Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

Zálohování a zabezpečení dat v internetovém obchodě

David Vomáčko

Bakalářská práce

2017

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2016/2017**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**David Vomáčko**
Osobní číslo:	**E14221**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Zálohování a zabezpečení dat v internetovém obchodě**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Cílem práce je prezentovat současné technologie zaměřené na zálohování a zabezpečení dat v internetových obchodech. Součástí práce je analýza současného stavu a návrh řešení pro vybranou internetovou firmu.

Osnova:

- Definice základních pojmů k problematice
- Technologie zaměřené na zálohování a zabezpečení dat v e-shopu
- Analýza současného stavu vybraného e-shopu
- Návrh aplikace vybraných technologií v praxi

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 35 stran**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

DOBDA, Luboš. Ochrana dat v informačních systémech. Vyd. 1. Praha: Grada, 1998. ISBN 80-716-9479-7.
DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno: Computer Press, 2004. ISBN 80-251-0106-1.
LÁTAL, Ivo. Ochrana informací, dat a počítačových systémů. 1. vyd. Brno: Eurounion, 1996. ISBN 80-858-5832-0.
PŘIBYL, Jiří a Jindřich KODL. Ochrana dat v informatice: podrobný průvodce tvorbou a správou webů. Vyd. 1. Praha: České vysoké učení technické, 1996. ISBN 80-010-1664-1.

Vedoucí bakalářské práce: **Ing. Renáta Bílková, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **4. září 2016**

Termín odevzdání bakalářské práce: **28. dubna 2017**

doc. Ing. Roman Provazníková, Ph.D.
děkanka

L.S.

doc. Ing. Pavel Petr, Ph.D.
vedoucí ústavu

V Pardubicích dne 4. září 2016

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako Školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 27. 4. 2017 David Vomáčko

ANOTACE

Cílem práce je popsat současné technologie zaměřené na zálohování a zabezpečení dat v internetových obchodech. Součástí práce je zároveň analýza současného stavu bezpečnosti a návrh řešení pro internetový obchod bazenpro.cz společnosti Brück AM.

KLÍČOVÁ SLOVA

Zálohování, zabezpečení, internetový obchod

TITLE

Backup and data security within the internet store

ANNOTATION

The goal is to describe current technologies focused on backup and data security within internet store. Part of the work is focused on analyzing actual state and proposing solution for internet store bazenpro.cz of a company Brück AM.

KEYWORDS

Backup, data security, internet store

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK

CCTV	Closed Circuit Television
CD	Compact Disc
CPU	Central processing unit
DMA	Direct memory access
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DVD	Digital Versatile Disc
EPS	Elektronická požární signalizace
EZS	Elektronická zabezpečovací signalizace
GB	GigaByte
HDD	Hard disk drive
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
Hz	Herz
I O	Input Output
IS	Informační systém
ISP	Internet service provider
Kb	Kilobyte
MB	Megabyte
MZS	Mechanické zábranné systémy
RAID	Redundant Arrays of Inexpensive Disks
SSL	Secure Sockets Layer
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus

Úvod

V dnešní době se internetové obchody staly nedílnou součástí života. Stále více zákazníků volí pohodlný nákup z domova. Ovšem s rozšířením každé služby se vždy najde někdo, kdo této situace chce zneužít ve svůj prospěch. Je tedy třeba dbát na bezpečnost dat, která v rámci internetového obchodu vznikají, jsou přenášena a skladována.

Problematika zabezpečení dat je velmi rozsáhlá a zahrnuje v sobě celou řadu relativně samostatných okruhů. Hlavními nároky na bezpečnost dat je zajištění jejich dostupnosti, důvěrnosti a integrity. K zajištění těchto nároků jsou využívány bezpečnostní mechanismy, které se dají rozdělit na čtyři kategorie: fyzického charakteru, logického charakteru, technického charakteru a administrativního charakteru. S problematikou zabezpečení dat úzce souvisí i jejich zálohování, mechanismus, při kterém jsou vybraná data ukládána na jiné médium, vzniká tedy jejich kopie, která se v případě poškození dat využije k jejich obnovení.

První část práce je zaměřena na zabezpečení dat v rámci jednotlivých charakterů přístupu k bezpečnosti dat, konkrétně tedy fyzického, logického, technického a administrativního. V rámci fyzické ochrany dat se práce zaměří na jejich ochranu před přírodními vlivy, požáry, nepovolanými osobami a před poruchami elektrické sítě. Logická ochrana dat bude popisovat především problematiku přístupu k informacím, jejich dostupnosti pro jednotlivé uživatele, techniky řízení a administraci těchto technik. Technická ochrana se bude zabývat především zajištěním dostupnosti a integrity, tj. neporušenosti dat. K tomuto se využívají disková pole RAID, která skrze redundantní (nadbytečná) data zajišťují neporušenost dat v případě poruchy paměťového média, především tedy pevného disku. Administrativní ochrana dat je definována způsoby, postupy a procedurami, které je nutné dodržovat pro udržení bezpečnosti IS, obsahuje také postupy práce, pokud se objeví problémy, především činnost v případě bezpečnostního incidentu.

Další část bude věnována zálohování dat, zejména nejčastějším médiím, která jsou k zálohování využívána. Rozdělena budou na přenosná média, disková pole a na internetové úložiště.

Závěr práce se zaměří na analýzu současného stavu zabezpečení dat v internetovém obchodě bazenpro.cz. Součástí bude i návrh řešení pro zlepšení bezpečnosti dat v rámci samotného obchodu a společnosti obchod vlastnící.

Cílem práce je tedy popsat současné technologie sloužící k zabezpečení a zálohování dat, současně s analýzou stavu zabezpečení a návrhem na zlepšení pro vybranou společnost.

1 ZABEZPEČENÍ DAT

V současné době má mnoho firem, ale i jednotlivců, svá data uložená ve formě počítačových souborů, které se nacházejí na pevném disku, ke kterému je možné přistupovat různými způsoby.

Hlavní požadavky na bezpečnost dat jsou:

Důvěrnost = požadavek, aby byla data dostupná pouze těm, kteří jsou k tomu oprávněni

Dostupnost = požadavek, aby byla data dostupná oprávněným osobám v okamžiku potřeby

Integrita = požadavek, aby byla data správná a úplná, aby tedy nedošlo k jejich modifikaci neoprávněnou osobou

K zajištění těchto požadavků jsou využívány bezpečnostní mechanismy, které můžeme rozdělit na 4 kategorie: fyzického charakteru, logického charakteru, technického charakteru a administrativního charakteru. [1]

1.1 Fyzická ochrana dat

Fyzická bezpečnost se zabývá především zabezpečením budov, ve kterých se data nacházejí, ochranou před přírodními vlivy a opatřeními proti neoprávněnému vniknutí osob do objektů. Dále se zabývá bezpečným uložením datových nosičů s informacemi a tiskových výstupů, způsoby ničení již nepotřebných informací a médií, ochranou proti požáru a vodě. Dalším velmi důležitým aspektem je zajištění nepřetržité dodávky stabilizované elektrické energie. Cílem fyzické ochrany je eliminace případné hrozby ještě dříve, než přijde do přímého kontaktu s vlastním výpočetním systémem. [2]

1.1.1 Přírodní vlivy

Přírodní katastrofy jsou charakteristické především tím, že jim nelze předcházet a zabránit jejich vzniku. Můžeme se pouze snažit včas je zjišťovat a soustředit se na snížení a omezení jejich možného dopadu a na rychlé odstranění případných nepříznivých následků. V naší zeměpisné oblasti naštěstí katastrofy typu zemětřesení nehrozí, což se ovšem nedá říct o povětrnostních vlivech. Vichřice se sice vyskytují nepatrně, avšak škody, které způsobí, většinou vyžadují vysoké náklady na odstranění. Je tedy vhodné volit vhodný způsob pojištění.

Záplavy jsou další přírodní hrozbou, která může firmu potkat a musí být vzata do úvahy již ve fázi návrhu objektu. Zde mohou být realizována jednak preventivní opatření a jednak systém

detektorů přítomnosti vody a zvýšené vlhkosti. Katastrofy způsobené vodou mohou být v podstatě dvou druhů:

Povodně – či obecněji stoupající voda. Jestliže majitel sleduje meteorologickou situaci, má zpravidla dost času na to, aby odstavil informační systém z provozu a přesunul alespoň nejdůležitější část datových nosičů do bezpečí. Pro účely evakuace by každá část systému měla být jasně vyznačena stupněm důležitosti, aby při odsunu mohli pomáhat i nekvalifikovaní pracovníci.

Závady ve vodovodních sítích - např. poruchy potrubí, izolace apod. Tyto závady působí velmi rychle, základním řešením je udržovat dobrý technický stav rozvodů vody v budovách. Pro případ rychlé evakuace je opět vhodné vyznačit stupně důležitosti komponent systému. [2]

1.1.2 Požáry

Oheň je nebezpečný nejen pro informační technologie, ale také pro obsluhující personál. Druhotné nebezpečí představuje pro technologie voda použitá při hašení požáru a kouř. Základní protiopatření proti požáru je monitorování výskytu ohně a kouře, instalace automatických hasicích systémů a přenosných hasicích přístrojů. Protipožární bezpečnost lze však také zvýšit řadou doplňkových technických a režimových opatření. Především se jedná o technické řešení konstrukce objektů a místností, které by neměly obsahovat snadno hořlavé materiály a nejvíce exponované prostory lze navíc chránit instalací protipožárních stěn, přepážek atd. Nejdůležitější části systému se umísťují v prostorech s vysokou pasivní požární bezpečností. [2]

1.1.3 Ochrana objektů

První překážkou pro potencionálního útočníka může být skutečnost, že nemá fyzický přístup k technickým zařízením a nosičům dat. Ochranu objektů v praxi realizujeme prevencí proti neoprávněnému vniknutí – různými zábranami ztěžujícími vniknutí do chráněné oblasti a detekcí – indikací neoprávněného vniknutí. Řada objektů má automatický dveřní systém založený například na principu čipových karet, sloužících k monitorování pohybu osob. Komplexní bezpečnostní systém kombinuje mechanické zábrany, signalizační zařízení a monitorovací systémy s organizačními opatřeními a ostrahou. Ochrana objektů zahrnuje řadu funkcí: protipožární ochranu, ochranu proti úniku vody a plynu, ochranu proti přerušení dodávky energie a ochranu proti vloupání. Nejdokonalejší zabezpečovací systémy všechny tyto funkce integrují do jednoho celku. Některé zajišťují i funkce řídící a regulační. [2] [3]

Ochrana objektu proti vloupání představuje cíl chránit objekt, osoby, které v objektu pracují a majetek před zloději. V systému ochrany objektů se vyskytují při určitém zobecnění tři základní aspekty:

1. objekt a v něm uložené hodnoty,
2. osoby, které v objektu pracují,
3. potencionální pachatel.

Objekt a v něm uložené hodnoty – kde každý objekt má určité základní vlastnosti, které buď zvyšují, anebo snižují jeho bezpečnost. Jsou to především funkce, které plní jeho určení, umístění na pozemku, půdorysné a výškové členění objektu, vnitřní dispozice, provoz v jednotlivých prostorech a jejich časový režim.

Osoby, které v objektu pracují – chování uživatelů chráněného objektu je dáno především funkcí objektu. Je nutno definovat, které osoby kdy a kam mohou vstupovat. I ta nejjednodušší (nejmírnější) ochrana předpokládá, že jí pracovníci v objektu své chování přizpůsobí a že je tedy svým způsobem omezuje. Čím rizikovější je provoz z hlediska napadení, tím vyšší jsou i nároky na chování lidí v takovém objektu a provozní režim musí být přísnější. Např. do místnosti serverů mohou vstupovat pouze osoby pověřené administrací serverů a osoby odpovědné za celkový provoz IS. Dobře vypracovaný bezpečností projekt by měl alespoň částečně počítat s nedokonalostí lidí – s jejich nedbalostí, zapomnětlivostí apod.

Potencionální pachatel – zatímco předchozí dva aspekty jsou více (objekt a provoz v něm) nebo méně (uživatelé) známy, pachatel je při projektování ochrany neznámý, a můžeme ho charakterizovat pouze s určitou pravděpodobností. Přitom zvážit jeho chování je ze všeho nejdůležitější, protože právě proti němu se popisovaná opatření zavádějí. Chování pachatele si projektant musí umět představit, simulovat jej a klást pachateli takové překážky, aby co nejvíce snížil pravděpodobnost jeho úspěchu. Nelegální přístup do objektu je nutno maximálně znesnadnit, zpomalit a učinit vše pro to, aby byl pachatel kvalifikovaně dopaden, pokud možno již při pokusu o proniknutí do objektu, kdy zatím nestihl způsobit větší škody. Podle závěrů statistických průzkumů provedených mezi dopadenými pachateli je zřejmé, že si vybírají objekty loupeže podle dvou následujících kritérií:

- Cena očekávané kořisti – toto kritérium nejsme schopni ovlivnit, protože je implicitně určeno požadavky na informační systém.

- Viditelné možnosti snadného vniknutí do objektu – obecně vniká pachatel do objektu stavebními otvory. Pronikání konstrukcí (obvodové zdivo, strop, podlaha) je výjimečné. Procentuální rozložení vniknutí do objektu je vyjádřené v tabulce. Z těchto údaj je tedy zřejmé, že nejohroženější část chráněného objektu je přízemí. [2]

Strážní služba

Strážní a ochranná služba je zaměřena zejména na plnění úkolů k zajištění ochrany života a zdraví osob a k ochraně majetku. Základní činnosti strážní služby zahrnují:

- kontrolu vstupu a osob do objektu a jejich evidenci,
- kontrolu vjezdu a výjezdu vozidel do a z objektu,
- kontrolu oprávněnosti vstupu do prostor chráněných EZS, systémem CCTV a kvalifikovaný zásah v případě vyhlášení poplachového signálu,
- kontrolu dodržování protipožárních opatření a zajištění ohlašovny požárů,
- periodické hlídkování zaměřené na vizuální kontrolu neporušenosti perimetru objektu a výskyt osob v jeho těsné blízkosti,
- ochrana zaměstnanců klienta před nežádoucími osobami,
- kontrolu neporušenosti inženýrských sítí,
- kontrolu technologických celků,
- zásah v případech k ochraně života a zdraví osob a k ochraně majetku klienta,
- ostrahu majetku uloženého v místech mimo standartní skladové plochy a úložiště. [4]

Elektronická zabezpečovací signalizace (EZS)

Při vstupu narušitele do střeženého prostoru je elektrický zabezpečovací systém (EZS) schopen opticky a akusticky signalizovat jeho přítomnost nebo vstup (pokus o něj). Za pomoci následujících prvků je vytvořen tzv. zabezpečovací řetězec, který umožňuje správnou funkci zabezpečovacích prostředků. Jedná se o:

- Čidlo, které dokáže bezprostředně reagovat na fyzikální změny spojené s narušením střeženého prostoru nebo s pohybem střeženého předmětu. Pokud dojde k této

reakci, vyšle čidlo poplachový signál nebo zprávu. Umístění se volí do míst, kde pachatel překonává chráněný prostor.

- Ústřednu, jejíž zásadní funkcí je sběr informací o stavu jednotlivých čidel a na základě rozhodovacího schématu vytvořeného obsluhou vyvolávat poplachové signály. Řídící pracoviště může obsahovat desítky smyček, které signalizují místo narušení pomocí kontrolek na displejích.
- Přenosové prostředky. Jejich cílem je přenést informace o poplachu ve střeženém místě do místa trvalé obsluhy. Může jím být pult centralizované ochrany Policie ČR, Městské policie nebo soukromé bezpečnostní služby.
- Signalizační zařízení má za úkol zajistit převedení předaných informací na vhodný signál, který vyhlásí poplach nebo výstrahu.
- Doplňková zařízení usnadňující ovládání systému. [5]

Televizní monitorovací systémy

Slouží k monitorování situace na exponovaných a významných místech, a to jak ve vztahu ke kriminalitě, tak ve vztahu k výrobním postupům, zajištění přehledu, operativnosti řízení a konečné možnosti snížení nákladů a ztrát. Systém CCTV představuje nezávislý kamerový systém (systém průmyslové televize), který může být buď provozován samostatně, nebo zakomponován do rozsáhlých bezpečnostních a řídících systémů. [6]

Systémy mechanických zábran

Mechanické zábranné systémy (MZS) jsou historicky nejstarším typem bezpečnostních systémů. Jedná se o základní prvek v oblasti ochrany majetku a osob, jelikož se dá říci, že každý bezpečnostní systém je potencionálně překonatelný. Hlavním úkolem MZS je vytvořit pachateli překážku, jejíž překonání je pro něj z hlediska časové náročnosti, použitých prostředků a vynaložené energie neúnosné. MZS obecně slouží především jako ochrana proti:

- neoprávněnému vniknutí do střeženého prostoru,
- odcizení, znehodnocení nebo poškození chráněných aktiv ve střeženém prostoru,
- manipulaci s nebezpečnými látkami či předměty.

MZS můžeme podle typu chráněných aktiv rozdělit do 3 kategorií, a to na ochranu:

- **Obvodovou** (perimetrickou) - prvky MZS jsou instalovány vně chráněného objektu a jejich hlavním úkolem je zajištění bezpečnosti ve vyhrazeném prostoru. Prostor je

vymezen katastrálními hranicemi pozemku, většinou tvořenými přírodními nebo umělými překážkami. Jedná se tedy o oplocení či ohrazení pozemku včetně průchodů a průjezdů, jako jsou branky, brány, závory apod.

- **Plášťovou** – hovoříme o zabezpečení vnější části chráněného objektu, tedy veškerých standardních i nestandardních stavebních otvorů, jako jsou dveře, okna, zásobovací otvory a šachty apod. Příkladem mohou být bezpečnostní dveře, skla, fólie, rolety, mříže, kování, pomocné zámkové a zamykací systémy aj.
- **Předmětovou** – jejím primárním určením je zabezpečení cenných předmětů či utajovaných informací před odcizením, znehodnocením nebo neoprávněné manipulaci. Obecně se jedná o pokladny, trezory, trezorové a bezpečnostní skříně, bezpečnostní zavazadla pro přepravu cenin a hotovosti, bezpečnostní plomby apod. [7]

Systémy monitorování pohybu osob

Automatická (automatizovaná) kontrola vstupu oprávněných osob do objektu a jejich pohyb v bezpečnostních zónách objektu je významným doplňkem zkvalitnění strážní služby. Existuje celá řada identifikačních systémů, které se liší podle principu činnosti (magnetický proužek, čárový kód, čipové karty), především v množství poskytnutých informací o nositeli karty (oprávnění vstupu do zón, osobní údaje apod.) pro potřeby řídicího systému.

Při návrhu systému monitorování pohybu osob je důležité specifikovat především tyto informace:

- umístění a počet kontrolovaných zón pohybu, jejich rozloha,
- hierarchii přístupu do zón,
- složení a strukturu informací, které musí identifikační nosič poskytovat,
- technologii a princip snímání (kontaktní = bezkontaktní),
- požadavky na vazby do jiných informačních systémů. [2]

1.1.4 Bezpečné uložení nosičů dat a jejich bezpečná likvidace

Bezpečné uložení nosičů informace

Informace na záložních a archivních nosičích představují téměř ideální cíl útoku. Přístup k nim není chráněn hesly nebo jinými přístupovými kontrolami tak, jako k informacím uloženým přímo v počítači. Potencionální útočník má tedy mnohem snadnější situaci. Přenosné

nosiče přitom obsahují stejně citlivé informace jako ostatní části systému. Ochrana dat na těchto paměťových médiích se realizuje především fyzickým zabezpečením – jejich bezpečným uložením. Praktickou realizaci nabízejí např. bezpečnostní schránky na ukládání datových kopií a trezory s protipožárními vrstvami. Trezory mohou být různého druhu:

- trezor umístěný ve zdi,
- trezor umístěný v podlaze,
- pokladnička (malá, samostatná),
- depositář (obsahuje otvor, do kterého je možné snadno vhodit např. dokument),
- sejf (velký, těžký). [8]

Z hlediska integrace jednotlivých bezpečnostních systémů je vhodná i kombinace mechanického zabezpečení s možností napojení těchto schránek na celkový elektronický zabezpečovací systém, popř. připojení na pult centrální ochrany. [2]

Ničení nosičů informace

S rychlým rozvojem IT technologií velmi často vyvstává potřeba výměny datových zařízení, jako jsou pevné disky, datové pásky a další zařízení. Tato média mnohdy obsahují důvěrná firemní data, která musí být chráněna před přístupem neoprávněných osob. Možné zneužití těchto dat je důvodem, proč je bezpečná likvidace tak důležitá.

V každé organizaci nebo firmě, kde se pracuje s důvěrnými daty (např. osobními údaji, čísly kreditních karet, informacemi o produktech, prodejními reporty atd.), existuje nebezpečí jejich zneužití. Mnoho organizací řeší problém bezpečné likvidace médií obsahující takováto data.

Pouhé smazání souborů neznamená, že data byla z médií fyzicky odstraněna. Odborníci na IT technologie jsou schopni obnovit data dokonce i z nosičů, které byly formátovány. Mnoho organizací se zbavuje nebo prodává počítače obsahující důvěrná data týkající se svých zákazníků. Pro bezpečnou likvidaci dat se používají dvě metody: programová (softwarová) a fyzická (hardwarová) metoda.

Softwarová metoda – spočívá ve smazání dat za pomoci programového vybavení. Výhodou této metody je možnost opětovného použití smazaných médií.

Hardwarová metoda – spočívá v nevratném smazání dat z médií za použití demagnetizátorů (degausseru). Použitím demagnetizátoru dojde k úplnému a nevratnému smazání všech dat zapsaných na médiích a média již nadále nejsou použitelná. [9]

Kancelářské skartovací stroje

Skartovací zařízení slouží především k ničení papírových dokumentů tiskových sestav, disket, pásek ze streamerů, kazet a barvicích pásek z jehličkových tiskáren. Principem je rozstříhání nebo rozřezání ničeného dokumentu na pásky, nebo ještě menší plochy, z nich složit původní originál je obdobné jako skládání stavebnice. Puzzle (list formátu A4 je možné rozřezat až na 2200 dílů rozměru 1,9x15mm). Skartovače by měly být umístěny v místě, kde údaje vznikají, tzn. přímo u tiskáren, kopírek a počítačů, jen tak zajistíme, aby nosiče dat byly po použití spolehlivě ochráněny, tzn. zlikvidovány. [2]

Přepisovače magnetických médií

Jedním z často používaných způsobů mazání dat je demagnetizace (degaussing) za použití speciálního zařízení. Demagnetizace umožňuje trvalé odstranění magneticky zapsaných dat i z nefunkčních pevných disků, datových pásek, a umožňuje vrácení médií výrobci, nebo jejich ekologickou likvidaci. Demagnetizátor vytváří silné elektromagnetické pole, které je klíčové pro eliminaci dat. Data jsou po demagnetizaci nenávratně smazána a média již nadále nejsou použitelná. Starší typy datových pásek, např. DLT, DDS, audio a video kazety, lze po demagnetizaci opětovně použít. [10]

Zásady výstavby objektů

Prosazovaní požadavků zabezpečení budovy začíná už při jejich projektování. Projekt výstavby (popř. rekonstrukce) musí tedy respektovat všechna doporučení, která vycházejí z bezpečnostní analýzy a stanovené koncepce budování bezpečnosti organizace. U objektů především vyhodnocujeme:

- Vhodnou dislokaci, kde jde především o seismické aktivity, blízkost elektrických rozvodů velmi vysokého napětí, ropovodů, plynovodů a jiných inženýrských sítí.
- Předpokládaný urbanistický rozvoj okolí objektu. Jde o blízkost jiných objektů a staveb s ohledem na jejich charakter, a přístupové komunikace k objektu.

Výše popsané vlivy můžeme zpravidla jen částečně ovlivnit. To, co však musí zůstat pod kontrolou a vlivem osob odpovědných za prosazování bezpečnosti, je návrh vnitřních bezpečnostních mechanismů. Jsou to:

- elektronická požární signalizace,
- elektronická zabezpečovací signalizace,

- monitorovací systémy pohybu osob v objektu,
- rozmístění a definice typů čidel,
- použití protipožárních materiálů,
- antistatická opatření. [2]

Místnosti serverů

Zvláštní důraz je nutno položit na budování místností serverů. Servery představují jedno z nejlákavějších míst pro nelegální zájemce o naše informace. Na nich je největší kumulace informací, dat a programů. Bezpečnému umístění počítačů je z těchto důvodů nutno věnovat zvýšenou pozornost a v maximální možné míře je znepřístupnit nepovolaným osobám. [8]

Základní požadavky na místnosti serverů:

- Požární ochrana – detekce požáru, protipožární dveře a další protipožární opatření.
- Ochrana proti vyplavení a povodním – umístění datového centra mimo záplavové zóny a další protipovodňová opatření.
- Konektivita a připojení k internetu – vysoká úroveň připojení na páteřní síť internetu a jištění výpadku připojení.
- Nepřetržití elektrické napájení neboli ochrana proti výpadku elektřiny, záložní zdroj napájení.
- Fyzické zabezpečení přístupu do prostor, autorizace osob, zajištění proti vniknutí neoprávněných osob nebo proti poškození či jinému útoku.
- Bezpečnostní monitoring – 7 dní v týdnu, 24 hodin denně, bezpečnostní kamery, detektory pohybu, indikátory dveří, CCTV. [11]

1.1.5 Technické zabezpečení provozu

Výpadky a kolísání elektrické energie, tedy především napěťové špičky, jsou příčinou řady škod při zpracování dat. Statistiky připisují až 60-70 % závad informačních technologií právě chybám v dodávkách elektrické energie.

K základním typům nestabilit elektrických rozvodů patří:

- Výpadek napětí – výpadek delší než dvě periody, způsobený poruchou elektrické sítě, vypadnutím jističe atd.
- Podpětí – dlouhodobý stav, při kterém je napětí v síti nižší o více než 15 %. Může také docházet ke krátkodobému podpětí v důsledku zapínání spotřebičů s vysokým výkonem.
- Přepětí – dlouhodobý stav, při kterém je napětí v síti vyšší o více než 10 %, například z důvodu malé poptávky po elektrické energii. Krátkodobé přepětí je způsobeno například vypínáním vysoce výkonných spotřebičů.
- Napěťové rázy – napěťové špičky velmi vysokého napětí s dobou trvání 10 až 100 mikrosekund. Jsou způsobovány přeskokem jisker a elektrostatickými výboji.
- Kolísání frekvence – odchylka od standartních 50 Hz.
- Harmonické zkreslení průběhu napětí – způsobeno nelineární zátěží v síti.
- Šum – šumová složka obsažená v síti. Zdroji jsou regulační systémy, relé, mikrovlnné záření atd. [8]

V praxi je proti těmto problémům využíván napájecí zdroj UPS – Uninterruptible Power Supply zajišťující dodávku elektrické energie pro zařízení, u kterých nemůže dojít k přerušení provozu. Využívá se nejenom při přerušení dodávky ze sítě, ale například i pro zajištění požadované kvality dodávané energie při kolísání napětí v síti, napěťových špičkách nebo podpětí. Schopnost zajištění dodávky energie při kompletním výpadku je u UPS ve většině případů poměrně krátká (v řádech jednotek až desítek minut), ale stačí pro zajištění nepřetržité dodávky energie, dokud není spuštěn záložní zdroj. Existuje několik druhů UPS, které se liší principem činnosti a s tím spojenou kvalitou výstupního napětí. [12]

1.1.6 Napájecí zdroje UPS

Jedná se o nepřerušitelný zdroj napájení, nebo také zařízení zásobující počítač proudem v případě náhlého přerušení přívodu elektrického proudu. [13]

Typ off-line

Nejjednodušším typem UPS zdroje je typ off-line. Jeho napájecí výstup, kde jsou připojeny zálohované spotřebiče, je propojen přímo se vstupem do zdroje a energie z akumulátorů je dodávána pouze při výpadku elektrického proudu. Při běžném provozu se zároveň neustále

dobíjí akumulátorový podsystém přes měnič napětí. Při výpadku napájení z elektrické sítě přepne relé výstup zdroje na elektrický měnič, který převádí stejnosměrné napětí akumulátorů střídavě. Výhodou tohoto řešení jsou malé ztráty elektrické energie ve zdroji (účinnost je skoro 100 %) a nízká pořizovací cena. Velkou nevýhodou je nemožnost filtrovat kolísání sítě (napěťové a frekvenční výkyvy), tento nedostatek je částečně možné eliminovat vstupními a výstupními filtry, a určitá doba potřebná k přepnutí na napájení z akumulátorů (řádově milisekundy). [14]

Typ on-line

U tohoto zdroje je vstupní napájení vedeno přes vstupní měnič napětí, který převádí střídavé napětí na stejnosměrné do akumulátorů. Ty se dobíjejí a zároveň se stejnosměrné napětí výstupním měničem převádí zpět střídavé napětí na výstup zdroje. Tímto postupem se napětí zbavuje všech nestabilních charakteristik. Při výpadku je bez jakéhokoliv přepínání (které je samo o sobě elektrickým kmitem) dodávána energie z akumulátorů, toto řešení především odbourává nežádoucí přepínání a odstraňuje všechny poruchy, které přicházejí na vstup zdroje, tj. šumy, elektrické pulsy, přepětí a podpětí. Tento princip má samozřejmě i některé nevýhody. Akumulátory jsou neustále připojeny a mohou se přebíjet a zahřívat, což snižuje jejich životnost. Přeměna elektrického napětí na stejnosměrné a následně znova na střídavé způsobuje energetické ztráty. Tyto zdroje bývají většinou vybaveny zároveň tzv. okruhem – bypass, který přepojuje vstup zdroje přímo na výstup a obchází měniče (z UPS je vlastně prodlužovací šňůra). Využívá se při práci na akumulátorech nebo při přetížení výstupního měniče. [14]

Požadavky na napájecí zdroje UPS:

- vysoká hustota akumulace energie,
- nízké samovolné vybíjení,
- rychlé nabíjení,
- nízké náklady na údržbu,
- vysoká spolehlivost,
- rychle dodaný výkon. [15]

1.2 Logická ochrana dat

Logická ochrana dat zahrnuje mechanizmy, jimiž se operační systémy či jiný software snaží předejít neautorizovanému přístupu k citlivým informacím či datům. Obecně lze tyto mechanizmy rozdělit na tři části:

Kryptografické algoritmy – jsou matematické funkce, jejichž hlavním cílem je zajištění důvěrnosti, integrity a dostupnosti. Na jejich bezpečnosti a správném použití stojí podstatná část soudobé kryptografie.

Kryptografické protokoly – jsou metody popisující vzájemnou komunikace mezi jednotlivými zařízeními. V podstatě se jedná o distribuované algoritmy, kdy jsou jednotlivé kroky „propojeny“ komunikací uskutečňovanou přes prostředí bez fyzické bezpečnosti.

Řízení přístupu – má oproti algoritmům a protokolům do značné míry omezenou použitelnost, protože nutným předpokladem je existence důvěryhodného prostředí. [16]

1.2.1 Řízení přístupu k informacím

Řízení přístupu se zabývá vztahem mezi objekty a subjekty. Objektem informačního systému je pasivní prvek, který obsahuje nebo přijímá informaci (uživatel, program, proces atd.). Subjektem informačního systému je aktivní prvek, který způsobuje předání informace mezi objekty nebo změnu stavu systému (soubor, databáze, záznamové médium atd.). Řízení přístupu zahrnuje po tři po sobě jdoucí kroky, a to identifikaci, autentizaci a autorizaci.

- **Identifikace** subjektu je tvrzení subjektu o své identitě. Identitou nemusí být pouze totožnost, ale může jí být také schopnost, skupinová příslušnost, případně negace těchto vlastností.
- **Autentizace** subjektu je proces ověření jeho identity splňující požadovanou míru záruky.
- **Autorizace** je poskytnutí nebo odmítnutí přístupu subjektu k objektu na základě práv přidělených autoritou.

Příkladem řízení přístupu může být přihlašování do svého e-mailového účtu, kde v okamžiku zadání uživatelského jména provádíme identifikaci. Tvrdíme, že jsme to my s tímto uživatelským jménem. Ovšem tímto jménem by se mohl pokusit přihlásit i kdokoliv jiný, proto je potřeba zadat správné heslo, což je autentizace. Pokud správné heslo zadáme, získáme přístup

do požadované e-mailové schránky, a nikoliv do schránky jiného uživatele, získání toho správného přístupu je tedy autorizace. [8]

1.2.2 Rozdělení technik řízení přístupu

Poté, co je subjekt identifikován a autentizován, musí být autorizován, aby získal přístup ke zdrojům a mohl vykonávat požadované akce. Základním principem řízení přístupu je implicitně odepřít přístup, pokud není přístup explicitně umožněn určitému subjektu. K tomu se používají různé techniky, které lze rozdělit:

- **Technika přenechání volnému uvážení**
- **Techniky nepřenechání volnému uvážení**
  - **Mandátní technika**
  - **Technika potřeby znát**
  - **Technika založená na roli**
  - **Technika založená na úkolu**

1.2.3 Technika přenechání volnému uvážení

Tato technika spočívá v uvážení vlastníka dat, který explicitně definuje možnosti přístupu jednotlivých subjektů k tomuto objektu. Implementace je často realizována prostřednictvím použití seznamu přístupových práv jednotlivých subjektů. Technika neumožňuje centrální řízení systému, spoléhá se na zodpovědnost vlastníka dat, který by měl být na jejich ochraně nejvíc zainteresován. Tato technika je dynamičtější než ostatní techniky. [8]

1.2.4 Techniky nepřenechání volnému uvážení

Tyto techniky jsou založeny na systému pravidel, jimiž jsou různé restrikce a filtry, které určují, co se může a nesmí vyskytnout v systému, jaký typ subjektů smí do systému přistupovat a jaká práva mají. Tyto techniky nejsou založeny na administrátorově nebo vlastníkově rozhodnutí, ale právě na těchto pravidlech. Nezaměřují se na konkrétní identitu subjektu, ale na specifické profily vytvořené pro zařazení každého uživatele. Tyto techniky jsou vhodné pro taková prostředí, ve kterých jsou přístupová práva často měněna. Příkladem takového systému je firewall, který zpřístupňuje pouze povolené služby internetu.

Techniky nepřenechání volnému uvážení využívají abstrakce, kdy jsou podobné entity umístěny do skupin, tříd nebo rolí, kterým jsou přiřazeny příslušná bezpečnostní opatření.

Dochází poté k zjednodušení řízení bezpečnosti umožněním přiřazení bezpečnostních opatření skupině entit. [8]

Mandátní technika spočívá v použití klasifikačních štítků, kdy každý štítek reprezentuje určitou bezpečnostní doménu, což je prostor spravován příslušnou bezpečnostní politikou. Subjekty se označí štítkem podle míry jejich oprávnění a objekty se označí štítkem podle jejich úrovně citlivosti.

Technika potřeby znát je rozšířením mandátní techniky a spočívá v tom, že subjekt může přistupovat k objektům se stejným nebo nižším štítkem, ale pouze pokud to současně vyžaduje plnění jeho pracovních úkolů. Jedná se tedy o hybridní klasifikaci objektů a subjektů, kombinaci hierarchické klasifikace a rozčleněné klasifikace.

Technika založená na roli definuje práva subjektu přistupovat k objektům prostřednictvím tzv. rolí subjektu. Například vrcholový manažer má vyšší práva ke zdrojům, než např. brigádník. Subjekt má pouze práva připadající příslušné roli, práva nelze individuálně upravovat. Technika nepředpokládá, že by subjekt patřil do více skupin neboli měl více rolí, ale objevují se trendy toto omezení zrušit. Technika umožňuje úzce provázat bezpečnostní politiku a organizační strukturu organizace, je tedy vhodná pro prostředí s častými personálními změnami.

Technika založená na úkolu spočívá v řízení přístupu, které je založeno na přiřazené úloze, ne na konkrétní identitě subjektu. Subjekty tedy přistupují k objektům prostřednictvím tzv. úkolu subjektu. [8]

1.2.5 Administrace řízení přístupu

Administrace řízení přístupu subjektů k objektům představuje kolekci úkolů a povinností, která je přidělena administrátorovi. Mezi hlavní úkoly patří:

- správa uživatelských účtů,
- zaznamenávání aktivit uživatelů,
- řízení přístupových práv.

1.2.6 Správa uživatelských účtů

Bez správy uživatelských účtů nelze zajistit ustanovení identity, vykonání autentizace, její ověření prostřednictvím autorizace a zajistit účtovatelnost. Správa uživatelských účtů zahrnuje:

- **Tvorbu nových uživatelských účtů**
- **Správu stávajících uživatelských účtů**
- **Rušení neplatných uživatelských účtů**

Tvorba nových uživatelských účtů (registrace) bývá zahájena formálním požadavkem personálního oddělení na vytvoření nového uživatelského účtu pro nového zaměstnance, který obsahuje klasifikaci bezpečnostní úrovně, do které má být nový zaměstnanec zařazen. Tento požadavek schvalují současně vedoucí příslušného oddělení a bezpečnostní administrátor. Po schválení je účet vytvořen a zaměstnanci se přiřadí identifikační číslo a dočasné heslo.

Správa stávajících uživatelských účtů spočívá především se změnami autorizačních práv. Organizace se statickou hierarchickou strukturou a nízkou mírou fluktuace (nepravidelného a nesoustavného pohybu) zaměstnanců mají méně náročnou správu než organizace s dynamickou organizační strukturou. Při změně práv probíhá podobná procedura schvalování jako při tvorbě nového účtu.

Rušení neplatných uživatelských účtů znamená smazání nebo zneplatnění uživatelského účtu. Tento proces je vhodné zautomatizovat a provázat s personálním oddělením, například zneplatnit účet v případě pozastavení výplat. [8]

1.3 Technická ochrana dat

Žádné technické prostředky zatím nedokáží pracovat bez chyb a výpadků. Technická bezpečnost řeší ochranu dat použitím odpovídajícího technického vybavení – jeho kvalitním výběrem a zjištěním potřebné spolehlivosti, a servisních služeb dodavatelů technologií během provozu informačního systému. Je to tedy ochrana dat pomocí využití vhodného technického vybavení. Pod tímto pojmem však v technické bezpečnosti chápeme především zajištění dostupnosti a integrity, tj. neporušenosti informací.

Základním problémem vztahu technické vybavení – data jsou paměťová zařízení. Jako jediná část výpočetní techniky totiž paměťová zařízení, disky a pásky obsahující mechanické součástky, které jsou jednak poruchové (více než ostatní elektronické součástky v počítači) a protože vykonávají určité mechanické pohyby (pohyb snímací hlavy po ploše disku), i pomalé. Diskové operace zabírají zhruba 50 % výkonu počítače a podílejí se z 27 % na jeho poruchách.

Technická bezpečnost řeší problém nosičů dat tak, že navrhuje systémy s vysokou redundancí, tj. s vysokou odolností proti chybám. [2]

1.3.1 Disková pole RAID

S rostoucím výkonem počítačů neustále rosou i požadavky provozovaných aplikací na datový prostor disků. Aby bylo možné tyto požadavky uspokojit, musejí se neustále přidávat další disky s velkou kapacitou, což je finančně nákladné a s počtem disků přímo úměrně roste i pravděpodobnost poruchy některého z nich, tím pádem i ztráty části dat.

Zvětšování diskového prostoru lze vyřešit instalací spolehlivých a velmi drahých velkokapacitních disků, anebo často používanou technologií diskových polí RAID (Redundant Arrays of Inexpensive Disks). Filozofií RAID je použití většího množství levných, běžně dostupných disků, na nichž jsou uložena jednak samotná data a jinak i pomocné informace, které v případě závady na jednom disku (popř. na více) umožní jednoduchou (automatickou) rekonstrukci zničených dat.

Redundance označuje část dat, která mohou být odstraněna – ztracena, poškozena, bez ztráty informace.

Vlastnosti diskových polí

Spolehlivost = původní cíl, kvůli němuž disková pole vlastně vznikla. Jejich implementací do informačního systému se stala výměna vadných disků za provozu samozřejmostí.

Vysoký výkon – disková pole se zpravidla nasazují v systémech, pracujících s velkými objemy dat bez ohledu na to, zda jde např. o obrazové aplikace nebo o databázový server. Počínaje úrovní RAID 3 je s odolností proti ztrátě dat řešena zároveň i výkonnost diskového subsystému. Je to způsobeno tím, že zatímco výkon CPU vzrostl o několik řádů, výkon pevných disků vzrostl za stejný čas pouze řádově. Tento velký rozdíl znamená, že výkonové omezení výpočetního systému je dnes právě v diskových operacích. Přidáme-li k tomu ještě neustále stoupající nároky na objem přenášených dat, jsme u jádra problému, Je zřejmé, že lákavé zvyšování pouze výkonu procesoru (případě procesorů) není dostatečným řešením a můžeme se dostat do situace, kdy jedinou další cestou ke zvyšování výkonu výpočetního systému bude zrychlení diskových operací.

Otevřenost – jak softwarová, tak i hardwarová. Diskový systém by měl umožňovat přechod na jiný operační systém nebo jiný typ hostitelského počítače bez větších technických komplikací.

Flexibilita – možnost rozčlenit datový prostor podle potřeb uživatelů nebo nároků operačního systému, možnost sdílet diskové pole několika hostitelskými počítači, a to třeba i různých hardwarových platforem s různými operačními systémy a možnost výměny jednotlivých technických prostředků v závislosti na vývoji nebo změněných podmínkách provozu informačního systému.

Nevýhody

Použité disky (RAID 0 až 5) musí mít stejnou kapacitu a charakteristiky – počet hlav, stop a sektorů, pokud možno i stejné provedení. V případě výměny disku musí být k dispozici disk stejných vlastností a u déle provozovaných systémů se tyto disky musejí zajišťovat dopředu (později se už daný typ nemusí sehnat). [2]

1.3.2 Dělení diskových polí podle způsobu ovládání připojených disků

Softwarové ovládání – jedná se zpravidla o vlastnost (službu) operačního systému nebo speciální program, který přímo přebírá řízení přístupu k diskům a pracuje s nimi jako s virtuálním diskovým polem. Toto řešení je velice nevýhodné, protože značně zatěžuje samotný operační systém další úlohou, kterou musí neustále řešit a snižuje výkonnost celého systému. Při výpadku operačního systému je potom větší nebezpečí porušení integrity dat. Významnou slabinou tohoto řešení je také omezení použití diskového pole pouze na operační systém, který jej obsluhuje. Pokud na stejném počítači nastartujeme jiný operační systém, bude se mu diskové pole jevit jako běžné disky a nebude navíc z něho schopen číst, protože data budou mezi nimi rozdělena podle principu ukládání dané úrovně. [17]

Hardwarové ovládání – hardwarový řadič je umístěn v počítači a jeho logika řídí přístup k datům, čímž jsou eliminovány nevýhody softwarového řešení. Výkonnost je nesrovnatelně větší a zpravidla je možnost provozu pod různými operačními systémy. [17]

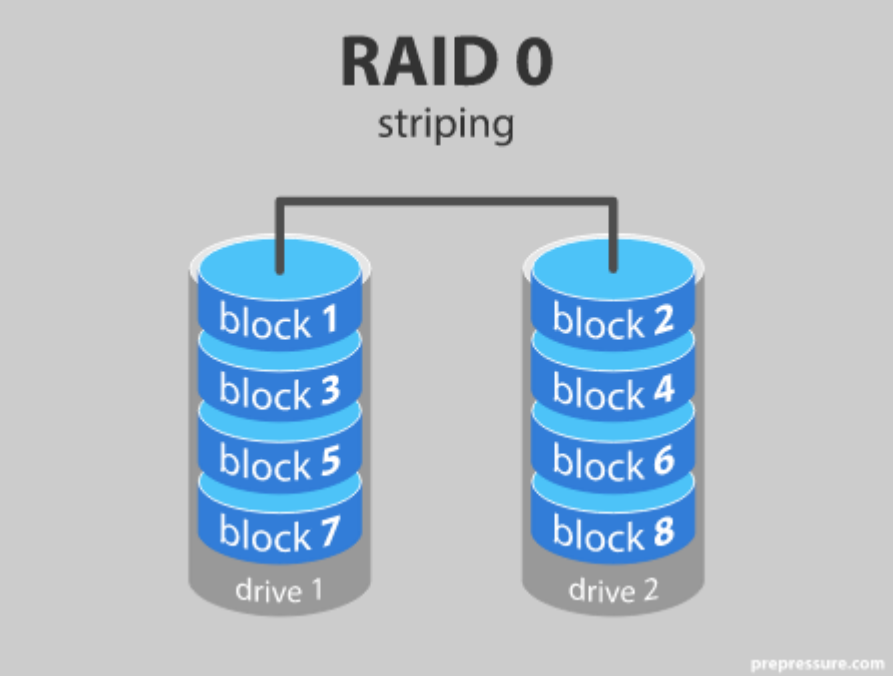
Podle fyzického umístění se dělí na:

- Interní, kde jsou ovladače umístěny ve vnitřním prostoru serveru. Výhodou interního RAID je možnost použít řadič, který je sběrnicí. Desky jsou umístěny do více slotů základní desky počítače, a tím se rozšíří datový kanál mezi operační paměti počítače a diskovým subsystém. Nevýhodou je závislost na technické spolehlivosti počítače a závislost na hardwarové platformě. V případě poruchy hostitelského počítače se v krátkém čase obtížně obnovuje provoz výpočetního systému.

- Externí RAID – je systém zcela samostatný, na hostitelský počítač se připojuje většinou přes sběrnici SCSI. Jeho kladem je nezávislost na technických prostředcích počítače a hardwarových platformách, což je výhodné při přepojování diskového pole na jiný počítač, dojde-li k poruše. Některé implementace diskových polí umožňují i připojení na více hostitelských počítačů zároveň. [2]

1.3.3 RAID 0

Tato úroveň nezajišťuje bezpečnost, ale pouze zrychluje zápis a čtení dat. Její použití je významné v systémech, které požadují vysoký výkon a není nutno zajišťovat bezpečnost informací. Ukládaná data se zapisují na jednotlivé disky v blocích. Velikost jednoho bloku je zpravidla 64 kB. Soubor je rozdělen na takto velké bloky a první blok je zapsán na první disk, druhý blok na druhý disk atd. Výhodou je zvýšení přenosové rychlosti v důsledku paralelní práce stejných disků. Zvýšení rychlosti odpovídá počtu disků v sestavě. Nevýhodou je to, že při výpadku jednoho disku je ztracena ta část souboru, která je na tomto disku uložena, a tím dojde k porušení integrity celého datového souboru. Velikost volného datového prostoru je rovna součtu velikostí připojených disků. [18]

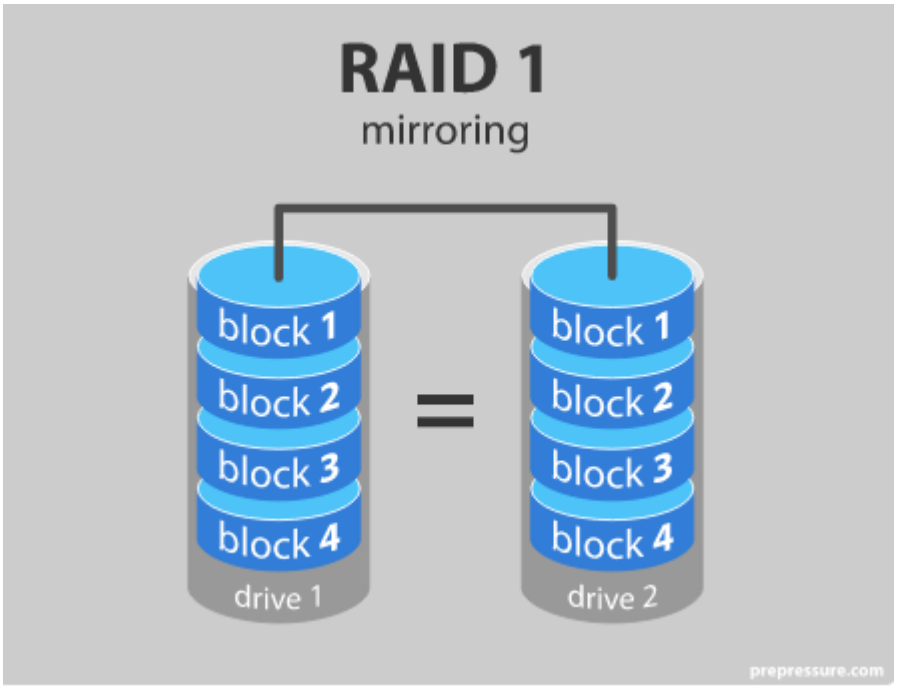


Obrázek 1: RAID 0

Zdroj:[19]

1.3.4 RAID 1

Bezpečnost dat je zajištěna duplicitním zápisem dat na dva stejné disky (zrcadlení dvou disků, oblast jednoho se zrcadlí na druhém – je jeho přesnou kopií). Nevýhodou tohoto řešení je omezení možnosti provádět v jednom okamžiku pouze jednu operaci zápisu a výsledná poloviční kapacita disků. Dochází také k větší zátěži procesoru a kanálu DMA. Výhodou je však opět relativní jednoduchost tohoto řešení, nízká cena, jeho častá integrace přímo do operačních systémů a maximální bezpečnost. Přístup k diskům může být realizován buď jedním (mirroring) nebo dvěma datovými kanály (duplexing). Duplexing je výhodnější, protože má vyšší odolnost proti poruchám řadiče a datových kabelů. [18]



Obrázek 2: RAID 1

Zdroj:[19]

1.3.5 RAID 2

Data lze obnovit pomocí tzv. Hammingova kódu, který umožňuje detekovat a odstraňovat chyby dat. Soubory jsou uloženy na bitech na datových discích a bity Hammingova kódu jsou uloženy na discích kontrolních. Velkou nevýhodou tohoto principu je zatížení procesoru a časové zpoždění, způsobené výpočtem opravených dat při zápisu. Při čtení je přenosová rychlost přibližně stejná jako u RAID 0. Kontrolní disky zabírají zhruba 30-50 % celkové diskové plochy. Tato úroveň byla překonána vyššími RAID a dnes se běžně nepoužívá. [2]

1.3.6 RAID 3

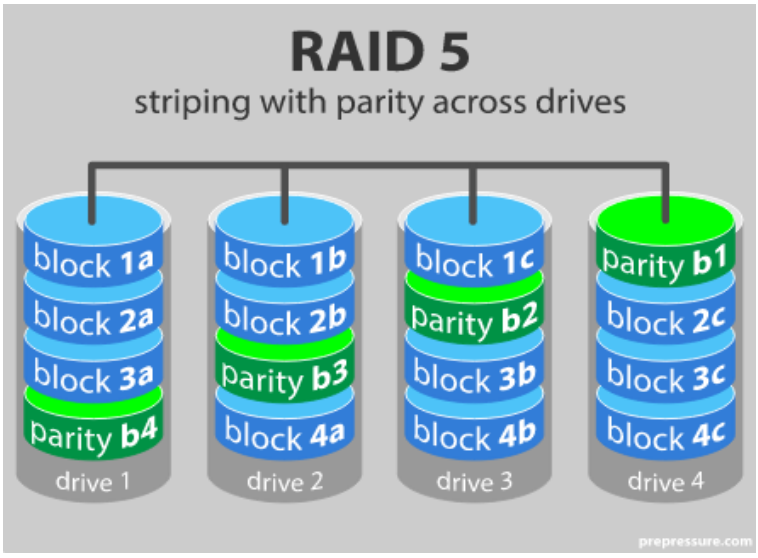
Obnovu dat zajišťuje v tomto případě ukládání informace na jeden paritní disk. Data jsou po bitech uložena na několika datových discích. Běžně se používají sestavy se dvěma až čtyřmi datovými a jedním paritním diskem (paritní disk zabere 20-33 % celkového diskového prostoru). Nevýhodou je možnost provádět v jednom okamžiku pouze jednu vstupně-výstupní (I O, Input Output) operaci. Tato úroveň se uplatní především tam, kde je požadován rychlý přístup k jednomu velikému souboru (např. obrazové aplikace). Naprosto nevhodné je její používání u databázových nebo souborových serverů. [2]

1.3.7 RAID 4

Obnovitelnost dat je opět zajištěna paritou, ale hlavní nedostatek úrovně RAID 3, tj. neschopnost provádět v jednom okamžiku více I O operací, byl odstraněn zápisem dat po bajtech, ne bitech. Operace čtení je několikrát rychlejší (než u jednoho disku) a zápis je o něco pomalejší. Redundance je 1/(N+1), kde N je celkový počet datových disků. [2]

1.3.8 RAID 5

RAID 5 vychází z RAID 4. Obnovitelnost dat je zabezpečena paritní informací uloženou cyklicky mezi data na všech discích současně (každý disk rozdělen na 5 částí – jedna část je parita). V případě výpadku jednoho disku se jeho data dopočítají. Tím je také odstraněn nedostatek předešlých úrovní, tj. jediné operace zápisu. Počet současně prováděných operací zápisu je roven polovině počtu disků. Velkost paritního prostoru je opět 1/(N+1). [18]

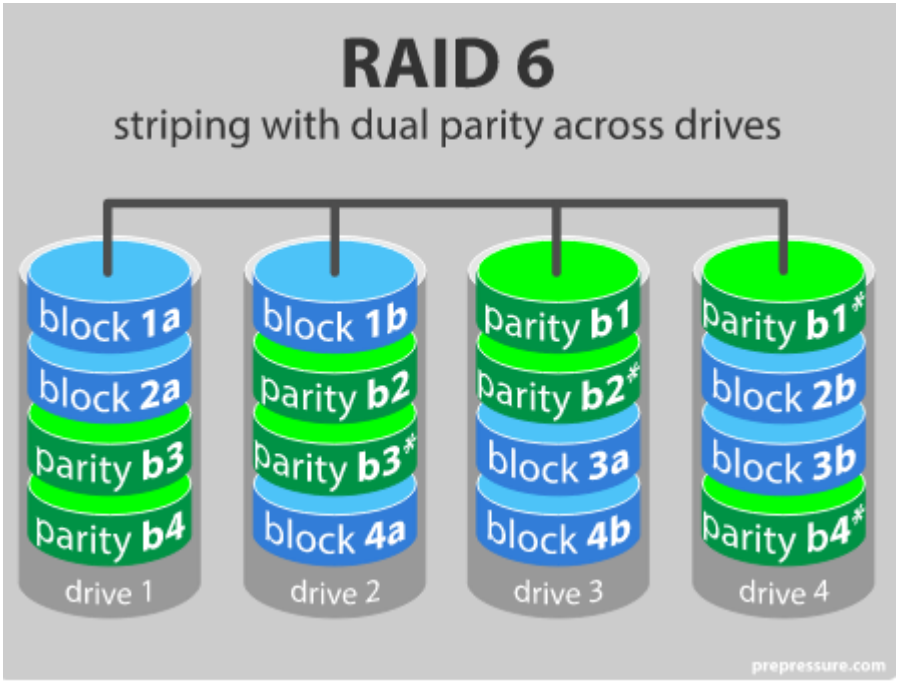


Obrázek 3: RAID 5

Zdroj:[19]

1.3.9 RAID 6

Jedná se spíš o teoretickou záležitost. Specifikace byla sice definována, ale k praktickému využití nedošlo. Paritní informace je uložena jako u úrovně RAID 5, ale je umístěna dvojnásobně – na dvou různých discích. Výhodou je možnost výpadku dvou disků současně, aniž by se narušila integrita dat. Nevýhodou jsou extrémně dlouhé časy při zápisu. Velkost paritního prostoru je 2/(N plus 2). Redundantní informace je ukládána dvojím způsobem. [18]



Obrázek 4: RAID 6

Zdroj:[19]

1.3.10 RAID 7

Byl navržen firmou Storage Computer Corporation, která je vlastníkem patentu na tuto technologii. Architektura RAID 7 je zcela odlišná od všech předcházejících úrovní. Zatímco nižší úrovně jsou ve způsobu zpracování dat paralelními strukturami, což znamená nutnost instalace jednoho typu disku se stejnými parametry, u RAID 7 mluvíme o architektuře asynchronní. Instalované disky mohou být různého typu, kapacitu i formátu a od různých výrobců. Obnovitelnost dat je zajištěna paritní informací, která umožňuje rekonstrukci dat i při výpadku několika disků zároveň.

V systému jsou definovány tři skupiny disků – datové, paritní a stand-by (Hot-spare rezervní). Tyto používá systém automaticky k rekonstrukci dat, dojde-li k havárii disku. Pro odstranění rizika selhání logiky diskového pole je možné řídící logiku zálohovat zdvojením

(Sub-Systém Faul Tolerance). Přístupová doba se pohybuje okolo 2 milisekund. Základním principem asynchronní architektury je vzájemná nezávislost disků. Každý z nich je nezávisle řízen a má vlastní datovou cestu. To znamená, že na každý disk nebo SCSI interface lze přistupovat nezávisle na ostatních. Každá datová cesta navíc obsahuje vlastní case paměť. Asynchronní je také hierarchie řízení a využití datové sběrnice. Interní operační systém pracující v reálném čase nezávisle na hostitelském počítači řídí všechny vstupně-výstupní přenosy individuálně na všech discích pole. Na rozdíl od RAID 5, který lze rozšiřovat pouze po násobcích velikosti jeho specifické skupiny pro zápis, velikost diskové kapacity RAID 7 lze rozšiřovat lineárně. [2]

1.4 Administrativní ochrana dat

Režimovou bezpečnost tvoří komplex administrativních opatření, nařízení a systém kontrol pro zajištění bezpečnosti informačního systému. Pomocí těchto nástrojů se prosazuje respektování právních norem a zákonů (mezinárodních a národních) a bezpečnostních standardů a normativů v provozu informačního systému. Režimová bezpečnost definuje způsoby, postupy a procedury, které je nutné dodržovat pro udržení bezpečnosti IS a postupy práce, pokud se objeví problémy, především činnost v případě bezpečnostního incidentu. Respektování administrativně legislativních metod ochrany je významné z hlediska trestně právních následků při narušení bezpečnosti informačního systému a považuje se za rozhodující kritérium při posuzování charakteru vzniklých škod a určování viníků a míry jejich zavinění.

Základní procedury:

- Procedury, definující režim vstupu do objektů a místností a způsoby kontroly. Vedení přehledu o přítomnosti osob v objektech a vyhrazených prostorech.
- Metodika výběru a prověřování osob pro výkon funkcí na citlivých úsecích.
- Definice oprávněných a zakázaných činností uživatelů informačního systému, kontrola přístupu k jednotlivým zařízením a rozsah oprávnění pro manipulaci s nimi.
- Použití kryptografické ochrany. Metody generování šifrovacích klíčů a jejich distribuce, uložení a likvidace.
- Procedury způsobu označování a evidence médií. Postupy při ničení médií.
- Způsoby bezpečného zálohování dat a uložení záložních a archivních médií.

- Postup připojení nového počítače do IS.
- Postup při zřízení nového uživatelského účtu – kdo je povoluje atd.
- Postup při rušení uživatelského účtu – kdo oznamuje a komu.
- Metodika nastavení přístupových práv.
- Postup přihlášení se k systému a odhlášení.
- Postup při odchodu z pracoviště (např. zamknutí obrazovky).
- Způsoby testování požadovaných bezpečnostních parametrů. [2]

1.4.1 Řešení bezpečnostních incidentů

Opravdová panika nastává při prvním vážnějším bezpečnostním incidentu. Někdo se snaží najít pachatele, většina vedoucích funkcionářů se vrhne na administrátory a vytkne jim i to, že dýchají a pak najednou všichni zjistí, že nikdo netuší, co by měl vlastně správně dělat, a kdo něco dělá, situaci ještě zhoršuje. Asi jen výjimečně jsou předem připraveny materiály a doporučení, podle kterých by se organizace měla řídit v případě bezpečnostního incidentu.

Základní postup a pravidla řešení bezpečnostního incidentu:

- podezření na napadení informačních systému je nutné ihned hlásit,
- všechny diskriminované účty musejí okamžitě změnit heslo,
- kontrola všech účtů, jsou-li oprávněné, a zda není nějaký navíc, tzv. černá duše,
- kontrola nastavení přístupových práv a systémové politiky,
- kontrola bezpečnostních vztahů mezi doménami,
- přejmenování účtů s právy administrace. [2]

2 ZÁLOHOVÁNÍ DAT

Jedná se o mechanismus, při kterém jsou vybraná data ukládána na jiné médium, vzniká tedy jejich kopie. V případě poškození původního média jsou data obnovena ze zálohy. Z uvedeného vyplývá, že při obnově nemusíme získat všechna data, zvláště ta, která byla vytvořena od posledního zálohování. V dnešní době však existují systémy, které se o zálohování starají automaticky a na zálohovací média ukládají pouze data, která se od poslední zálohy změnila, čímž šetří čas a životnost médií, kdy nedochází k častým přepisům. Zálohování se dá též dělit na několik druhů:

- **Úplné zálohování** – jedná se o vytvoření záložní kopie všech souborů v určité oblasti.
- **Diferenciální zálohování –** zaznamenává změny, které proběhly od plné zálohy. Nespornou výhodou je úspora času a prostoru pro uložení dat oproti úplnému zálohování.
- **Inkrementální zálohování –** zálohování pouze souborů, které se změnily od posledního úplného zálohování nebo inkrementálního zálohování.
- **Zálohování vybraných dat –** jde o zálohování pouze zvolených souborů, adresářů a systémových oblastí.
- **Záloha systémových oblastí disku** – je záloha, kde jsou uloženy vitálně důležité informace pro zpřístupnění disku a o jeho struktuře, o adresářové a souborové struktuře, pro zavádění operačního systému.
- **Zálohování pouze dat –** jedná se o strategii zálohování, při níž nejsou zálohovány programy, ale pouze datové oblasti (soubory). Volba této strategie souvisí s relativně snadnou obnovou programů reinstalací. [20]

2.1 Disková pole

Velice častým způsobem zálohování je duplikování nosičů dat, či distribuovaným ukláním částí dat na několik disků zároveň. Tato problematika je popsána výše v technické bezpečnosti a diskových polích RAID.

2.2 Přenosná média

Jedná se o zajímavou alternativu k diskovým polím, zvláště díky možnosti jednoduché přenositelnosti médií. Data se zálohují např. na CD a DVD, flashdisky, či externí pevné disky. Ovšem tato média mají svá omezení, zejména se jedná o jejich kapacitu a životnost. Přenosná média jsou tedy vhodná zejména k drobným zálohám dokumentů, fotografií, či jiným nepříliš kapacitně náročným datům.

2.2.1 CD a DVD

Disky CD se nabízejí nejčastěji v kapacitě 700 MB, a kromě hudebního odvětví jsou dnes na ústupu. Zejména díky svojí nízké kapacitě a fyzické velikosti. Mají ovšem velice dobrou životnost dat na nich uložených, za dobrých podmínek i 100 let. DVD disky nabízejí vyšší kapacity než CD, konkrétně 4,7 GB, v případě dvouvrstvého DVD potom 8,5 GB. Poskytuje také efektivnější korekci chyb. Tyto disky dosahují stejné životnosti jako CD. [21]

2.2.2 Flashdisky

Jedná se o zařízení, které se připojuje pomocí sběrnici USB. Charakteristické je svojí kompaktností, odolností vůči fyzickému poškození a nabízí vyšší kapacitu než CD nebo DVD, v dnešní době i stovky GB. Jejich nevýhodou je však nízká životnost uložených dat, která v ideálních podmínkách dosahuje cca 10 let.

2.2.3 Externí HDD

Jde o klasický pevný disk uložený většinou v plastovém pouzdru, vybaveném potřebnou elektronikou pro připojení pomocí USB. Oproti flashdisku nabízejí vyšší kapacitu, vykoupenou svými rozměry a náchylnosti k mechanickému poškození. Data na nich uložená mají životnost kolem 50 let.

2.3 Internetové úložiště

Velice zajímavou variantou zálohování je ukládání dat přes internet na různá úložiště. Tento prostor bývá většinou zpoplatněn a rychlost zálohování závisí na rychlosti připojení k internetu. Zálohování větších objemů dat tímto způsobem může být velice zdlouhavé. Provozovatelé placených služeb ovšem garantují vlastní pravidelné zálohování a v případě poškození disků v serveru ihned obnovují data z vlastních záloh. Další výhodou tohoto typu zálohování je přístup k datům prakticky odkudkoliv, kde je dostupné připojení k internetu. [21]

3 INTERNETOVÝ OBCHOD BAZENPRO.CZ

V následující kapitole se budu zabývat popisem internetového obchodu **bazenpro.cz** společnosti Brück AM. Obchod slouží k prodeji bazénové a jezírkové chemie. Dále bude popsáno zabezpečení v rámci firmy a návrh možných opatření pro zlepšení bezpečnosti dat a jejich zálohování.

3.1 O společnosti

Brück AM spol. s r.o., byla založena v roce 1993 a výrobu v Zámrsku u Vysokého Mýta zahájila o dva roky později. Dnes je nejvýznamnější evropskou pobočkou německé rodinné firmy Brück GmbH z Ensheimu. Mateřská společnost má více než 85letou strojírenskou tradici a bohaté zkušenosti například s dodávkami pro vesmírný program Ariane, plynovod Nord Stream nebo pro vodovodní síť v New Yorku. Certifikace významných společností jako jsou TÜV, Lloyds Register, DET NORSKE VERITAS apod. ji předurčují vyrábět a prodávat do široké škály průmyslových odvětví.

Český Brück vyrábí nejrůznější součásti rotačního charakteru pro energetický a petrochemický průmysl, stavebnictví, dopravu, potravinářství či farmacii. Patří k nejmodernějším a technologicky nejlépe vybaveným strojírenským provozům u nás. Má uzavřený výrobní cyklus s uceleným řetězcem více než 70 výrobních zařízení pro řezání, lisování, válcování, tepelné zpracování a mechanické obrábění. V nepřetržitém provozu je již řadu let používá pro těžké i lehké obrábění na karuselech a horizontálních soustruzích, ale také na frézkách, vrtačkách a obráběcích centrech. Pomocí magnetických upínacích systémů Brück AM obrábí výkovky, výpalky, jednotlivé segmenty mezikruží, svařence nebo odlitky.

Brück AM zaměstnává v Česku zhruba 250 lidí. O internetový obchod **bazenpro.cz,** zabývající se prodejem bazénové a jezírkové chemie, se starají dva zaměstnanci z obchodního oddělení a jeden člen IT týmu.

3.1.1 Fyzická ochrana

Jak již bylo popsáno výše, fyzická bezpečnost se zabývá především zabezpečením budov, ve kterých se data nacházejí, ochranou před přírodními vlivy a opatřeními proti neoprávněnému vniknutí osob do objektů.

Pro konkrétní internetový obchod je tedy nutné zjistit, kde je umístěn firemní server, jak se k němu dostat a jak je fyzicky chráněn. V první řadě je nutné server umístit do příslušné

místnosti, která musí splňovat požadavky na bezpečné uložení a ochranu dat. Je nutné brát v potaz náročnost na chlazení serveru, ochranu proti požáru, povodním a závadám ve vodovodních sítích. Místnost, kde se server nachází, musí být vybavena různými senzory pro detekci nežádoucích situací, například požárními detektory. Firemní server pro přístup k síti společnosti se nachází v suterénu hlavní budovy společnosti, kde je dobře chráněn proti přírodním vlivům a případným požárům, díky bezpečnostním dveřím. Co se týče chlazení, místnost je vybavena systémem pro sledování teploty a větráním. Dodávka elektrické energie je zde chráněna napájecím zdrojem UPS typu on-line. Internetový obchod je provozován na webhostingu společnosti INTERNET CZ a. s. působící pod značkou FORPSI.

FORPSI se pyšní užíváním špičkových technologií pro zabezpečení dat. Datacentrum je pod stálým dohledem a stěžejní infrastruktura je řešena redundantně. Přístup do datacentra a technologických prostor je zabezpečen čipovým systémem a pohyb osob v prostorách je monitorován. Okolí datacentra je nepřetržitě monitorováno pomocí kamerového systému. Fyzické zabezpečení je dále řešeno pomocí detektorů požáru, automatickým alarmem a plynových hasícím systémem Siemens s inertním hasicím plynem FM200. Dodávka elektrické energie je chráněna pomocí UPS. Bateriový sál je oddělen od ostatních prostor datacentra a nabízí dvě na sobě nezávislé skupiny UPS. Společnost je v případě rizik vybavena vlastním záložním zdrojem energie (dieselgenerátorem) s podzemní nádrží pro agregátor o objemu 6000 l. Jsou zde přítomny vlastní trafostanice se dvěma transformátory a napájení probíhá ze dvou nezávislých elektrických větví.

Sídlo společnosti Brück AM spol. s r.o. se nachází na otevřeném prostranství, venkovní prostory jsou monitorovány pomocí kamerových systémů a jsou ohraničeny plotem. Vjezd na parkoviště je zabezpečen závorami a je se na něj možné dostat pomocí čipové karty zaměstnance, která mimo jiné slouží jako evidence pro příchody a odchody z pracoviště, nebo na pokyn ostrahy, která sídlí právě u vjezdu do společnosti. Ostraha tedy monitoruje veškerý pohyb ve venkovních prostorech a příjezdy a odjezdy dopravních prostředků. Jak již bylo zmíněno, tak server se nachází v hlavní budově společnosti, ta je sama o sobě velice dobře zabezpečeným místem. Kromě recepce jsou zde kanceláře, jídelna a zasedací místnosti. Server se nachází v suterénu budovy, cesta k němu vede skrz recepci, chodbu sousedící s jídelnou a několika kancelářemi. Následuje monitorované schodiště a poté další chodba a v poslední řadě zamčené bezpečnostní dveře. Potencionální útočník by tedy musel překonat množství bezpečnostních prvků, aby se mohl fyzicky dostat do serverové místnosti.

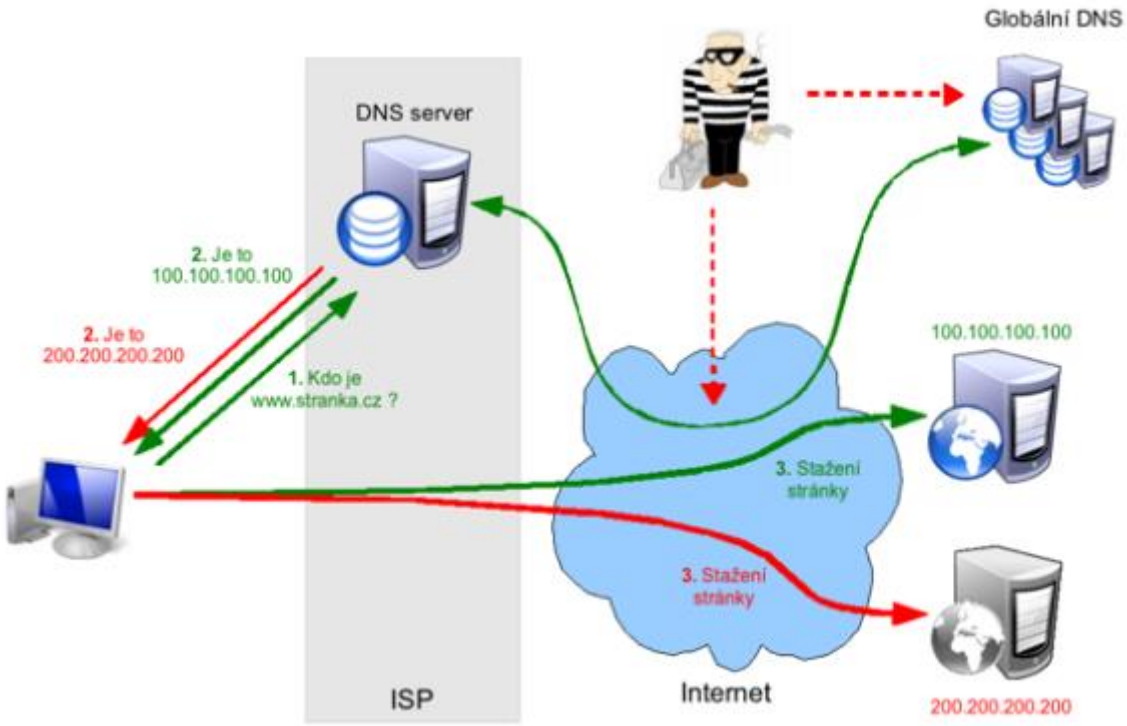
V rámci fyzické ochrany je nutné chránit i data vzniklá použitím internetového obchodu. V okamžiku nákupu jsou data uživatele zpracována a dochází ke vzniku faktury za objednané zboží. V rámci společnosti zde dochází k uchování fyzické kopie faktury, která je uložena do pořadače. Je tedy nutné zajistit správné umístění, aby nedošlo k neoprávněnému přístupu k datům, která se na faktuře nacházejí. Pořadače pro aktuální rok jsou umístěny v kanceláři zaměstnance, který vyřizuje objednávky z obchodu. Na konci roku jsou přesunuty do archivu společnosti, kde jsou uchovány po dobu stanovenou zákonem. Po uplynutí této doby jsou následně záznamy skartovány.

3.1.2 Logická ochrana

Logická ochrana dat zahrnuje mechanizmy, jimiž se operační systémy či jiný software snaží předejít neautorizovanému přístupu k citlivým informacím či datům. V rámci společnosti je tedy nutné vyřešit, jaká přístupová práva bude mít každý zaměstnanec, který bude využívat firemní síť. V rámci internetového obchodu je nutné zajistit, aby registrovaný uživatel nemohl provádět neautorizované změny a aby byl přístup k databázi s daty poskytnut pouze osobám, které jsou oprávněné s nimi nakládat. Správa internetového obchodu je realizována pomocí doplňku PrestaShop v rámci webhostingu. Přihlášení do tohoto doplňku probíhá pomocí emailové adresy a hesla, které obsahuje podmínku velkého znaku a číslice, nový účet může vytvořit pouze uživatel s administrátorskými právy. V rámci společnosti mají aktuálně přístup do správy internetového obchodu tři pracovníci. Jedná se o dva členy obchodního oddělení, které vyřizuje objednávky a aktualizuje zboží, a jednoho člena IT týmu, který má na starost chod internetového obchodu. V rámci společnosti je přístup do firemní sítě chráněn právy uživatelských účtů na jednotlivých počítačích, ve většině případů není možné instalovat vlastní software bez administrátorského hesla. Je tím zajištěno, aby pracovník nemohl instalovat aplikace, které by mohly přistupovat k prostředkům, které by mohly ohrozit bezpečnost firemních dat.

Webhosting poskytuje ochranu pomocí SSL certifikátů a rozšíření DNNSEC. Protokol SSL slouží k zabezpečení komunikace šifrováním, k autentizaci komunikujících stran a zajišťuje zabezpečení komunikace proti odposlechu. Při odesílání citlivých dat má uživatel jistotu, že komunikuje s tím, s kým opravdu chtěl komunikovat. Ustavení SSL spojení funguje na principu asymetrické šifry. Každá z komunikujících stran má dvojici šifrovacích klíčů: veřejný a soukromý. Veřejný klíč je nutné zveřejnit a zajistit jeho správné předání všem, kteří jej budou chtít použít. Pokud pomocí tohoto klíče kdokoliv zašifruje zprávu, je zajištěno, že ji bude moci

rozšifrovat jen majitel použitého veřejného klíče odpovídajícím soukromým klíčem. DNSSEC je rozšíření systému doménových jmen (DNS), které zvyšuje jeho bezpečnost. DNSSEC poskytuje uživatelům jistotu, že informace, které z DNS získal, byly poskytnuty správným zdrojem, jsou úplné a jejich integrita nebyla při přenosu narušena. DNSSEC zajistí důvěryhodnost údajů získaných z DNS. Všechny internetové služby využívají systém doménových jmen. Jeho základním principem je to, že umožňuje v adresách těchto služeb používat jména, která jsou srozumitelná a snadno zapamatovatelná pro člověka, namísto čísel, která jsou srozumitelná a potřebná pro počítače. V praxi to pak funguje tak, že kdykoliv uživatel použije jmennou adresu nějaké internetové služby (webové stránky, emailovou adresu atd.), je nutné ji přeložit pomocí DNS na adresu číselnou a na tuto číselnou adresu se pak počítač obrátí, aby se spojil se službou, kterou uživatel chce použít. V případě, že někdo dokáže podvrhnout číselnou adresu, uživatel se, aniž bude cokoliv tušit, dostane na úplně jiné místo, a vůbec se nespojí se službou, kterou očekával. Může to vypadat třeba jako na následujícím obrázku.



Obrázek 5: DNS adresa

Zdroj: dnssec.cz

Uživatel napíše do svého prohlížeče adresu a za normálních okolností vše probíhá zeleně označenou cestou – použije server svého poskytovatele připojení (ISP), a ten z globálního DNS systému získá číselnou adresu, se kterou se uživatel spojí a používá službu, kterou chtěl. V případě, že je však číselná adresa podvržena, pak vše probíhá červeně označenou cestou,

a uživatel je spojen s jinou službou, aniž cokoli tuší. Toto může být v rámci internetového obchodu velký problém např. při platbě kartou. Služba DNNSEC však zajišťuje, aby k napadení výše popsaným způsobem nedošlo.

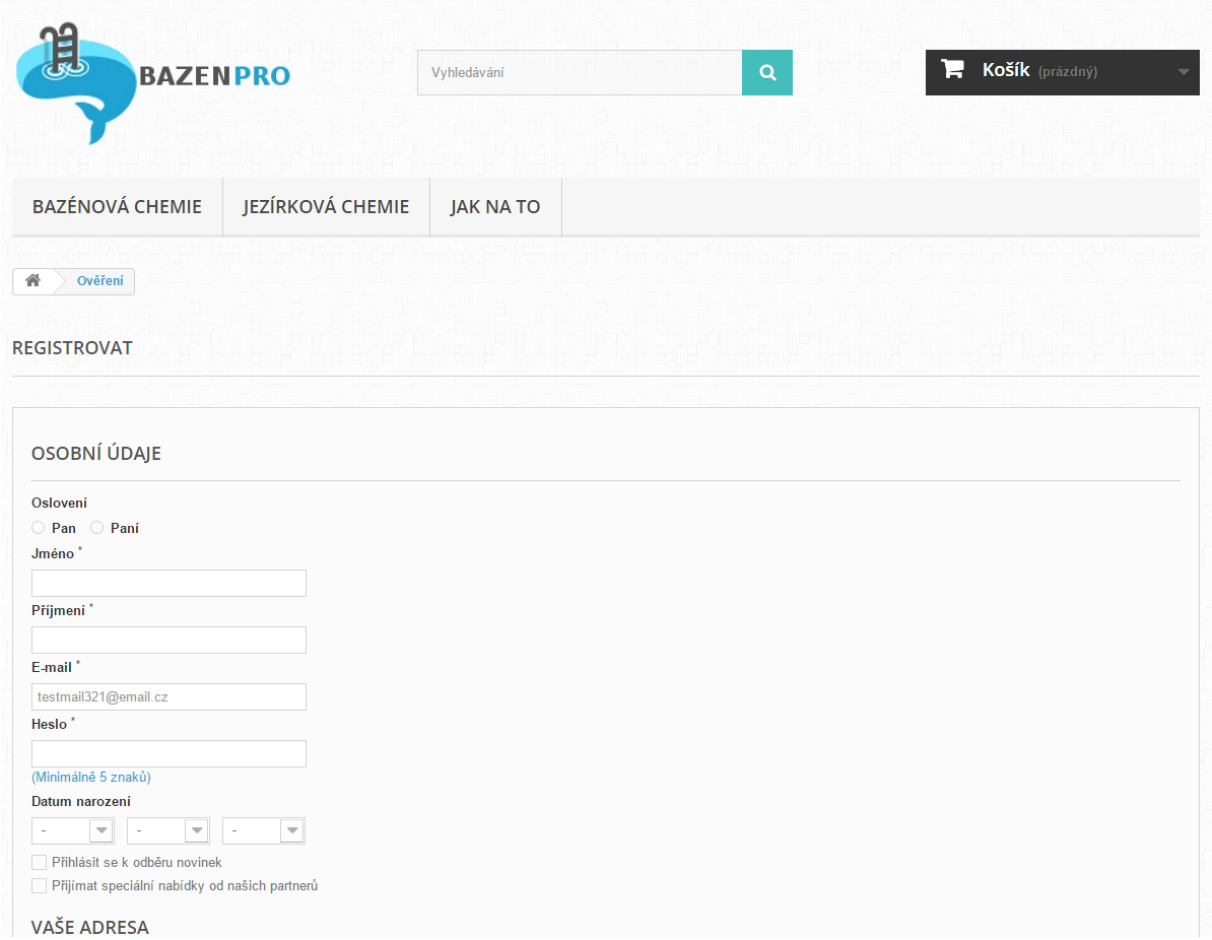
3.1.3 Technická ochrana a zálohování

Jedná se o ochranu dat pomocí využití vhodného technického vybavení. Pod tímto pojmem však v technické bezpečnosti chápeme především zajištění dostupnosti a integrity, tj. neporušenosti informací. Technická bezpečnost řeší problém nosičů dat tak, že navrhuje systémy s vysokou redundancí, tj. s vysokou odolností proti chybám. Redundance se dá též označit jako nadbytečnost. Jedná se o část dat, která mohou být odstraněna, aniž by došlo ke ztrátě informace. Redundancí se zabývají disková pole RAID, která jsou popsána výše. Pole RAID v tomto případě slouží i k zálohování dat, protože při poruše např. jednoho disku nedojde ke ztrátě dat, jelikož se data nacházejí na několika discích zároveň. Data internetového obchodu jsou složena ze samotného kódu stránky, databáze produktů a databáze registrovaných uživatelů a jsou uložena a spravována na webhostingu. Problém zde může nastat při přenosu informace k pracovníkovi, který má objednávky z obchodu na starost, a následném zadání do ekonomického systému. Z webhostingu informace ohledně objednávky putují do emailové schránky a jsou následně pracovníkem manuálně zadávány do ekonomického systému. Zde vidím problém, protože největší slabinou systému je zde lidský faktor. Problém bych řešil propojením internetového obchodu a ekonomického systému, aby nedošlo k porušení informací při přenosu.

3.2 Prostředí internetového obchodu

3.2.1 Registrace uživatele

Pro registraci uživatele a tvorbu nového účtu slouží registrační formulář, kde uživatel zadá svoje jméno, příjmení, email, adresu a telefon. Uživatel si také zvolí přístupové heslo, které musí obsahovat nejméně 5 znaků. Následně se ke svému účtu přihlašuje pomocí emailové adresy a zvoleného hesla.

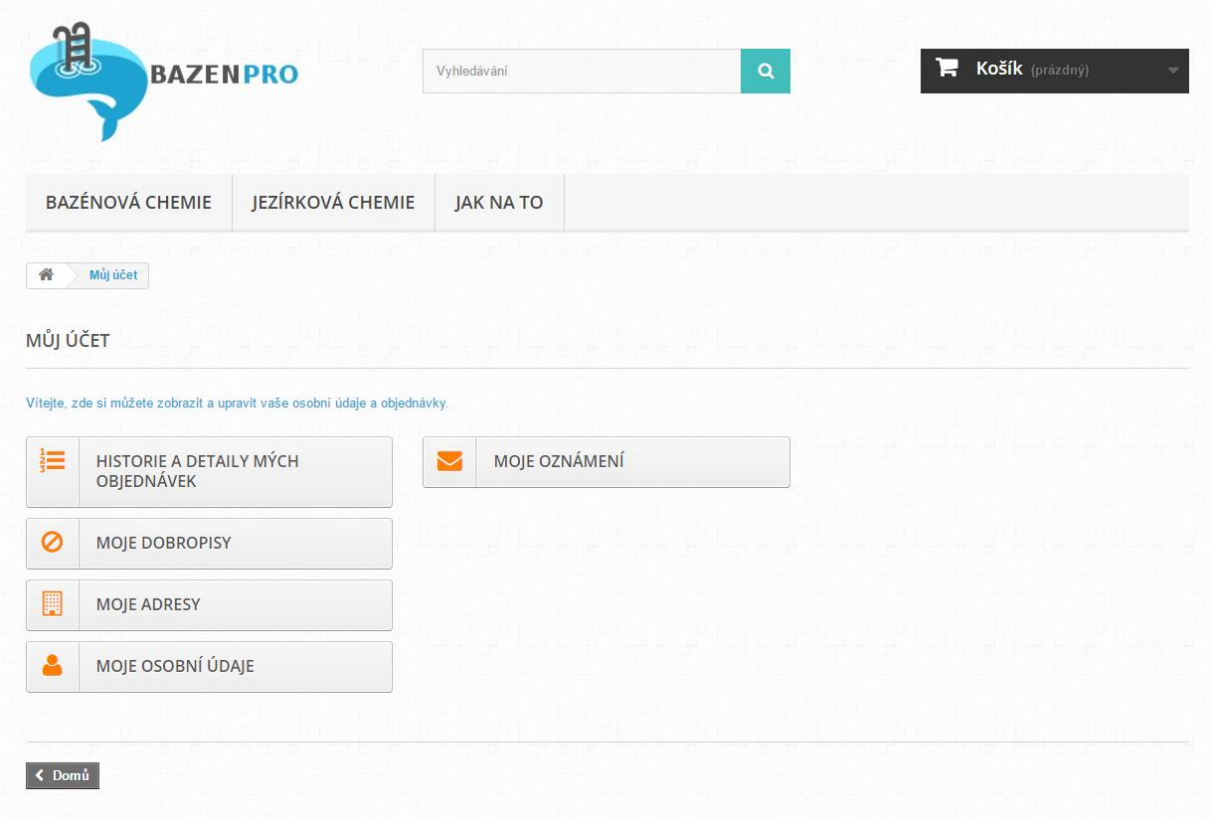


Obrázek 6: Registrační formulář

Zdroj: bazenpro.cz

3.2.2 Účet uživatele

Uživatelský účet slouží uživateli k lepšímu přehledu o jeho objednávkách a usnadňuje opakovaný nákup zboží. Uživateli se po registraci a následném přihlášení objeví možnost zobrazení historie a detailů jednotlivých objednávek, dobropisů, správa adres, správa osobních údajů a oznámení od internetového obchodu.



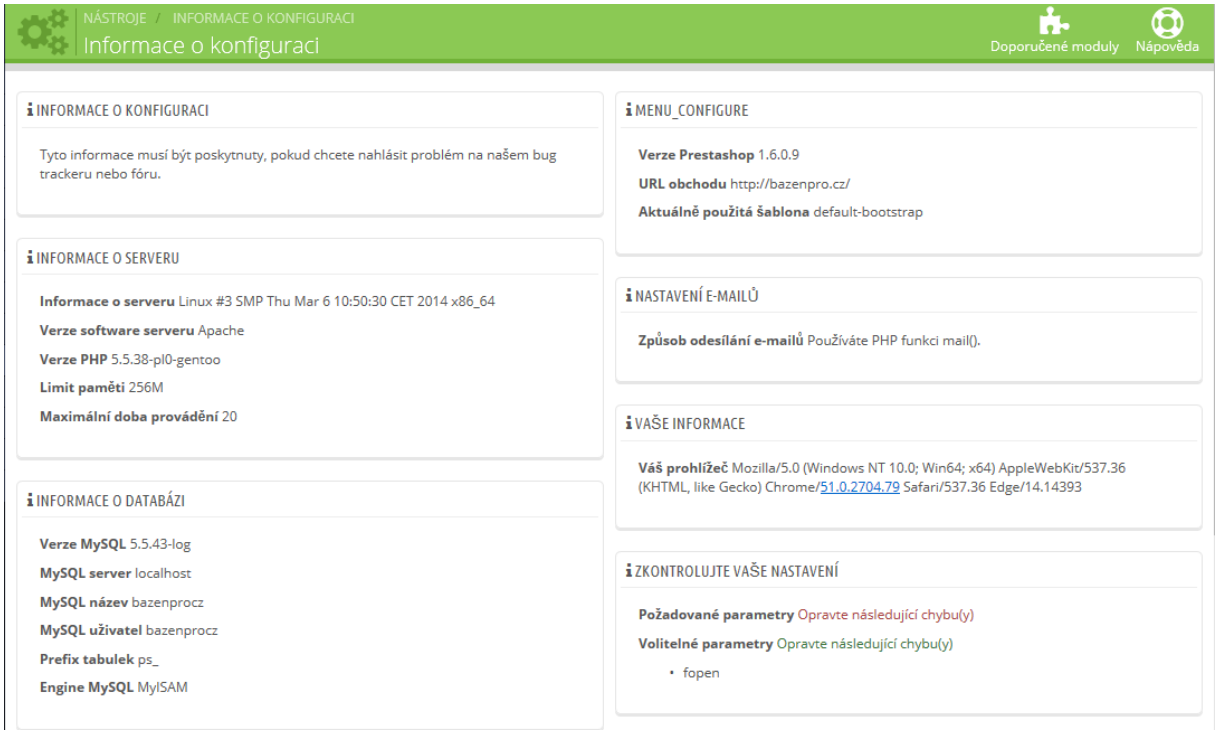
Obrázek 7: Po přihlášení

Zdroj: bazenpro.cz

3.2.3 Administrace

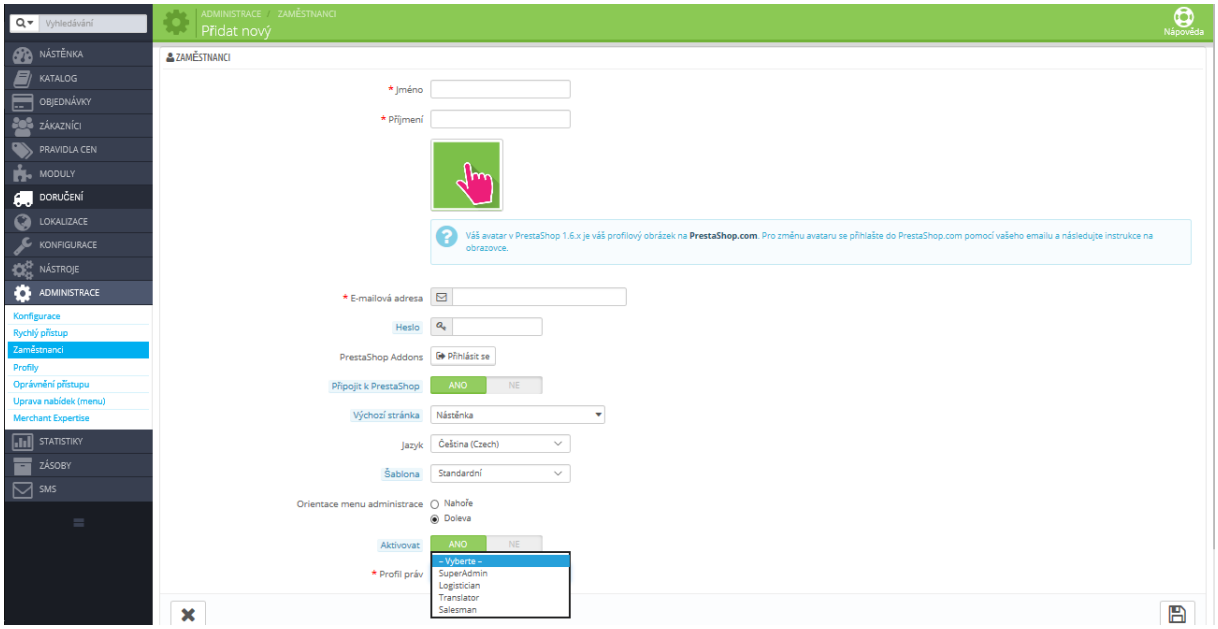
Pro potřeby správy internetového obchodu slouží administrátorské rozhraní, ve kterém je možné přidávat a upravovat jednotlivé produkty z nabídky a slouží také ke správě uživatelských účtů. Tento systém by neměl být přístupný uživateli, aby nedošlo k neoprávněným změnám např. ceny zboží. Jak již bylo zmíněno, ke správě obchodu slouží doplněk PrestaShop. Na obrázku níže jsou vidět základní informace o konfiguraci. V rámci správy lze přiřadit zaměstnanci jeden ze čtyř profilů práv: SuperAdmin, Logistician, Translator a Salesman. Každý z těchto profilů má vlastní oprávnění přístupu. SuperAdmin je výchozím nastavením v rámci doplňku, jeho práva nelze nijak měnit, uživatel s tímto oprávněním má práva přistupovat kamkoliv. Může přidávat nové zboží do katalogu, spravovat objednávky, nahlížet do záznamů o zákaznících, nastavovat pravidla cen, přidávat moduly, spravovat zásoby, zobrazovat statistiky, přidávat a mazat uživatele. Profil Logistician umožňuje uživateli prohlížet katalog, sledovat objednávky, zjistit adresu zákazníka, spravovat skladové zásoby a možnosti doručení. Nejméně práv má profil Translator, který má možnost zobrazit si katalog produktů a v rámci lokalizace měnit překlady. Posledním profilem je Salesman, který má podobná práva jako

Logistician, ovšem nemá možnost upravovat skladové zásoby a možnosti doručení, může však přistupovat ke statistikám prodejů v rámci obchodu.



Obrázek 8: Informace o konfiguraci

Zdroj: bazenpro.cz

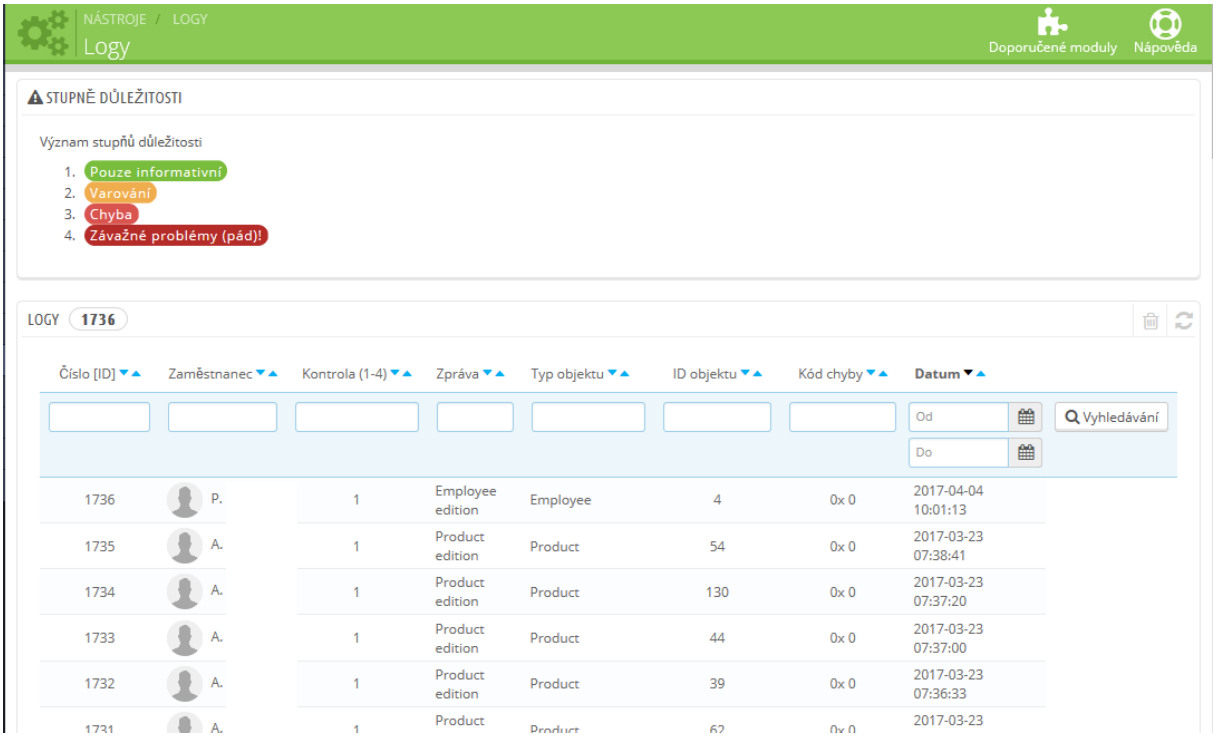


Obrázek 9: Tvorba nového uživatele

Zdroj: bazenpro.cz

3.2.4 Logování

Důležitou součástí chodu a správy internetového obchodu je logování činností jednotlivých uživatelů. Logy zaznamenávají události odehrávající se v systému, aby mohly podat záznam o činnostech tak, aby bylo možné pochopit chování systému a diagnostikovat případné problémy. V rámci chodu konkrétního internetového obchodu se zaznamenává, jaký zaměstnanec změnu provedl, jakou má změna dopad na systém, krátký popis činnosti, oblast, ve které byla provedena a datum provedení.



Obrázek 10: Logování

Zdroj: bazenpro.cz

3.3 Návrh řešení

Internetový obchod společnosti je uložen na webhostingu, kde k němu mohou přistupovat zákazníci pomocí protokolu http. Mimo objednávky si mohou založit vlastní účet pro přehled o objednávkách. Administrace zaměstnanci je řešena pomocí doplňku PrestaShop. K administraci mají přístup tři zaměstnanci, veškeré změny, které v rámci obchodu provedou, jsou zaznamenávány pomocí logů.

3.3.1 Fyzická bezpečnost

Žádné zabezpečení není bezchybné a vždy se dá najít skulina v použitém systému. V rámci fyzické bezpečnosti jsou data chráněna dobře a nejsou nutná žádná opatření. Server společnosti je umístěn v zabezpečené místnosti a též archiv s kopiemi faktur. Zvolený poskytovatel webhostingu disponuje moderními technologiemi pro zajištění bezpečnosti dat.

3.3.2 Logická bezpečnost

Logická bezpečnost by ovšem zasloužila vylepšení. Už při samotném vstupu do internetového obchodu hlásí prohlížeč, že spojení s webem není bezpečné. Tento problém je spojen s použitím protokolu HTTP namísto bezpečnějšího HTTPS, toto se týká také přihlášení do administrace obchodu. Poskytovatel webhostingu tuto možnost nabízí za mírný poplatek, který se z mého pohledu zdá adekvátní, takže bych této možnosti jistě využil. Dále bych určitě implementoval rozšíření DNNSEC, popsané výše. Další problém vidím při registraci uživatele do internetového obchodu, kde jsou na jeho emailovou adresu odeslány přihlašovací údaje, včetně hesla v textové podobě. Toto mi přijde velice nevhodně řešené, protože mnoho uživatelů používá stejné heslo do více služeb a pokud by došlo k jeho úniku, mohlo by to mít značné následky. Heslo bych v textové podobě určitě neposílal, spíše bych využil možnosti resetování hesla v případě zapomenutí.

Navrhnutá opatření:

- Použití protokolu HTTPS pro obchod a jeho administraci.
- Implementace rozšíření DNNSEC.
- Změna údajů zasílaných na emailovou adresu zákazníka.

3.3.3 Technická bezpečnost

Technická bezpečnost se dá také vylepšit. Jak bylo popsáno výše, informace ohledně objednávky putují z webhostingu do emailové schránky zaměstnance, který je následně zadává do ekonomického systému. Zde může zásluhou lidského faktoru dojít k chybě v zadávaných datech. Toto lze vyřešit propojením internetového obchodu a ekonomického systému, ovšem pokud by společnost chtěla spojení provést, určitě musí prvně vyřešit problémy v logickém zabezpečení a použít protokol HTTPS.

Navrhnutá opatření:

- Propojení internetového obchodu a ekonomického systému.
- Související použití protokolu HTTPS pro obchod a administraci.

3.3.4 Administrativní bezpečnost

V rámci administrativní bezpečnosti bych viděl problém v právech zaměstnanců při přístupu do administrace obchodu, kde každý ze tří pracovníků má práva SuperAdmin. Pokud by se některý ze zaměstnanců rozhodl ostatní smazat, nebude mu to činit problémy. Řešení tohoto problému je velice snadné, stačilo by použít jiný profil práv, či jednotlivým zaměstnancům vytvořit práva přímo v rozsahu činností, které v rámci internetového obchodu provádějí. Zaměstnancům obchodního oddělení by určitě neuškodilo školení ohledně fungování administrace, sami vypověděli, že s její obsluhou mají často problémy.

Navrhnutá opatření:

- Změna práv zaměstnanců starající se o chod obchodu.
- Proškolení zaměstnanců.

ZÁVĚR

Cílem této bakalářské práce je popsat současné technologie zaměřené na zálohování a zabezpečení dat v internetových obchodech a zároveň analýza současného stavu a návrh řešení pro vybranou firmu. Před analýzou internetového obchodu bazenpro.cz byly vysvětleny základní pojmy a postupy vztahující se k bezpečnosti dat.

Práce se nejprve zaměřuje na charakteristiku jednotlivých přístupů k zajištění bezpečnosti dat, konkrétně se jednalo o fyzický přístup, logický přístup, technický přístup a administrativní přístup. V rámci fyzické ochrany dat byly popsány základní mechanismy sloužící k zabezpečení dat před přírodními vlivy, požáry, nepovolanými osobami a poruchami v rozvodné elektrické síti. Dále byly vysvětleny základní technologie pro monitoring osob, požadavky na umístění a vybavení místnosti se servery. V logické ochraně dat je zahrnuto především řízení přístupu k informacím, které je rozděleno na techniky přenechání či nepřenechání volnému uvážení. Technická ochrana dat se zaměřuje na problematiku diskových polí RAID, jsou zde vylíčeny základní principy jejich fungování, možnosti přístupu, umístění a jejich výhody a nevýhody. Administrativní ochrana je popsána základními procedurami, které je nutné dodržovat pro udržení bezpečnosti IS, dále jsou zde postupy a pravidla při řešení bezpečnostních incidentů.

Další část práce je věnována zálohování dat, jsou zde stručně objasněny základní druhy zálohování, přenosná média, na která se zálohy ukládají, konkrétně se jedná o CD a DVD disky, flashdisky a externí pevné disky. Je zde zmíněna i možnost ukládání zálohovaných dat na internetové úložiště.

Závěrečná část práce je zaměřena na analýzu současného stavu zabezpečení internetového obchodu bazenpro.cz a současně i návrh opatření pro zlepšení tohoto stavu. Jsou zde popsány jednotlivé přístupy k zabezpečení dat (fyzický, logický a technický) z první části práce. Dále je charakterizováno prostředí a fungování internetového obchodu, včetně rolí jednotlivých zaměstnanců, kteří mají přístup k administraci obchodu. Navrhnutá bezpečnostní opatření byla konzultována se všemi členy týmu a v současné době se pracuje na jejich implementaci.

LITERATURA

[1] PŘIBYL, Jiří a Jindřich KODL. *Ochrana dat v informatice*. Praha: České vysoké učení technické, 1996. ISBN 80-01-01664-1.

[2] DOBDA, Luboš. *Ochrana dat v informačních systémech*. Praha: Grada, 1998. ISBN 80-7169-479-7.

[3] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

[4] *Strážní služba*. [online]. [cit 2017-14-06]. Dostupné z: http://www.cms-top.cz/strazni-sluzba

[5] UHLÁŘ, Jan. *Technická ochrana objektů*. 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-313-0.

[6] *Systémy průmyslové televize CCTV*. [online]. [cit 2017-14-06]. Dostupné z: http://www.hdelektro.cz/index.php?nabidka=1&str=21

[7] *Mechanické zábranné systémy.* [online]. [cit 2017-14-06]. Dostupné z: http://www.bepo.eu/shortcode/mzs

[8] HUB, Miloslav. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice: Univerzita Pardubice, 2013. ISBN 978-80-7395-701-8.

[9] *Jak zlikvidovat důvěrná data?.* [online]. [cit 2017-14-06]. Dostupné z: http://storage.diskus.cz/newslwtter/344-jak-zlikvidovat-duverna-data-.html

[10] *Degaussing – bezpečné mazání dat.* [online]. [cit 2017-14-06]. Dostupné z: http://storage.diskus.cz/katalog-sluzeb/10-0-degaussing---bezpecne-mazani-dat.html

[11] *Datové centrum (Data Centre).* [online]. [cit 2017-14-06]. Dostupné z: https://managementmania.com/cs/datove-centrum-data-centre

[12] *Záložní zdroje elektrické energie – 2.díl: Statické zdroje*. [online]. [cit 2017-14-06]. Dostupné z: http://oenergetice.cz/technologie/zalozni-zdroje-elektricke-energie-2-dil-staticke-zdroje/

[13] PETRO, Jozef. *Výkladový slovník internetu*. Praha: CP Books, 2005. ISBN 80-722-6222-x.

[14] RASMUSSEN, Niel. *Různé typy systémů UPS* [online]. [cit. 2017-04-14]. Dostupné z: http://www.apc.com/salestools/SADE-5TNM3Y/SADE-5TNM3Y_R7_CZ.pdf

[15] MARKIEWITZ, H., KLAJN,A.: *Resilience Improving Reliability with Standby Power Supplies*, 6/2003, Dostupné z: http://www.leonardo-energy.org/drupal/node/3001.

[16] MATYÁŠ, Vašek a Jan KRHOVJÁK. *Autorizace elektronických transakcí a autentizace dat i uživatelů*. Brno: Masarykova univerzita, 2008. ISBN 978-80-210-4556-9.

[17] *Hardware RAID versus Software RAID* [online]. [cit. 2017-04-14]. Dostupné z: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/3/html/System_Administration_Guide/s1-raid-approaches.html

[18] DOČEKAL, Michal. *Správa linuxového serveru: RAID teoreticky* [online]. [cit. 2017-04-14]. Dostupné z: https://www.linuxexpres.cz/praxe/sprava-linuxoveho-serveru-raid-teoreticky

[19] *RAID* [online]. 2017 [cit. 2017-04-14]. Dostupné z: https://www.prepressure.com/library/technology/raid

[20] ZELENKA, Josef, Karel NAIMAN a Pavel ČECH. Ochrana dat: informační bezpečnost - výkladový slovník. Hradec Králové: Gaudeamus, 2002. ISBN 80-7041-197-x.

[21] BUDAI, David, Stanislav JANŮ a Dominik DĚDIČEK. *Bible vypalování a zálohování 2012*. Brno: Extra Publishing, 2011. ISSN 1802-1220.