie státního oblastního archivu Pelhřimov*. In. [online]. 2008.Dostupné z: http://www.mza.cz/pelhrimov/historie.php

2. PhysOrg. *Počet uživatelů internetu na celém světě dosahuje dvě miliardy* In. [online].2011 [cit.2011-01-26]. Dostupné z: http://www.physorg.com/news/2011-01-internet-users-worldwide-billion.html

3. Linuxexpres. *Hacker vs. cracker*. In. [online].2008 [cit.2008-05-14]. Dostupné z: http://www.linuxexpres.cz/blog/hacker-vs-cracker

4. Cyberlawsindia.net. *White hat hackeři*. In. [online].2008 Dostupné z: http://www.cyberlawsindia.net/white-hat.html

5. Cyberlawsindia.net. *Grey hat hackeři*. In. [online].2008 Dostupné z: http://www.cyberlawsindia.net/grey-hat.html

6. Cyberlawsindia.net. *Black hat hackeři*. In. [online].2008 Dostupné z: http://www.cyberlawsindia.net/black-hat.html

7. Elisacomputer. *Raid.* In. [online].2008 Dostupné z: http://www.elisacomputer.cz/texts/raid.html

8. Storage. *Odborná sekce*. In. [online].Dostupné z: http://www.storage.cz/775-lto-dlt-slr-co-je-lepsi

9. SVATOŠOVÁ, Helena. Studie. *Návrh zákona o ochraně utajovaných informací*. In. [online].2003-2004. Dostupné z: http://www.iure.org/sites/default/files/article/downloads/07_navrh_zakona_o_ochrane_utajovanych_informaci.pdf

10.Úřad pro ochranu osobních údajů. *Stanovisko č. 1/2006*.In. [online].leden 2006. Dostupné z: http://www.uoou.cz/files/stanovisko_2006_1.pdf

11. ZDNet. *Proč přestane RAID 5 fungovat*. In. [online]. 2007.Dostupné z: http://www.zdnet.com/blog/storage/why-raid-5-stops-working-in-2009/162?tag=search-results-rivers;item4

12. SKLENÁK, Vilém. *Data informace znalosti a internet*. In. [online]. Dostupné z: http://books.google.cz/books?id=UJh-gLdTH8IC&printsec=frontcover&hl=cs#v=onepage&q&f=false

13. NECRORAISES. *Internetová válka 2012*. In. [online].2012 Dostupné z: http://www.necroraisers.com/novinky/necroraisers/1117-internetova-valka-2012-vzpoura-internetu-a-jeho-budoucnost/

14.Vesmír. *Počátky počítačové techniky nebyly jednoduché*. In. [online].duben 2005 Dostupné z: http://www.vesmir.cz/clanek/pocatky-pocitacove-techniky-nebyly-jednoduche

15. Chlad, Radim. *Historie internetu*. In. [online].Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2000/xchlad.htm

16. Týden.cz. *Před 20 lety se nám změnil život. Do Česka přišel internet* In. [online]. [cit.2012-02-10]. Dostupné z: http://www.tyden.cz/rubriky/media/internet/pred-dvaceti-lety-se-nam-zmenil-zivot-do-ceska-prisel-internet_224885.html

17. Technet.cz. *Dohodu ACTA přezkoumá evropský soudní dvůr*. In. [online]. [cit.2012-02-22]. Dostupné z: http://technet.idnes.cz/dohodu-acta-prezkouma-evropsky-soudni-dvur-fey-/sw_internet.aspx?c=A120222_135411_sw_internet_vse

18. SIEMENS. *Hybridní záznamová zařízení.* In. [online]. 2012.Dostupné z: https://www.cee.siemens.com/web/cz/cz/corporate/portal/home/infrastructure-cities/IBT/pozarni_a_bezpecnostni_systemy/cctv/hybridni_zz_hvr-rada_mx_3_generace/Pages/MX32324000900.aspx

19. Historie počítačů. *Jednotný systém elektronických počítačů*. In. [online]. 2005-2012. Dostupné z: http://www.historiepocitacu.cz/program-jsep.html

20. NBU. *Ochrana utajovaných informací* In. [online]. Dostupné z: http://www.nbu.cz/cs/ochrana-utajovanych-informaci/

21. Theancientworld. *Alexandrijská knihovna hoří*. In. [online]. [cit.2011-08-09] Dostupné z: http://theancientworld.blog.cz/1108/alexandrijska-knihovna-hori

22. Kerio. *Jak pracuje Bayes filtr a SpamAssassin.* In. [online]. Dostupné z: https://kb.kerio.com/article/jak-pracuje-bayes-filtr-a-spamassassin-560.html

23. RU.CZ. *Růst počtu uživatelů internetu v Čechách je stabilních 10 procent.*In. [online]. [cit. 2010-06-24] Dostupné z: http://www.irucz.ru/cz/zpravy/1/102000000000-ceska-republika/000-/102000610000-praha-hlm/304-internet/19149-rust-poctu-uzivatelu-internetu-v-cechach-je-stabilnich-10-proc/

24. REMIÁŠ, František. *Komunikační a informační systémy využívané při řešení mimořádných událostí na území jihočeského kraje*. České Budějovice. 2010. Bakalářská práce. Jihočeská univerzita.

25. MATĚJKA, Michal. Počítačová kriminalita, Computer press. 2002. ISBN 8072264192 počet stran 106

26. BOZP. *Zákaz mobilních telefonů na pracovišti* In. [online]. [cit. 2012-01-04] Dostupné z: http://bozpinfo.cz/rady/otazky_odpovedi/ochrana_pred_riziky/mobily_pracoviste120104.html

27. TP LINK. *Počet českých internetových uživatelů vzrostl za rok o více než 360 tisíc* In. [online]. [cit. 2011-08-03] Dostupné z: http://channelworld.cz/smb/mediaresearch-pocet-ceskych-internetovych-uzivatelu-vzrostl-za-rok-o-vice-nez-360-tisic-4600

28. ČESKO. Zákon č. 101/2000 Sb. ze dne 4. dubna 2000, o ochraně osobních údajů a o změně některých zákonů: *Sbírka zákonů ČR,*. 2000, částka 32.

29. ČESKO. Zákon č. 262/2006 Sb. ze dne 21. dubna 2006, Zákoník práce: *Sbírka zákonů ČR,*. 2006, částka 84.

30. PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. Brno: Computer press. počet stran 432. ISBN: 80-251-1278-0.

31. DELNET. *Provozování kamerového systému a zákony*. In. [online]. [1998-2011] Dostupné z: http://www.delnet.cz/slaboproude-systemy/kamerove-systemy-cctv/kamerovy-system-a-zakony.html

32. Internet a World Wife. *Historie počítačových sítí.* In. [online]. Dostupné z: http://ecom.ef.jcu.cz/web/download/teorie/p03-www_infrastruktura.pdf

33. Historie sítě internet. *Provoz internetu.* In. [online]. Dostupné z: http://ihistory.webzdarma.cz/index.php

34. O Webu cz. *Historie vzniku internetu.* In. [online]. Dostupné z: http://owebu.bloger.cz/Internet/Historie-vzniku-internetu

35. ČESKO. Zákon č. 412/2005 Sb. ze dne 21. září 2005, o ochraně utajovaných informací a o bezpečnostní způsobilosti: *Sbírka zákonů ČR*. 2005, částka 143.

36. ČESKO. Zákon č. 121/2000 Sb. ze dne 7. dubna 2000, o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon): *Sbírka zákonů ČR*. 2000, částka 36.

37. ČESKO. Zákon č. 361/2003 Sb. ze dne 23. září 2003, o služebním poměru příslušníků bezpečnostních sborů: *Sbírka zákonů ČR*. 2003, částka 121.

38. ČESKO. Zákon č. 499/2004 Sb. ze dne 30. června 2004, o archivnictví a spisové službě: *Sbírka zákonů ČR*. 2004, částka 173.

39. ČESKO. Usnesení vlády ČR č. 624/2004 ze dne 1. ledna 2002 pravidla, zásady a způsob zabezpečování kontroly užívání počítačových programů. 2002.

40. ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací: *Sbírka zákonů ČR*. 2005, částka 179.

41. Sbírka interních aktů generálního ředitele č. 50/2003 ze dne 20. listopadu 2003, kterým se stanoví osnova a obsah bezpečnostní politiky subjektů pro datové sítě HZS ČR.

42. Sbírka interních aktů ředitele HZS Jihočeského kraje 102/2004 ze dne 27. prosince 2004, kterým se stanoví pravidla Bezpečnostní politiky v oblasti informačních technologií HZS JčK.

7.2. Obrázky a tabulky:

Zdroj: http://www.root.cz/clanky/ceskoslovenske-osmibitove-pocitace-2-ndash-pmd-85/

Obr. č. 18: *8bitový počítač TNS Slušovice HC8*

Zdroj:http://www.root.cz/clanky/ceskoslovenske-osmibitove-pocitace-2-ndash-pmd-85/

Obr. č. 19: *Síť topologie klient server*

Zdroj: Vlastní

Obr. č. 20: *Topologie peer to peer*

Zdroj: Vlastní

Obr.č. 21: - *Schéma konvergované telekomunikační sítě HZS*

Zdroj: Vlastní

Obr. č. 22: *Grafické znázornění firewallu*

Zdroj: Vlastní

Obr. č. 23: *Firewall Cisco ASA*

Zdroje: http://www.ovh.cz/dedikovane_servery/firewall_dedikovane_servery.xml

Obr. č. 24: *Firewall Cisco PIX*

http://www.infracom.com.sg/products.php?product=CISCO851%252dK9-%252d-Ethernet-SOHO-Security-Router

Obr. č. 25: *Server HZS JčK*

Zdroj: Vlastní

Obr. č. 26: *Server HZS JčK*

Zdroj: Vlastní

Obr. č. 27: *LTO Roadmap*

Zdroj: http://www.storage.cz/775-lto-dlt-slr-co-je-lepsi

Obr. č. 28: *Zálohovací mechaniky*

Zdroj: Vlastní

Obr. č. 29: *Bayes filtr*

Zdroj: https://kb.kerio.com/article/jak-pracuje-bayes-filtr-a-spamassassin-560.html

Obr č. 31: *Organizační struktura*

Zdroj: Vlastní

Obr č. 30: *Organizační struktura*

Zdroj: Vlastní

Obr. č. 31: *Organizační struktura – ředitel kanceláře*

Obr. č. 46: *Hybridní záznamová zařízení (HVR) - řada MX 3. generace – MX3232 4000/900*

Zdroj: https://www.cee.siemens.com/web/cz/cz/corporate/portal/home/infrastructure-cities/IBT/pozarni_a_bezpecnostni_systemy/cctv/hybridni_zz_hvr-rada_mx_3_generace/Pages/MX32324000900.aspx

Obr. č. 47: *Alexandrijská knihovna*

Zdroj: http://theancientworld.blog.cz/1108/alexandrijska-knihovna-hori

Obr. č. 48: *Programovatelný tkalcovský stav*

Zdroj: http://commons.wikimedia.org/wiki/File:NMS_Jacquard_loom_2.JPG

Obr. č. 49: *Mechanický sčítací stroj*

Zdroj: http://pondicherry-mathseurosection.blogspot.com/2011/01/blaise-pascal.html

Obr. č. 50: *Počítač Z3*

Zdroj: http://www.computerhistory.org/timeline/?year=1941

Obr. č. 51: *Automatický počítací stroj*

Zdroj: http://www.sciencemuseum.org.uk/images/I031/10301732.aspx

Obr. č. 52: *Eniac*

Zdroje: http://www.telesanterno.com/10-febbraio-il-neonato-pesa%E2%80%A6-30-tonnellate-vagisce-il-primo-computer-0210.html

Obr. č. 53: *Univac II*

Zdroj: http://www.computermuseum.li/Testpage/UNIVAC-1-FullView-B.htm

Obr. č. 54: *Ural 2*

Zdroj: http://www.root.cz/clanky/historie-pocitacu-vyrabenych-v-sssr-2/#k01

Obr. č. 55: *Zablokovaná stránka*

Zdroj: megaupload.com

Obr. č. 56: *Zablokovaná stránka ODS*

Zdroj: http://www.ods.cz/

Obr. č. 57: *RAID 0*

Zdroj: https://www.computerscience1.net/RAID

Obr. č. 58: *RAID 1*

Zdroj: https://www.computerscience1.net/RAID

Obr. č. 59: *Kontrolní součty Raid 5*

Zdroj: Vlastní

Obr. č. 60: *RAID-5*

Zdroj: http://en.wikipedia.org/wiki/File:RAID_5.svg

Obr. č. 61: *RAID-6*

Zdroj: http://en.wikipedia.org/wiki/File:RAID_6.svg

Obr. č. 62: *RAID-10*

Zdroj: Vlastní

Tabulka č.1: Rizikové oblasti práce s daty

Tabulka č.2: Stupnice hodnot dopadu rizika

Tabulka č.3: Stupnice hodnot četnosti rizika

Tabulka č.4: Výsledné hodnoty rizikových oblastí

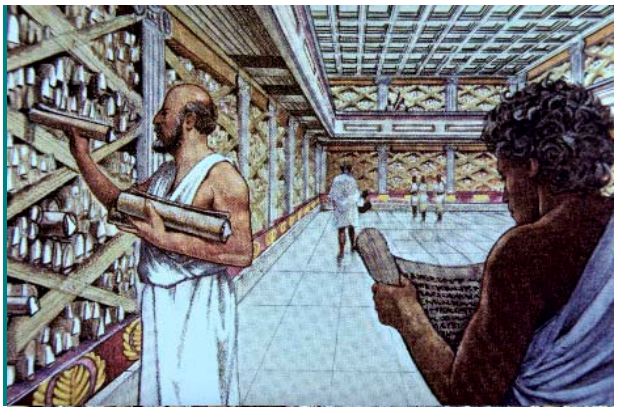
8 PŘÍLOHY

8.1 Příloha č. 1

Alexandrijská knihovna

Alexandrijská knihovna byla největší a nejslavnější knihovna starověku – součást vědeckého ústavu Múseion, vybudovaného z podnětu Ptolemaia I. kolem roku 295 př. n. l. Působili v ní učenci, spisovatelé a vědci, byl zde přeložen do řečtiny Starý zákon, přepsala se zde Homérova díla a učenci zde věděli i to, že Země není středem vesmíru. Obsahovala bezmála na 700 tisíc svitků a dala by se považovat za studnu antického vědění a učení z oborů astronomie, matematiky, lékařství, historie a fyziky. V roce 389 n. l. byla alexandrijská knihovna z podnětu fanatického pronásledovatele pohanů, alexandrijského biskupa Theofila, zničena vojsky římského císaře Theodosia I. Tím si římská církev uzurpovala monopol na vzdělanost, který přetrval až do roku 1444, kdy Cosimo de Medici založil první evropskou veřejnou knihovnu a začal tak narušovat dlouhotrvající monopol církve na vzdělávání. Jak uvádějí některé prameny zničením svitků a informacemi se zbrzdil vývoj lidstva nejméně o 1300 let. /21/

Teprve v první polovině 15. století mohučský zlatník Johannes Gutenberg zdokonalil vinný lis a vynalezl knihtisk. To znamenalo opravdovou revoluci v šíření informací - kniha, která mívala hodnotu převyšující celoživotní výdělek běžného rolníka, se náhle stává dostupná pro každého. Vznikly nové možnosti šíření rychlých a kvalitních informací i celá nová odvětví kultury a průmyslu, jako bylo vydávání novin a románů.



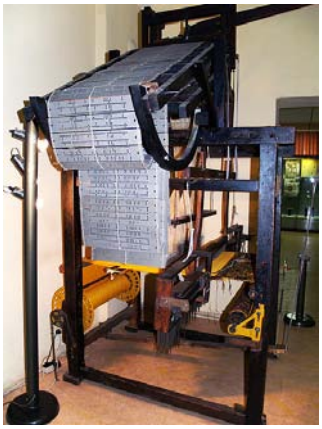
Obr.č.48: Alexandrijská knihovna

Zdroj: http://theancientworld.blog.cz/1108/alexandrijska-knihovna-hori

8.2 Příloha č. 2

Historie informačních technologií

Mezi prvními lidmi, kteří započali éru tohoto dosud neznámého odvětví lze označit francouzského filozofa a matematika Blaise Pascala (1623 -1662), který jako první, v roce 1652 sestrojil mechanický sčítací stroj. O téměř 150 let později, v roce 1801, známý průmyslník Jacquard, poprvé v praxi použil programové řízení, když zvolil děrné štítky s naprogramovaným vzorem látky pro řízení tkalcovského stavu. O necelé století později (přesně v roce 1890) byly štítky poprvé použity pro hromadné strojové zpracování dat při sčítání lidu v USA.



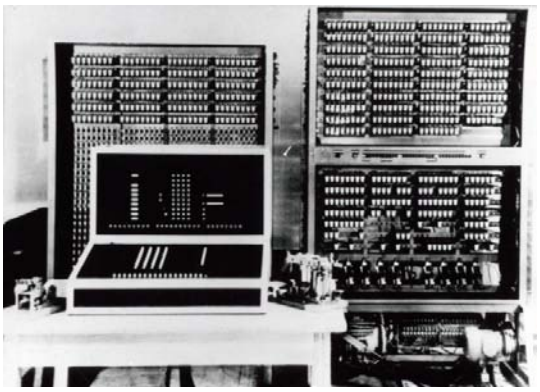
Obr. č. 49: Programovatelný tkalcovský stav

Obr. č. 50: Mechanický sčítací stroj

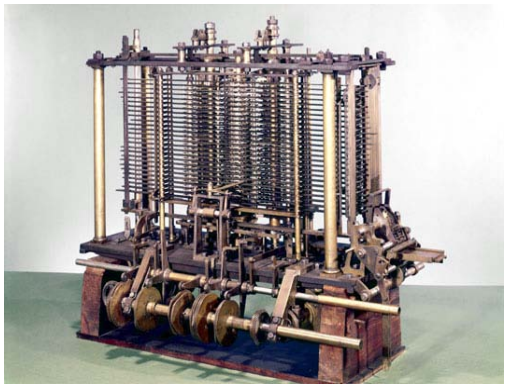
Zdroje: http://commons.wikimedia.org/wiki/File:NMS_Jacquard_loom_2.JPG
http://pondicherry-mathseurosection.blogspot.com/2011/01/blaise-pascal.html

S geniální myšlenkou propojit mechanický výpočetní stroj s programově řízeným strojem jako první přišel anglický matematik Charles Babbage (1791-187I). Roku 1834 navrhl programově řízený mechanický číslicový počítač, který nazval Analitical Engine. Stroj měl být vybaven aritmetickou jednotkou, pamětí pro 1000 padesáticiferných čísel, vstupem z děrných štítků a výstupem na primitivní tiskárnu. Programování se mělo provádět pomocí Jacquardouých děrných štítků. Návrhem Analytical Engine ovšem Babbage předběhl svou dobu natolik, že tehdejší dostupná technologie na tak složitou konstrukci nestačila. Z průkopníků nutno ještě jmenovat amerického průmyslníka a pozdějšího zakladatele firmy IBM, Hermana Holleritha, který na přelomu l9. a 20. století začal v masovém měřítku prosazovat používání

děrnoštítkových strojů. V období těsně před druhou světovou válkou byl vynález počítače již na spadnutí, výzkumné práce probíhaly souběžně v USA i v Evropě a to nezávisle na několika místech. Za konstruktéra opravdu prvního fungujícího počítače je považován němec Konrád Zuse. Z 2.300 ks relé sestrojil počítač Z3. Použil plovoucí desetinnou čárkou, binární aritmetiku a měl 22-bitové slovo. Původní Z3 byl zničen při bombardování Berlína na konci roku 1943. Nicméně, sám Zuse později dohlížel na rekonstrukci Z3 v roce 1960, který je nyní k vidění v Deutsches Museum v Mnichově.



Obr. č. 51: Počítač Z3

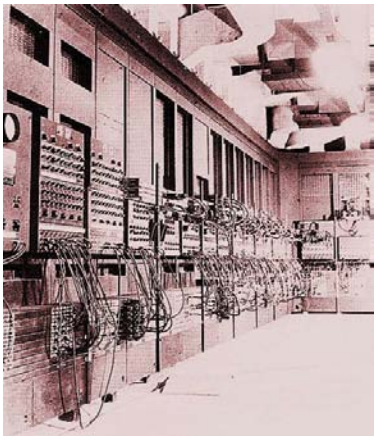


Obr. č. 52: Automatický počítací stroj

Zdroje: http://www.computerhistory.org/timeline/?year=1941
http://www.sciencemuseum.org.uk/images/I031/10301732.aspx

2. světová válka významnou měrou pozitivně zasáhla do vývoje počítačů. Zejména potřeba složitých armádních výpočtů (balistické dráhy střel, vývoj jaderné zbraně, rozvíjejí se letecký a raketový průmysl) zintenzivnily práce na sestrojení prvních počítačů. Když připočteme téměř neomezené finanční prostředky plynoucí do armádních projektů, nestálo již téměř nic v cestě. Z několika nezávislých skupin byl nakonec nejúspěšnější tým, který pracoval od roku 1943 na Pensylvánské universitě ve Philadelphii pod vedením J. Mauchlyho a J.P. Eckerta. V létě 1946 bylo sestrojeno a uvedeno do provozu elektronkové monstrum chlazené dvěma leteckými motory a nazvané ENIAC. Byl to pradědeček všech počítačů dneška. Od roku 1944 spolupracoval se skupinou Mauchlyho a Eckerta muž, který sice není vynálezcem počítače, ale jehož jméno je přesto doplňováno přívlastkem "otec výpočetní techniky"

John Von Neumann (1903-1957), který je považován za jednoho z největších matematiků našeho století. Narodil se a vyrostl v Budapešti jako vnuk rabína a syn úspěšného bankéře. Avšak nástup fašismu v Maďarsku ho přinutil odejít do USA, kde od roku 1930 působil na super prestižním Institute for Advanced Studies v Princetonu kde během války pracoval na konstrukci jaderných zbraní, a právě to ho přivedlo k prvním počítačům. Seznámil se podrobně s jejich nedostatky a dokázal na ně reagovat. Na rozdíl od ENIACu, který si "zabojovat" nestihl, přispěli jeho pováleční následníci rozhodující měrou ke konstrukci vodíkové zbraně a stali se tak elektronickými vojáky studené války. Současně však vstoupily počítače i do civilního sektoru. Prvním sériově vyráběným počítačem je model UNIVAC I v roce 1951. Padesátá léta byla ve výpočetní technice spíše érou nadšenců než érou profesionálních firem. Nově vznikající socialistické země včetně té naší se tato éra na dlouhé roky vyhýbala velikým obloukem. Ze západu se kupovat nemohlo a na východě nebylo co.



Obr. č. 53: Eniac **Obr. č. 54:** Univac II

Zdroje: http://www.telesanterno.com/10-febbraio-il-neonato-pesa%E2%80%A6-30-tonnellate-vagisce-il-primo-computer-0210.html
http://www.computermuseum.li/Testpage/UNIVAC-1-FullView-B.htm

Až koncem 60. let k nám byl dovezen sovětský počítač URAL, který byl úspěšně zprovozněn a později URAL II, pro který bylo nutno postavit novou budovu. Počítač neměl žádný operační systém a programoval se ve strojovém kódu tak, že se do formulářů psaly nuly a jedničky. Nejzajímavější byly periferie. Jako vnější paměť používal počítač děrnou pásku – nikoliv papírovou jako u dálnopisů, nýbrž exponovaný

kinofilm s perforací. A vyražení každé dírky vydalo ohlušující ránu. Nejzajímavější byla tiskárna. Základem byl ruský psací stroj. Pod každou klapkou bylo telefonní relé a od kotvy relé vedl přes pružinku ke každé klapce provázek. Když relé přitáhlo, zatáhlo za provázek a klapka vytiskla příslušnou bukvu. Ještě snad zmínka o paměti – stroj měl bubnovou paměť, kam se dalo zaznamenat neuvěřitelných 1024 36 místných dvojkových čísel nebo 2048 instrukcí. Výkon počítače představoval jen nepatrný zlomek toho, co má dnes k dispozici každá sekretářka.

Obr. č. 55: Ural 2

Zdroj: http://www.root.cz/clanky/historie-pocitacu-vyrabenych-v-sssr-2/#k01

Geniální vynález integrovaného obvodu neboli čipu v roce 1958, umožnil nástup nové generace počítačů a byl v konstrukci počítače poprvé využit firmou IBM v dubnu 1964. IBM zahájila třetí generaci počítačů a současně novověk počítačové éry. Přechod k integrovaným obvodům neznamenal jen miniaturizaci a zvýšení výkonu, ale též hospodárnější výrobu a tedy výrazné zlevnění počítačů. Stále však pro jejich provoz bylo potřeba budovat tzv. výpočetní střediska. Srdcem střediska byl sál počítače - veliká klimatizovaná místnost, v níž se nacházel vlastní stroj. Ve středisku obvykle pracovalo několik desítek lidí, specialistů, jako byli operátoři, technici počítače, technici periférií, systémoví a aplikační programátoři. Vlastní uživatelé počítače, kteří na něm chtěli řešit své konkrétní úlohy - například výpočet mezd, vědecké výpočty apod. - komunikovali pouze s obsluhou stroje, a to přesně vymezeným způsobem. Samotný počítač většina uživatelů vůbec nikdy nespatřila. U nás na „východě“ procházel vývoj v podstatě shodnými stádii, ovšem s několikaletým a stále rostoucím zpožděním. V 60. a 70. letech

u nás vzniklo postupně několik výrobních závodů, zaměřených na produkci systémů JSEP a SMEP. Šlo v podstatě o repliky počítačů IBM 360, později 370 a 4341 (řada JSEP) a počítačů HP 1000 (řada SMEP). Vyráběny byly zeměmi RVHP dle technologických možností jednotlivých zemí. Přesto že vycházely z velmi kvalitních, byť většinou již zastaralých vzorů. Problém byl v tom, že s rostoucí technologickou náročností novějších a novějších napodobovaných západních vzorů klesala schopnost východních výrobců dodat součástky i vyšší celky v potřebné kvalitě, takže počítače JSEP i SMEP trpěly vysokou poruchovostí. Vývoj ve světě šel tou dobou ovšem už docela jinudy. Zájem o počítače začal v Americe prudce růst od poloviny 60. let a trh se dožadoval "počítače pro jednoho člověka". Levný počítač, který by si mohl pořídit a provozovat jednotlivec. Rozhodujícím faktorem byl vývoj nových čipů s vyšší hustotou integrace. Kalifornská firma Intel dosáhla jako první hustoty integrace 1000 tranzistorů na čip a v roce 1971vyvinula první mikroprocesor, jenž se stal základem prvních osobních počítačů. Ty však ještě neoslovily široký spotřebitelský trh, šlo o drahé hračky pro domácí kutily, bez běžné klávesnice (ovládaly se vyťukáváním číselných kódů na sadě tlačítek, obvykle demontované z běžné kalkulačky), bez obrazovky (připojovaly se k televizoru), téměř bez praktického využití, navíc stále ještě velice drahé. /19/

Roku 1981 předvedla firma IBM světu svůj první osobní počítač, nazvaný prostě IBM PC (PC - Personal Computer). Tak začala doba "pécéček". IBM se od samého začátku orientovala na profesionálního uživatele, čemuž odpovídal jak výkon IBM PC, tak způsob jeho prodeje. IBM PC zaznamenal drtivý úspěch, a rychle po něm následovaly zdokonalené modely PC/XT (1983) a PC/AT (1984). IBM PC/AT. Z různých důvodů, mezi nimiž největší roli hrála zákonná antimonopolní omezení, IBM nikdy patentově nechránila většinu konstrukčních prvků počítačů PC. Díky tomu mohli další výrobci přijít na trh s tzv. kompatibilními počítači. První firmou vůbec, která zahájila výrobu kompatibilních počítačů, byla společnost Compaq (název odvozen od slov kompatibilita a kvalita). A brzy se výrobci PC počítali na stovky po celém světě.

8.3 Příloha č. 3

Historie internetu

Ne náhodou byl na základě rozsáhlé ankety internet zvolen vynálezem historie, např. před vynálezem knihtisku, očkováním, vynálezem elektřiny a penicilínu. Vše začalo v roce 1945 kdy v červencovém čísle amerického časopisu *The Atlantic Monthly* publikoval *Vannevar Bush* (1890-1974) svůj světoznámý *As We May Think,* jenž bývá považován za jeden ze základních kamenů informační vědy. Tento článek, který se týkal využití počítačů pro komunikaci je zajímavý tím, že byl napsán mnoho let před tím, než byly pro tuto úlohu skutečně poprvé počítače použity.

Rok 1957 přinesl Sputnik – první družici obíhající zemi, která byla vyvinuta v Sovětském Svazu. Na tento fakt reagovala Eisenhowerova vláda v USA založením *Advanced Research Projects Agency* (ARPA) zabývající se speciálním výzkumem.

V roce 1963 definoval *Theodor Holm Nelson* pojem *hypertext* a v roce 1965 jej publikoval. Vynálezce počítačové myši *Dr. Douglas C. Engelbart* měli za sebou první prezentace nástrojů k tvorbě hypertextu. Oba čerpali přímo z teoretických prací Vannevara Bushe, oba jsou jeho bezprostředními následovníky. /32/

První síť

První testovací síť byla instalována počátkem roku 1968 v Národní výzkumné laboratoři ve Velké Británii. Tato síť však neopustila hranice jedné budovy.

Jak už to bývá, přišel požadavek na vybudování podobné sítě a zároveň i potřebné finanční prostředky z resortu obrany, konkrétně od grantové agentury ministerstva obrany USA, s názvem ARPA (Advanced Research Projects Agency). Podle této grantové agentury byla experimentální síť, která vznikla v roce 1969 také pojmenována jako ARPANET. Až do poloviny osmdesátých let se internet nijak zvlášť nerozvíjel, byl omezen především na vládní a vojenské organizace.

V roce 1980 přišel ve švýcarském institutu pro jaderný výzkum CERN *Tim Berners-Lee* s myšlenkou hypertextu, což mělo usnadnit sdílení a aktualizaci informací mezi výzkumníky. V roce 1989 již měl CERN největší internetový server v Evropě a *Tim Berners-Lee* oživil tehdy zapomenutou myšlenku hypertextu. Již v listopadu

roku 1990 předvedl první prototyp WWW serveru jenž pojmenoval jednoduše *httpd* a 6. srpna 1991 na adrese http://info.cern.ch/ spustil první webové stránky. První browser (webový prohlížeč) s názvem *WorldWideWeb* byl zároveň i prvním WYSIWYG HTML editorem. Posléze byl přejmenován na Nexus.

V roce 1984 bylo k internetu připojeno pouhých 1000 počítačů. Velký rozvoj nenastával ani v nejbližších několika letech, nicméně v roce 1992 bylo k internetu připojeno již více než jeden milion počítačů. Nastává moderní doba, která ovlivní chování lidstva – nastává doba internetová.

Rokem 1993 začal internet v USA prožívat nebývalý rozmach, k internetu byl připojen Bílý dům. Byl vyvinut standard WWW, existuje již 50 WWW serverů. Od roku 1993 do roku 1995 se zdvojnásobil počet připojených počítačů k internetu. V roce 1995 je celkem v USA k internetu připojeno na dva milióny počítačů. Na celém světě je odhadováno v roce 1995 na 20 miliónů uživatelů internetu, v roce 2000 již pak přes 300 miliónů. V roce 2010 dle telekomunikační agentury OSN, Hamadoun Toure dosáhl počet uživatelů internetu 2 miliardy. /2/

Institucí, která od poloviny roku 1994 dbá zejména na rozvoj služby WWW, je WWW Consorcium (W3C). Konsorcium sdružuje lidi, kteří se podíleli v ústavu CERN na prvních krůčcích fenoménu jménem WWW . Ředitelem konsorcia není nikdo jiný, než tvůrce WWW Tim Berners-Lee. /33/

Provoz internetu

Internet je celosvětová počítačová síť, která dnes nemá vzhledem ke své rozsáhlosti žádného vlastníka. Oproti tomu, že za provoz internetu není nikdo konkrétně zodpovědný, funguje internet celkem bezproblémově. Internet řídí skupina dobrovolníků, zvaná internet Society (ISOC). Internet Society ustavila podvýbor zvaný internet Architecture Board (IAB), jehož členové vyvíjejí a určují standardy, prostředky, adresy a podobně. Jiná skupina dobrovolníků, pojmenovaná internet Engineering Task Force (IETF), se zabývá běžnými každodenními problémy provozu internetu.

Stejně tak podivně může vypadat způsob financování internetu. Představa, že internet je ze své podstaty zadarmo, je chybná. Udržovat v chodu počítače schopné obsloužit všechny žadatele, stojí velké peníze. A tyto peníze musí někdo zaplatit.

Jednotlivé instituce musí za to, že poskytují informace na internetu, opravdu platit, jako například federální vláda Spojených států, která prostřednictvím nadace National Science Foundation provozuje síť NSFnet. Na druhé straně uživatelé platí měsíční poplatky svému poskytovateli. A na prostřední úrovni poskytovatelé služeb platí za pronájem vysokorychlostních přenosových linek. /33/

Internet v Čechách

Historie českého internetu se začíná psát počátkem roku 1990. V té době ještě v bývalém Československu neexistovala žádná pevná linka kromě telefonních, a tak se první pokusy o vytvoření počítačové sítě děly pomocí komutovaných linek veřejné telefonní sítě. V březnu toho roku se do naší republiky dostává síť FIDO a následně v květnu pak síť EUnet, která propojovala zejména Unixové stanice. Ale už v říjnu roku 1990 k nám přichází síť EARN (European Academic and Research Network). Tato síť už "běhá" po pevných okruzích. Prvním uzlem této sítě byl střediskový počítač IBM 4381, který byl umístěn v Oblastním Výpočetním Centru (OVC) ČVUT v Praze. Přenosová rychlost linky směřující z pražského uzlu do rakouského národního uzlu EARN v Linci byla 9600 bps. (která měla již zmiňovaných 64 kbps), pracovaly všechny ostatní spoje na rychlosti 19,2 kbps. /15/

První experimentální připojení do internetu se uskutečnilo v listopadu 1991 mezi počítačem umístěným na ČVUT v Praze a počítačem Univerzity Jana Keplera v rakouském Linci. Krátce poté, 13. února 1992, se na Fakultě elektrotechnické ČVUT v Praze uspořádalo slavnostní setkání, na němž se oficiálně oznámilo připojení tehdejšího Československa k internetu a pozvaným odborníkům se předvádělo, jak toto připojení funguje. Tento den je proto označován za okamžik, kdy se naše země oficiálně připojila k internetu./15/

Šlo o datový okruh do Lince, který měl kapacitu 19,2 kb/s. Z dnešního pohledu to tedy bylo velmi pomalé připojení, ale jeho historický význam je opravdu mimořádný. K internetu tehdy měla přístup poměrně malá skupina pracovníků ČVUT v Praze. Jednalo se o sálový počítač IBM, který musel být kvůli své robustnosti umístěn v klimatizovaném počítačovém sále se zdvojenou podlahou. Měl obrovský příkon a o jeho provoz se starala skupina asi deseti lidí.

Již v roce 1991 byl podáván návrh na vybudování celorepublikové páteřní sítě. Ta měla propojovat všechna tuzemská akademická centra a dále by pak měly internet rozvádět metropolitní sítě. Na základě tohoto návrhu vnikly v Československu dva projekty na vybudování národních páteřních sítí, slovenské a české, přičemž propojení těchto dvou páteří bylo součástí projektu české strany (konkrétně šlo o spoj vedený z Prahy do Bratislavy) Český projekt dostal jméno FESNET (Federal Educational and Scientific NETwork). V červnu 1992 české ministerstvo školství schválilo projekt a uvolnilo na něj 20 milionů korun. V průběhu roku 1992 se písmeno F v názvu FESNET změnilo na C a tím vlastně vznikl CESNET (Czech Educational and Scientific NETwork). Na Slovensku se souběžně začala budovat siť SANET (Slovak Academic NETwork).

Síť CESNET byla zpočátku realizována hvězdicovou topologií se středovými uzly v Brně a v Praze. Ty byly propojeny pevnou linku o rychlosti 64 kbps. K těmto dvěma uzlům byly připojovány další uzly umístěné v našich akademických městech. Postupně byly připojeny České Budějovice, Hradec Králové, Liberec, Plzeň a další. V březnu roku 1993 byly uzly CESNETu rozmístěny už v 11 městech. Řada z těchto připojení byla realizována pomocí pronajaté pevné telefonní linky. A jaké byly tehdejší přenosové rychlosti? Kromě linky z Prahy do Brna připojena dvěma nezávislými spoji, kvůli zachování konektivity v případě výpadku některé z linek. Také se rozrostl počet linek směřujících za hranice naší země. Z původně jediného spoje vedoucího z Prahy do rakouského Lince byla vytvořena linka Praha-Vídeň. Později přibylo spojení Praha-Amsterodam realizované spojem o rychlosti 64kbps. (A s rozpadem Československa vznikl další zahraniční spoj Praha-Banská Bystrica). Na přelomu let 1994 a 1995 byla komunikační infrastruktura CESNETu v podstatě dobudována a pozornost se přesunula především na zvyšování přenosových rychlostí a s ním související zlepšování spolehlivosti. /15/

CESNET byl původně, jak již bylo řečeno, vybudován jako páteřní síť, která měla sloužit akademickým účelům. Propojeny tedy měly byt hlavně vysoké školy. Postupem času Ministerstvo školství, jako zřizovatel CESNETu rozšířilo jeho mandát i na komerční scénu. To znamená, že nevyužitou kapacitu sítě mohly využívat různé nevýdělečné i výdělečné organizace a ze získaných prostředků mohl pak CESNET

financovat svůj provoz a rozvoj. Tím se CESNET stal současně i poskytovatelem připojení k internetu. Nebyl ovšem jediným.

První čistě komerční firmou, která začala zprostředkovávat připojení k internetu, byla firma COnet, která začala provozovat síť CZnet, jež vznikla z pražského uzlu sítě EUnet. Tato síť disponovala 64kbitovou linkou vedoucí z Prahy do Amsterodamu.

Internetový Boom v zemích českých. Před rokem 1995 měl o internetu v našich zeměpisných šířkách ponětí jenom málokdo. Důvodem byla především výrazná absence komerční sféry na tomto poli. To se začíná měnit na přelomu let 1995 a 1996, kdy na trh vstupuje celá řada komerčních poskytovatelů připojení k internetu. Co bránilo dřívějšímu příchodu komerční scény? Vždyť republika byla v té době k internetu připojena tři roky! Byl to jeden nezanedbatelný fakt, do této doby totiž trval monopol firmy Eurotel, který se vztahoval mimo jiné i na veřejné služby přenosu dat. Pádem tohoto monopolu na sklonku roku 1995 se otevírá široké pole pro komerční využití internetu a s tím spojený rozmach. V roce 2011 bylo v České republice již 5,97 miliónu reálných uživatelů internetu, což je o 360 tisíc více než v roce 2010. /27/

8.4 Příloha č. 4

Možná ohrožení elektronických dat

Elektronická data jsou mnohem více zranitelná než jejich papírová obdoba. Neohrožují je jenom živelní katastrofy jako je tomu u dat papírových, ale i samotné selhání technologií, které slouží pro jejich uchovávání. Není výjimkou selhání magnetických médií, optických disků, pevných disků případně flash disků. S poměrně snadným způsobem kopírování elektronických dat je snadnější způsob zneužití, než tomu je u písemných dat. Zatímco tyto hrozby lze poměrně dobře eliminovat, mnohem větší hrozbou je napadení informačních technologií a v nich uchovaných dat prostřednictvím počítačových sítí, kterými jsou tyto propojeny. Tyto útoky jsou o to nebezpečnější, že mohou být uskutečněny nepozorovaně kdykoli 24h denně, 365dní v roce a navíc téměř anonymně. Vedle ztráty dat tak při útoku, může dojít i k jejich odcizení.

Napadení informačních technologií po sítích

Vnitřní útočník – útočník je většinou řadový zaměstnanec firmy, která byla napadena. Velkou výhodou je jednoduché dohledání útočníka. Kamerový systém nebo systémové zabezpečení v podobě záznamu veškerých aktivit na počítači je velmi efektivní nástroj dohledání útočníka.

Vnější útočník – ti jsou mnohem obtížněji vypátratelní, už jen z důvodu, že mohou operovat prakticky kdekoliv na světě. Při pátrání po vnějších útočnících jsou mnohdy zapojeny i různé státy i bezpečnostní organizace jednotlivých států.

Jestliže chceme hovořit o útocích, pak musíme nejdříve říci, kdo mohou být útočníci. Ty můžeme definovat podle jejich zkušeností, záměru či způsobu prolomení ochrany počítače. Rozlišujeme je do 3 základních typů.

Útočník amatér – ten se nepříliš orientuje v systémech a virech a proto je jeho nebezpečnost minimální. Amatér většinou neumí napsat skript ani vytvořit vir, a pokud prolomí obranu a dostane se do systému, pak je to buď díky tomu, že neobsahuje prakticky žádnou ochranu, nebo příčinou nějaké náhody. Proti útočníkům amatérům většinou stačí i minimální zabezpečení systémů.

Útočník hacker – ten bývá již dobře znalý a vzdělaný v daném oboru a tudíž dokáže vniknout do systémů i přes dobré zabezpečení. Hackeři se většinou rekrutují ze studentů IT oborů. Jsou v převážných případech přeci jenom limitováni časem a prostředky. Hackeři většinou jen sbírají informace, zkušenosti a někteří to berou jako sport. Podmnožinou útočníků hackerů jsou takzvaní crackeři. Zatímco hacker – se snaží dostat do systému prolomením ochrany, není jeho hlavním cílem zničit nebo ukrást informace, spíše jde jen o to dostat se přes zabezpečení. Namísto toho cracker – se zaměřuje hlavně na poškozování subjektů, jejichž systémovou ochranu prolomil. Snaží se tedy zničit, ukrást informace či jinak škodit.

Útočník profesionál – jak už ze samotného názvu vyplývá, jedná se o profesionálně organizovaného útočníka nebo skupiny útočníků, z čehož vyplývá nebezpečnost pro vyhlídnutou potencionální oběť útoku. Útočník profesionál je vysoce kvalifikovaný v IT systémech a velmi dobře se orientuje v HW a SW. Tito útočníci jsou velmi nebezpeční, ale většinou se zaměřují jen na perspektivní systémy, takže koncový uživatel počítače se zas až tak nemusí obávat přímého ohrožení. Tito útočníci bývají většinou součástí zločinné organizace nebo často i různými státy podporovaných skupin určených pro případ vedení kybernetických válek.

Z nejrůznějších médií se však dovídáme, že v podstatě v převážné většině o hackerech neví vůbec nic, anebo jen neúplné informace. Jen tak se dá vysvětlit, proč často zaměňují pojmy "hacker" a "cracker". Hacker v původním významu rozhodně neznamená nějakého člověka, který chce ničit, škodit, krást, atd. Tato činnost je typická právě pro crackery. Cílem hackera je dostat se do cizího systému, stroje apod., ale nikoli s úmyslem někoho anebo něco či nějakou instituci poškodit natož tak cokoli zničit, ale upozornit na bezpečnostní chyby, nedostatky a rizika, jenž objevil právě při průniku do cizího systému. Možná je to málo známé, ale hackeři mají svou etiku. Základní rozdíl je v tom, že hackeři věci vytvářejí a crackeři je ničí. /3/

Hacker má dnes význam velmi odlišný od významu, ve kterém vznikl. Původně se tak označovali programátoři, kteří měli za úkol vyhledávat chyby v systémech a opravovat je tak, aby fungovaly efektivněji a bezchybně. Tyto zásahy v systémech se nazývají v anglickém jazyce slovem „Hack“ a odtud se odvodil název Hacker. Nejranější způsob hacku se ještě netýká počítačových systémů, ale obyčejného

tkalcovského stavu. Datoval se rok 1801 ve Francii, kdy tkadlec Jacquard vymyslel tkalcovský stav natolik automatizovaný, aby potřeboval minimální lidskou sílu.

Masově hack začala používat jedna z protiválečných organizací: Hippies. Jejich vůdce Abbie Hoffmann se dorozumíval se svými kolegy pomocí telefonů, které nikdy nemusel platit. Stejně tak jako John Draper, který roku 1971 zjistil, že dokáže obelstít telefonní ústředny pomoci píšťalky. Pokud píšťalka dokázala vyloudil zvuk o frekvenci 2600 Hz, pak jeho hovor byl zdarma. Dnes nejsou hackeři a crackeři natolik neškodní, jako jejich historičtí předchůdci. /25/

Script Kiddies – jsou neuznávanými v hackerské komunitě a spíše jsou považovány za atrapy a špatné hackery. Obvykle využívají existující a dobře známé metody, jež využívají k získání neoprávněného přístupu k počítačovým systémům a nesnaží se implementovat vlastní kód. A jak tento hacker funguje? Využívá toho, že většina lidí si ani neuvědomuje možné dopady svého chování na internetu. Ti často rychle zjistí, že stahování souborů z volných webových stránek je obecně nepříliš dobrý nápad, protože tyto stažené programy mají často destruktivní doplňky. Nevědomky si potom na svém PC zajistí spuštění nechtěného kódu, který jim přidá například účet root do místního systému a je možné obejít zabezpečení pomocí hesla.

White hat – hacker, který zastává původní smysl hacku. Hledá chybu v systémech a upozorní na ni, případně ji opraví. Nicméně nikdy nezneužívá svého postavení a nenapadá servery nebo webové hostingy. Je vnímán jako etický hacker, a je v oblasti informačních technologií osoba, která je eticky proti zneužívání počítačových systémů. Uvědomění si, že internet dnes spojuje lidi z celého světa a dělá vše na obranu jeho integrity. White hat se obecně zaměřuje na zajištění bezpečnosti IT systémů, zatímco Black hat (opak) by chtěl proniknout do nich. Je také velmi často popisován jako ten, který se snaží proniknout do systémů nebo sítí s cílem pomoci majitelům systému tím, že je upozorní na bezpečnostní nedostatky. Mnoho takových lidí je zaměstnáno u firem pro počítačovou bezpečnost. Základní rozdíl mezi Black a White hat hackery je to, že White hats hacker tvrdí, že se drží etických zásad. Stejně jako Black hat i White hat je často důvěrně obeznámen s vnitřními detaily bezpečnostních systémů, a může se vlámat do tajů strojového kódu, když potřebuje najít řešení

na složité problémy. Některé zdroje používají termín Gray hats a označují tím někoho kdo se nachází na rozhraní mezi Black a White. /4/

Gray hat – zastává názor, že zveřejnění informací o chybě v systému napomáhá jeho bezpečnosti. Je to hacker, který je většinou jsou mezi „dobrým“ a „zlým“ hackerem. Ve společenství počítačové bezpečnosti, se definuje jako zručný hacker, který někdy působí legálně, někdy v dobré víře, a někdy nelegálně . Jedná se o hybrid mezi Black a White hats. Obvykle nemá osobní zisk nebo nemá nekalé úmysly, ale může, i když nemusí občas páchat trestnou činnost v průběhu jejich činnosti. Provádí pronikání do systémů nepozorovaně a ukončí tuto činnost ještě před zjištěním s minimálními škody. V důsledku toho Grey hats má tendenci provádět činnosti, jako je testování, monitoring, nebo méně destruktivní způsoby přenosu dat a vyhledávání. Osoba, která pronikne do počítačového systému a jednoduše vloží své jméno, že při tom nedošlo k poškození. /5/

Black hat – kriminální hacker, kterého zajímá vlastní obohacení. Black hat je člověk, který ohrožuje bezpečnost počítačového systému bez souhlasu oprávněné osoby, typicky s nepřátelskými úmysly. Obvykle Black hat je osoba, která využívá své znalosti využívá zranitelnosti spíše pro soukromý zisk, než odhalování zranitelnosti systémů. Black hat se mnohdy snaží rozšířit díry v systémech, a nečiní žádné pokusy o opravu software aby zabránil ostatním, také ohrozit systém, nad nímž již získal bezpečnou kontrolu. /6/

Metody útoků na Informační technologie. Techniky pro vloupání do systému můžou zahrnovat pokročilé programovací schopnosti a sociální inženýrství, ale častěji se jednoduše použije poloautomatických software. Software využívající slabé stránky systému např: buffer overflow, integer overflow, poškození paměti, útoky formátovacím řetězcem, cross-site scripting, cross-site, vpravení kódu a SQL vpravení chyby apod.

DoS, DDoS útoky. DoS(Denial of Service) je jeden z nejčastějších typů útoků. Dochází při něm k zahlcení programů, počítače či celých počítačových systémů a sítí a dojde tak k vyčerpání zdrojů, které jsou určeny k běžnému chodu. DoS se od DDoS (Distributed Denial of Service) liší tím, že napadá pouze jeden počítač, jedná se tedy o primitivnější útok, který lze poměrně snadno zastavit tím, že napadený systém odstaví

napadenou část. DDoS útok je sofistikovanější. Využívá při útoku soustavu mnoha počítačů a počítačových sítí, kdy každý z počítačů má svoji roli a útok je koordinován.

Buffer overflow, neboli „přetečení zásobníku“ je způsob napadení operačních systémů, kdy se využije chyba programátora systému a zaútočí se na zásobníky. Tyto zásobníky operační systém využívá k odkládání dočasných dat, pokud je zásobník přeplněn, systém, nebo jeho části, přestává fungovat.

Útoky přes WWW. Tyto útoky využívají především databáze, kdy přes SQL Injection hacker vloží přes nechráněný vstup do databáze svůj vlastní kód. Jakmile je kód do databáze vložen, může data jakkoliv upravovat, mazat či vynášet. Tento způsob útoku využívá chyby programátora databáze.

Trojský kůň je typ malware, který se dostane do počítače a po jeho spuštění odstaví firewall, antivirové programy, rezidentní štíty, anti-spyware programy a podobně. Po odstavení ochran počítače posílá přes internet zprávu hackerovi či dalším virům, kde pak dojde ke specifickému útoku.

Spyware. Tento typ programu, infiltrace do počítače (velmi často po napadení trojským koněm) shromažďuje osobní data či hesla a odesílá je pomocí internetu pryč. Spyware – sleduje činnosti uživatele programu a neustále odesílá přes internet potřebné informace tvůrci. Dnes mnoho freeware aplikací obsahuje právě Spyware. V dnešní době se spyware rozšiřuje právě hlavně přes internet a využívá chyb v prohlížečích internetových aplikací, které umožňují instalaci programu bez akceptování uživatele. Projevem programu může být zpomalení počítače. Do kategorie spyware jsou umístěny následující programy.

Phishing – princip útoku je, že útočník kontaktuje osobu (uživatele) přes e-mail a vydává se za známou organizaci, jako jsou banky, administrátoři apod. Celé snažení útočníka je zaměřené na získání důležitých či osobních informací, aby uživateli mohl vykrást bankovní konto. Nejznámějším incidentem byla kauza Citibank, kde Vladimir Levin roku 1997 ukradl z kont uživatelů Citibank celých 10,7 miliard korun českých.

Vishig – dnes mnohem rozšířenější odrůda phishingu. Princip tohoto útoku spočívá rovněž v poslání e-mailové pošty, která vypadá jako od důvěryhodné instituce (administrator, banka, úřad apod.) a v ní je uvedeno telefonní číslo. Další komunikace mezi útočníkem a obětí je osobní přes telefon. Tímto způsobem nic netušící oběť začne

důvěřovat útočníkovi a po pár dobrých radách při opravě systému, které většinou zapříčiní útočník viry, je někdy i ochotna prozradit osobní informace.

Viry jsou široká skupina programů, které škodí operačnímu systému, mažou data, upravují je, mohou dokonce ničit hardware například pomocí přepětí nebo nestandardními příkazy pro ovládání například pevných disků či optických mechanik. Jsou primárním nebezpečím, které bezprostředně ohrožuje data každého uživatele PC. Každý uživatel počítače mněl dbát na co nejlepší ochranu svých dat pomocí specifických programů - antivirů. V praxi bývá tato situace mnohdy podceňována především z důvodů nízké počítačové gramotnosti většinových uživatelů. V organizaci je situace o mnoho lepší, neboť se o tuto problematiku starají IT odborníci. Viry můžeme rozdělit na 4 druhy.

- *Klasické viry* – ty infikují soubor, a pokud je antivir nenalezne, pak se začnou šířit do celého systému. Jsou velmi podobní biologickým virům.
- *Bootovací viry* – viry jsou umístěné v bootovací části počítače a spouští se vždy při načítání systému v počítači.
- *Stealth viry* – jsou takové, které nejsou vidět v seznamu procesů a díky tomu jsou těžce dohledatelnými.
- *Polymorfní viry* – jejich zdrojový kód obsahuje náhodně generované části a díky nim je pro antivirový program velmi těžké nalézt a zničit vir.

Zvláštní skupinu tvoří Spam – ten není počítačovým virem v pravém slova smyslu, ale jde o nevyžádanou poštu, která při velkém objemu znepříjemňuje práci uživatele PC. V rámci České republiky spam upravuje zákon č. 480/2004 o některých službách informační společnosti v platném znění. Tento zákon upravuje fakt, že nezákonný spam je pouze ten, který uživatel předem neodsouhlasil. Dělíme tedy Spam do 2 kategorií:

Opt-in – je uzákoněn v českém zákoníku jako zákon č. 480/2004, kde se říká, že nikdo nesmí zasílat spam bez povolení.

Opt-out – patří do zákonů USA, kdy uživateli mohou posílat veškeré spamy automaticky. Pokud koncový uživatel již nechce pobírat spam, pak musí sám napsat a požádat o zamezení zasílání spamu. Až tehdy je spam nezákonný.

Nové hrozby

Informační technologie a zejména pak právě počítačové sítě umožnili vzniknout novým hrozbám, o kterých jsme neměli před několika desítkami let ani tušení. Vedle nejrůznějších forem kriminality, kterou zejména celosvětová síť internet umožňuje páchat je to přímé ohrožení dat a technologií a technologických procesů.

Kyberprostor. Termín kyberprostor se používá pro označení virtuálního světa vytvářeného moderními technologiemi, tj. počítači, telekomunikačními sítěmi paralelně ke světu „reálnému". Kybernetická kriminalita jako termín, vychází z anglického překladu Cybercrime. Jedná se o kriminalitu, odehrávající se v kyberprostoru, což je virtuální svět vytvořený moderními technologickými prostředky např. počítači. V současné době jedinci nebo organizované skupiny, které mohou chtít prolomit nějakou ochranu dat, neustále zdokonalují dešifrovací techniku. Neustálá evoluce v tomto odvětví je zapříčiněna a také omezena vývojem v oblasti ICT (Information and Communication Technologies). Mezi nejznámější kybernetické zločiny patří incident z 27. dubna v roce 2007 v Estonsku, kdy bylo zcizeno velké množství dat z výzkumné agentury NASA. Hackeři nejčastěji využívají nepozornosti uživatelů, či slabě zabezpečených infrastruktur, jako tomu bylo v Estonsku. Dnes již není problém falšovat e-mailové adresy, jména, což umožňují dnešní sociální sítě na internetu, apod. Kybernetická kriminalita je nový jev, který se dostává stále více a více do popředí nejen díky způsobeným škodám a ztrátám, které jsou značné, ale hlavně obtížná zjistitelnost pachatelů, která jim zajišťuje určité bezpečí. Česká republika má státní agenturu, jejímž hlavním úkolem je odhalovat pachatele útoků a pomoci při jejich eliminaci. Nazývá se BIS (Bezpečnostní informační služba). Podle zákona o zpravodajských službách ČR (č. 153/1994 Sb.) se BIS zabývá získáváním, shromažďováním a vyhodnocováním následujících informací:

- Hrozby terorismu
- Aktivity ohrožující bezpečnost nebo významné ekonomické zájmy státu
- Činnost cizích zpravodajských služeb na našem území
- Záměry nebo činy mířící proti demokratickým základům, svrchovanosti a územní celistvosti ČR
- Aktivity organizovaného zločinu

- Činnosti ohrožující utajované informace

Velice často skloňovaný název v souvislosti s kybernetickou kriminalitou je kybernetický terorismus. Účastníci mohou být jednotlivci, sub-státní systémy, tajní agenti a spekuluje se i o infiltraci státní moci do tohoto odvětví. Cíle kybernetického terorismu jsou různé, nejčastěji se zaměřují na získávání informací nebo podkopávání infrastruktury daného státu. Uvažuje se možnosti existence incidentu, který se nazývá Kybernetická válka (cyber war). Kybernetická válka je izolována od širšího konfliktu, odvíjí se v prostředí zcela odlišném od tradičního vedení boje a nabízí nekrvavou alternativu nebezpečí a nákladnosti moderní války.

V dnešní době mnoho států jako je třeba USA, Francie, Velká Británie investuje významné částky do zlepšení a ochrany infrastruktury a obchodů v zemi před možnými útoky. Federální vláda USA v roce 2010 spustila program, který se nazývá „Perfektní občan“. Tento program by měl detekovat veškeré pokusy i úspěšné útoky na soukromé podnikatelské subjekty, ale i na státní úřady a státní firmy, které mohou představovat potencionální nebezpečí pro občany, jako jsou jaderné elektrárny apod. Smlouvu na celkem 100 miliónů dolarů získala ve veřejné soutěži firma Raytheon Corp. Cílem programu je vytvořit celostátní databázi útoků a následně instituce, které budou mít přístup k daným informacím. Díky tomu budou moci zefektivnit bezpečnost a ochranu dat.

Rok 2012 - Začátek kybernetické války? Americká vláda sepsala zákony SOPA (Stop On-line Piracy Act), PIPA (Protect IP Act) a ACTA (Anti-Counterfeiting Trade Agreement), které by měly pomoci chránit duševní vlastnictví, ale to za cenu negativního dopadu na celý internet v podobě svobody a nezávislosti. To se nelíbilo mnohým internetovým firmám jako třeba anglické Wikipedii či Googlu a 18. ledna 2012 protestovaly. Den nato přišel šok a vláda brutálním způsobem zrušila službu na sdílení dat MegaUpload a pozatýkala šéfa a šest akcionářů. Internet se vzbouřil a v čele se skupinou Anonymous začaly útoky na různé státní instituce.

Vzbouření proti zákonům SOPA, PIPA a ACTA. 18. 1. 2012 zahájily protestní akci proti americkým zákonům SOPA a PIPA. Anglická Wikipedie nahradila své stránky protestním oznámením a znemožnila tak přístup k největší internetové encyklopedii. Do protestů se zapojily i společnosti jako Google, Firefox a další. Co by

znamenalo prosazení jednoho ze dvou zákonů pro internet si ukážeme na příkladu, který byl publikován na webu cn130.com. Kdyby zákon platil a vy byste například hodili kamarádům na sociální síť odkaz na nový film, tak byste se nejen vy dopustili trestného činu (přestupku), ale také:

- Facebook (který tomu měl zabránit)
- Váš provozovatel internetu (měl vám znemožnit přístup ke stránce s nelegálním obsahem)
- Provozovatel hostingu, kde byl film umístěn (měl si to pohlídat)
- Google či Seznam, přes který jste film našli
- Reklamy na stránce (pomáhají financovat nelegální činnost)
- Banka, přes kterou jste zaplatili možnost pro rychlejší stahování (pomáhá financovat nelegální činnost)
- A spousta dalších, co o tom nevěděli, ale měli vědět – třeba elektřina.

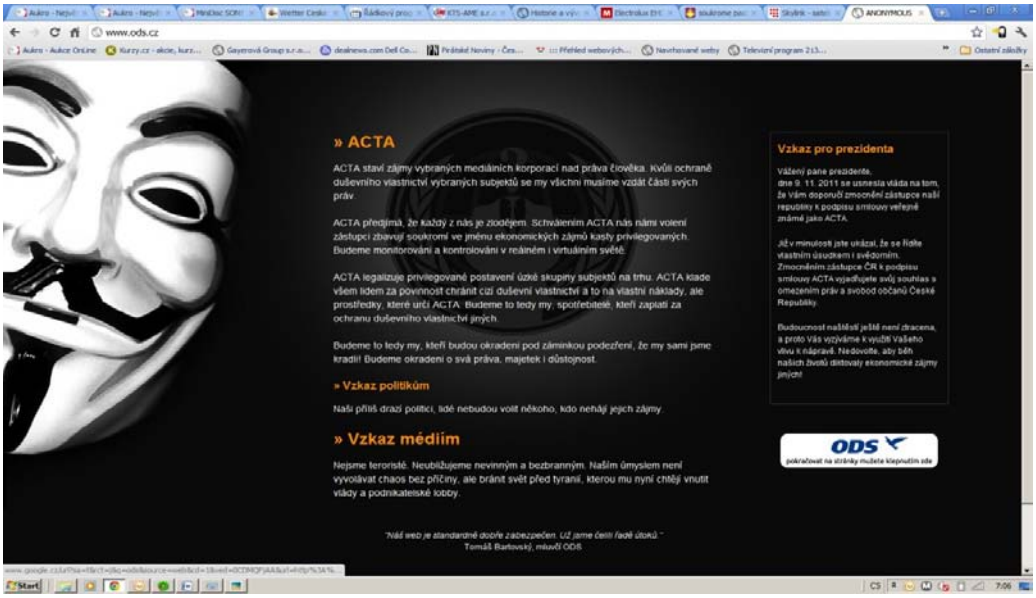
Zákony podporovali především vydavatelé filmového a hudebního průmyslu a další firmy využívající autorské právo, které díky internetu přicházejí o velké množství zisků (CNN, Nike, RIAA nebo News Corporation). Naopak zákony nepodporovaly mnohé společnosti, jejichž byznys je postaven především na internetu (Apple, Google, Microsoft, Zynga, Facebook či Mozzila). Zdá se, že opozice byla silnější a protesty proti SOPA (Stop On-line Piracy Act) a PIPA zafungovaly - senátoři ruší jejich projednávání. Americká vláda však den po protestu udělala něco, proti čemu se vzbouřil doslova celý internet. Brutální odstřihnutí MegaUpload.com a zatčení jejich šéfů. Den po protestu, tedy 19. 1. 2012 americká vláda brutálně zrušila největší službu ke sdílení dat Mega Upload.com a zatkla zakladatele Kima Dotcoma (Kim Schmitz) a dalších šest společníků (mezi kterými byl i slovenský grafik). Rovněž byl zabaven majetek v odhadované výši 50 milionů dolarů. MegaUpload.com byl 15. nejnavštěvovanějším serverem na světě a od roku 2005 si přišel na pěkných 175 milionů dolarů, přičemž údajně způsobil škodu za půl miliardy USD. Pro srovnání MegaUpload vygeneroval ročně 42 milionů dolarů, zatímco největší český portál ke sdílení dat Ulož.to generuje v zisku zhruba jen 4 miliony korun.

Obr. č. 56: Zablokovaná stránka

Zdroj: megaupload.com

Tento zásah byl plánován určitě na několik měsíců dopředu, neboť se do protestu zapojily i policejní složky ze zemí jako Hong Kong, Nizozemí, Anglie a tak dále. Můžeme se tedy jen domnívat, zda byl zásah den po protestu pouhou náhodou nebo promyšleným tahem, jak navodit strach. Každopádně to vedlo tak trochu k největší kybernetické „válce“.

První kybernetická válka – Anonymous proti vládě. Anonymous je skupina hackerů, která pomocí DDoS útoků shazuje weby.



Obr. č. 57: Zablokovaná stránka ODS

Zdroj: http://www.ods.cz/

Napadené nebyly jen americké weby, ale také už i některé evropské země. Útoky postily třeba Polsko, neboť se chystaly podepsat dohodu o duševním vlastnictvím boje proti pirátství ACTA. Střídavě tak vypadávaly polské weby důležitých státních institucí. Odstaven byl i web francouzského prezidenta Sarkozyho, který pochválil Američany za odstavení služby MegaUploadu. /13/ Anonymous napadly i český web České protipirátské unie.

Pokračování útoků Anonymous.

5.února opět zaútočili na web ODS a zmocnili se osobních údajů 30 tis. členů politické strany ODS.

3. února – Polsko odložilo ratifikaci ACTA

6. února- Česká republika odložila ratifikaci ACTA

10. února-Německo pozastavilo ratifikaci ACTA

14.února-Bulharsko pozastavilo ratifikaci ACTA

15.února-Chorvatsko a Nizozemsko pozastavilo ratifikaci ACTA

17. února. 2012 server ZDNet.com hlásil hacknutí tří webů consumer.gov, ncpw.gov a business.ftc.gov. Anonymous napadení zdůvodnili nesouhlasem s ratifikací dohody ACTA, kterou vláda USA připravila spolu s dalšími zeměmi, zároveň vyhrožují dalšími odvetnými akcemi, pokud bude dohoda ACTA podepsána ostatními státy. /17/

8.5 Příloha č. 5

RAID pole

Disková pole byla zkonstruována, především pro zvýšení bezpečnosti ukládání dat na pevných discích. Dalším důvodem použití pole je vytvoření větší diskové kapacity, než se vyrábí v podobě samostatného disku. Pole se ve zkratce nazývají RAID. Nejprve to znamenalo Redundant Array of Inexpensive Disks, dnes se zkratka překládá spíše jako Redundant Array of Independent Disks.

RAID pole je složeno z obyčejných sériově vyráběných pevných disků, které nejsou nijak upravovány. Technologie RAID prošla postupným vývojem, kdy byly zjištěné nedostatky odstraňovány nebo bylo odlišným přístupem dosaženo vyššího výkonu výsledného RAID pole.

Odlišné způsoby ukládání dat jsou realizovány buď softwarově nebo hardwarově. V softwarovém řešení obsluhuje zápis do pole RAID operační systém (resp. speciální mezivrstva nebo přímo ovladač zařízení) a proto se jedná o nejlevnější řešení, které však trpí některými nedostatky, jako např. snížení rychlosti. Hardwarové řešení tyto nedostatky odstraňuje pomocí speciálního zařízení řadiče, který obstarává obsluhu RAID sám a hlavní procesor počítače tak není zatěžován. Problémem je, že většina lacinějších RAID řadičů na trhu je ve skutečnosti softwarově řízena, takže se o hardwarové řešení nejedná.

Pokud dojde při provozu RAID pole k výpadku některého disku resp. členu pole, dostane se pole do tzv. *degradovaného stavu,* ve kterém je jeho výkon typicky nižší, avšak stále jsou všechna uložená data k dispozici. Správce počítače vymění havarovaný disk za nový a ten začlení zpět do pole, čímž začne tak zvaná *rekonstrukce* pole, při které jsou dopočítány chybějící údaje a zapsány na nový disk. Data jsou typicky během rekonstrukce stále přístupná. Po dokončení rekonstrukce je RAID pole opět tak zvaně *synchronizováno*. Někdy je v poli trvale k dispozici rezervní disk, takže rekonstrukce pole může být zahájena zcela automaticky.

RAID pole vytváří logický (virtuální) úložný prostor, se kterým se dá typicky pracovat stejným způsobem, jako by to byl jediný pevný disk. Jednotlivé disky v poli nazýváme *členy pole*. Implementace RAID pole je typicky taková, že data

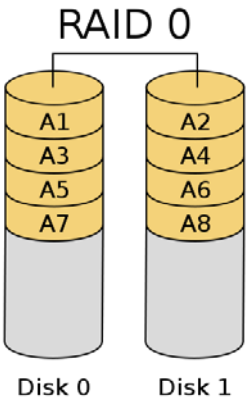
na degradovaném nebo právě rekonstruovaném poli jsou stále k dispozici, i když obvykle se sníženým výkonem (rychlostí čtení a zápisu).

Častou chybou je považování RAID pole za zálohování dat. Skutečná záloha však vyžaduje doplňující operace. Uložení dat na bezpečné místo, jejich fyzické zabezpečení, šifrování zálohy, možnost návratu ke starší verzi dat apod. Proto není možné při používání RAID pole samotné zálohování vyloučit.

Druhy Raid polí:

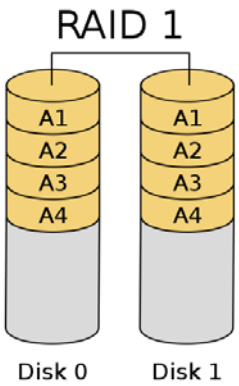
RAID-0

Stripe. Data se rozmisťují střídavě po všech discích z pole, chybí redundance - ztráta jednoho disku znamená ztrátu všech dat z pole. Výkon je ze všech typů RAID nejlepší, kapacita pole je rovna počtu disků. Důvodem použití je výkon, tedy zvýšení přenosové rychlosti nebo propustnosti dat tam, kde na uchování dat nezáleží tak, jako na rychlosti, například při stříhání videa. Toto pole se nepoužívá se k ochraně dat, ale ke zvýšení kapacity.



Obr. č. 58: RAID 0

Zdroj: https://www.computerscience1.net/RAID



Obr. č. 59: RAID 1

Zdroj: https://www.computerscience1.net/RAID

RAID-1

Zrcadlení. Data se zrcadlí na všechny disky z pole. Kapacita pole je rovna velikosti nejmenšího disku. Čtení z pole je rychlejší (lze číst najednou z více disků), zápis je pomalejší (zapisuje se na všechny disky současně). Pole udrží data při selhání

n-1 disků (kde n je počet disků v poli). Je známé zrcadlení, kdy se na dva disky stejných kapacit ukládají totožné informace, a při výpadku jednoho disku se bez přerušení pokračuje v činnosti. Jednoduchá implementace, často čistě softwarová, zato je potřeba 100% diskové kapacity navíc. Z hlediska výkonu pomalejší zápis (zapisuje se 2x), rychlejší čtení (řadič může střídat požadavky mezi disky, "rozdávat práci"). Použití tohoto řešení je nejjednodušší způsob zabezpečení dat zejména u serverů.

RAID-5

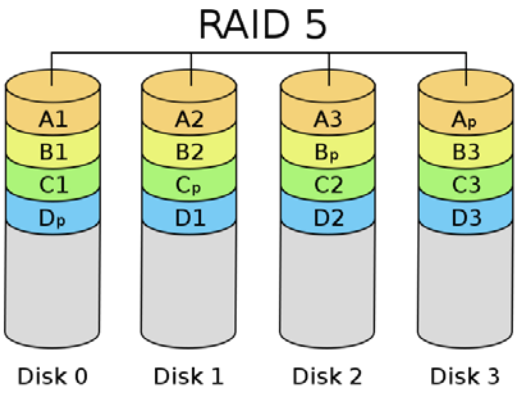
Redundantní pole s distribuovanou paritou. Minimální počet disků jsou 3. Režie je 1 disk z n-diskového pole. Máme-li například pole RAID-5 z 5 disků o kapacitě 36 GB, užitečná kapacita je 4x36=144 GB a 1 disk je režie. Data se zapisují postupně na disky 0,1... až na poslední disk se zapíše parita. Při výpadku některého disku pak máme buď všechna data (a nepotřebujeme paritu), nebo máme část dat a paritu a chybějící data ze ztraceného disku umíme dopočítat z dat, která máme a parity. Výkon při čtení je dobrý, zápis je pomalejší. RAID-5 je pole, kde data jsou distribuovány mezi tři disky minimálně, přičemž kapacita pole je rovna součtu dvou disků. Zbytková kapacita je využita pro kontrolní součty operace eXclusive-OR exkluzivní nebo která je vypočítána takto:

data 1	0011
data 2	0101
výsledek XOR	**0110**

Obr. č. 60: Kontrolní součty Raid 5

Zdroj: Vlastní

Při poruše jednoho z disků je možné zpětně dopočítat, jaká data obsahoval. Pokud například víme, že jedna z hodnot je 0 a druhá 1 (nezávisle na pořadí), je jasné, že třetí hodnota musí být 1 (0 XOR 1 = 1). Logická operace XOR prováděná na několikabajtovém rozsahu je jednoduchá, umí jí spočítat každý procesor.

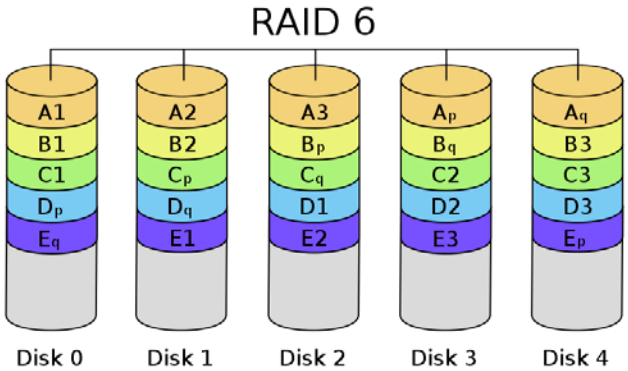


Obr. č. 61: RAID-5

Zdroj: http://en.wikipedia.org/wiki/File:RAID_5.svg

RAID-6

Je pole typu RAID-5 ještě s jedním paritním diskem navíc. Minimem jsou čtyři disky. Paritní blok není jeden, ale dva. Pole je odolné proti výpadku dvou disků. Důvodem použití je ta skutečnost, že při obrovských kapacitách dnešních disků trvá rekonstrukce pole při výpadku disku dosti dlouho, a po dobu rekonstrukce již pole není chráněno proti výpadku dalšího disku. Navíc se u RAID-5 může stát, že právě při rekonstrukci, kdy se kvůli rekonstrukci chybějících dat čtou kompletní povrchy všech zbývajících disků pole, se na některém z těchto disků narazí na chybu čtení, která se dosud v provozu nemusela projevit, řadič takový disk taktéž odpojí a neštěstí je hotovo - úplná ztráta dat celého pole. Výkon RAIDu 6 je podobný jako výkon RAIDu 5, náročnost na výpočetní výkon je ovšem o něco vyšší (počítají se dva paritní bloky).

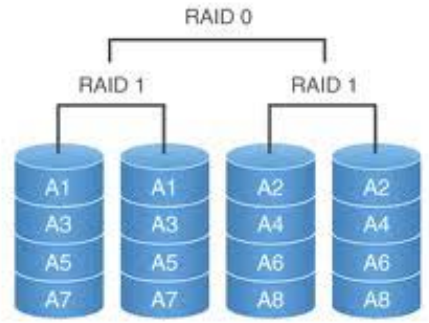


Obr. č. 62: RAID-6

Zdroj: http://en.wikipedia.org/wiki/File:RAID_6.svg

RAID-10

Je kombinace RAID-0 (stripe) a RAID-1 (zrcadlo). Jedná se vlastně o zrcadlený stripe. Minimální počet disků 4, režie 100% diskové kapacity navíc. Poskytuje nejvyšší výkon v bezpečných typech polí, podstatně rychlejší než RAID-5 zejména při zápisu. Další výhodou je odolnost proti ztrátě až 50% disků (naproti tomu RAID-5 odolává ztrátě pouze jednoho disku). /7/



Obr. č. 63: RAID-10

Zdroj: Vlastní