VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH PLÁNU OBNOVY PRO INFRASTRUKTURU PODNIKATELSKÉ FAKULTY

DRAFT RECOVERY PLAN FOR THE INFRASTRUCTURE OF THE FACULTY OF BUSINESS AND MANAGEMENT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Jan Srnec**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Jan Srnec**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2020/21

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

Návrh Plánu obnovy pro infrastrukturu podnikatelské fakulty

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem práce je návrh Plánu obnovy pro infrastrukturu podnikatelské fakulty ve formě metodiky a potřebných směrnic.

Základní literární prameny:

ČSN ISO/IEC 27001, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky, Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27031, Informační technologie - Bezpečnostní techniky - Směrnice pro připravenost informačních a komunikačních technologií pro kontinuitu činnosti organizace, 2016.

ISO/IEC 24762 Information technology — Security techniques – Guidelines for information and communications technology disaster recovery services, 2008.

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

PRESTON C. W. Backup & Recovery. Sebastopol. O'Reilly Media, 2009. ISBN 978-0-596-10246-3.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2020/21

V Brně dne 28.2.2021

L. S.

Mgr. Veronika Novotná, Ph.D. ředitel	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Tato diplomová práce se zabývá návrhem plánu obnovy při katastrofě pro serverovnu Ústavu informatiky Fakulty podnikatelské při VUT v Brně. V první části jsou popsána teoretická východiska jednotlivých částí plánu obnovy, která slouží jako podklad pro samotný návrh. V druhé části práce je uveden popis serverovny Ústavu informatiky a vše, co se týče jeho IT aktiv. Třetí část se zabývá samotným návrhem plánu obnovy při katastrofě, který bude sloužit jako vnitřní směrnice školy a podklad pro dokument o systému řízení kontinuity činností.

Klíčová slova

kybernetická bezpečnost, plán obnovy při katastrofě, rizika, server, IT služby

Abstract

This diploma thesis deals with the proposal of a “Disaster Recovery Plan” for the Informatics department at BUT’s Faculty of Business and Management. The first part consists of theoretical basis of crucial parts of disaster recovery plan, which is the very foundation for the proposal itself. The second part follows up with a description of the server room of the Informatics department, in particular its IT equipment. The third part deals with the very disaster recovery plan proposal which will function as a school code regulation and a foundation for a Business Continuity Management System document.

Key words

cyber security, disaster recovery plan, threats, server, IT services

Bibliografická citace

SRNEC, Jan. *Návrh Plánu obnovy pro infrastrukturu podnikatelské fakulty* [online]. Brno, 2021 [cit. 2021-05-14]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/133637. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

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

V Brně dne 16. května 2021 ……

Poděkování

Rád bych vyjádřil poděkování vedoucímu mé diplomové práce panu Ing. Petrovi Sedlákovi za ochotu a cenné rady při vedení práce. Dále bych chtěl poděkovat rodině za trpělivost a podporu během mého studia.

OBSAH

ÚVOD 12

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ 13

1 TEORETICKÁ VÝCHODISKA PRÁCE 14

1.1 Základní pojmy 14

1.2 Analýza rizik 16

1.3 ISMS 17

1.4 Řízení kontinuity činností 18

1.5 Plán obnovy při katastrofě 21

1.5.1 Cílový čas a bod obnovy 21

1.5.2 Struktura DR plánu 23

1.5.3 Předpoklady kvalitního DR plánu 24

1.5.4 Druhy DR plánů 25

1.5.5 Testování DR plánu 26

1.6 Použité normy a legislativa 27

1.6.1 Řada norem ISO 27000 27

1.6.2 ISO 22301 28

1.6.3 ISO 24762 29

1.6.4 NIST 800-184 29

1.6.5 Vyhláška č. 82/2018 sb. 29

2 ANALÝZA SOUČASNÉHO STAVU 30

2.1 Stručný popis lokality a budovy 30

2.2 Analýza současné infrastruktury 30

2.3 Fyzická aktiva a jejich ohodnocení 32

2.3.1 Fyzické a virtuální servery 34

2.3.2 Návaznost serverů 35

2.3.3 Servery s prioritou 1 37
2.3.4 Servery s prioritou 2 38
2.3.5 Servery s prioritou 3 39
2.3.6 Servery s prioritou 4 39
2.3.7 Podpůrná infrastruktura 40
2.4 Aktiva služeb a jejich ohodnocení 42
2.4.1 Návaznost služeb 43
2.4.2 Služby s prioritou 1 44
2.4.3 Služby s prioritou 2 45
2.4.4 Služby s prioritou 3 45
2.4.5 Služby s prioritou 4 46
2.4.6 Externí služby 46
2.5 Analýza rizik 47
2.5.1 Tabulky pro ohodnocení zranitelností a hrozeb 47
2.5.2 Zranitelnosti fyzických aktiv 48
2.5.3 Hrozby fyzických aktiv 50
2.5.4 Zranitelnosti služeb 52
2.5.5 Hrozby služeb 54
2.5.6 Další hrozby 55
3 VLASTNÍ NÁVRH PLÁNU OBNOVY 57
3.1 Definování DR plánu 57
3.2 Sestavení DR týmu 57
3.2.1 Role a zodpovědnosti DR týmu 58
3.3 Důležité kontakty 58
3.3.1 Kontakty interních pracovníků 58
3.3.2 Kontakty externích služeb 59
3.4 Postup při obnovení aktiv a služeb 59

3.4.1 Kontrola bezpečnosti perimetru 59
3.4.2 DR plán pro servery s prioritou 1 60
3.4.3 DR plán pro servery s prioritou 2 61
3.4.4 DR plán pro servery s prioritou 3 61
3.4.5 DR plán pro servery s prioritou 4 62
3.4.6 DR plán pro podpůrnou infrastrukturu 62
3.4.7 DR plán pro služby s prioritou 1 63
3.4.8 DR plán pro služby s prioritou 2 63
3.4.9 DR plán pro služby s prioritou 3 63
3.4.10 DR plán pro služby s prioritou 4 64
3.4.11 DR plán v případě úniku vody 64
3.4.12 DR plán v případě požáru 65
3.5 AAR 66
4 PŘÍNOSY PRÁCE A DOPORUČENÍ 67
4.1 Doporučení 67
4.1.1 Zavedení ISMS 67
4.1.2 Cloudové úložiště 67
4.1.3 Plán záloh 68
4.1.4 Dieselový generátor 68
4.1.5 Dohoda o úrovni poskytovaných služeb 68
4.1.6 Vyšší počet zaměstnanců 69
4.1.7 Další doporučení 69
4.2 Přínosy práce 69
4.3 Ekonomické zhodnocení 71
4.3.1 Kalkulace tvorby DR plánu externí firmou 71
4.3.2 Kalkulace DR plánu jako služby 71
ZÁVĚR 73

SEZNAM POUŽITÝCH ZDROJŮ 75
SEZNAM POUŽITÝCH OBRÁZKŮ 79
SEZNAM POUŽITÝCH TABULEK 80
SEZNAM POUŽITÝCH ZKRATEK 81
SEZNAM PŘÍLOH 82

ÚVOD

V dnešní době si už jen velmi těžko lze představit život bez elektronických zařízení a komunikačních technologií, které využíváme v každodenních činnostech a které nám zjednodušují, zrychlují a obohacují náš život. Běžný uživatel se dostává do kontaktu pouze s koncovými zařízeními, jakými jsou počítače, mobilní terminály, tablety a podobně, pomocí nichž a patřičných aplikací na nich komunikujeme s informačními systémy (servery) či mezi sebou navzájem. Avšak tato komunikace by nebyla možná bez síťové infrastruktury. A každá taková infrastruktura je dnes a denně vystavována různým typům nebezpečí, která by ji mohla vyřadit z provozu. Toto nebezpečí nehrozí jen infrastruktuře, ale i veškerým informacím, se kterými pracujeme. Z toho důvodu se zavedl pojem informační bezpečnost. Státní legislativa nařizuje již v mnoha případech zavádět standard ISMS (Systém řízení bezpečnosti informací), který má zabránit nežádoucím incidentům či vzniklým škodám.

A právě plán obnovy při katastrofě neboli anglicky „*Disaster Recovery Plan"* (dále DR plán), kterým se tato diplomová práce zabývá, je nedílnou součástí ISMS. Konkrétně se jedná o plán obnovy pro infrastrukturu Ústavu informatiky na Fakultě podnikatelské při VUT v Brně. Tento plán napomáhá k co nejrychlejší obnově systému v případě různorodých katastrofických scénářů.

V České republice se ISMS začíná rozšiřovat na univerzitní půdu, což jsou určitě nezbytné kroky. Univerzitní kampusy jsou vybaveny síťovou infrastrukturou stejně tak, jako velké firmy, kde je tato legislativa povinností. A případné poškození těchto technologií může napáchat nemalé škody. Ztráta citlivých dat či vyřazení školní sítě z provozu je nemilým problémem. Zvláště pak v této době, kdy se kvůli koronavirové epidemii odehrává téměř veškerá výuka online.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Cílem této práce je návrh plánu obnovy v případě katastrofy pro komunikační infrastrukturu Ústavu informatiky na Fakultě podnikatelské při VUT v Brně. Takový plán je v dnešní době nedílnou součástí téměř veškerých firem s vlastním IT oddělení. A nyní se toto opatření dostává i do povědomí univerzitního prostředí. Dle norem by každá struktura informačních a komunikačních technologií měla splňovat patřičné meze ISMS, kterého je plán obnovy při katastrofě součástí.

V teoretické části práce jsou představeny potřebné pojmy a samotná problematika ISMS. Jelikož plán obnovy při katastrofě spadá pod systém řízení kontinuity procesů, je jedna kapitola věnována i této oblasti. Dále je tato část zaměřena na teoretické pozadí samotného plánu obnovy při katastrofě a v práci využitou analýzu rizik.

DR plán je konkrétně zaměřen na serverovnu Ústavu informatiky v budově Fakulty podnikatelské. Analýza prostředí využívá dodaný seznam serverů, které se v místnosti nachází a seznam služeb, které servery poskytují. Analýza rizik je provedena dle legislativních standard a s využitím vyhlášky o kybernetické bezpečnosti. Tato analýza proběhla na základě konzultací s IT pracovníky školy. Tím jsou zohledněny reálné hrozby a rizika, které mohou serverovnu poškodit. V práci je znázorněn půdorys serverovny s detailním popisem analyzovaných prvků. K zakreslení bylo využito převážně softwaru Microsoft Visio.

Poslední část práce se zaměřuje na nedostatky, které byly zjištěny v rámci analýzy. Jsou zde také uvedena patřičná doporučení, která mohou zmíněně nedostatky eliminovat. Dále jsou uvedeny přínosy této diplomové práce a ekonomické zhodnocení řešení.

1 TEORETICKÁ VÝCHODISKA PRÁCE

Tato kapitola se zabývá teorií potřebnou jak k analýze prostředí, tak k samotnému návrhu plánu obnovy. Jsou zde uvedeny základní pojmy týkající se analýzy rizik, ISMS a samotného plánu obnovy v případě katastrofy. Dále jsou uvedeny potřebné normy, které tuto problematiku řeší.

1.1 Základní pojmy

Zde jsou stručně popsány pojmy, které budou v následující teoretické části, ale i v dalších částech diplomové práce hojně využívány. Znalost těchto pojmů ulehčí pochopení celé problematiky této práce.

- **Informační a komunikační technologie –** tento pojem vznikl pro pojmenování přenosu a zpracovaní dat. Jedná se o data informační a komunikační, mezi které můžeme řadit např. přenos hlasu nebo videa. Název vznikl z anglického „*Information and Communication Technology“,* zkráceně ICT. (1)
- **Informační systém –** jedná se o systém, který slouží ke správě informací. Díky využití různých organizačních zdrojů dokáže informační systém s informacemi pracovat nebo je uchovat či distribuovat. (2)
- **Aktivum –** soubor hmotných, či nehmotných věcí, které jsou pro danou organizaci nebo osobu nějakým způsobem významné a mají pro ně určitou hodnotu. Mezi aktiva patří např. i dobré jméno společnosti, nebo lidé a jejich zkušenosti. (3) Aktiva lze hodnotit dle toho, jaký význam pro majitele a chod společnosti mají. Hodnotí se i zranitelnost aktiva. (4, s. 12)
- **Server –** jedná se o výkonný počítač, jehož hlavním úkolem je poskytovat možnost ostatním počítačům se k němu připojit a další určité služby. Největší rozdíl mezi klasickou pracovní stanicí a serverem je v příslušném softwaru, kde je provedeno rozdílné nastavení různých parametrů. Často se využívá sjednocování více počítačů, tak aby byl server co nejvýkonnější. Servery se hojně využívají i jako sdílená datová úložiště (5)
- **Datová úložiště –** datová úložiště slouží k ukládání dat (informací), která bývají pro chod daných společností velmi důležitá. I z tohoto důvodu se řeší určitá

bezpečnost uložených dat na serverech. Dochází tak k jejich zálohování, díky kterému lze data kompletně, nebo alespoň částečně obnovit. Produkuje se stále více dat, a proto je potřeba stále větší kapacita těchto úložišť. (6)

- **Akumulátorový záložní zdroj –** (dále jen „záložní zdroj“). Jedná se o zařízení, které je zapojeno mezi napájecí sítí a zařízením, které má být napájeno. V případě výpadku hlavní zdrojové sítě se sepne záložní zdroj, který obsahuje akumulátor. Ten po určitou dobu dokáže poskytovat energii a zajistit tak neustálý chod napájeného zařízení, nebo alespoň možnost napájené zařízení bezpečně vypnout. Můžeme se často setkat s použitím zkratky UPS, která pochází z anglického názvu *„Uninterruptible Power Supply“*. (7)
- **Switch –** česky také přepínač, je hardwarové síťové zařízení většinou serverového komplexu. Nejčastěji je přepínač využíván jako aktivní prvek počítačové sítě. Díky němu lze propojit velké množství zařízení v síti, a právě toho se mnohdy využívá k propojení serverů a napojení případného monitoringu. (5)
- **Bezpečnost informací –** jedná se o snahu zachovat tři základní aspekty informací, mezi které se řadí důvěrnost, integrita a dostupnost. Důvěrnost je vlastnost, která v tomto případě značí, že daná informace není dostupná nebo odhalena nežádoucím stranám. Integrita zajišťuje úplnost a správnost informace. Přístupnost a možnost okamžitého použití v případě požadavku zajišťuje dostupnost informací. (8)
- **Hrozba –** v případě hrozby lze mluvit o okolnosti, události, aktivu, osobě nebo subjektu, které mohou zapříčinit bezpečnostní incident nebo způsobit jinou škodu. U hrozby se nejčastěji hodnotí její nebezpečnost, přístup a motivace. Nebezpečnost je chápána jako schopnost způsobit škodu. Přístup je brán jako možnost hrozby působit na dané aktivum. Lze zde mluvit i o frekvenci výskytu hrozeb. Motivace hrozby značí, jaký má daný subjekt zájem o naplnění určité hrozby. (4, s. 15)
- **Zranitelnost –** zranitelnost lze chápat jako slabinu nebo nedostatek určitého aktiva. Hrozba využívá zranitelnosti k jejímu naplnění. Zranitelnost je vždy přiřazena ke konkrétní hrozbě a značí, jak moc může daná hrozba aktivum ohrozit. (4, s. 12)

- **Riziko –** riziko je vnímáno jako nebezpečí vzniku škody. Jedná se o nežádoucí vývoj situace oproti vývoji předpokládanému. K řízení rizik slouží jejich analýza. Ta zahrnuje identifikaci aktiv a jejich ohodnocení a stanovení příslušných hrozeb a zranitelností. (4, s. 11)

1.2 Analýza rizik

Analýza rizik je velmi užitečný nástroj, který umožňuje následné řízení rizik. Zavedení vhodných opatření zabraňuje mnoha bezpečnostním incidentům. Analýza rizik se skládá z několika kroků:

1. **Identifikace aktiv** – nejprve je nutné identifikovat aktiva, se kterými se dále pracuje.
2. **Ohodnocení aktiv** – ohodnocení probíhá na základě pořizovací hodnoty aktiva, jeho důležitosti pro daný subjekt, náklady na překlenutí případných škod způsobených poškozeným aktivem a náklady na odstranění případných škod na aktivu samotném.
3. **Identifikace hrozeb** – dochází k definování hrozeb působících na určitá aktiva.
4. **Stanovení míry zranitelnosti** – různá aktiva mají různé míry zranitelnosti. Zde dochází k určení míry zranitelnosti pro určité aktivum a hrozbu.

Poté, co jsou provedeny tyto kroky, mohou být dále podrobněji analyzovány různé hrozby a zranitelnosti. Finální hodnotu rizika získáme vynásobením hodnoty aktiva s příslušnou hodnotou hrozby. Hodnotu hrozby lze určit pomocí tabulky uvedené dále v práci. V ní figuruje míra dopadu hrozby a pravděpodobnost jejího výskytu. Obě zmíněné položky mohou nabývat hodnot 1 až 5, kde 1 značí nejmenší míru dopadu a nejnižší pravděpodobnost výskytu hrozby. Naopak hodnota 5 značí nejvyšší míru dopadu a nejvyšší pravděpodobnost výskytu hrozby. Vynásobením těchto hodnot získáme hodnotu hrozby, se kterou se může počítat v předchozím vzorci.

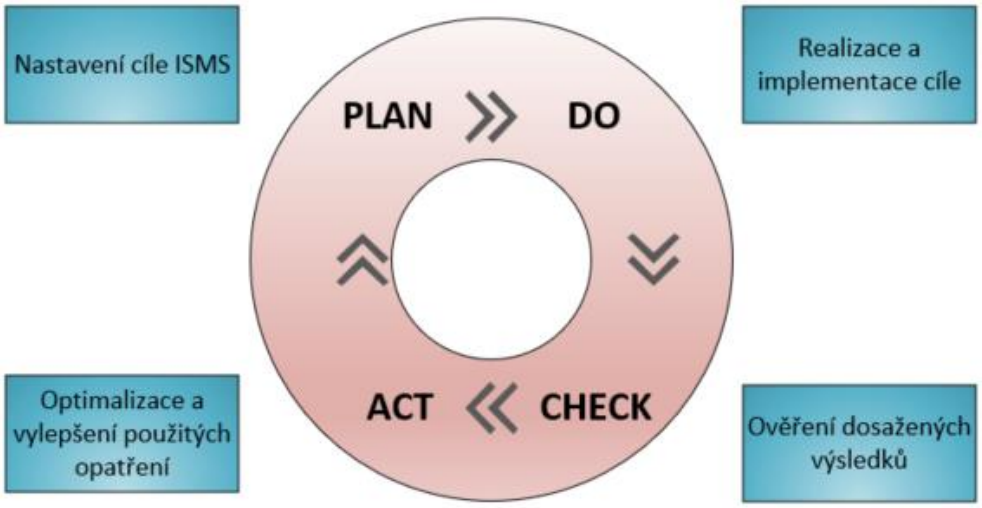
Na základě získaných hodnot lze určit, která rizika mohou nejvíce aktiva ohrozit a následně pak provádět různá opatření, která mají za úkol minimalizovat pravděpodobnost výskytu rizika nebo omezit výši případných škod. (4, s. 11-16)

Tabulka č.1: Tabulka pro ohodnocení hrozby (vlastní tvorba dle (9))

		Míra dopadu				
		1	**2**	**3**	**4**	**5**
Míra pravděpodobnosti	**5**	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

1.3 ISMS

ISMS je zkratka pro anglický název *„Information Security Management System“*, česky Systém řízení informační bezpečnosti. Jedná se o standard, který řídí ochranu informací v organizaci. ISMS lze také definovat jako stále se opakující proces, který zlepšuje stav informační bezpečnosti v organizaci. Základním principem ISMS je tzv. PDCA cyklus. Tato zkratka pochází z anglických slov *„Plan-Do-Check-Act“* – plánovat, dělat, kontrolovat a jednat. Nejdříve se plánuje vhodné zlepšení, poté se realizuje. Následuje kontrola zavedeného opatření a poté finální úprava a implementace. (10, s. 14,25)



Obrázek 1: PDCA cyklus (vlastní tvorba dle (10, s. 25))

Systém řízení informační bezpečnosti se řídí řadou norem ISO 27000 a má tedy jasně stanovenou strukturu. Mezi hlavní pilíře ISMS patří určení informačních aktiv, která budou podléhat řízení. Dále analýza rizik u těchto aktiv z hlediska bezpečnosti informací. Následuje výběr a implementace zvolených bezpečnostních opatření. Tyto tři kroky vedou ke snížení pravděpodobnosti poškození, nebo neoprávněné manipulaci s těmito informačními aktivy. (10, s. 16)

1.4 Řízení kontinuity činností

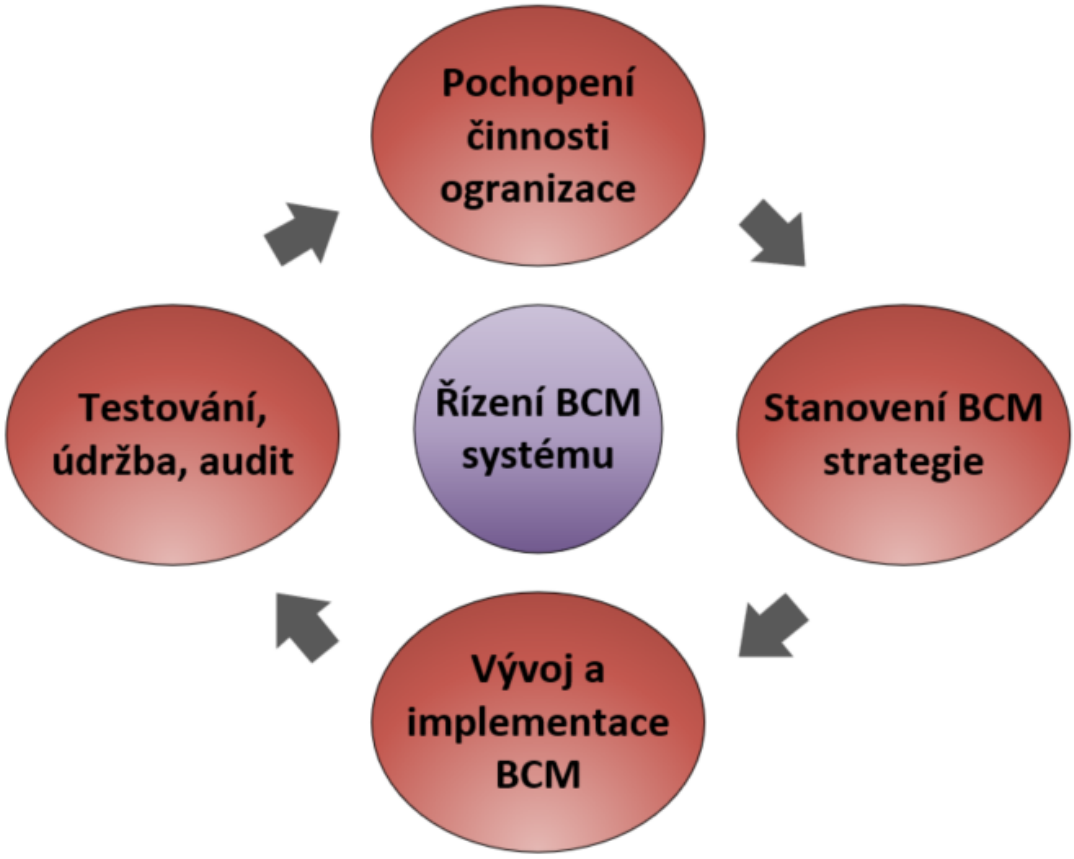
Pro tento pojem se využívá zkratka BCM z anglického „*Business Continuity Management*“. Označuje řídící proces, který zajišťuje neustálý chod určitého systému. U nás se tento proces nazývá Řízení kontinuity činností organizace. Jeho cílem je zajistit plynulost a stálý chod klíčových procesů v organizaci. Tento řídící proces se začal rozvíjet v USA již v 80. letech 20. století. V této lokaci dochází k častému výskytu přírodních katastrof, které zapříčinily obrovské výpadky v celém průmyslu i službách. Úlohou BCM nebylo pouze stanovit správnou reakci na určité situace, ale i těmto situacím předcházet. Hlavním cílem vždy bylo co nejrychlejší obnovení provozu a výroby, a to v co nejvyšší možné kvalitě. (11) (12)

První terminologie, která se snažila tuto oblast sjednotit, se objevila v roce 1988 zároveň se vznikem amerického institutu *„Disaster recovery Institute International“*. Díky této organizaci v roce 1993 spatřila světlo světa první standardizovaná norma ohledně této problematiky. Její název zněl *„Professional Practices for Business Continuity Planners“* a už zde se BCM zaměřovalo převážnou částí na řízení kontinuity informačních a komunikačních technologií, jelikož právě na ICT byla většina klíčových procesů závislá. Je samozřejmé, že vývoj různých technologií má dopad na vývoj BCM. Je tedy téměř nutností sledovat trendy v tomto oboru, pokud chce organizace zajistit tu nejlepší možnou kontinuitu provozu. (12)

Jak již bylo zmíněno, hlavním cílem BCM je zajistit určitou plynulost provozu organizace. Toho se snaží dosáhnout tím, že snižuje pravděpodobnost výskytu různých incidentů, které mohou provoz omezit nebo úplně zastavit a poskytuje rámec rychlého obnovení v případě pozastavení provozu. Veškerá tato snaha je vyvíjena k docílení maximalizace hodnot organizace, jako jsou tržby, základní poskytované služby

zákazníkům, udržení hlavní činnosti organizace ve stálém provozu bez přerušení, nebo udržení důvěry zákazníků. Samozřejmě se tyto hodnoty mohou v každém oboru podnikání lišit. (13)

Je důležité zmínit i životní cyklus BCM. Ten se skládá ze čtyř fází. Lze zde spatřit podobnost s PDCA cyklem systému ISMS. První fází je pochopení činnosti firmy. Je důležité organizaci důvěrně poznat, aby jí mohl být sestrojen opravdu vyhovující BCM plán. Dalším krokem je stanovení strategie. Strategie musí být vždy podložena patřičnými analýzami a určuje, které činnosti je potřeba v případě havárie přednostně obnovit nebo předpokládaný časový harmonogram obnovy. Další fáze obsahuje samotný vývoj BCM a jeho následnou implementaci. Posledním krokem je testování, údržba a audit, který je nejlépe zajistit externí firmou. (13)

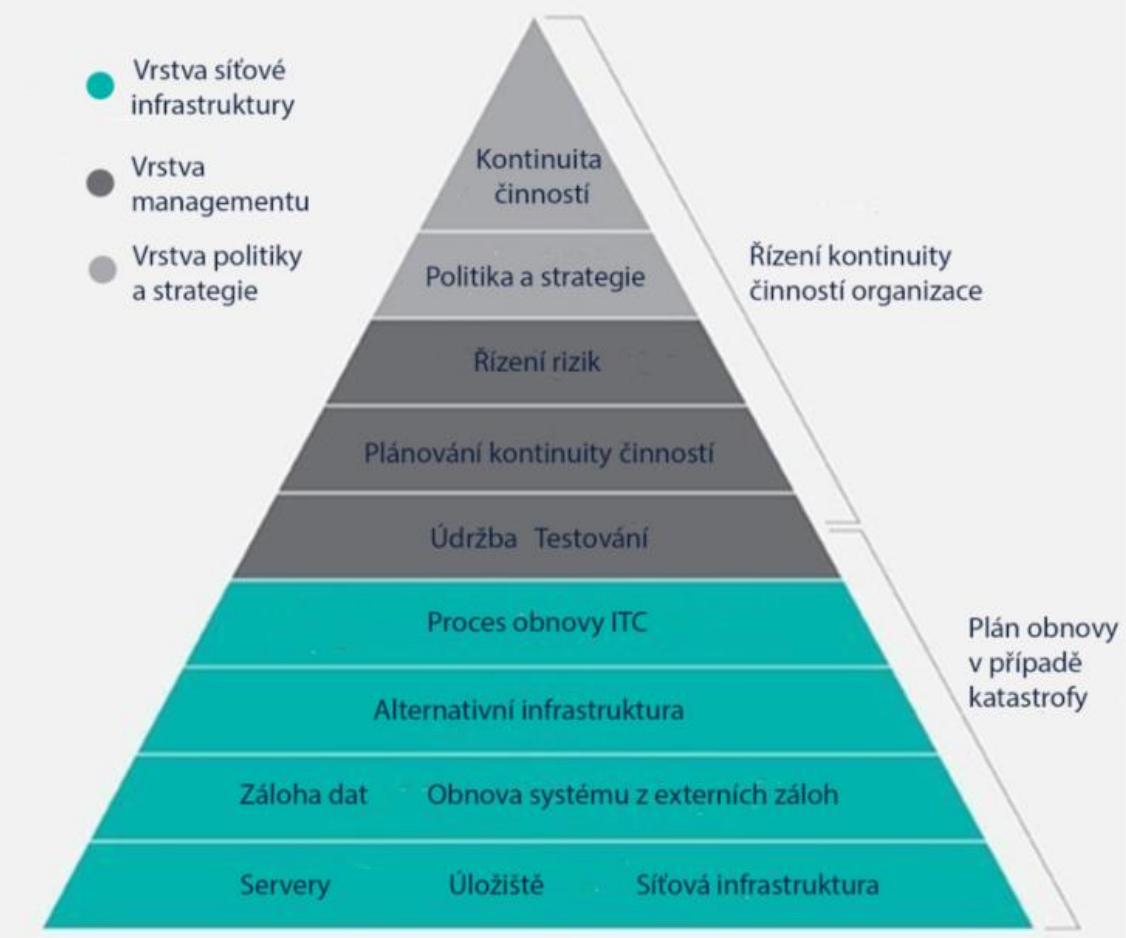


Obrázek 2: Životní cyklus BCM (vlastní tvorba dle (13))

Na následujícím obrázku je BCM rozdělen do pyramidy a do tří různých vrstev. První vrstvou je vrstva infrastruktury, kde jsou základem servery, úložiště a síťová infrastruktura. Dále do této skupiny patří záloha dat a externí obnova dat. Následuje

alternativní infrastruktura. Ta zajišťuje náhradní zázemí pro ICT technologie v případě poškození toho primárního. Poslední položkou této vrstvy je samotný proces obnovy ICT.

Druhá vrstva managementu je složena z údržby, testování, plánování kontinuity činností a řízení rizik. Poslední vrstvou je vrstva politiky a strategie. Jak lze pozorovat na obrázku, celá pyramida je navíc rozdělena do dvou částí. První, spodní část, tvoří Plán obnovy v případě katastrofy a druhou částí je Řízení kontinuity činností v organizaci. A právě Plán obnovy v případě katastrofy tvoří nedílnou část BCM a detailně je popsán v následující kapitole.



Obrázek 3: Plánování BCM (vlastní tvorba dle (11))

1.5 Plán obnovy při katastrofě

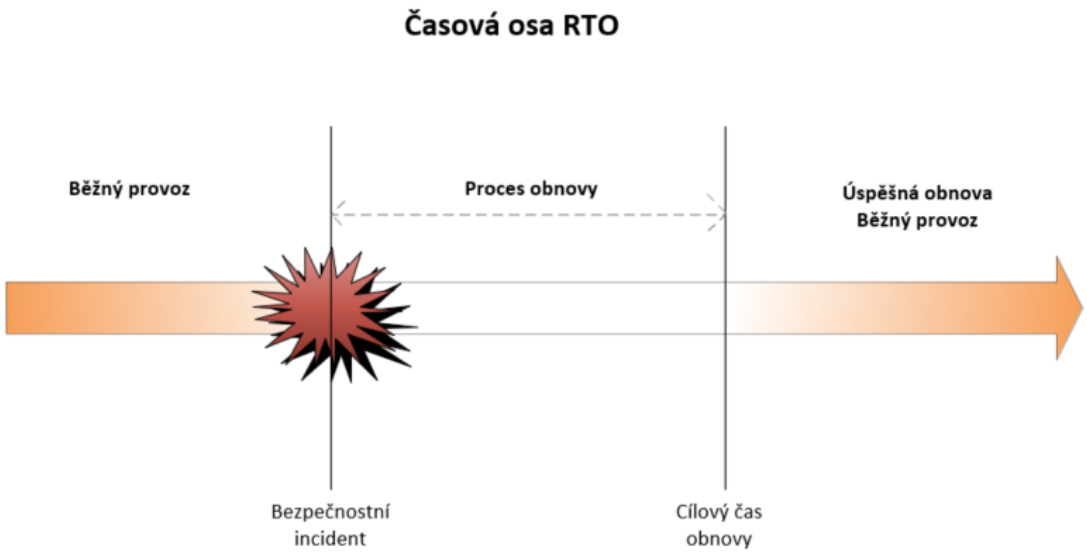
Tento název je přeložen z anglického *„Disaster Recovery Plan“* a v psaných textech se hojně zkracuje pouze na „DR plán“. Jedná se o soubor postupů, nástrojů a zásad, které zajišťují obnovu informačních a komunikačních technologií po katastrofě, ať už se jedná o katastrofu přírodní nebo o katastrofu zapříčiněnou lidským pochybením. DR plán je důležitou součástí BCM a lze ho také popsat jako schopnost organizace poskytovat kritické informační technologie i po mimořádném bezpečnostním incidentu, tedy katastrofě. Úkolem je zajistit předem stanovené ICT činnosti v předem stanoveném čase tak, aby nebyla narušena kontinuita provozu organizace. (14)

W. Curtis Preston přirovnává tvorbu DR plánu k malování mostů ve městě, kdy malíř začne malovat na jedné straně řeky, dokud se nedostane na druhý břeh. Poté začíná malovat další most z druhého břehu na ten první a pokračuje pořád dokola. Prakticky nikdy nepřestává malovat. A stejné je to i s DR plánem. Často se stává, že i hotový DR plán se musí kompletně od začátku předělat kvůli rychlému vývoji počítačových technologií. Je důležité plán neustále měnit a testovat tak, aby bylo jisté, že bude vždy fungovat. (15)

1.5.1 Cílový čas a bod obnovy

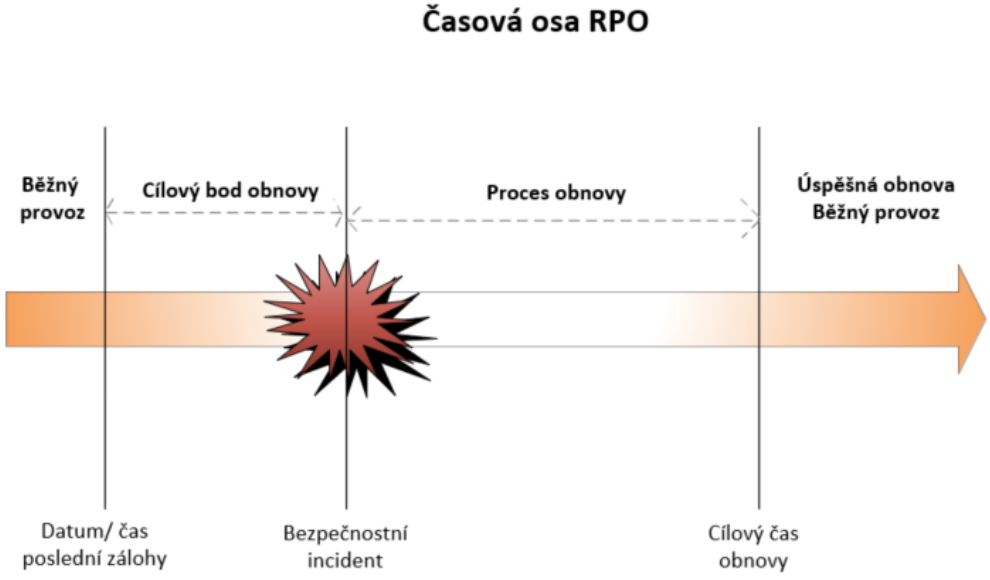
Cílový čas obnovy a bod obnovy jsou dvě důležité metriky, které nám říkají, jak dlouho bude systém nefunkční a kolik dat můžeme v případě katastrofy ztratit. Obě tyto metriky jsou důležité jak pro plánovaní BCM, tak i pro realizaci DR plánu. (16)

Cílový čas obnovy – jedná se o sjednanou dobu, za kterou musí být systém ITC obnoven. V praxi se využívá zkratka RTO, která pochází z anglického názvu *„Recovery Time Objective“.* Kromě času zde může být řešena i úroveň, na kterou musí být dané služby obnoveny. RTO se většinou stanovují k různým katastrofickým scénářům zvlášť, tak aby co nejvíce odpovídaly realitě. (17) Při katastrofě může dojít např. k nahrazení poničených komponentů, přeprogramování systému a následnému testování. Veškeré tyto zásahy potřebují svůj čas, a je velmi důležité zmínit, že čím kratší čas obnovy je vyžadován, tím více narůstají výsledné finanční náklady na obnovu. (16)



Obrázek 4: Časová osa RTO (vlastní tvorba dle (16))

Cílový bod obnovy – tento pojem úzce souvisí se zálohováním a obnovou dat a využívá se pro něj zkratka RPO z anglického *„Recovery Point Objective"*. Jedná se o dobu, kdy byla data naposledy zálohována. Samozřejmě v každém odvětví se četnost provádění záloh liší. Například v bankovnictví je nutné zálohovat data téměř v reálném čase. Je zřejmé, že i zde platí inverzní vztah mezi hodnotou RPO a vynaloženými finančními náklady. Čím častěji jsou zálohy prováděny, tím je potřebnější výkonnější zálohovací systém a infrastruktura. (16)



Obrázek 5: Časová osa RPO (vlastní tvorba dle (16))

1.5.2 Struktura DR plánu

Obecně DR plán nemá stanovenou pevnou strukturu, která by se musela dodržovat, ale existuje spousta odborných publikací, ve kterých je uveden doporučený postup při jeho tvorbě. Doporučenou strukturu lze také vypozorovat v příslušných normách týkajících se informační bezpečnosti a plánu obnovy při katastrofě.

Hlavička – obsahuje název dokumentu a organizace, které se plán obnovy týká. Je zde uveden rok poslední aktualizace a verze plánu. Neměl by chybět ani obsah plánu. (18)

Definování – je důležité určit, čeho konkrétně se plán týká a co vše má řešit. Vymezit tak hranice pro potřebnou analýzu k vytvoření plánu.

DR tým – tým pro obnovu po katastrofě je velmi důležitá součást DR plánu. Jedná se o skupinu jednotlivců, která se v případě bezpečnostního incidentu řídí plánem obnovy a snaží se zajistit, aby byla doba obnovy co nejkratší. Členové tohoto týmu mají přiděleny různé role a zodpovědnosti. Vedoucí týmu by měl být vysoce postavený manažer, který má za úkol dohlížet na celý tým a schvalovat veškerá rozhodnutí a postupy. Dalším, členem je koordinátor krizového řízení – tedy krizový manažer. Tato osoba iniciuje samotné postupy při řešení nastalých problémů. Jeho úkolem je stanovit správnou strategii pro určitý problém vzniklý katastrofou. Dále do týmu patří odborníci na jednotlivé ICT odvětví. Jedná se například o specialistu na síťovou infrastrukturu, podpůrnou infrastrukturu, nebo servery. Posledním členem je osoba pro dohled nad IT službami. Ta monitoruje veškeré technologie a dohlíží na to, jestli veškeré komponenty a aplikace společně fungují, tak jak mají. (19)

Seznam důležitých kontaktů – seznam kontaktů je věc, která by měla být umístěna téměř na začátku DR plánu. A to proto, že jedna z prvních věcí, která se při zjištění havárie děje, je kontaktování DR týmu. Seznam musí obsahovat kontakty (mobilní číslo, e-mail, adresa) na celý DR tým. Dále se zde budou nacházet kontakty na osoby, které jsou spojeny s danou organizací, ale nejsou součástí DR týmu. Jedná se např. o kontakt na správce budovy, zaměstnance vrátnice nebo majitele organizace. Další položkou kontaktů jsou sjednané externí služby, kde se jedná o různé servisní zásahy atd. Samozřejmě zde nesmí chybět linky na veškerá tísňová volání. (20)

Postupy při obnovování – tato část DR plánu zahrnuje podrobné pokyny, jak postupovat v případě katastrofy. Tyto postupy mohou být specifikovány pro různé

scénáře. Před zhotovením těchto postupů se doporučuje vyhotovit analýzu aktiv a rozdělit je do různých skupin dle důležitosti pro chod organizace. K těmto skupinám se poté sestavují scénáře. Většinou existují speciální scénáře pro přírodní katastrofy, jakými jsou vichřice, zemětřesení, nebo povodeň. (21)

Další důležitou součástí DR plánu může být šablona pro zaznamenávání bezpečnostních incidentů nebo testů, které v organizaci proběhly. Obecně se pro tato hlášení využívá zkratka AAR z anglického *„After-action report“*. Tento dokument může být velmi klíčový při řešení budoucích problémů. Lze se díky němu poučit z chyb, ale také praktikovat řešení, která byla v minulosti úspěšná. (22)

1.5.3 Předpoklady kvalitního DR plánu

Předpokladem kvalitního DR plánu je i proaktivní přístup IT týmu k řešení krizových situací a k DR plánu samotnému. Většina společností jej má zavedený, ale jen minimum se věnuje kontrole jeho aktuálnosti. Mnoho takových plánů navíc nepokrývá veškeré možné scénáře, které mohou nastat. Podrobnosti se u jednotlivých plánů většinou liší, ale existuje určitý rámec, který by měl zajistit kvalitu jakéhokoliv DR plánu, a to bez ohledu na to, jaká situace nastane. Jedná se o 4 základní pilíře popsané v následujících odstavcích. (23)

Standardizovaná komunikace

Strategie komunikace je jednou z nejdůležitějších součástí každého DR plánu. V případě zastaralého telefonního seznamu s kontakty na celý DR tým budete jen těžko řešit krizovou situaci. Pokud tým není schopný komunikace, nemůže ani řešit daný problém. Doporučuje se kontrolovat aktuálnost kontaktních údajů minimálně jednou za šest měsíců a využívat placenou komunikační platformu. U volně přístupných platforem hrozí přerušení služby bez upozornění uživatele. (23)

Připravenost DR týmu

V případě katastrofy se musí DR tým držet DR plánu. Je nutné myslet na to, že celá funkcionalita kritické infrastruktury může být závislá na vzdáleném zásahu DR týmu. Proto musí být tento tým proškolen a schopen vzniklé problémy vyřešit různými způsoby. Za běžných podmínek má DR tým přístup k veškerým monitorovacím nástrojům a prostředkům ke správě kritické infrastruktury. Při bezpečnostním incidentu

tomu tak být nemusí. Proto je důležité nastavit podmínky vzdáleného řízení co nejvíce podobné tomu jako za běžného provozu. (23)

Monitoring

Další důležitou součástí DR týmu je schopnost neustále sledovat dané metriky. Při havárii pracuje DR tým, ale i koncoví uživatelé jinak než obvykle. Je tedy nutné co nejdříve zřídit pozorovací panel, který kontroluje časovou odezvu aplikací či webu, šířku pásma nebo jiné IT utility. (23)

Plán zálohování

Zálohování je v dnešní době téměř samozřejmostí. Dle DR plánu nestačí zálohovat pouze primární služby, ale i služby vedlejší. Cílem je udržet základní systém vždy online. Kvalitní DR plán není o tom, že umožní navrátit systém do chodu během hodiny nebo pár minut, ale o tom, že se snaží systém udržet stále v chodu. (23)

1.5.4 Druhy DR plánů

„Samoobslužný“ DR plán – V tomto případě se jedná o DR plán, který si kompletně tvoří samotná organizace. Veškeré plánování, údržbu, testování atd. si společnost zajišťuje sama. To znamená, že i všechny nutné analýzy, jako je např. analýza rizik, si organizace musí vyhotovit sama. Výhodou může být minimalizace nákladů a nezávislost výběru technologií, které si firma pro DR plán zvolí. Naopak ne vždy je zhotovený DR plán na dostatečné úrovni a ušetřené finance mohou být potřeba v několikanásobném množství při likvidaci škod, které DR plán nepokryl. Anglicky se tento způsob nazývá *„Self-service DR Plan“.* (24)

„Asistovaný“ DR plán – Název je přeložen z anglického výrazu *„Assisted DR Plan“.* Externí firma poskytne pracovníky a konzultanty, kteří pomohou navrhnout DR plán. Ale i v tomto případě je k DR plánu (záloha dat) využito stávajících interních aktiv. Zjednodušeně lze tedy říct, že externí firma DR plán navrhne a pomůže s jeho implementací. Firmě tak odpadá spousta administrativní práce s DR plánem. DR tým ale tvoří zaměstnanci IT interní firmy. Stále je tedy potřeba udržovat IT tým s potřebnými schopnostmi a znalostmi. Je zde samozřejmě možnost převést kritickou část DR plánu pod správu externí firmy. Tím je ale celé řešení mnohem dražší. (24)

DR plán spravovaný specializovanou společností – Anglicky *"Managed DR Plan"*. Jedná se o nejkomplexnější, ale zároveň taky o nejdražší možnost DR plánu. Interní IT tým zde kompletně přenechá veškerou práci, co se DR plánu týče, externí firmě. Základem těchto DR plánů bývá SLA, tedy smlouva o zajištění provozu. Jsou v ní stanoveny cíle obnovy (RPO) a čas potřebný k obnově (RTO). Externí služba musí být informována o jakýchkoliv změnách co se IT týče, aby mohla reagovat příslušnými změnami v DR plánu. Poskytovatel služby je plně zodpovědný za implementaci, testování i údržbu. Toto řešení je většinou řešeno přes cloud a náklady jsou zde opravdu vysoké. (24)

1.5.5 Testování DR plánu

Po vytvoření sebelepšího DR plánu existuje jedna jediná spolehlivá věc, pomocí které lze zjistit, zda DR plán funguje. Touto věcí je testování. Smyslem DR plánu je proaktivně snižovat rizika spojená s případnou katastrofou a testování DR plánu snižuje riziko, že nebude DR plán fungovat. V následujících řádcích jsou uvedeny čtyři kroky, které by měly zajistit správné testovaní DR plánu. (25)

Co se bude testovat? – Je dobré stanovit, které části DR plánu budou testovány. Většinou se provádí testy těch systémů, které jsou pro společnost kritické. U testování jednotlivých systémů je vhodné pozorovat různé závislosti mezi nimi a zaznamenávat si je (např. závislost služby Exchange na službách DNS a Active Directory). (25)

Jak často se bude testovat? – Zde se doporučuje zaměřit na to, jak často se systémy, aplikace a procesy, na které je DR plán zaměřen, mění. Nejvhodnější je testovat určitý DR plán po každé provedené změně v daném systému. Samozřejmě může být nastavena i pravidelná frekvence testů (např. pololetně nebo ročně). (25)

Jakou metodou se bude testovat? – Existují čtyři různé metody testování. Při výběru metody je důležité myslet na to, že cílem je ověřit, zda DR plán bude reálně funkční. První metodou je **jednoduchá kontrola plánu.** V této metodě se prochází plán a určí se jeho zastaralé části a doplní se ty, které chybí. Dalším testováním je tzv. **testování od stolu**. Při něm tým projde kompletní DR plán a diskutuje o jeho proveditelnosti a podrobných krocích. Prochází se všechny scénáře obnovy, aby se zjistilo, zda jsou proveditelné. Třetím druhem testování je **simulace scénářů**. Dochází v podstatě

k provedení DR plánu v omezeném prostředí. To znamená, že jsou vybrány konkrétní části sytému, které jsou postupně testovány. Při tomto testování většinou bývá omezen provoz organizace, nedochází k zasažení celého systému. Posledním testem je **úplná simulace DR plánu**, při kterém, stejně jako u předchozího testu, dochází k naplnění a testování všech scénářů. Jediný rozdíl je v tom, že test může zasáhnout celý systém a probíhá za plného provozu. (25)

Aktualizace DR plánu – testy mohou potvrdit, že DR plán je v pořádku a nepotřebuje žádné úpravy. Můžou také ale odhalit různé nedostatky a chyby. Ty je potřeba vždy řešit a plán aktualizovat. (25)

Testování je jednou z nejdůležitějších částí DR plánu a bez jeho provedení nemůžeme vědět, zda funguje. Spolu s DR plánem je tedy nezbytné zavádět i strategie jeho testování. (25)

1.6 Použité normy a legislativa

V této kapitole jsou popsány normy, kterými se diplomová práce řídí. Je zde naznačeno, co každá z norem řeší a jakým problémem se zabývá. Většina použitých norem patří pod normu ISO 27000.

Normy jsou používány z mnoha důvodů. Díky nim mohou menší firmy konkurovat těm větším, co se provedení různých řešení týče. Pomáhají udržet ten nejmodernější trend v daném odvětví a tím jsou veškerá opatření vysoce zefektivněna. Další výhodou je použití společné terminologie nejen v průmyslovém odvětví. (14)

1.6.1 Řada norem ISO 27000

Jedná se o mezinárodní řadu norem, která se zabývá informační bezpečností. Poskytuje nám rámec pro ochranu informačních aktiv a zajišťuje integritu, dostupnost a důvěrnost informací. Nejdůležitější normy této řady, týkající se této diplomové práce, jsou popsány dále.

ISO 27000 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Přehled a slovník – tato norma shrnuje danou

problematiku a zavádí určitou terminologii, která se objevuje v celé řadě těchto norem. (26, s. 48)

ISO 27001 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky – dá se říct, že se jedná o hlavní normu z rodiny norem ISO 27000. Definuje požadavky na komplexní řešení informační bezpečnosti, které může zajistit potřebnou certifikaci. Tento standard řeší bezpečnost veškerých informačních technologií, dat, aplikací, ale i papírových dokumentů a znalostí. Od roku 2013 se věnuje i problematice ochrany osobních údajů. (26, s. 48)

ISO 27002 - Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Soubor postupů – tato norma obsahuje více jak 5000 možností, jak řešit bezpečnost informací. Díky ní lze rychle zjistit současný stav bezpečnosti a poté přijít s patřičnými opatřeními. (26, s. 49)

ISO 27005 - Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací – jak je patrné z názvu, tato norma stanovuje doporučení pro řízení rizik. Nicméně, aby bylo možné použít tuto metodiku opravdu na všechny organizace, norma nestanovuje konkrétní metodu řízení rizik, nýbrž nabízí výběr z několika typů řešení. Tyto metody jsou samozřejmě kompetentní s řízením rizik informační bezpečnosti. (26, s. 51)

1.6.2 ISO 22301

Norma ISO 22301 se zaobírá požadavky pro zajištění kontinuity činností v podnikání. Jednoduše řečeno se jedná o normu řešící BCM. Aktuální verze pochází z roku 2019 a oproti verzi z roku 2012 prošla několika změnami. Většinou se jedná o zjednodušení definic, tak aby byla lépe srozumitelná a snadněji aplikovatelná na všechny organizace. V normě jsou uvedeny např. požadavky na systém managementu a jsou zde upraveny podmínky pro kontinuitu, tak aby řešení bylo co nejlépe přizpůsobitelné současné době. (27)

1.6.3 ISO 24762

Tento standard je zaměřen na podporu ISMS z hlediska kontinuity činností a obnovy při katastrofě. Normu lze brát jako velmi rozsáhlý průvodce pro tvorbu DR plánu. Obsahuje nejen aspekty týkající se tvorby DR plánu, ale i doporučení ohledně jeho implementace, provozu, monitorování, údržby a testování. Norma je určena jak pro organizace, které si chtějí DR plán pořídit svépomocí, tak i pro firmy, které ho nabízejí jako službu. (28)

1.6.4 NIST 800-184

NIST 800-184 je všeobecnou příručkou o obnovení původního stavu systému po bezpečnostním incidentu. Tato publika vznikla v USA v roce 2016 a může být velmi užitečným pomocníkem při tvorbě DR plánu a jeho užívání. (18)

1.6.5 Vyhláška č. 82/2018 sb.

Celý název této vyhlášky zní Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat. Používá se však zkrácený název Vyhláška o kybernetické bezpečnosti. Vyhláška upravuje obsah a strukturu bezpečnostní dokumentace, obsah a rozsah bezpečnostních opatření. Dále typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů, náležitosti a způsob hlášení kybernetického bezpečnostního incidentu. Další položkou jsou náležitosti oznámení o provedení reaktivního opatření a jeho výsledku, vzor oznámení kontaktních údajů a jeho formu, způsob likvidace dat, provozních údajů, informací a jejich kopií. Ve vyhlášce jsou uvedeny i nejčastější kybernetické hrozby a zranitelnosti. (29)

2 ANALÝZA SOUČASNÉHO STAVU

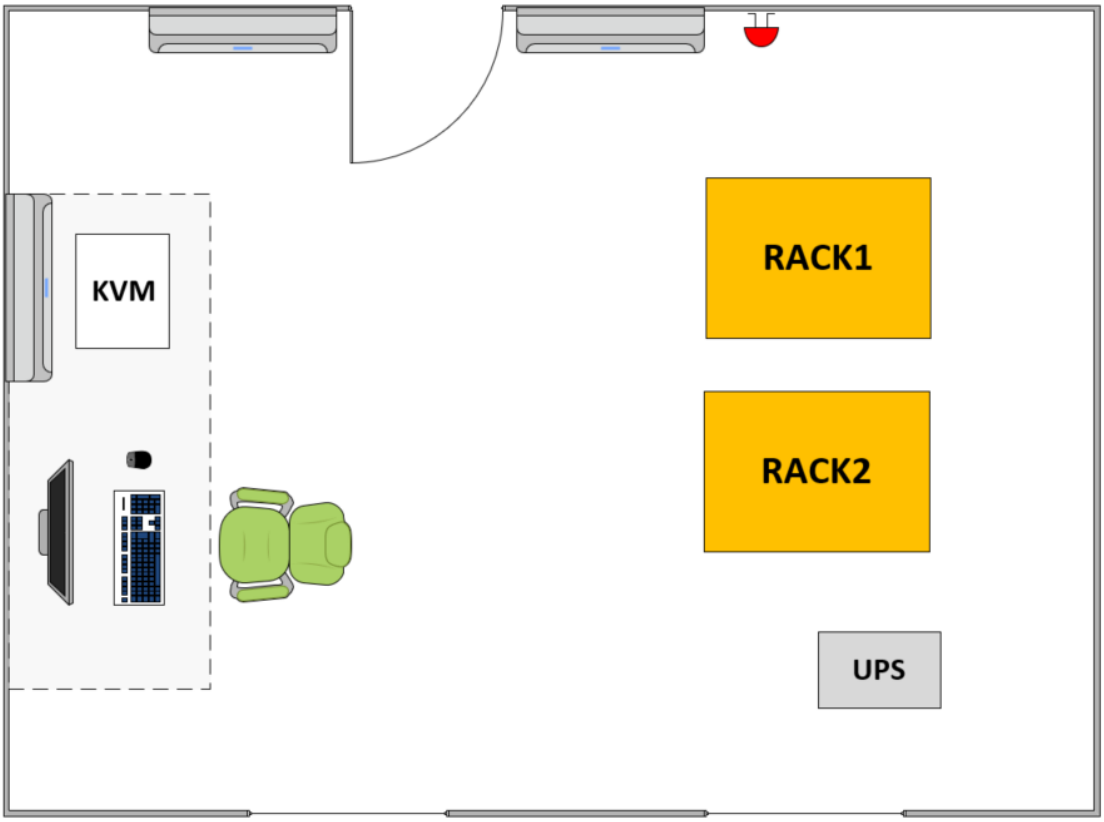
V této kapitole je stručně popsána serverovna Ústavu informatiky a její jednotlivé části, kterých se plán obnovy týká – tedy hlavně servery a prvky fyzické infrastruktury. Je potřeba zjistit současný stav ISMS a sestavit seznam aktiv, kterých se DR plán týká. Dále bude provedena analýza rizik, hrozeb a případných následků. Budou zde také uvedeny další potřebné podklady pro DR plán, jako je potřebné rozdělení aktiv do skupiny dle priority důležitosti pro chod sítě celého ústavu.

2.1 Stručný popis lokality a budovy

Podnikatelská fakulta, které se tato práce týká, spadá pod Vysoké učení technické v Brně. Nachází se v Králově Poli na ulici Kolejní 4. Budova, tak jak ji nyní známe, byla zpřístupněna roku 2004. Fakultu navštěvují studenti z České republiky, Slovenska, ale i spousta studentů z jiných zahraničních zemí. Celkem školu navštěvuje přibližně 3200 studentů. V budově se nachází několik serveroven, tato práce se však zabývá jen jednou z nich. Jedná se o místnost P278. Její umístění je ve 2. podlaží Fakulty podnikatelské.

2.2 Analýza současné infrastruktury

Serverovna Ústavu informatiky, na kterou se DR plán vztahuje, se nachází ve 2. podlaží fakulty. Je opatřena bezpečnostním zámkem a kamerovým systémem. Ke klíči od tohoto zámku mají přístup jen pověření zaměstnanci a jeden univerzální klíč se nachází na vrátnici. Ten může být použít v případě nepřítomnosti zmíněných zaměstnanců. Serverovna je vybavena klimatizací. Konkrétně se jedná o 3 chladicí jednotky. Servery se díky nim nepřehřívají a v místností teplota nepřekročí hranici 25 stupňů Celsia. V místností se nachází dva datové stojany (tzv. Rack), v kterých jsou umístěny servery, úložiště a aktivní prvky. Naproti stojanům se servery je umístěn pracovní stůl s židlí, který slouží jako místo pro správu serverů. Podrobný plánek serverovny je uveden dále v práci.



Obrázek 6: Půdorys serverovny (vlastní tvorba v Microsoft Visio)

V serverovně se nachází celkem 13 fyzických serverů. Dále jsou zde některé servery virtualizovány. Nejdůležitějším síťovým prvkem je switch s označením SW2, na který jsou všechny servery napojeny. Propojení zajišťuje vždy jeden patchcord. Tento switch je současně napojen na hlavní fakultní switch, který je umístěn v hlavní síťové serverovně. Součástí datových stojanů jsou i datová úložiště, kterých je celkem 7. Tato úložiště jsou využita pro ukládání dat zaměstnanců a různých záloh. Nesmí se opomenout i záložní zdroj UPS, který v případě výpadku proudu udrží veškeré komponenty v chodu po jednu hodinu. Na zdi nalezneme i nouzový vypínač, kterým lze, pokud je to nutné, vypnout proud v celé místnosti. Poslední součástí serverovny je administrátorská jednotka KVM, díky které lze spravovat veškeré servery. Samozřejmostí je i správa serverů vzdáleným přístupem pomocí zařízení KVM. Detailněji jsou veškeré komponenty popsány v následující kapitole, konkrétně v seznamu aktiv.

2.3 Fyzická aktiva a jejich ohodnocení

Předpokladem DR plánu je alespoň určitá míra zavedení ISMS v dané organizaci. Bohužel k dohledání není žádná verze ISMS, a proto je nutné sestavit novou analýzu rizik dle podkladů z teoretické části diplomové práce. Nejdříve je potřeba vytvořit seznam aktiv, který bude obsahovat veškeré servery a úložiště, které v místnosti běží. Dále i fyzická aktiva, jako jsou klimatizace, záložní jednotka napájení, či monitor ke KVM switchi. Samostatnou skupinou aktiv jsou služby.

Tato kapitola je zaměřena na analýzu fyzických aktiv a jejich následné ohodnocení. Fyzická aktiva jsou seřazena v následující tabulce. Pod fyzická aktiva spadají fyzické servery, úložiště, switche a jiné komponenty v serverovně. Na serverech běží různé služby. A právě služby tvoří druhou skupinu aktiv. Některé z nich jsou pro chod Ústavu informatiky i celé podnikatelské fakulty nezbytné, bez některých může fakulta s omezeními fungovat.

Servery jsou od tří různých firem, jedná se o Fujitsu, Dell a HP. Datová úložiště jsou od firem Fujitsu a Synology. Aktiva jsou v tabulce ohodnocena podle důležitosti, a to od hodnoty 2 až do hodnoty 5. Hodnota 5 značí největší míru důležitosti aktiva pro chod celého systému, naopak hodnota 2 míru důležitosti nejmenší. V následujících kapitolách jsou zanalyzované veškeré fyzické i virtuální servery a poté rozděleny do 5 skupin dle priority důležitosti pro chod systému a fyzické infrastruktury. Toto rozdělní slouží i ke specifičtějšímu přístupu při tvorbě plánu obnovy při katastrofě, kdy pro každou ze skupin bude vytvořen samostatný plán. Pátou skupinu tvoří aktiva podpůrné infrastruktury. Vše je detailněji popsáno dále v práci.

Tabulka č.2: Seznam fyzických aktiv (vlastní tvorba)

Typ aktiva	Interní označení	Popis	Ohodnocení aktiva
server	admin1 FYZ	administrace domén	3
server	conf FYZ	konfigurační server	2
server	fdc3 FYZ DNS	řadič domén	5
server	kamery FYZ	kamerový dohled	4
server	monitw FYZ	monitoring hardware	2
server	sql3	witness server	5
server	term1 FYZ	terminálový server	3
server	sejf	zálohy	4
server	V4	server určený k vytváření virtualizací	5
server	V5	server určený k vytváření virtualizací	5
server	V6	server určený k vytváření virtualizací	5
server	V7	server určený k vytváření virtualizací	5
server	V8	server určený k vytváření virtualizací	5
storage	S1backup	záloha úložišť	4
storage	fbmbackup via MFMT	záloha dat zaměstnanců (další záloha na Vserveru)	2
storage	fbmfs3 via MGMT	data zaměstnanců	4
server	itservis	podpora IT	2
storage	stor1	kamerové úložiště	4
storgae	vstor1	úložiště pro virtualizace	5
storage	vstor2	úložiště pro virtualizace	5
storage	vbackup	záloha virtualizace	5
UPS	UPS Eaton	8kVA, 3F, 1h zálohy	5
switch	SW2	hlavní switch – napojení na servery	5
KVM	Kvm	switch management serverů	2
monitor	monitor	monitor, myš a klávesnice	2
chladicí jednotky	klimatizace	celkem 3 ks po obvodových zdech	5
SW61/62	SW61/62	podpůrné switche	5

2.3.1 Fyzické a virtuální servery

Fyzické servery už byly představeny jako fyzická aktiva, nyní se na ně podíváme pouze z hlediska serverů. Součástí této kapitoly jsou i virtualizace, které běží na virtualizačních serverech V4, V5, V6, V7 a V8. Kromě serverů pracují následující kapitoly i s úložišti, které jsou pro komplexní sytém nepostradatelná. V následující tabulce jsou uvedeny veškeré servery a úložiště. Pokud se jedná o virtuální server, je u něj vždy uveden i server, na kterém virtualizace běží. Každý server je i ohodnocen z hlediska důležitosti pro chod informačního systému. Tabulka slouží pro lepší orientaci v celém serverovém systému a v následujících kapitolách je využita pro rozdělení serverů dle priorit.

Tabulka č.3: Fyzické a virtuální servery (vlastní tvorba)

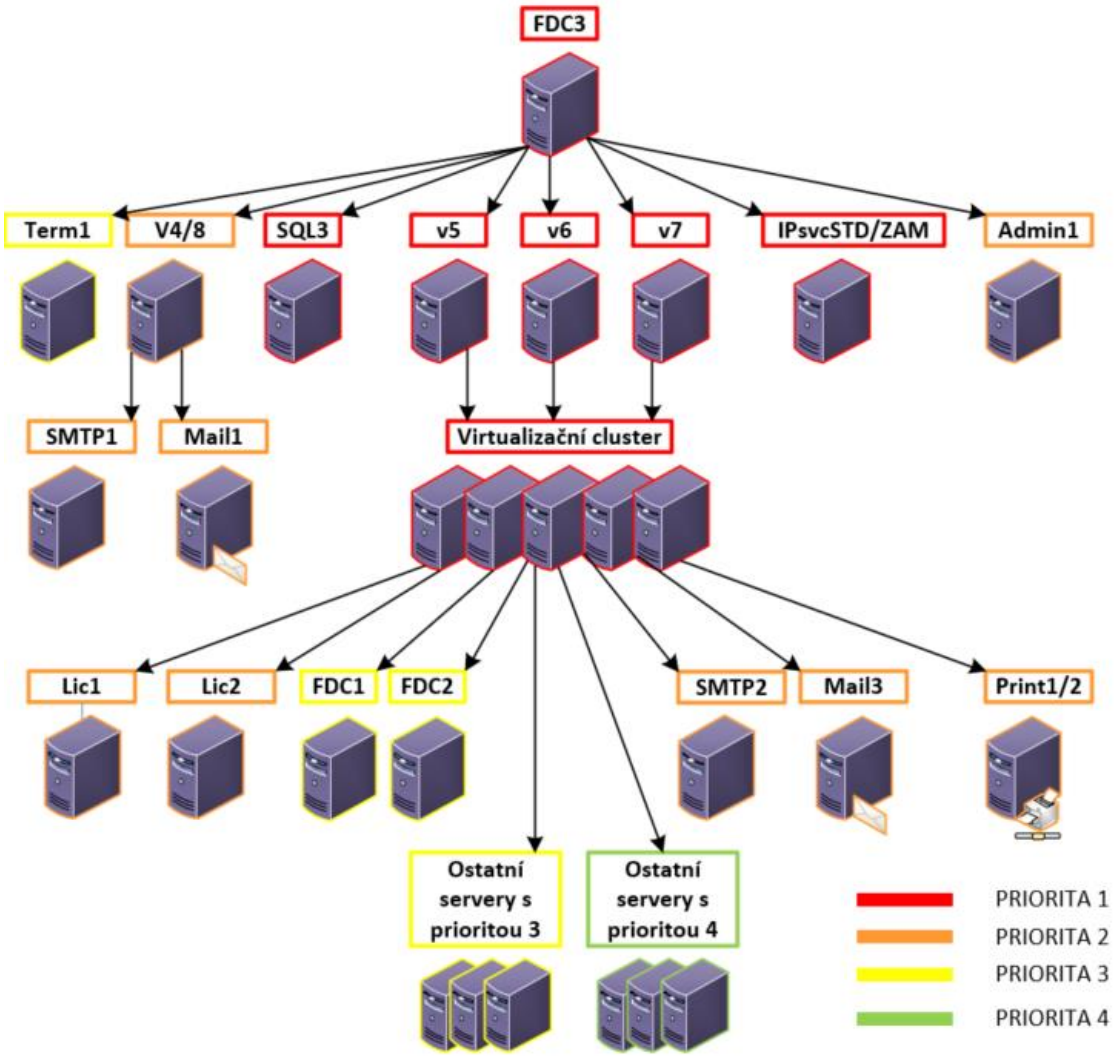
Typ serveru	Interní označení	Popis	Ohodnocení serveru
fyzický	fdc3 FYZ DNS	administrace domén	5
fyzický	IPsvcSTD FYZ	manažerský server, simulace Uranius	5
fyzický	IPsvcZAM FYZ	databázový server Pohoda	5
fyzický	sql3 FYZ	virtualizace aplikačního serveru	5
fyzický	v5 FYZ blade	aplikační server	5
fyzický	v6 FYZ blade	aplikační server	5
fyzický	v7 FYZ blade	podpora výuky	5
úložiště	vstor1 CM0	server pro certifikační autorizaci	5
úložiště	vstor2 CM0	konfigurační server	5
fyzický	admin1 FYZ	administrace domény	4
fyzický	kamery FYZ	kamerový dohled	4
fyzický	lic1	licenční server 1	4
fyzický	lic2	licenční server 2	4
fyzický	mail1 v4	poštovní server 1	4
virtuální	mail2 v2018	poštovní server 2	4
virtuální	print	tiskový server starý	4
virtuální	print2	tiskový server nový	4
virtuální	smtp1 v4	hraniční server Exchange	4
virtuální	smtp2	hraniční server Exchange	4
fyzický	v4 fyz	virtualizace mail1 a smtp1	4
fyzický	v8 FYZ	virtualizace, Exchange plán, mail3 a smtp3	4
virtuální	fbmfs3 via MGMT	home adresáře uživatelů	4
virtuální	stor1	kamerové úložiště	4
virtuální	app1 V1	manažerský server, simulace Uranius	3

Typ serveru	Interní označení	Popis	Ohodnocení serveru
virtuální	app2	stormware Pohoda	3
virtuální	app3 V2	Orsystem	3
virtuální	app4	Pharis	3
virtuální	app5	Pharis optimalizátor, LINUX	3
virtuální	aris	Aris BMP server na WS2016	3
virtuální	plm 01	LAPROCO - produkční server	3
virtuální	plm02	LAPROCO - testovací server	3
virtuální	sql2	MSSQL 2017 výuka, Bizagi DB, WS2017	3
fyzický	term1 FYZ	terminálový server	3
virtuální	fdc1 v2018	schema master, domain naming	3
virtuální	fdc2 v2018	infrastructure master, synchronizace	3
fyzický	conf FYZ	konfigurační server	2
virtuální	ca	certifikační server	2
fyzický	monitw FYZ	monitoring hardwaru + služeb	2
virtuální	timer1	spouští naplánované skripty	2
úložiště	fbmBackup	záloha home adresářů	2
fyzický	itservis	úložiště pro instalace (IT podpora)	2
úložiště	vbackup	záložní úložiště pro virtualizaci	2

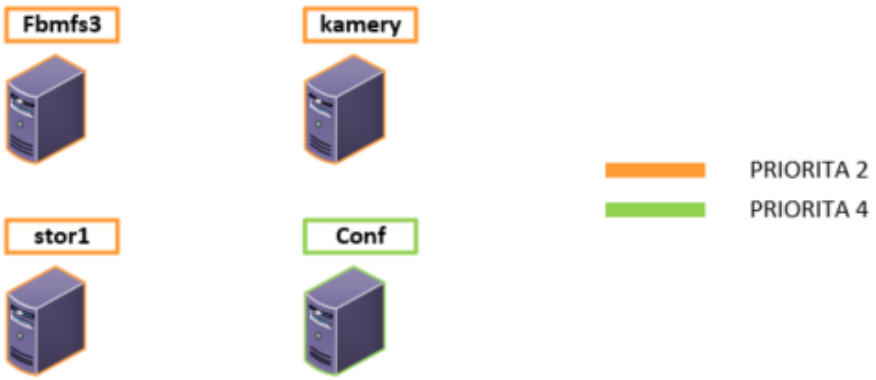
2.3.2 Návaznost serverů

Samozřejmostí je jistá závislost serverů a úložišť, tedy to, jak na sebe servery a úložiště navazují. Znamená to, že daný sever nebo úložiště nemůže bez jiného serveru fungovat. To je znázorněno na obrázku na další straně. Díky tomuto schématu si lze celý systém lépe představit a zmapovat kritická místa. Servery jsou rozděleny do skupin dle priority důležitosti. Jednotlivé skupiny jsou pak označeny různými barvami. Červená barva značí skupinu serverů s nejvyšší prioritou 1. Následuje priorita 2, která je označena oranžově. Žlutá barva značí prioritu 3 a priorita 4 je pod zelenou barvou. V celém systému se nachází i nezávislé servery. Ty běží samostatně bez ohledu na stav ostatních a jsou znázorněny zvlášť na dalším obrázku.

Samozřejmě chod serverů je závislý na přísunu elektrické energie, který je v případě výpadku zajištěn přes UPS. To znamená že bez funkčního záložního zdroje není možný chod serverů. Stejné to je i s chladicím systémem serverovny, který musí být neustále funkční. Tyto dvě skutečnosti nejsou v následujícím schématu uvažovány.



Obrázek 7: Kontinuita serverů a služeb (vlastní tvorba v Microsoft Visio)



Obrázek 8: Samostatně fungující servery (vlastní tvorba v Microsoft Visio)

2.3.3 Servery s prioritou 1

Do této skupiny jsou zařazeny servery a úložiště, které v případě výpadku znamenají nemožnost přihlásit se do jakéhokoliv PC na fakultě. S nadsázkou lze říct, že pokud učitel nechce celou hodinu psát křídou na tabuli, ale potřebuje k výuce využít počítač, tak to nelze. Nikdo z učitelů a studentů tedy nemůže pokračovat ve výuce a studiu s počítačovou podporou.

Hlavním komponentem sítě je server FDC3, který je základem pro celou doménu. S ním je úzce spjat server SQL3. Patří sem i virtuální servery V5-7, které jsou zapojeny v redundanci a tvoří virtuální klastr pro většinu virtuálních serverů, a tím pádem jsou velmi důležité. IP adresy v síti rozdělují servery IPsvcSTD a IPsvcZAM, kde první zmíněný zajišťuje IP adresy pro laboratoře a druhý pro zaměstnance. Posledním prvkem této skupiny jsou datová úložiště, kde jsou uchovány nejdůležitější zálohy – vstor1 a vstor2. U každého serveru je zmíněn jeho výrobce. V případě, že se jedná o virtuální server, je uvedeno, na kterém virtualizačním serveru běží. Tato skupina má nejvyšší přiřazenou prioritu 1, a proto musí být vždy zprovozněna jako první a v co nejkratším čase.

Tabulka č.4: Servery s prioritou 1 (vlastní tvorba)

SERVERY S PRIORITOU 1		
Název serveru/ úložiště	**Výrobce**	**Služba/popis**
fdc3 FYZ DNS	Fujitsu	DNS server
IPsvcSTD FYZ	virtualizace V5-7	DHCP+DNS laboratoře
IPsvcZAM FYZ	virtualizace V5-7	DHCP+DNS zaměstnanci
sql3 FYZ	Fujitsu	MSQL 2017, EA, Uranius, Witness server
v5 FYZ blade	Fujitsu	virtualizace produkce v2018
v6 FYZ blade	Fujitsu	virtualizace produkce v2018
v7 FYZ blade	Fujitsu	virtualizace produkce v2018
vstor1 CM0	Fujitsu	tier 2 virtualizace
vstor2 CM0	Fujitsu	tier 1 virtualizace

2.3.4 Servery s prioritou 2

Tato skupina serverů zajišťuje základní sadu služeb pro studenty i zaměstnance. V případě jejich výpadku lze pokračovat v práci a výuce, ale jen za omezených podmínek. Jedná se např. o tisk, poštovní služby atd. Dále se do této skupiny řadí kamerový server a jeho datové úložiště nebo datové úložiště pro data zaměstnanců školy a jeho záloha. Nejdůležitější je server ADMIN1. Jde o řídící server, díky kterému lze ostatní servery a služby, které na nich běží spravovat. Pro přehlednost jsou opět servery z této skupiny uvedeny v tabulce níže.

Tabulka č.5: Servery s prioritou 2 (vlastní tvorba)

SERVERY S PRIORITOU 2		
Název serveru/ úložiště	**Výrobce**	**Služba/popis**
admin1 FYZ	Fujitsu	administrace domény
kamery FYZ	HP	kamerový dohled
lic1	virtualizace V5-7	licenční server 1
lic2	virtualizace V5-7	licenční server 2
mail1 v4	virtualizace V4,8	poštovní server 1
mail2 v2018	virtualizace V4,8	poštovní server 2
print	virtualizace V5-7	tiskový server starý
print2	virtualizace V5-7	tiskový server nový
smtp1 v4	virtualizace V4,8	hraniční server Exchange
smtp2	virtualizace V4,8	hraniční server Exchange
v4 FYZ	Fujitsu	virtualizace mail1 a smtp1
v8 FYZ	Dell	virtualizace, Exchange plán, mail3 a smtp3
fbmfs3 via MGMT	Synology	home adresáře uživatelů
stor1	Synology	kamerové úložiště

2.3.5 Servery s prioritou 3

Zde se jedná o servery, které poskytují různé aplikace pro výuku. Při výpadku nelze využívat pomocné rozhraní, jako jsou mySQL server, či jiné softwary, které běží na školních serverech. Znamená to tedy, že výuka pokračovat může, ale pouze s omezenými podmínkami a bez využití zmíněných výukových programů. Většina z těchto serverů je virtuálních a běží na virtualizačním klastru V5-7.

Tabulka č.6: Servery s prioritou 3 (vlastní tvorba)

SERVERY S PRIORITOU 3		
Název serveru	**Výrobce**	**Služba/popis**
app1 V1	virtualizace V5-7	manažerský server, simulace Uranius
app2	virtualizace V5-7	stormware Pohoda
app3 V2	virtualizace V5-7	Orsystem
app4	virtualizace V5-7	Pharis
app5	virtualizace V5-7	Pharis optimalizátor, LINUX
aris	virtualizace V5-7	Aris BMP server na WS2016
plm 01	virtualizace V5-7	LAPROCO - produkční server
plm02	virtualizace V5-7	LAPROCO - testovací server
sql2	virtualizace V5-7	MSSQL 2017 výuka, Bizagi DB, WS2017
term1 FYZ	Fujitsu	terminálový server
fdc1 v2018	virtualizace V5-7	schema master, domain naming
fdc2 v2018	virtualizace V5-7	infrastructure master, synchronizace

2.3.6 Servery s prioritou 4

Při problémech se servery z této skupiny nikdo žádnou změnu téměř nezaznamená. Zaměstnanci školy i studenti mohou dál pokračovat ve své práci. Pouze zaměstnanci IT vidí tento problém. Jedná se o různé certifikace, plánování updatů Windows a spouštění jiných skriptů. Součástí této skupiny je server, který slouží k monitoringu hardwaru a služeb.

Tabulka č.7: Servery s prioritou 4 (vlastní tvorba)

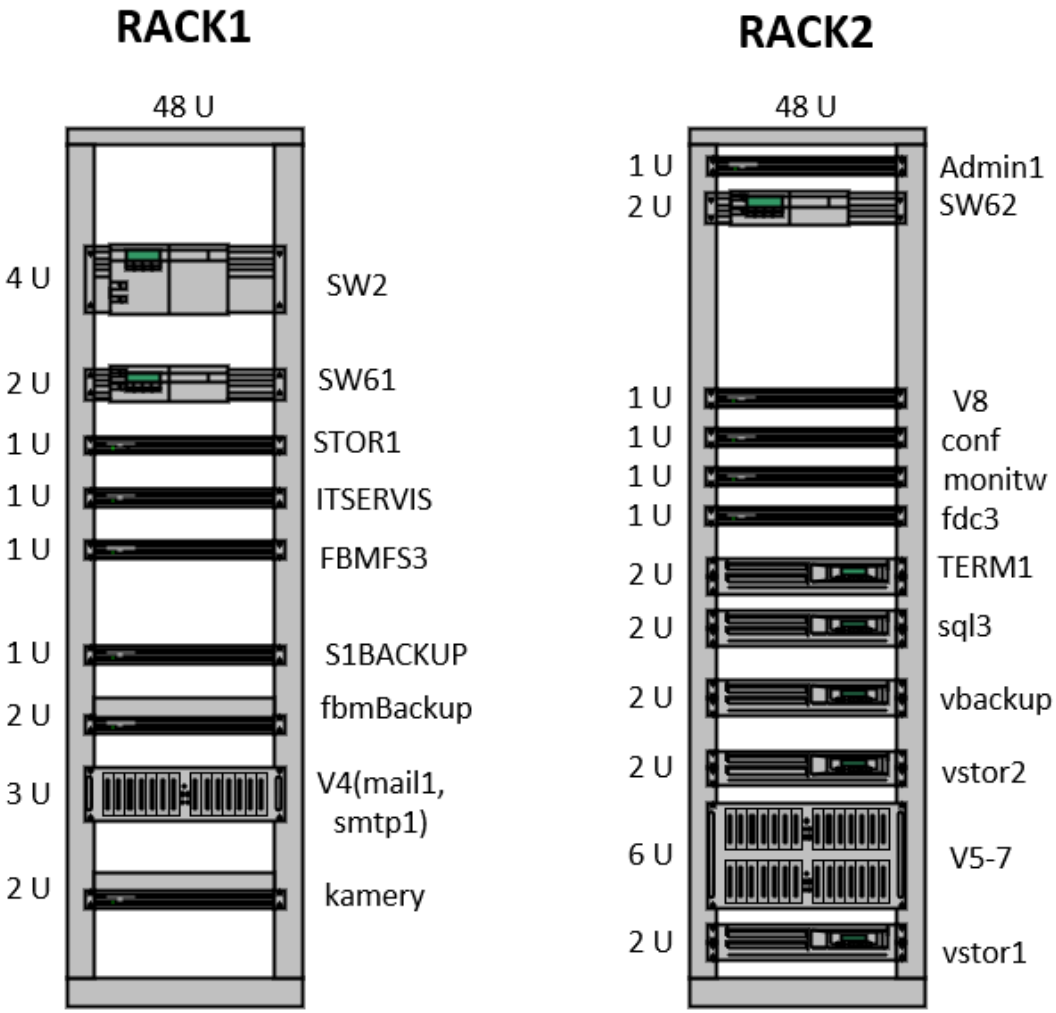
SERVERY S PRIORITOU 4		
Název serveru/ úložiště	**Výrobce**	**Služba/popis**
conf FYZ	Fujitsu	konfigurační server
ca	virtualizace V5-7	certifikační server
monitw FYZ	Fujitsu	monitoring hardwaru + služeb
timer1	virtualizace V5-7	spouští naplánované skripty
fbmBackup	Synology	záloha home adresářů
itservis	Synology	úložiště pro instalace (IT podpora)
vbackup	virtualizace V5-7	záložní úložiště pro virtualizaci

2.3.7 Podpůrná infrastruktura

Hlavním prvkem fyzické infrastruktury serverovny je switch s označením SW2. Ten je napojen na hlavní fakultní síť a zároveň jsou na něj napojeny všechny servery. Tento switch se nachází ve vrchní části datového stojanu s označením RACK1. Ten můžeme pozorovat na obrázku na další straně, kde je znázorněno fyzické rozložení serverů a úložišť ve stojanech. Na obrázku jsou vyobrazeny jen servery, nikoliv kabelážní prvky. Všechny servery a úložiště jsou propojeny s hlavním switchem vždy jen jedním datovým kabelem.

Jak už je v této práci zmíněno, všechny servery i switche jsou napojeny na elektrickou síť přes záložní zdroj UPS, který v případě výpadku elektrického proudu udrží serverovnu při chodu po dobu jedné hodiny. Pokud i po jedné hodině není stále elektrický proud k dispozici, dojde k bezpečnostnímu vypnutí všech serverů. Je to z důvodu nemožnosti chlazení, kdy by mohlo dojít k přehřátí serverů, což by způsobilo nenávratné škody. Chlazení je zajištěno třemi chladicími jednotkami, které jsou umístěny na stěnách serverovny.

Všechny servery jsou napojeny i na kontrolní switch KVM, který se nachází ve stejné místnosti na pracovním stole. Propojení je zajištěno opět datovými kabely. Switch zajišťuje snadnou správu a kontrolu všech serverů přímo z místnosti. Na tento switch se lze připojit i vzdáleným přístupem a lze tak servery spravovat na dálku.



Obrázek 9: Fyzické rozložení serverů (vlastní tvorba v Microsoft Visio)

Tabulka č.8: Podpůrná infrastruktura (vlastní tvorba)

PODPŮRNÁ INFRASTRUKTURA		
Název aktiva	**Výrobce**	**Popis**
UPS	UPS Eaton	záložní zdroj, 8kVA, 3F, 1h zálohy
SW2	HP	podpůrný switch
SW61	HP	podpůrný switch
SW62	HP	spouští naplánované skripty
KVM	Aten	KVM switch pro management serverů
chladicí jednotky	Fujitsu	3 klimatizační jednotky
monitor		monitor, myš a klávesnice ke KVM

2.4 Aktiva služeb a jejich ohodnocení

Aktiva služeb jsou také ohodnocena dle důležitosti pro chod Ústavu informatiky. Nejnižší hodnota je 2, nejvyšší 5. Dle toho jsou služby, stejně jako fyzická aktiva rozděleny do skupin dle priorit 1–4. Poslední podskupinou aktiv služeb jsou již zmíněné externí servisní služby, jako je například servis UPS nebo chladicích jednotek. Všechny podskupiny služeb jsou detailně popsány v následujících kapitolách. Následující rozdělení je velice důležité jak pro analýzu rizik, tak hlavně pro sestavení plánu obnovy. DR plány jsou vytvořeny pro každou skupinu služeb samostatně. Tím jsou mnohem konkrétnější a řeší mnohonásobný počet bezpečnostních incidentů.

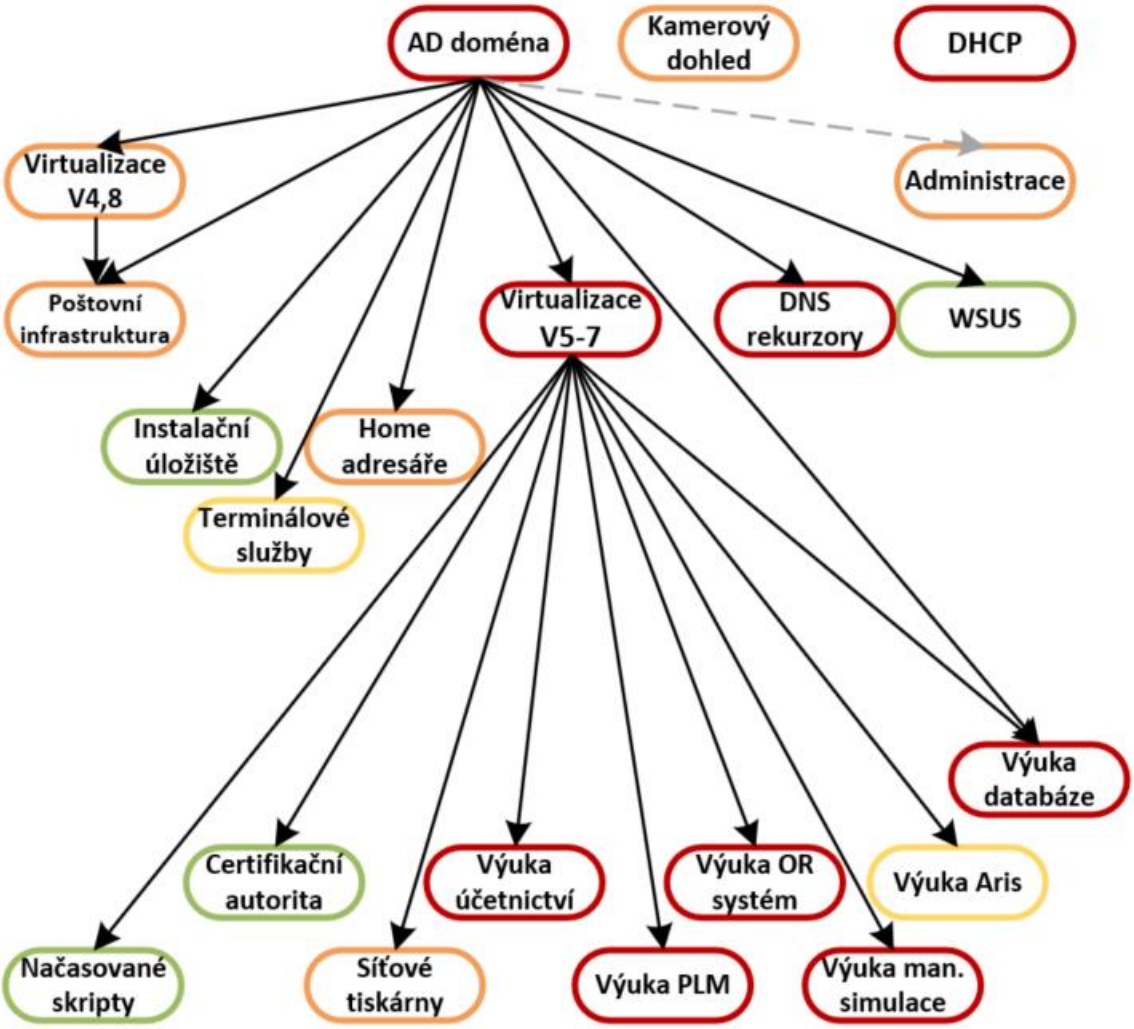
Tabulka č.9: Aktiva – služby (vlastní tvorba)

Druh aktiva	Interní označení	Příslušné servery/ popis	Hodnota
interní služba	AD doména	FDC3, FDC1, FDC2	5
interní služba	DHCP	IPsvcSTD + IPsvcZAM	5
interní služba	DNS rekurzory	IPsvcSTD, IpsvcZAM	5
interní služba	virtualizace	V5, V6, V7 (alespoň 2 musí fungovat)	5
	virtualizace pošta	V4 (náhrada V8)	5
interní služba	výuka-účetnictví	SQL3 + APP2 + LIC1	5
interní služba	výuka-databáze	SQL2	5
interní služba	výuka-manažerská simulace	APP1 + SQL3	5
interní služba	výuka-OR systém	SQL3 + APP3	5
interní služba	výuka-PLM	SQL3 + PLM01 + APP4 + APP5 + LIC3	5
interní služba	administrace	ADMIN1	4
interní služba	kamerový dohled	Kamery + stor1	4
interní služba	poštovní infrastruktura	(MAIL1, MAIL2) + (SMTP1, SMTP2) + SQL3	4
interní služba	síťové tiskárny	PRINT2	4
interní služba	home adresáře uživatelů	FBMFS3 + FBMbackup	4
interní služba	výuka-aris	ARIS	3
interní služba	terminálové služby	TERM1 + LIC1	3
interní služba	WSUS	CONF + ADMIN1 (Windows server update services)	3
interní služba	certifikace autorit	CA	3
interní služba	Načasované skripty	TIMER1	3
interní služba	instalační úložiště	ITSERVIS	3

2.4.1 Návaznost služeb

Stejně jako servery, i služby jsou provázány jistou závislostí na jiných službách. To znamená, že jedna služba nemůže bez té druhé fungovat. Pak tu jsou samozřejmě i služby, které běží samostatně. Na dalším obrázku je závislost jednotlivých služeb názorně vyobrazena. Díky tomuto grafu lze snadněji rozdělit služby dle priorit a navrhnout pro každou skupinu samostatný DR plán.

Je samozřejmé, že služba ke své funkčnosti potřebuje funkční servery, na kterých běží. A stejně tak servery potřebují elektrickou energii a chlazení. Tyto skutečnosti nejsou v následujícím schématu znázorněny a jsou brány jako samozřejmost.



Obrázek 10: **Kontinuita služeb** (vlastní tvorba v Microsoft Visio)

Stejně jako u kontinuity serverů, i zde jsou služby označeny různými barvami dle priority důležitosti. Služby s prioritou 1 jsou označeny červeně, služby s prioritou 2 oranžově, služby s prioritou 3 žlutě a zelená barva značí služby s prioritou 4. V následujících kapitolách jsou jednotlivé skupiny služeb podrobněji popsány.

2.4.2 Služby s prioritou 1

Do skupiny s prioritou 1 jsou zařazeny služby, bez kterých není možná funkčnost počítačové sítě na podnikatelské fakultě. Není možné se vůbec přihlásit do PC. Dále sem patří služby, které zajišťují výukové programy pro studenty. U každé služby jsou uvedeny vždy servery a úložiště, které musí být funkční pro chod dané služby. Tak tomu je i u všech následujících prioritních skupin služeb.

Nepostradatelnou službou je AD doména, bez které se normální uživatel nedokáže přihlásit do systému, a navíc na ní závisí většina ostatních služeb. Další důležitou službou je virtualizace V5-6. Ta poskytuje prostor pro 9 virtualizačních serverů. Dále do této skupiny patří služba DHCP a již zmíněné výukové programy.

Tabulka č.10: Služby s prioritou 1 (vlastní tvorba)

SLUŽBY S PRIORITOU 1	
Název služby	**Příslušné servery a úložiště**
AD doména	FDC3, FDC1, FDC2
DHCP	IPsvcSTD + IPsvcZAM
DNS rekurzory	IPsvcSTD, IpsvcZAM
virtualizace V5-7	V5, V6, V7 (alespoň 2 musí fungovat) + VSTOR1 + VSTOR2
výuka-účetnictví	SQL3 + APP2 + LIC1
výuka-databáze	SQL2
výuka-manažerská simulace	APP1 + SQL3
výuka-OR systém	SQL3 + APP3
výuka-PLM	SQL3 + PLM01 + APP4 + APP5 + LIC3

2.4.3 Služby s prioritou 2

Do skupiny s prioritou 2 jsou zařazeny služby, které v případě výpadku neovlivní chod systému ani výuky. Jedná se o služby administrace serverů, kamerový dohled, síťové tiskárny a domovské adresáře uživatelů. Dále sem spadá virtualizace V4 a její záloha V8, na kterých běží poštovní služby.

Tabulka č.11: Služby s prioritou 2 (vlastní tvorba)

SLUŽBY S PRIORITOU 2	
Název služby	**Příslušné servery a úložiště**
administrace	ADMIN1
kamerový dohled	kamery + stor1
virtualizace V4, V8	V4, náhrada V8, pouze pro poštovní služby
poštovní infrastruktura	(MAIL1, MAIL2) + (SMTP1, SMTP2) + SQL3
síťové tiskárny	PRINT2
home adresáře uživatelů	FBMFS3+FBMbackup

2.4.4 Služby s prioritou 3

Skupina služeb s prioritou 3 obsahuje pouze dvě položky. Patří sem služba Aris, která slouží pro výuku, ale je momentálně nevyužívána. Druhou položkou jsou terminálové služby, které vyžadují chod serverů TERM1 a LIC1.

Tabulka č.12: Služby s prioritou 3 (vlastní tvorba)

SLUŽBY S PRIORITOU 3	
Název služby	**Příslušné servery a úložiště**
výuka – aris	ARIS
terminálové služby	TERM1 + LIC1

2.4.5 Služby s prioritou 4

Poslední skupinou s nejnižší prioritou 4 jsou služby, které využívají převážně jen IT zaměstnanci Ústavu informatiky. Služba WSUS slouží k aktualizování a servisu Windows Server. Dále do této skupiny patří služba certifikační autorita, instalační úložiště a načasované skripty, které umožňují spustit naplánované údržby systému.

Tabulka č.13: Služby s prioritou 4 (vlastní tvorba)

SERVERY S PRIORITOU 4	
Název serveru	**Služba a úložiště**
WSUS	CONF + ADMIN1 (windows server update services)
certifikační autorita	CA
načasované skripty	TIMER1
instalační úložiště	ITSERVIS

2.4.6 Externí služby

Mezi externí služby se řadí např. servis klimatizací, UPS, ale i serverů či úložišť. Je důležité zmínit, že univerzita nemá uzavřeny servisní smlouvy na klimatizace ani na UPS *„Service-level agreement“*, tedy smlouvy s prodejci, které zajišťují provoz techniky a zavazují prodejce k okamžité nápravě případných komplikací. Smlouvy o servisu produktů, které má škola uzavřeny, se vztahují na výrobky Dell a Fujitsu. Služba *„Hi-Tech services“* je smluvní servis pro komponenty od firmy Fujitsu a služba *„ProSupport“* se vztahuje na komponenty od firmy Dell. Pro produkty od firmy HP nebyla žádná smlouva uzavřena a jsou tedy v tomto směru bez podpory.

Tabulka č.14: Externí služby (vlastní tvorba)

Externí služby	
Název služby	**Popis**
Hi-Tech services	smluvní servis na produkty Fujitsu
ProSupport	smluvní servis na produkty Dell

2.5 Analýza rizik

V analýze rizik je využito rozdělení aktiv na fyzická aktiva, která jsou zastoupena prioritními skupinami 1-4 se servery a úložišti. Dále bude z hlediska rizik ohodnocena i podpůrná infrastruktura. Druhou skupinu aktiv k analýze rizik tvoří služby. Konkrétně jsou analyzovány prioritní skupiny služeb 1-4.

Rizika jsou rozdělena na zranitelnosti a hrozby. Dále v textu se nachází tabulky, kde je vysvětleno ohodnocení těchto dvou podskupin. Dále je využito seznamu zranitelností a hrozeb ze Sbírky zákonů č.82/2018. Jedná se o kybernetickou vyhlášku, která by měla mít zpracované všechny obecné zranitelnosti a rizika týkající se informační bezpečnosti.

Hodnota jednotlivých zranitelností a rizik je v tabulkách vždy vynásobena hodnotou dané skupiny aktiv a vzniká tak celková hodnota zranitelností nebo rizika pro danou skupinu. Nejnižší hodnota může být 2, maximum 25. Čím vyšší hodnota vychází, tím musíme brát větší zřetel na danou zranitelnost nebo riziko.

2.5.1 Tabulky pro ohodnocení zranitelností a hrozeb

Dle následujících tabulek lze jednoduše ohodnotit jednotlivé zranitelnosti a hrozby, které mohou nastat, a se kterými se musí počítat. Tabulky jsou převzaty z vyhlášky o kybernetickém zákonu. Zranitelnosti i rizika jsou v nich rozděleny do čtyř skupin, a to dle míry závažnosti dopadu a pravděpodobnosti výskytu. Je zde uvedena úroveň zranitelnosti či hrozby, popis a hodnota pro další výpočty při analýze rizik. Úroveň s nejnižší hodnotou 1 je označena „nízká“. To znamená, že zranitelnost téměř neexistuje nebo se objeví jednou za více než 5 let. Rizika zařazená do této skupiny lze akceptovat. Naopak skupina s nejvyšší číselnou hodnotou 5 značí vysokou míru zneužití zranitelnosti a obrovský dopad rizika, které se musí neprodleně řešit. Tato úroveň je nazvána „kritická“.

Tabulka č.15: Úrovně zranitelností (vlastní tvorba dle (29))

Úroveň	Popis	Hodnota
Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.	**1**
Střední	Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.	**2**
Vysoká	Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.	**3**
Kritická	Zneužití zranitelnosti je pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.	**4**

Tabulka č.16: Úrovně hrozeb (vlastní tvorba dle (29))

Úroveň	Popis	Hodnota
Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.	**1**
Střední	Hrozba je málo pravděpodobná, až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.	**2**
Vysoká	Hrozba je pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.	**3**
Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.	**4**

2.5.2 Zranitelnosti fyzických aktiv

Tato podkapitola odhaluje zranitelnosti – tedy slabá místa systému. V tabulce jsou vypsány zranitelnosti dle Sbírky zákonů č. 82/2018 – Vyhláška o kybernetické bezpečnosti. Jednotlivé zranitelnosti jsou ohodnoceny podle hodnotících tabulek

zmíněných výše v této práci a vynásobeny s hodnotou dané skupiny aktiv. Ohodnocení zranitelností probíhá zvlášť pro každou ze skupin aktiv.

Tabulka č.17: Zranitelnosti fyzických aktiv (vlastní tvorba)

	Skupiny aktiv				
	SERVERY S PRIORITOU 1	**SERVERY S PRIORITOU 2**	**SERVERY S PRIORITOU 3**	**SERVERY S PRIORITOU 4**	**PODPŮRNÁ INFRASTRUKTURA**
nedostatečná údržba informačního a komunikačního systému	10	8	6	4	10
zastaralost informačního a komunikačního systému	25	20	20	15	10
nedostatečná ochrana vnějšího perimetru	5	4	3	2	5
nedostatečné bezpečnostní povědomí uživatelů a administrátorů	10	8	6	4	10
nevhodné nastavení přístupových oprávnění	10	8	6	4	10
nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů	20	16	12	8	20
nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	-	-	-	-	-
nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	15	12	9	6	15
nedostatečná ochrana aktiv	10	8	6	4	10
nevhodná bezpečnostní architektura	20	16	12	8	20
nedostatečná míra nezávislé kontroly	20	16	12	8	20
neschopnost včasného odhalení pochybení ze strany zaměstnanců	15	12	9	6	15

Jako nejzávažnější zranitelnost je považována zastaralost informačního a komunikačního systému. Nejde ani tak o zastaralost, jako spíš o to, že v serverovně je umístěn určitý typ virtuálního klastru, do kterého již firma Fujitsu nedodává vhodné moduly. V případě zničení některého z modulů, nebo potřeby rozšíření virtualizace by

tato skutečnost byla příčinou velkých problémů. Nový virtualizační klastr stojí několik milionů korun. Mezi další významné zranitelnosti patří nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů. Na Ústavu informatiky není zaveden ISMS, který by tyto události řešil. Naštěstí pravděpodobnost výskytu takovéto události je minimální. Další zranitelností s celkem vysokým ohodnocením je nevhodná bezpečnostní architektura. A to ze dvou důvodů: Zaprvé chybí externí redundance serverů a zadruhé nad serverovnou se nachází sociální zařízení. V případě prasklého potrubí a průsaku vody do serverovny nastávají obrovské problémy.

2.5.3 Hrozby fyzických aktiv

Hrozby – tedy možné příčiny vzniku bezpečnostního incidentu jsou vypsány a ohodnoceny v následující tabulce. Seznam hrozeb byl opět čerpán ze Zákona č. 82/2108 – Vyhláška o kybernetické bezpečnosti. Ohodnocení jednotlivých skupin aktiv probíhá dle tabulky ohodnocení hrozeb. Tedy čím vyšší hodnota, tím je hrozba pravděpodobnější a její dopad závažnější. Tyto hodnoty jsou posléze opět vynásobeny s hodnotou dané skupiny aktiv.

Tabulka č.18: Hrozby fyzických aktiv (vlastní tvorba)

	Skupiny aktiv				
	SERVERY S PRIORITOU 1	SERVERY S PRIORITOU 2	SERVERY S PRIORITOU 3	SERVERY S PRIORITOU 4	FYZICKÁ INFRASTRUKTURA
porušení bezpečnostní politiky, provedení neoprávněných činností zneužití oprávnění ze strany uživatelů a administrátorů	15	12	9	6	15
poškození nebo selhání technického anebo programového vybavení	20	16	12	8	20
zneužití identity	5	4	3	2	5
užívání programového vybavení v rozporu s licenčními podmínkami	5	4	3	2	5
škodlivý kód (například viry, spyware, trojské koně)	20	16	12	8	20
narušení fyzické bezpečnosti	10	8	6	4	10
porušení poskytování služeb elektronických komunikací nebo dávek elektrické energie	20	16	12	8	20
zneužití nebo neoprávněná modifikace údajů	5	4	3	2	5
ztráta odcizení nebo poškození aktiva	5	4	3	2	5
nedodržení smluvního závazku ze strany dodavatele	10	8	6	4	10
pochybení ze strany zaměstnanců	20	16	12	8	20
zneužití vnitřních prostředků, sabotáž	5	4	3	2	5
dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	10	8	6	4	10
nedostatek zaměstnanců s potřebnou odbornou úrovní	25	20	15	10	25
cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	10	8	6	4	10
zneužití vyměnitelných technických nosičů dat	5	4	3	2	5
napadení elektronické komunikace (odposlech, modifikace)	5	4	3	2	5

Mezi největší hrozby pro fyzická aktiva patří nedostatek zaměstnanců s potřebnou odbornou úrovní. Serverovnu mají na starost dva zaměstnanci. Jeden je zaměstnán na Ústavu informatiky na plný úvazek, druhý na 1/3. To znamená, že serverovna je pod odborným dohledem pouze 40 hodin v týdnu. Zbylých 128 hodin je hlídána pouze teplota serverovny personálem na vrátnici. Tento personál ovšem neví o správě ICT zařízení téměř nic. Z tohoto důvodu by mohlo dojít v případě bezpečnostního incidentu

ke znatelným škodám. Další velkou hrozbou je dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb. Serverovna je vybavena záložním zdrojem UPS, který vydrží napájet servery a chlazení pouze jednu hodinu. V případě delšího výpadku proudu je tak nutné servery vypnout.

2.5.4 Zranitelnosti služeb

Stejně jako u fyzických aktiv, tak i u aktiv služeb bude dosaženo výsledné hodnoty vynásobením hodnoty aktiva s hodnotou zranitelnosti.

Tabulka č.19: Zranitelnosti služeb (vlastní tvorba)

	Skupiny aktiv			
	SUŽBY S PRIORITOU 1	SLUŽBY S PRIORITO 2	SLUŽBY S PRIORITOU 3	SLUŽBY S PRIORITOU 4
nedostatečná údržba informačního a komunikačního systému	15	12	9	6
zastaralost informačního a komunikačního systému	15	12	9	6
nedostatečná ochrana vnějšího perimetru	-	-	-	-
nedostatečné bezpečnostní povědomí uživatelů a administrátorů	15	12	9	6
nevhodné nastavení přístupových oprávnění	15	12	9	6
nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů	10	8	6	4
nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	15	12	9	6
nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	15	12	9	6
nedostatečná ochrana aktiv	15	12	9	6
nevhodná bezpečnostní architektura	-	-	-	-
nedostatečná míra nezávislé kontroly	10	8	6	4
neschopnost včasného odhalení pochybení ze strany zaměstnanců	15	12	9	6

U služeb nevyčnívá žádná výraznější zranitelnost. Lze zmínit nedostatečnou údržbu informačního a komunikačního systému, což může být způsobeno přílišným vytížením personálu. Stejnou příčinu můžeme hledat i u nedostatečného monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování. Dva lidé, kdy pouze jeden z nich pracuje pro univerzitu na plný úvazek, nemohou stíhat monitorovat veškeré užívání služeb.

2.5.5 Hrozby služeb

Tabulka č.20: Hrozby služeb (vlastní tvorba)

	Skupiny aktiv			
	SUŽBY S PRIORITOU 1	SLUŽBY S PRIORITO 2	SLUŽBY S PRIORITOU 3	SLUŽBY S PRIORITOU 4
porušení bezpečnostní politiky, provedení neoprávněných činností zneužití oprávnění ze strany uživatelů a administrátorů	10	8	6	4
poškození nebo selhání technického anebo programového vybavení	10	8	6	4
zneužití identity	5	4	3	2
užívání programového vybavení v rozporu s licenčními podmínkami	5	4	3	2
škodlivý kód (například viry, spyware, trojské koně)	10	8	6	4
narušení fyzické bezpečnosti	5	4	3	2
porušení poskytování služeb elektronických komunikací nebo dávek elektrické energie	5	4	3	2
zneužití nebo neoprávněná modifikace údajů	5	4	3	2
ztráta odcizení nebo poškození aktiva	5	4	3	2
nedodržení smluvního závazku ze strany dodavatele	5	4	3	2
pochybení ze strany zaměstnanců	10	8	6	4
zneužití vnitřních prostředků, sabotáž	5	4	3	2
dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	5	4	3	2
nedostatek zaměstnanců s potřebnou odbornou úrovní	20	16	12	8
cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	5	4	3	2
zneužití vyměnitelných technických nosičů dat	15	12	9	6
napadení elektronické komunikace (odposlech, modifikace)	5	4	3	2

I u hrozeb pro aktiva služeb musí být zmíněn nedostatek zaměstnanců s potřebnou odbornou úrovní. Stejný personál, který má na starosti chod infrastruktury serverovny, má na starost i chod služeb. Je zřejmé, že zvládat oba tyto úkony musí být časově velmi náročné. Lze tedy předpokládat velkou vytíženost zaměstnanců, a tím pádem větší

pravděpodobnost jejich pochybení. Další hrozbou s vyšším ohodnocením je zneužití vyměnitelných technických nosičů dat. K počítačům zapojeným do sítě mají přístup všichni studenti. Je jen otázkou času, než někdo využije volného přístupu k zásuvkám USB a pokusí se infiltrovat do sítě. Přesto se předpokládá, že studenti k takovému jednání nepřistoupí a proti cizím osobám je přístup k počítačům zabezpečen dveřmi s elektronickým zámkem.

2.5.6 Další hrozby

Mezi tyto hrozby mohou být zařazeny přírodní katastrofy. Nicméně zemětřesení, hurikán i povodně jsou v této lokalitě nepravděpodobné. Proto jsou mezi tyto hrozby zařazeny možnost požáru, vodovodní havárie a selhání lidského faktoru z hlediska kontroly serverovny.

Požár je nejspíše nejméně pravděpodobnou hrozbou z této skupiny. Budova je vybavena protipožárními čidly, hasicími přístroji a je zavedena požární směrnice, která nám říká, jak v případě požáru postupovat. Nicméně tato směrnice je obecná a vztahuje se na celou budovu. Proto je nutné vytvořit samostatný DR plán v případě požáru i pro serverovnu. Zde musí být zohledněn materiál elektrické kabeláže, který je v případě vzplanutí velice toxický a životu nebezpečný.

Další hrozbou je vodovodní havárie. Zde hrozí největší nebezpečí havárií vodovodního potrubí od sociálního zařízení, které se nachází v podlaží nad serverovnou. Už několikrát se stalo, že praskla např. přípojná hadička k WC a voda začala prosakovat do patra serverovny. Naštěstí tento průsak nevedl přímo do místnosti serverovny, ale do chodby před ní. I tak je nutné se touto hrozbou zaobírat, a i pro ni sestavit příslušný DR plán.

Poslední hrozbou z této skupiny je hrozba lidského selhání. Konktrétně se jedná o selhání pracovníka na vrátnici univerzity, který má za úkol pravidelné obchůzky. Ty zahrnují i kontrolu serverovny. Tento zaměstnanec má k dispozici i kontrolní terminál, kde vidí aktuální teplotu v serverovně. Univerzita již byla svědkem situace, kdy zaměstnanec na vrátnici noční obchůzky neprováděl poctivě a bohužel ve stejný čas selhal i kontrolní terminál teploty serverovny. V serverovně vzrostla teplota nad nepřípustnou hranici, ale nikdo se o tom nedozvěděl. Nehoda byla odhalena až ráno,

kdy přišli do práce zaměstnanci Ústavu informatiky. To už však bylo několik disků tzv. „uvařeno“ a nenávratně poškozeno.

Existuje mnoho dalších situací, kdy byla bezpečnost serverovny ohrožena. Např. ohlášená odstávka elektrické energie na sobotu, o které se od správy budovy zaměstnanci Ústavu informatiky nedozvěděli. Správa budovy si řekla, že v sobotu se neučí, tak není nutné tuto informaci předat dále. Tím došlo k velkému problému a vypnutí systému. K dalšímu incidentu mohlo dojít, když probíhalo umývání oken v budově externí firmou. Tato firma dostala univerzální klíč a mohla se tak dostat do všech místností. Když na firmu, která zrovna byla v serverovně narazili zaměstnanci Ústavu informatiky, spatřili kýbl s vodou položený přímo na jednotce UPS. Zde stačilo opravdu málo, a mohlo dojít k obrovskému neštěstí. Pro tyto hrozby nelze sestrojit DR plán, ale je nutné vyvodit přiměřená opatření a doporučení, která budou uvedena v kapitole 4 této diplomové práce.

3 VLASTNÍ NÁVRH PLÁNU OBNOVY

Tato kapitola se věnuje sestavení samotného plánu obnovy v případě katastrofy. DR plán je založen na předchozí analytické části práce. Stěžejními částmi jsou seznam aktiv, jejich rozbor a analýza rizik. Jsou zde podrobně rozepsána jednotlivá východiska, na kterých je plán obnovy založen. Dále jsou zde upřesněny jednotlivé role zaměstnanců, jejich odpovědnosti a kontakty. DR plán je vždy navrhnut zvlášť pro jednotlivé skupiny, do kterých byla aktiva rozdělena v analytické části práce. Dále je rozvedeno několik možných rizikových scénářů, které mohou nastat a případné kroky, jak v takových situacích postupovat. Směrnice DR plánu a další důležité dokumenty, jako je seznam důležitých procesů a priorita jejich obnovy, tabulka důležitých zaměstnanců a jejich kontakty, budou uvedeny v přílohách.

3.1 Definování DR plánu

Jak už je zřejmé z analytické části, DR plán se týká serverovny Ústavu informatiky Fakulty podnikatelské při VUT v Brně. Konkrétně plán obnovy při katastrofě řeší servery, úložiště, podpůrnou infrastrukturu a služby, které Ústav informatiky poskytuje. Tato aktiva jsou rozdělena do skupin dle analytické části a pro každou z nich je vytvořen speciální plán obnovy.

Nejdříve je však nutné stanovit DR tým, který bude DR plány obstarávat a řídit se jimi. Je také nezbytné utvořit seznam důležitých kontaktů, které jsou hojně v nouzových situacích využívány.

3.2 Sestavení DR týmu

Tzv. DR tým je sdružení pracovníků Ústavu informatiky, kteří mají za úkol likvidovat bezpečnostní incidenty, které nastaly. Tým se skládá z několika rolí, kde každý člen má různé zodpovědnosti. Tyto role a zodpovědnosti jsou rozepsány v následující kapitole. Tabulka DR týmu je uvedena v DR plánu v přílohách. Ústav informatiky do ní pak doplní příslušná jména.

3.2.1 Role a zodpovědnosti DR týmu

První rolí je vedoucí DR týmu. Většinou jím bývá vedoucí celého IT oddělení. Má na starost schvalování strategie a specifických postupů při likvidování katastrofy. Pod jeho záštitu spadá i schvalování rozpočtu při řešení bezpečnostních incidentů.

Pod vedoucím DR týmu se nachází krizový manažer. Ten řídí samotný DR tým od začátku bezpečnostního incidentu až po jeho likvidaci. Dohlíží na stanovené postupy a koordinuje práci týmu. Je u něj vyžadována patřičná zkušenost při řešení podobných krizových situací.

Mezi ostatní členy DR týmu patří zaměstnanci, kteří mají praktické znalosti v dané oblasti. Zde se může např. rozlišovat specialista na řešení incidentů se servery a úložišti nebo specialista na síťové prvky. Tito členové jsou pro DR plán zcela nezbytní. Většinu problémů vyřeší rychle a bez větších potíží, protože čerpají z předchozích zkušeností. Mezi jejich úkoly patří incident identifikovat, poté sestavit strategii řešení k odstranění problému a také ji implementovat, a nakonec obnovit poškozená aktiva systému.

Posledním členem DR týmu je specialista na monitoring IT služeb, které Ústav informatiky poskytuje. Dbá na konzistenci dat, správnou integraci služeb, nastavení a konfiguraci.

3.3 Důležité kontakty

Součástí DR plánu je i tabulka s důležitými kontakty. Ta bude uvedena v příloze u DR plánu, stejně jako tabulka s DR týmem. Mezi tyto kontakty řadíme důležité pracovníky univerzity včetně DR týmu. Tato skupina bude popsána v kapitole Kontakty interních pracovníků. Dále sem řadíme kontakty na externí služby, které jsou využity v případě, kdy je řešení bezpečnostního incidentu nad rámec DR týmu.

3.3.1 Kontakty interních pracovníků

Kontakty DR týmu jsou v případě katastrofy velmi důležité. Komunikace je základem úspěchu většiny kritických situací. U daného jména jsou vždy uvedena všechna dostupná čísla na mobilní telefony i pevnou linku, e-mailová adresa a adresa trvalého

bydliště. DR tým by tyto kontakty měl mít vždy uložené v mobilním zařízení připravené k použití. Dále jsou do této skupiny kontaktů zařazeny kontakty na správce budovy a vrátnici, kancelář vedoucího Ústavu informatiky nebo děkanát fakulty. Kontakt na správce budovy může být využit například při požadavku na okamžité uzavření hlavního uzávěru vody v případě vodovodní havárie. Důležitým úkolem je i pravidelná aktualizace a kontrola kontaktů. Ta by měla probíhat minimálně jednou za 6 měsíců.

3.3.2 Kontakty externích služeb

Do externích služeb jsou zařazeny servisní služby výrobců používaných serverů, úložišť a jiných fyzických aktiv. Dvě servisní služby od výrobce Fujitsu a Dell jsou smluvní. Zbytek aktiv smluvní servisní službu nemá. I tak je nutné tyto kontakty uvést, aby bylo možné zajistit co možná nejrychlejší servis, nebo náhradu aktiva v případě potřeby. Dále sem patří kontakty tísňových linek, mezi které patří hasiči, policie ČR, záchranná služba a městská policie.

3.4 Postup při obnovení aktiv a služeb

V této kapitole jsou popsány DR plány pro jednotlivé skupiny aktiv. Je téměř nemožné sestrojit jeden plán obnovy pro celou serverovnu a když už se k takovému postupu přistoupí, bývá plán velmi zmatečný a nejasný. Proto je zde vytvořeno DR plánů několik.

Jednotlivé postupy jsou uvedeny i v příloze, kde je uveden celý DR plán v podobě, v jaké ho bude využívat Ústav informatiky Fakulty podnikatelské při VUT.

3.4.1 Kontrola bezpečnosti perimetru

Položkou každého DR plánu jednotlivých skupin serverů, úložišť a podpůrné infrastruktury je kontrola bezpečnosti perimetru. Jedná se o kontrolu serverovny a jejího okolí. Cílem je zjistit, zda nedošlo k nějakému bezpečnostnímu incidentu, který by mohl poškodit zařízení v serverovně nebo místnost samotnou. Kontrola bezpečnosti perimetru je popsána v následujícím odstavci.

Při vstupu do serverovny zjistíme, zda nebyl jakýmkoliv způsobem poničen zámek nebo dveře serverovny. Dále probíhá kontrola fyzického stavu místnosti. Ta musí být zavřená, UPS a chladicí jednotky funkční. Servery, úložiště a switche nesmí jevit známky fyzického poničení. Pokud je zřejmé, že někdo násilím vniknul do místnosti, poničil servery, nebo je dokonce odcizil, je nutné okamžitě kontaktovat policii České republiky. V případě známek vniknutí vody nebo požáru, je zapotřebí okamžitě aktivovat příslušný DR plán. Pokud je vše v pořádku, lze pokračovat v průběhu aktuálního DR plánu.

3.4.2 DR plán pro servery s prioritou 1

Tato skupina serverů má nejvyšší prioritu, protože bez její funkčnosti se prakticky nelze přihlásit na jakýkoliv počítač v této síti. Proto je důležité obnovit chod těchto aktiv v co nejkratším čase. Veškeré funkce by měli být napraveny nejpozději do 12 hodin od zjištění poruchy. V následujícím odstavci bude popsán postup jak při poškození, týkající se této skupiny s prioritou 1 postupovat.

Prvním krokem je kontrola bezpečnosti perimetru. To znamená, že serverovna musí být v normálním stavu a nesmí vykazovat známky poničení, či jiné neobvyklé věci, jako je například voda na podlaze atd. Samozřejmostí je funkční náhradní zdroj, který musí být pod elektrickým proudem. Stejně tak musí být zapnuté chladicí jednotky na stěnách serverovny. Dalším krokem je kontrola fyzického propojení veškerých serverů. Pokud je vše v pořádku, může se přikročit k zapnutí systému.

Nejdříve je nutné ruční zapnutí serveru FDC3. Ten tvoří základ domény. Poté se mohou v libovolném pořadí spustit virtualizace V5-7, servery SQL3, vstor1 a 2, IPsvc pro zaměstnance i laboratoře a úložiště vstor1 a vstor2. Veškeré spouštění probíhá ručně, stejně jako u serveru FDC3. Nyní by měla být celá skupina s prioritou 1 plně funkční.

Pokud bude zjištěn problém při kontrole serverovny nebo při spouštění jakéhokoliv zařízení, je potřeba neprodleně kontaktovat příslušnou osobu nebo firmu, která je k danému aktivu vázána v seznamu kontaktů. Například pokud bude poničena klimatizace, dochází k přechodu na DR plán pro podpůrnou infrastrukturu a tím pádem ke kontaktování příslušné servisní společnosti, která je smluvně zavázána zařízení

opravit. Stejně se musí postupovat u jakéhokoliv zařízení v serverovně, pokud ho není schopen zprovoznit DR tým sám.

Souhrnný postup pro obnovu skupiny je uveden v přílohách práce, stejně jako seznam důležitých kontaktů. Nutností je zapsání každého bezpečnostního incidentu do AAR formuláře, který je popsán dále v práci a jeho vzor je uveden taktéž v přílohách.

3.4.3 DR plán pro servery s prioritou 2

Skupina se týká vesměs serverů, na kterých běží základní služby poskytované zaměstnancům a studentům školy. U této skupiny aktiv s prioritou 2 je stanovena max. doba obnovy na 24 hodin. To znamená, že servery mohou být nedostupné maximálně 24 hodin od nahlášení jejich poruchy.

Po zjištění nebo nahlášení poruchy je nejdříve nutné zjistit skutečný stav daného serveru neboli provést ověření. Pokud je server opravdu nedostupný, přistoupí se k opravě. Pokud tuto opravu není schopen DR tým provést, musí dojít ke kontaktování příslušných osob k daným serverům či úložištím. Jak už bylo zmíněno, tyto kontakty jsou uvedeny v seznamu důležitých kontaktů. Po úspěšné opravě je nutné provést kontrolu funkčnosti. Jedná se o test, za účelem zjištění, zda server opravdu funguje tak jak má. Tento test provádí DR tým. Dalším krokem je oznámení o funkčnosti serveru tomu, kdo nahlásil jeho poruchu. Nedílnou součástí je opět zapsání události do AAR. V případě zjištění jakéhokoliv jiného problému v serverovně musí být okamžitě přistoupeno k příslušnému DR plánu.

3.4.4 DR plán pro servery s prioritou 3

Tato skupina zaštiťuje převážně servery poskytující prostor pro služby určené pro výuku. Limit pro obnovu chodu těchto serverů je určen na 48 hodin od zjištění poruchy. Postup probíhá velmi podobně jako u skupiny s prioritou 2. Po nahlášení nedostupnosti serveru dojde k ověření jeho stavu. Pokud kontrola výpadek potvrdí, dochází k opravě DR týmem, nebo kontaktování příslušných osob, dle daného serveru. Nejdříve se DR tým pokusí zapnout servery na dálku, pokud tak nelze učinit, je nutný fyzický zásah v serverovně. Po opravě následuje kontrola funkčnosti serveru a dále ohlášení

o zprovoznění osobě, která výpadek nahlásila. Opět nesmí chybět zápis události do AAR a při zjištění jiných problémů je samozřejmostí aktivace příslušného DR plánu.

3.4.5 DR plán pro servery s prioritou 4

Při výskytu problému ve skupině serverů s prioritou 4 není nikterak ovlivněna skupina zaměstnanců ani studentů. Tento incident pozorují pouze IT pracovníci. Z toho důvodu je doba obnovy problému stanovena na 5 pracovních dní, tedy 120 hodin od zjištění problému.

Postup je opět velmi podobný předchozím dvěma skupinám. Po zjištění problému se DR tým pokusí danou chybu opravit. Pokud tak nelze učinit, musí kontaktovat příslušné orgány. Po opravení dochází ke kontrole serveru a následuje zápis do ARR. Při zjištění jiných problémů se musí postupovat podle příslušného DR plánu.

3.4.6 DR plán pro podpůrnou infrastrukturu

Podpůrná infrastruktura je klíčem k chodu celého systému. Pokud nefunguje záložní zdroj UPS, nebo chladicí jednotky, nemůžou běžet ani servery a tím pádem ani služby.

V případě zjištění poruchy některého z těchto výše zmíněných prvků podpůrné infrastruktury je nutná jeho oprava do 12 hodin od zjištění. Před přikročením k opravě je nutné opět zkontrolovat bezpečnost perimetru serverovny a zjistit, zda nejsou poškozena i další zařízení. Pokud opravu není schopen zajistit samotný DR tým, je nutné kontaktovat servisní služby. V případě nefunkčních klimatizačních jednotek je nutné omezit počet běžících serverů tak, aby nedošlo k celkovému přehřátí. Zde se doporučuje ponechat funkční pouze skupinu serverů s prioritou 1. Pokud je zjištěna porucha jednotky UPS, je doporučeno vypnout veškeré servery, neboť by mohlo při výpadku dodávky elektrické energie dojít k jejich nenávratnému poškození. Po znovuzprovoznění podpůrné infrastruktury probíhá kontrola funkčnosti veškerých serverů a kontrola dostupnosti služeb. Pokud byly servery vypnuty, je nutné při jejich zprovozňování postupovat dle daných postupů. Na samý závěr nesmí chybět zaznamenání celého bezpečnostního incidentu do AAR.

3.4.7 DR plán pro služby s prioritou 1

V případě, že je zjištěna nebo nahlášena nedostupnost některé ze služeb s prioritou 1 je nejdříve nutné dostupnost služby vzdáleně ověřit. Pokud je služba opravdu nedostupná, je nutné ji zprovoznit do 12 hodin od zjištění problému. Je potřeba kontaktovat možné uživatele služby a informovat je o její nedostupnosti. DR tým podstupuje kroky nutné k obnovení služby. V DR plánu jsou vždy uvedeny servery a úložiště, na kterých daná služba závisí. Pokud tedy službu nelze zprovoznit, lze hledat příčinu problému u zmíněných serverů nebo úložišť. Dochází tak k přechodu na DR plán, který se zabývá daným serverem či úložištěm. Po vyřešení problému a obnově služby je opět potřebná kontrola dostupnosti služby. Poté dochází k oznámení znovuzprovoznění dané služby tomu, kdo chybu nahlásil i skupině uživatelů, kteří službu užívají. Posledním krokem je zápis do ARR.

3.4.8 DR plán pro služby s prioritou 2

Služby s prioritou 2 nejsou pro výuku tak důležité, proto je čas na jejich opravu stanoven na 48 hodin. Kroky v plánu obnovy při katastrofě jsou téměř shodné jako u skupiny služeb s prioritou 1. Po nahlášení nebo zjištění nedostupnosti je daná služba a její dostupnost ověřena. Je vhodné oznámit nedostupnost služby jejím uživatelům. Pokud nelze službu spustit, musí se DR tým zaměřit na servery a úložiště, na kterých služba běží. Dochází k aktivaci DR plánu, jehož jsou dané servery, případně úložiště součástí. Po zprovoznění služby je opět nutné službu ověřit a až poté se může přistoupit k oznámení zprovoznění služby. Samozřejmostí je zápis do reportů bezpečnostních incidentů AAR.

3.4.9 DR plán pro služby s prioritou 3

Mezi služby s prioritou 3 patří pouze dvě služby. Jsou jimi služba Aris, která slouží k výuce, ale momentálně je nevyužita, a terminálové služby. Protože tyto služby nejsou nikterak důležité pro výuku nebo chod systému, byl čas na jejich obnovu stanoven na 168 hodin.

DR plán pro tuto skupinu má totožnou podobu jako plán pro skupinu služeb s prioritou 2. Liší se jen požadovaná doba obnovy. I zde, jako u každého DR plánu pro služby, je uvedena tabulka se servery a úložišti, na kterých služby běží. Jednotlivé kroky plánu obnovy jsou uvedeny v přiloženém DR plánu.

3.4.10 DR plán pro služby s prioritou 4

Jelikož služby spadající do této skupiny slouží výhradně zaměstnancům IT Ústavu informatiky při FP a nemají vliv na průběh výuky, či chod školní počítačové sítě, byla maximální doba pro obnovení těchto služeb stanovena na 336 hodin, tedy dva týdny.

Plán pro obnovu je i v tomto případě shodný s přechozími plány obnovy pro služby. I když se jedná o nejnižší prioritu, je nutné dodržovat stanovené postupy, které jsou uvedeny v příloze.

3.4.11 DR plán v případě úniku vody

Pokud je zjištěn výskyt vody v serverovně, nebo patrný průsak z vyššího patra budovy, je nutné neprodleně vypnout serverovnu nouzovým tlačítkem na zdi. Poté je potřeba zajistit, aby se voda nedostala k serverům, nebo jiným elektronickým zařízením. V opačném případě by mohlo dojít k nenávratnému poškození. Samozřejmostí je i nalezení zdroje úniku vody a uzavření hlavního uzávěru k tomuto zdroji. Nyní je vhodné informovat uživatele systému o jeho nedostupnosti. Po opravě vodovodní havárie, která by měla být hotova nejpozději do 48 hodin, je nutné zkontrolovat serverovnu. Musí být zajištěno precizní vysušení celé místnosti. Pokud se zjistí, že voda zatekla do některého ze zařízení, je nezbytné kontaktovat servisní oddělení příslušného aktiva pro jeho opravu. V případě, že aktivum nelze opravit, je nutné pořídit aktivum nové. Až v okamžiku, kdy je serverovna kompletně vysušena a zbavena vody, je možné opětovné spuštění systémů. Po spuštění následuje celková kontrola serverů, úložišť a služeb a až poté je možné oznámit opětovnou dostupnost služeb. Celý postup musí být samozřejmě zaznamenán do AAR, tak jako u všech bezpečnostních incidentů.

3.4.12 DR plán v případě požáru

V případě požáru dochází k ohrožení i lidských životů. Proto je na prvním místě nahlášení požáru a následná evakuace budovy. Pokud to však situace dovoluje a požár je minimální, nebo v jiné části budovy, pokusí se přítomný pracovník Ústavu informatiky o nouzové vypnutí serverovny červeným tlačítkem. Při odchodu ze serverovny zavře dveře, aby zabránil rychlému vniknutí požáru. Po opuštění budovy je pracovník povinen zavolat na požární tísňovou linku a požár ohlásit. Opravy serverovny probíhají dle závažnosti požáru a poničení aktiv, místnosti a případně celé budovy. Samozřejmostí je snaha o co nejrychlejší znovuzprovoznění celého systému. Je důležité zmínit, že tento DR plán podléhá univerzitní požární směrnici.

3.5 AAR

Součástí této práce je i tzv. *„After-action Report“*, který je zmíněn u každého z DR plánu. Jedná se o dokument, do kterého se zaznamenávají provedené bezpečnostní testy či bezpečnostní incidenty. Dokument je tvořen šablonou, která se nachází v příloze. Tento dokument je nezbytnou součástí DR plánu a slouží k pozdějšímu vyhodnocení testu nebo bezpečnostního incidentu. Lze vyvodit, kdy DR tým postupoval dobře, a kdy naopak udělal nějakou chybu. Těmto chybám se v budoucnu může díky AAR krizový tým vyvarovat.

Hlavičku dokumentu tvoří název organizace, číslo a den aktuální revize DR plánu, popis testu či bezpečnostního incidentu, datum začátku a konce testu či bezpečnostního incidentu. Dále je uveden seznam všech položek určených k vyplnění.

První položkou je důvod a zaměření AAR, kde musí být uvedeno, proč vůbec k zápisu do dokumentu došlo. Další pole je pro určení, čeho se daný test nebo incident týkal (například servery nebo infrastruktura). Třetí položkou je popis incidentu nebo testu. Zde je potřeba zhruba popsat, co se vlastně dělo. Následující pole popisuje cíle testu nebo následky incidentu. Následují tabulky. Tabulka pod číslem 5 slouží pro identifikaci použitých dokumentů. Může se jednat o smlouvy, směrnice, seznam kontaktů, nebo DR plán, dle kterého se postupovalo. Další tabulka obsahuje pole pro vyplnění osob, které se testu nebo řešení incidentu účastnili. Musí obsahovat také jejich pozice a za co jsou dané osoby zodpovědné. Následuje položka pro uvedení zaměstnanců, kteří vyplňují tento dokument. Měly by zde být uvedeny jejich kontakty, role a osobní posudek testu nebo bezpečnostního incidentu. Předposlední pole, tabulka č. 8, slouží pro sdělení jednotlivých nálezů a závěrů. U této položky musí být vždy prvně uveden objekt nebo oblast, které se zjištění týká. Dále uvedení zdroje, kde je detailnější popis nálezu nebo problému. Následuje popis nápravy nebo řešení. Nesmí chybět pověřená osoba, která je zodpovědná za danou opravu nebo její dokončení a je zde i pole pro případné poznámky. Na závěr je potřeba uvést krátkou sumarizaci provedeného testu nebo prodělaného bezpečnostního incidentu. Měl by zde být krátce shrnut celý incident, jeho následky, zjištění a kroky nutné k nápravě.

4 PŘÍNOSY PRÁCE A DOPORUČENÍ

V této kapitole jsou popsány přínosy práce pro Ústav informatiky, ale i různá doporučení a opatření, které mohou pomoci k větší bezpečnosti serverovny Ústavu informatiky. Doporučení vyplývají z analýzy serverovny, kde bylo zjištěno několik nedostatků.

4.1 Doporučení

Během zpracování této práce bylo zjištěno několik nedostatků, které mohou ohrožovat chod serverovny. Některé vyplynuly z analytické části práce, na jiné upozornili zaměstnanci Ústavu informatiky. Asi největším nedostatkem je absence ISMS. Tato certifikace je v dnešní době na univerzitní půdě téměř samozřejmostí, zde se s ní však nesetkáme. Doporučení, jak tyto nedostatky napravit, je popsáno na následujících stránkách.

4.1.1 Zavedení ISMS

Asi největším nedostatkem je absence ISMS. Definování chráněných aktiv, řízení rizik a jejich opatření je nutností a tomuto problému by se Ústav měl v co nebližší době věnovat. Při případné implementaci ISMS lze vycházet částečně i z této diplomové práce, kde je provedena potřebná analýza aktiv.

4.1.2 Cloudové úložiště

Jediná data, která jsou zálohována, jsou data zaměstnanců školy. Tato zálohovaná data jsou navíc uložena ve stejné místnosti a stejném datovém stojanu, jako data originální. Z toho důvodu může nastat situace, kdy budou oba nosiče poškozeny zároveň a dojde ke kompletní ztrátě dat.

Na místě je tedy řešení tohoto problému fyzickým rozdělením těchto úložišť, kdy by se jedno z nich mělo nacházet v jiné místnosti (nejlépe v jiné budově) než to druhé. Dalším řešením je pořízení externí služby cloudového úložiště. Cena za cloudové uložiště se

pohybuje od 15 000 Kč do 50 000 Kč v závislosti na požadované kapacitě. Tuto službu lze využít i k zálohování dalších dat, nebo konfigurací, kde by však cena služby znatelně vzrostla. Nicméně jsou data zálohována tímto způsobem chráněna před veškerými hrozbami a lze je kdykoliv obnovit.

4.1.3 Plán záloh

Tato kapitola úzce souvisí s kapitolou uvedenou výše. Jak již bylo zmíněno, v serverovně dochází k zálohování pouze dat zaměstnanců. Bylo by vhodné rozsah záloh rozšířit a vytvořit potřebný plán záloh, který v organizaci chybí. Plán záloh by měl obsahovat informace o tom, co zálohovat, kdy zálohovat a kam zálohovat.

U plánu záloh je nutné stanovit i dobu obnovy záloh – tedy za jak dlouhou dobu lze zálohy obnovit. Nutností je i pravidelné testování čitelnosti záloh – tedy zda lze vůbec zálohy obnovit.

4.1.4 Dieselový generátor

V serverovně se sice nachází záložní zdroj elektrické energie UPS, ale ten udrží serverovnu při chodu pouze 1 hodinu. Z tohoto důvodu je více než vhodné zřídit na Fakultě podnikatelské dieselový nebo jiný generátor, který by poskytoval zdroj energie i za delšího výpadku. Tento generátor lze využít i pro další serverovny, které se na fakultě nachází.

4.1.5 Dohoda o úrovni poskytovaných služeb

Při zpracování diplomové práce bylo zjištěno, že Ústav informatiky nemá uzavřen žádný *„Service-level agreement“*, dále jen SLA. SLA je smlouva mezi uživatelem služby nebo techniky a jejím poskytovatelem, která může zajišťovat např. včasný servis aktiva, nebo jeho náhradu. Doporučuje se uzavřít SLA pro veškeré servery a úložiště. To může být ale finančně velmi náročné, a proto je vhodné uzavřít SLA alespoň pro chladicí jednotky a záložní zdroj elektrické energie UPS, bez kterých servery nemohou

správně fungovat. Tato smlouva by měla zajišťovat okamžitý servis, minimální délku opravy a případnou výměnu zařízení. (30)

4.1.6 Vyšší počet zaměstnanců

Jak již bylo v práci zmíněno, serverovnu spravují 2 lidé. Jeden z nich na plný úvazek, druhý na třetinový. To znamená, že více jak 60 % pracovní doby je k dispozici pro správu serverovny pouze jeden kvalifikovaný zaměstnanec. V případě jakéhokoli většího incidentu to může mít obrovský dopad na konečné následky. A netýká se to jen incidentů. Ke správě serverovny je potřeba více zaměstnanců obecně. Z těchto důvodů by bylo nejlepší přijmout alespoň jednoho dalšího zaměstnance na plný úvazek.

4.1.7 Další doporučení

Mezi další doporučení, které pomůže v prevenci proti bezpečnostním incidentům nebo v případě jejích řešení je zavedení tzv. *„Knowledge Base“*. Jedná se o dokument, kde jsou zaznamenány různé postupy a znalosti, které mohou být využity v případě výskytu problému. Do tohoto dokumentu by měly být zaznamenávány veškeré osvědčené postupy, které byly využity v případě řešení bezpečnostních incidentů týkajících se serverovny Ústavu informatiky. Tzv. kniha znalostí může vycházet i z reportů zachycených v ARR a měl by ji znát každý člen DR týmu, ale i řadový zaměstnanec Ústavu informatiky pracující v perimetru serverovny.

Posledním doporučením je auditování přihlašovaní do administrativního serveru. Díky tomu bude zřejmé, kdo se do admin serveru přihlásil, a kdo jaké změny provedl. Lze tak snadněji vyvodit důsledky případného vzniklého problému. V dnešní době by měl být auditing logů součástí každé serverovny.

4.2 Přínosy práce

Tato diplomová práce přináší kompletní plán obnovy pro serverovnu Ústavu informatiky na fakultě podnikatelské při VUT v Brně. DR plán je nezbytnou součástí ISMS, které by mělo být na fakultě zavedeno. DR plán je uveden v příloze, a jelikož byl

po celou dobu zpracování diplomové práce konzultován s odborníky z oboru IT bezpečnosti a zaměstnanci Ústavu informatiky, je připraven k okamžitému využití. V případě, že se jim bude ústav řídit, může být zabráněno obrovským škodám, které by v jiném případě mohly nastat. To se netýká jen fyzických škod, ale i škod způsobených nuceným přerušení výuky. K tomuto přerušení výuky by v případě nefunkčnosti serverovny z velké míry došlo. O to větší je přínos této práce v době, kdy převážná část výuky probíhá online a služby serverovny jsou tak důležitější než kdy jindy.

Díku tomu, že byl DR plán zpracován jako diplomová práce, nebylo nutné ho nechat zpracovat zaměstnanci ústavu nebo externí firmou. Zaměstnanci jsou už tak pracovně velmi vytížení a jen těžko by tuto časově náročnou práci vtěsnali do svých rozvrhů. Na druhé straně zpracování externí firmou obnáší veliké finanční náklady, které byly díky této práci ušetřeny. To je podrobněji rozebráno v části ekonomického zhodnocení.

Tato práce dále poslouží jako podklad pro budoucí zpracování řízení kontinuity činností pro Ústav informatiky. Začátek tvorby tohoto dokumentu je plánován na září roku 2021 a dokončení má proběhnout v květnu 2022. BCM bude plynule navazovat na tuto diplomovou práci a očekává se také velký přínos pro celou fakultu. Zhotovitel BCM může čerpat z poznatků provedených analýz a využít samotný DR plán.

Samotné provedení této diplomové práce může sloužit jako metodika při zpracování plánů obnovy pro jiné subjekty, či firmy, které mají podobnou ICT architekturu. Veškeré kroky jsou provedeny dle stanovených norem a plán obnovy obsahuje všechny požadované náležitosti.

Kromě hlavního cíle práce, kterým bylo navrhnout plán obnovy při katastrofě pro Ústav informatiky, byla navrhnuta i šablona záznamového archu pro hlášení tzv. „*After Action Report*“. Tato velmi užitečná věc časem přináší spoustu ulehčení při řešení bezpečnostních incidentů. Jedná se totiž o záznam veškerých incidentů nebo testů a jejich následků nebo výsledků, které v dané serverovně nastaly, nebo byly provedeny. Při budoucích incidentech tak lze lehce z tohoto dokumentu čerpat a použít užitečné závěry z předchozích postupů.

4.3 Ekonomické zhodnocení

Ústav informatiky díky tomuto DR plánu může ušetřit nejen díky předejití obrovským škodám na aktivech serverovny a ztrátě dat, ale i na tvorbě nebo samotném provozu DR plánu externí firmou. Vytvořit DR plán externí firmou stojí nemalé finanční prostředky, které by případně musel ústav vynaložit. To stejné platí pro DR plán jako poskytovanou službu, kde se navíc platí měsíční poplatek za provoz této služby. Příkladové kalkulace pro oba případy jsou uvedeny v následujících podkapitolách.

4.3.1 Kalkulace tvorby DR plánu externí firmou

V tomto případě se jedná o službu, kdy externí firma poskytne své pracovníky, kteří jsou vysláni do společnosti, která si chce nechat zhotovit DR plán. Ti nejprve musí provést kompletní analýzu ICT, tak jako je provedena v této práci. Samozřejmostí je i analýza rizik, která už bývá mnohdy provedena v rámci ISMS. To ovšem v případě ICT serverovny Ústavu informatiky, jak již bylo uvedeno, není pravda. Zde prozatím ISMS zavedeno není.

Z výše uvedených informací lze složit přibližnou kalkulaci tvorby DR plánu. Přibližná hodnota mzdy u takovéto práce je 500 Kč/h. Odhadovaný čas analýzy je 20 pracovních dní, což dělá 160 hodin práce. Dále se musí připočíst čas strávený tvorbou samotného DR plánu. Odhadovaná doba této činnosti je 10 dní, tedy 80 hodin. Další položkou je částka za samotné zprostředkování DR plánu, která se pohybuje kolem 20 000 Kč. Po kalkulaci vyhází celková částka na 140 000 Kč. I přesto, že se jedná o hrubý odhad lze říct, že Ústav informatiky tuto částku v případě aplikování DR plánu, který obsahuje tato diplomová práce, ušetří 140 000 Kč.

4.3.2 Kalkulace DR plánu jako služby

DR plán jako služba neboli zkráceně DRaaS z anglického *„Disaster Recovery as a Service“*, poskytuje oproti předchozímu řešení nepřetržitý servis externí firmy. V kalkulaci tedy lze počítat se základem ceny předchozí služby, a navíc se musí přičíst měsíční náklady za samotnou službu DRaaS. Zde probíhá kalkulace podle počtu serverů

a velikosti serverů, které mají být v případě katastrofy obnoveny. Ceny se v tomto oboru velmi liší, ale vesměs se jedná o celkem vysoké sumy. Například při kalkulaci pro Ústav informatiky bylo počítáno jen se servery s prioritou 1. Jedná se o 7 fyzických serverů a úložišť a 1 virtualizaci. Při zadání parametrů serverů se průměrná cena za DRaaS pohybovala okolo 15 000 Kč měsíčně. To znamená, že v případě tohoto řešení by Ústav informatiky musel zaplatit přibližně 140 000 Kč za zhotovení analýzy a tvorbu DR plánu a dále by musel platit 180 000 Kč ročně za DRaaS.

Samozřejmě tyto služby jsou primárně poskytovány pro aktiva patřící do kritické infrastruktury a lze je různě kombinovat. Může to např. vypadat tak, že DR plán pro kritické servery a aplikace spravuje externí firma a ostatní aktiva zůstávají pod správou IT oddělení společnosti. Je nutné zmínit, že se jedná o velmi nákladné služby, ale na druhou stranu jsou poté aktiva chráněna tím nejlepším možným způsobem, a data lze obnovit i při kompletní fyzické destrukci serverovny.

ZÁVĚR

Hlavním cílem této diplomové práce bylo navrhnout plán obnovy v případě katastrofy pro serverovnu Ústavu informatiky na Fakultě podnikatelské při VUT v Brně, který v případě bezpečnostních incidentů zajistí jistou kontinuitu chodu a rychlou obnovu celého zařízení. Navrhovaný DR plán splňuje stanovený hlavní cíl práce a plně se řídí danými normami řady ISO/IEC 27000, normou ISO/IEC 24762 a příslušnými vyhláškami.

V první části práce byla představena potřebná teoretická východiska objasňující problematiku informační bezpečnosti, a hlavně DR plánu samotného. Dále byly popsány normy ISO/IEC a vyhlášky, které se danou problematikou zabývají. Na základě těchto poznatků se přistoupilo k analytické části.

V analytické části byl zjištěn aktuální stav bezpečnostní stránky a proběhla analýza dané serverovny a jejich aktiv. Servery a služby byly pro účely tvorby DR plánu rozděleny do jednotlivých skupin dle priorit a byla provedena analýza rizik.

Samotný návrh DR plánu je řešen v třetí části této diplomové práce. Nejdříve byla definována oblast DR plánu, tedy čím se konktrétně tento DR plán zabývá. Dále bylo definováno sestavení DR týmu a seznam důležitých kontaktů. Hlavní částí této kapitoly jsou postupy v případě bezpečnostních incidentů pro jednotlivé prioritní skupiny serverů a služeb. Kromě těchto postupů jsou uvedeny i postupy při konkrétních událostech jako je požár, či průsak vody do serverovny. Kompletní DR plán určený pro okamžité nasazení na Ústav informatiky je uveden v přílohách práce.

Ve čtvrté části jsou uvedena doporučení, která vychází ze zjištěných nedostatků při analýze serverovny. Dále je uvedeno ekonomické zhodnocení a byla provedena srovnávací kalkulace různých možností implementace DR plánů.

Na závěr byly shrnuty veškeré přínosy této diplomové práce, kde hlavním přínosem je reálné využití DR plánu na Ústavu informatiky a implementování tak jednoho ze zásadních prvků informační bezpečnosti. Fakulta díky tomuto plánu obnovy ušetří nemalé finanční prostředky, a to jak díky jeho sestrojení a implementaci, ale i za případné vzniklé škody, které jsou tímto plánem ošetřeny. Nad rámec cíle práce byla sestrojena i šablona pro zaznamenávání reportů z proběhlých bezpečnostních incidentů, která je velkým přínosem při řešení budoucích problémů.

Tato diplomová práce poslouží jako podklad pro zpracování dokumentu o řízení kontinuity procesů na Ústavu informatiky a lze ji využít i jako metodiku pro tvorbu plánů obnovy při katastrofě v podobném prostředí.

SEZNAM POUŽITÝCH ZDROJŮ

(1) POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-86898-38-5.

(2) *ISO/IEC 2382:2015 Information technology — Vocabulary*. ISO/IEC JTC 1 Information technology, 2015, 4 s.

(3) KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, 2019. ISBN 978-80-88168-34-8.

(4) JORDÁN, Vilém a Viktor ONDRÁK. *Infrastruktura komunikačních systémů II: kritické aplikace*. Vydání první. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-80-214-5240-4.

(5) *IT SLOVNÍK.CZ* [online]. Praha, 2008 [cit. 2021-05-03]. Dostupné z: https://it-slovnik.cz/

(6) HILBERT, Martin a Priscila LÓPEZ. The World's Technological Capacity to Store, Communicate, and Compute Information. *Science* [online]. **332**(6025) [cit. 2021-05-03]. Dostupné z: doi:10.1126/science.1200970

(7) DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

(8) *ČSN EN ISO/IEC 27000: Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník*. 369790. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2020, 32 s.

(9) *Odborná podpora provozovatelů vodovodů při zpracování rizikové analýzy* [online]. Praha: Státní zdravotní ústav, 2017 [cit. 3.5.2021]. Dostupné z: http://www.ekomonitor.cz/sites/default/files/filepath/prezentace/02_odborna_podpora_praha_2017_fin..pdf

(10) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

(11) MOORE, John. What is BCDR? Business continuity and disaster recovery guide. *TechTarget* [online]. 2020 [cit. 2021-05-03]. Dostupné z: https://searchdisasterrecovery.techtarget.com/definition/Business-Continuity-and-Disaster-Recovery-BCDR?_gl=1*100zjk3*_ga*MzY2NTYxNzUzLjE2MTg0MTE2OTA.*_ga_RRBYR9CGB9*MTYyMDA1OTM5OS40LjEuMTYyMDA1OTQ5NS4w&_ga=2.229795550.392309938.1620059399-366561753.1618411690

(12) SZABADOS, Ľubomír. *Business continuity management: príručka manažéra = manager's handbook*. Bratislava: TATE International Slovakia, 2008. Príručka manažéra. ISBN 978-80-969747-2-6.

(13) Iso 22301 BCMS. *Eqaworld* [online]. Seoul, Korea: Digital-ro, 2000 [cit. 2021-05-04]. Dostupné z: https://www.eqaworld.com/html/iso/bcms.htm

(14) WONG, Jeremy. *The Resilient IT Infrastructure*. Bisci, 2013.

(15) PRESTON, W. Curtis. *Backup & Recovery*. Sebastopol: O'Reilly Media, 2006. ISBN 978-0-596-10246-3.

(16) KIRVAN, Paul. RPO vs. RTO: Understand the differences in backup metrics. *TechTarget* [online]. TechTarget, 2020 [cit. 2021-05-05]. Dostupné z: https://searchstorage.techtarget.com/feature/What-is-the-difference-between-RPO-and-RTO-from-a-backup-perspective

(17) SINGH, Jaspreet. Understanding RPO and RTO. *Druva* [online]. Druva Inc., 2015 [cit. 2021-05-05]. Dostupné z: https://www.druva.com/blog/understanding-rpo-and-rto/

(18) *Guide for Cybersecurity Event Recovery: NIST Special Publication 800-184*. NIST, 2016. Dostupné také z: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

(19) BERNSTEIN, Corinne. Disaster recovery team. *TechTarget* [online]. [cit. 2021-05-06]. Dostupné z: https://searchdisasterrecovery.techtarget.com/definition/disaster-recovery-team?_gl=1*10vr7zj*_ga*MzY2NTYxNzUzLjE2MTg0MTE2OTA.*_ga_RRBYR9CGB9*MTYyMDI4NTI2Ni4xMy4xLjE2MjAyODY3NTMuMA..&_ga=2.166907644.392309938.1620059399-366561753.1618411690

(20) KIRVAN, Paul a Sonia LELII. Free IT disaster recovery plan template and guide. *TechTarget* [online]. TechTarget [cit. 2021-05-06]. Dostupné z: https://searchdisasterrecovery.techtarget.com/feature/IT-disaster-recovery-DR-plan-template-A-free-download-and-guide?_gl=1*yd8vs7*_ga*MzY2NTYxNzUzLjE2MTg0MTE2OTA.*_ga_RRBYR9CGB9*MTYyMDMwMTQxNS4xNi4xLjE2MjAzMDE0NzEuMA..&_ga=2.242887616.392309938.1620059399-366561753.1618411690

(21) BETAN, Harwey a Paul CROCETTI. 10 steps for optimal IT disaster recovery plan design. *TechTarget* [online]. TechTarget [cit. 2021-05-06]. Dostupné z: https://searchdisasterrecovery.techtarget.com/tip/Ten-things-that-must-be-included-in-IT-disaster-recovery-plans

(22) EARLS, Alan R. After-action report template and guide for DR planning. *TechTarget* [online]. TechTarget [cit. 2021-05-06]. Dostupné z: https://searchdisasterrecovery.techtarget.com/tip/After-action-report-template-and-guide-for-DR-planning

(23) KIRSCH, Brian. 4 components of a disaster recovery plan to prepare for a crisis. *TechTarget* [online]. 2016 [cit. 2021-05-05]. Dostupné z: https://searchitoperations.techtarget.com/tip/4-components-of-a-disaster-recovery-plan-to-prepare-for-a-crisis

(24) DRaaS decisions: Key choices in disaster recovery as a service. *Computer Weekle* [online]. 2020, , 1-6 [cit. 2021-04-14]. Dostupné z: https://www.computerweekly.com/feature/DRaaS-decisions-Key-choices-in-disaster-recovery-as-a-service

(25) A disaster recovery testing strategy is key to successful DR. *TechTarget* [online]. [cit. 2021-05-05]. Dostupné z: https://searchdisasterrecovery.techtarget.com/tip/A-disaster-recovery-testing-strategy-is-key-to-successful-DR

(26) DRASTICH, Martin. *Systém managementu bezpečnosti informací*. 1. vyd. Praha: Grada, 2011. Průvodce (Grada). ISBN 978-80-247-4251-9.

(27) KIRVAN, Paul. ISO 22301:2019 vs. previous versions: What's changed?. *TechTarget* [online]. [cit. 2021-05-06]. Dostupné z: https://searchdisasterrecovery.techtarget.com/tip/ISO-223012019-vs-previous-versions-Whats-changed

(28) *ISO/IEC 24762: Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services*. Switzerland: ISO/IEC, 2008, 78 s.

(29) *Sbírka zákonů Česká republika: Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)*. Břeclav: Moraviapress, 2018, . ISSN 1211-1244.

(30) KIRVAN, Paul. Free service-level agreement template for DR plans. *TechTarget* [online]. [cit. 2021-05-07]. Dostupné z: https://searchdisasterrecovery.techtarget.com/Free-service-level-agreement-template-for-disaster-recovery-programs?_gl=1*1m6v20b*_ga*MzY2NTYxNzUzLjE2MTg0MTE2OTA.*_ga_RRBYR9CGB9*MTYyMDI4MTU2My4xMi4xLjE2MjAyODE2MDIuMA..&_ga=2.140774512.392309938.1620059399-366561753.1618411690

SEZNAM POUŽITÝCH OBRÁZKŮ

Obrázek 1: PDCA cyklus 17
Obrázek 2: Životní cyklus BCM 19
Obrázek 3: Plánování BCM 20
Obrázek 4: Časová osa RTO 22
Obrázek 5: Časová osa RPO 22
Obrázek 6: Půdorys serverovny 31
Obrázek 7: Kontinuita serverů a služeb 36
Obrázek 8: Samostatně fungující servery 36
Obrázek 9: Fyzické rozložení serverů 41
Obrázek 10: Kontinuita služeb 43

SEZNAM POUŽITÝCH TABULEK

Tabulka č.1: Tabulka pro ohodnocení hrozby....17
Tabulka č.2: Seznam fyzických aktiv....33
Tabulka č.3: Fyzické a virtuální servery....34
Tabulka č.4: Servery s prioritou 1....37
Tabulka č.5: Servery s prioritou 2....38
Tabulka č.6: Servery s prioritou 3....39
Tabulka č.7: Servery s prioritou 4....40
Tabulka č.8: Podpůrná infrastruktura....41
Tabulka č.9: Aktiva – služby....42
Tabulka č.10: Služby s prioritou 1....44
Tabulka č.11: Služby s prioritou 2....45
Tabulka č.12: Služby s prioritou 3....45
Tabulka č.13: Služby s prioritou 4....46
Tabulka č.14: Externí služby....46
Tabulka č.15: Úrovně zranitelností....48
Tabulka č.16: Úrovně hrozeb....48
Tabulka č.17: Zranitelnosti fyzických aktiv....49
Tabulka č.18: Hrozby fyzických aktiv....51
Tabulka č.19: Zranitelnosti služeb....53
Tabulka č.20: Hrozby služeb....54

SEZNAM POUŽITÝCH ZKRATEK

DR	Disaster Recovery
BCM	Bussiness Continuity Management
IT	Information Technology
ISMS	Informatic Security Management System
ICT	Information and Communication Technologies
DRaaS	Disaster Recovery as a Service
UPS	Uninterruptible Power Supply
RTO	Recovery Time Objective
RPO	Recovery Point Objective
AAR	After-action Report

SEZNAM PŘÍLOH

PŘÍLOHA Č.1 DR plán..... I

PŘÍLOHA Č.2 Šablona pro report bezpečnostního incidentu/testu (AAR)..... XVII

PŘÍLOHA Č.1 DR plán

Ústav informatiky

Fakulta podnikatelská

Vysoké učení technické v Brně

PLÁN OBNOVY V PŘÍPADĚ KATASROFY

DISASTER RECOVERY PLAN

Brno 2021

Obsah DR plánu

1. URČENÍ DR PLÁNU III
2. DR TÝM III
3. DŮLEŽITÉ KONTAKTY III
4. POSTUPY PŘI INCIDENTECH V

1. URČENÍ DR PLÁNU

Tento DR plán je určen pro serverovnu a poskytované služby Ústavem informatiky na Fakultě podnikatelské při VUT v Brně. Cílem tohoto DR plánu je správné řešení bezpečnostních incidentů a tím předejít větším škodám. Aktiva serverovny jsou rozdělena do několika skupin dle priorit důležitosti a pro každou skupinu je sestaven samostatný DR plán. Součástí plánu jsou i tabulky s důležitými kontakty a členy DR týmu.

K aktivaci DR plánu dochází, pokud tak rozhodne vedoucí DR týmu, nebo krizový manažer.

DR plán je nutné jednou ročně testovat i aktualizovat.

2. DR TÝM

Jméno	role	zodpovědnosti
	Vedoucí DR týmu	Schvalování (postupů, strategií, rozpočtu…)
	Krizový manažer	Dohled, řízení a koordinace DR týmu
	Specialista na monitoring IT služeb	Monitoring IT služeb (konzistence dat, integrace služeb, nastavení a konfigurace)
	Člen 1	Servery a úložiště
	Člen 2	Síťová infrastruktura
	Člen 3	

3. DŮLEŽITÉ KONTAKTY

Kontakty je nutné aktualizovat nejméně jednou za 6 měsíců.

Kontakty na DR tým

Jméno	Mobil	E-mail	Adresa

Kontakty na interní pracovníky

Název	Mobil/pevná linka	E-mail
Správce budovy		
Vrátnice		
Děkanát		
Vedoucí Ústavu informatiky		

Kontakty externích služeb

Název	Tel. číslo	E-mail/WWW
Hi-Tech services – Fujitsu	+420 543 234 017 +420 733 539 602	hts@hts.cz
Dell Pro Support	+420 225 308 649	
Servis chladicích jednotek	+420 543 210 162	info@daimond.cz
Servis jednotky UPS	+420 224 253 915	info@silekro.cz
Servis výrobků Synology		https://www.synology.com/cs-cz/support
Servis výrobků HP	+420 381 489 169	hpservis@vspdata.cz

Tísňová volání

Název	Telefonní číslo
Policie ČR	158
Záchranná služba	155
Hasičský záchranný sbor ČR	150
Městská policie	156
Jednotné evropské číslo tísňového volání	112

4. POSTUPY PŘI INCIDENTECH

V případě zjištění jakéhokoliv incidentu, který vyžaduje fyzický zásah v serverovně, musí nejdříve dojít k celkové bezpečnostní kontrole perimetru serverovny. Následující body musí být splněny:

- Není fyzicky poškozen vstup do serverovny, nejsou patrné jiné známky neoprávněného vniknutí do serverovny
- Serverovna má zajištěn přívod el. energie a záložní zdroj je plně funkční
- Není patrné fyzické poškození infrastruktury a jiných aktiv v serverovně
- Chladicí systém je plně funkční
- Nejsou patrné stopy požáru nebo vody

V případě zjištění jedné nebo více závad uvedených výše, je neprodleně nutné začít řešit její nápravu. Při známkách násilného vniknutí, poničení nebo odcizení serverů je nutné kontaktovat PČR a incident ohlásit.

Servery a úložiště s prioritou 1

SERVERY A ÚLOŽIŠTĚ S PRIORITOU 1		
Název serveru/ úložiště	**Výrobce**	**Služba**
fdc3 FYZ DNS	Fujitsu	DNS server
IPsvcSTD FYZ	virtualizace V5-7	DHCP + DNS laboratoře
IPsvcZAM FYZ	virtualizace V5-7	DHCP + DNS zaměstnanci
sql3 FYZ	Fujitsu	MSQL 2017, EA, Uranius, Witness server - virtualizační cluster
v5 FYZ blade	Fujitsu	virtualizace produkce v2018
v6 FYZ blade	Fujitsu	virtualizace produkce v2019
v7 FYZ blade	Fujitsu	virtualizace produkce v2020
vstor1 CM0	Fujitsu	tier 2 virtualizace
vstor2 CM0	Fujitsu	tier 1 virtualizace

V případě zjištění výpadku u skupiny serverů a úložišť s prioritou 1 je nutné postupovat následovně:

Maximální doba obnovy: 12 h

1. Ověření dostupnosti serverů
2. Kontrola perimetru serverovny
3. Ruční spuštění serveru fdc3
4. Ruční spuštění virtualizace V5-7, servery SQL3, vstor1 a 2, IPsvc pro zaměstnance i laboratoře a úložiště vstor1 a vstor2. V libovolném pořadí.
5. Kontrola funkčnosti
6. Zápis do AAR

Servery a úložiště s prioritou 2

SERVERY A ÚLOŽIŠTĚ S PRIORITOU 2		
Název serveru/ úložiště	**Výrobce**	**Služba**
admin1 FYZ	Fujitsu	administrace domény
kamery FYZ	HP	kamerový dohled
lic1	virtualizace V5-7	licenční server 1
lic2	virtualizace V5-7	licenční server 2
mail1 v4	virtualizace V4,8	poštovní server 1
mail2 v2018	virtualizace V4,8	poštovní server 2
print	virtualizace V5-7	tiskový server starý
print2	virtualizace V5-7	tiskový server nový
smtp1 v4	virtualizace V4,8	hraniční server Exchange
smtp2	virtualizace V4,8	hraniční server Exchange
v4 FYZ	Fujitsu	virtualizace mail1 a smtp1
v8 FYZ	Dell	virtualizace, Exchange plán, mail3 a smtp3
fbmfs3 via MGMT	Synology	home adresáře uživatelů
stor1	Synology	kamerové úložiště

V případě zjištění výpadku u skupiny serverů a úložišť s prioritou 2 je nutné postupovat následovně:

Maximální doba obnovy: 24 h

1. Ověření dostupnosti serverů
2. Zprovoznění serverů vzdáleným přístupem (pokud nelze, přikročí se na krok č. 3)
3. Kontrola perimetru serverovny
4. Oprava a zprovoznění serverů DR týmem (případné kontaktování příslušných servisních služeb)
5. Kontrola funkčnosti
6. Zápis do AAR

Servery a úložiště s prioritou 3

SERVERY A ÚLOŽIŠTĚ S PRIORITOU 3		
Název serveru/ úložiště	**Výrobce**	**Služba**
app1 V1	virtualizace V5-7	manažerský server, simulace Uranius
app2	virtualizace V5-7	stormware Pohoda
app3 V2	virtualizace V5-7	Orsystem
app4	virtualizace V5-7	Pharis
app5	virtualizace V5-7	Pharis optimalizátor, LINUX
aris	virtualizace V5-7	Aris BMP server na WS2016
plm 01	virtualizace V5-7	LAPROCO - produkční server
plm02	virtualizace V5-7	LAPROCO - testovací server
sql2	virtualizace V5-7	MSSQL 2017 výuka, Bizagi DB, WS2017
term1 FYZ	Fujitsu	terminálový server
fdc1 v2018	virtualizace V5-7	schema master, domain naming
fdc2 v2018	virtualizace V5-7	infrastructure master, synchronizace

V případě zjištění výpadku u skupiny serverů a úložišť s prioritou 2 je nutné postupovat následovně:

Maximální doba obnovy: 48 h

1. Ověření dostupnosti serverů
2. Zprovoznění serverů vzdáleným přístupem (pokud nelze, přikročí se na krok. č. 3)
3. Kontrola perimetru serverovny
4. Oprava a zprovoznění serverů DR týmem (případné kontaktování příslušných servisních služeb)
5. Kontrola funkčnosti
6. Zápis do AAR

Servery a úložiště s prioritou 4

SERVERY A ÚLOŽIŠTĚ S PRIORITOU 4		
Název serveru/ úložiště	**Výrobce**	**Služba**
conf FYZ	Fujitsu	konfigurační server
ca	virtualizace V5-7	certifikační server
monitw FYZ	Fujitsu	monitoring hardwaru + služeb
timer1	virtualizace V5-7	spouští naplánované skripty
fbmBackup	Synology	záloha home adresářů
itservis	Synology	úložiště pro instalace (IT podpora)
vbackup	virtualizace V5-7	záložní úložiště pro virtualizaci

V případě zjištění výpadku u skupiny serverů a úložišť s prioritou 2 je nutné postupovat následovně:

Maximální doba obnovy: 120 h

1. Ověření dostupnosti serverů
2. Zprovoznění serverů vzdáleným přístupem (pokud nelze, přikročí se na krok. č. 3)
3. Kontrola perimetru serverovny
4. Oprava a zprovoznění serverů DR týmem (případné kontaktování příslušných servisních služeb)
5. Kontrola funkčnosti
6. Zápis do AAR

Podpůrná infrastruktura

PODPŮRNÁ INFRASTRUKTURA		
Název aktiva	**Výrobce**	**Popis**
UPS	UPS Eaton	záložní zdroj, 8kVA, 3F, 1h zálohy
SW2	HP	podpůrný switch
SW61	HP	podpůrný switch
SW62	HP	spouští naplánované skripty
KVM	Aten	KVM switch pro management serverů
chladicí jednotky	Fujitsu	3 klimatizační jednotky
monitor		monitor, myš a klávesnice ke KVM

UPS (doba obnovy: 12 h)

V případě zjištění výpadku či poruše funkčnosti záložní jednotky napájení UPS je nutné postupovat následovně:

1. Ověření funkčnosti jednotky UPS, ověření možnosti servisního bypassu.
2. Kontrola perimetru serverovny
3. Vypnutí serverů a úložišť
4. Oprava a zprovoznění jednotky UPS (případné kontaktování příslušných servisních služeb)
5. Kontrola funkčnosti
6. Spuštění serverů a úložišť dle příslušných DR plánů
7. Zápis do AAR

Chladicí jednotky (doba obnovy: 12 h)

V případě zjištění výpadku či poruše funkčnosti chladicích jednotek je nutné postupovat následovně:

1. Ověření funkčnosti chladicích jednotek
2. Kontrola perimetru serverovny
3. Omezení chodu serverů a úložišť pouze na servery a úložiště s prioritou 1
4. Oprava a zprovoznění chladicích jednotek (případné kontaktování příslušných servisních služeb)
5. Kontrola funkčnosti
6. Spuštění serverů a úložišť zbylých priorit dle příslušných DR plánů
7. Zápis do AAR

Ostatní prvky podpůrné infrastruktury (doba obnovy: 12 h)

V případě zjištění výpadku či poruše funkčnosti ostatních prvků podpůrné infrastruktury je nutné postupovat následovně:

1. Ověření funkčnosti daného prvku
2. Kontrola perimetru serverovny
3. Oprava a zprovoznění příslušného prvku (případné kontaktování příslušných servisních služeb)
4. Kontrola funkčnosti
5. Zápis do AAR

Služby s prioritou 1

SLUŽBY S PRIORITOU 1	
Název sužby	**Příslušné servery a úložiště**
AD doména	FDC3, FDC1, FDC2
DHCP	IPsvcSTD + IPsvcZAM
DNS rekurzory	IPsvcSTD, IpsvcZAM
virtualizace V5-7	V5, V6, V7 (alespoň 2 musí fungovat) + VSTOR1 + VSTOR2
výuka-účetnictví	SQL3 + APP2 + LIC1
výuka-databáze	SQL2
výuka-manažerská simulace	APP1 + SQL3
výuka-OR systém	SQL3 + APP3
výuka-PLM	SQL3 + PLM01 + APP4 + APP5 + LIC3

V případě zjištění nedostupnosti či poruše funkčnosti některé ze služeb s prioritou 1 je nutné postupovat následovně:

Maximální doba obnovy: 12 h

1. Vzdálené ověření dostupnosti služby
2. Oprava a zprovoznění (pokud to nelze, a je zjištěna chyba u příslušných serverů, aktivuje se k nim příslušný DR plán)
3. Opětovné ověření dostupnosti služby
4. Ohlášení dostupnosti služby
5. Zápis do AAR

Služby s prioritou 2

SLUŽBY S PRIORITOU 2	
Název sužby	**Příslušné servery a úložiště**
administrace	ADMIN1
kamerový dohled	Kamery + stor1
virtualizace V4, V8	V4, náhrada V8, pouze pro poštovní služby
poštovní infrastruktura	(MAIL1, MAIL2) + (SMTP1, SMTP2) + SQL3
síťové tiskárny	PRINT2
home adresáře uživatelů	FBMFS3 + FBMbackup

V případě zjištění nedostupnosti či poruše funkčnosti některé ze služeb s prioritou 2 je nutné postupovat následovně:

Maximální doba obnovy: 48 h

1. Vzdálené ověření dostupnosti služby
2. Oprava a zprovoznění (pokud to nelze, a je zjištěna chyba u příslušných serverů, aktivuje se k nim příslušný DR plán)
3. Opětovné ověření dostupnosti služby
4. Ohlášení dostupnosti služby
5. Zápis do AAR

Služby s prioritou 3

SLUŽBY S PRIORITOU 3	
Název služby	**Příslušné servery a úložiště**
výuka-aris	ARIS
terminálové služby	TERM1 + LIC1

V případě zjištění nedostupnosti či poruše funkčnosti některé ze služeb s prioritou 3 je nutné postupovat následovně:

Maximální doba obnovy: 168 h

1. Vzdálené ověření dostupnosti služby
2. Oprava a zprovoznění (pokud to nelze, a je zjištěna chyba u příslušných serverů, aktivuje se k nim příslušný DR plán)
3. Opětovné ověření dostupnosti služby
4. Ohlášení dostupnosti služby
5. Zápis do AAR

Služby s prioritou 4

SLUŽBY S PRIORITOU 4	
Název sužby	**Příslušné servery a úložiště**
WSUS	CONF + ADMIN1 (Windows server update services)
certifikační autorita	CA
načasované skripty	TIMER1
instalační úložiště	ITSERVIS

V případě zjištění nedostupnosti či poruše funkčnosti některé ze služeb s prioritou 4 je nutné postupovat následovně:

Maximální doba obnovy: 336 h

1. Vzdálené ověření dostupnosti služby
2. Oprava a zprovoznění (pokud to nelze, a je zjištěna chyba u příslušných serverů, aktivuje se k nim příslušný DR plán)
3. Opětovné ověření dostupnosti služby
4. Ohlášení dostupnosti služby
5. Zápis do AAR

DR v případě požáru

V případě zjištění požáru je nutné řídit se vnitřní směrnicí Fakulty podnikatelské o požáru. Pokud to dané podmínky dovolují, pak je možné podniknout tyto kroky:

1. Vypnutí aktiv v serverovně nouzovým vypínačem
2. Zavolat na tísňovou linku, zavřít dveře od serverovny a opustit budovu
3. Po zpřístupnění budovy kontrola perimetru serverovny
4. Případná oprava poničené serverovny a oprava nebo pořízení aktiv
5. Spuštění serverů a úložišť
6. Kontrola funkčnosti
7. Zápis do AAR

DR v případě vniku vody do serverovny

V případě zjištění výskytu nebo průsaku vody do serverovny je nutné podniknout tyto kroky:

1. Vypnutí aktiv v serverovně nouzovým vypínačem
2. Zabezpečit aktiva před kontaktem s vodou
3. Vypnutí uzávěru vody, ze kterého dochází k úniku
4. Po opravě havárie zkontrolovat veškerá aktiva
5. Případná oprava poničené serverovny a oprava nebo pořízení aktiv
6. Spuštění serverů a úložišť
7. Kontrola funkčnosti
8. Zápis do AAR

PŘÍLOHA Č.2 Šablona pro report bezpečnostního incidentu/testu (AAR)

Report bezpečnostního incidentu/testu (AAR)

Název organizace: VUT Brno, FP, ÚIS

Číslo a datum poslední revize: _____

Datum a čas události: _____

Jednalo se o:

□ Test (popis testu): _____

□ Bezpečnostní incident (popis incidentu): _____

Obsah AAR

1 DŮVOD A ZAMĚŘENÍ AAR XIX
2 OBJEKTY ARR XIX
3 POPIS TESTU NEBO INCIDENTU XIX
4 DOPAD TESTU NEBO INCIDENTU XIX
5 SOUVISEJÍCÍ DOKUMENTY XIX
6 ÚČASTNÍCI TESTU NEBO INCIDENTU XX
7 ZHOTOVITELÉ AAR XX
8 ZJIŠTĚNÍ XXI
9 ZÁVĚR AAR XXI

1 DŮVOD A ZAMĚŘENÍ AAR

- stručný popis, čeho se AAR týká (test nebo bezpečnostní incident)

2 OBJEKTY ARR

- stručný popis, jaké objekty test nebo bezpečnostní incident zasáhl (např. server, služba nebo infrastruktura)

3 POPIS TESTU NEBO INCIDENTU

- stručný popis, o jaký bezpečnostní incident šlo nebo popis postupu při testování

4 DOPAD TESTU NEBO INCIDENTU

- stručný popis, co daný bezpečnostní incident způsobil nebo jakých výsledků mělo být při testu dosaženo a zda jich dosaženo bylo

5 SOUVISEJÍCÍ DOKUMENTY

- tabulka může obsahovat různé smlouvy, předpisy, či směrnice týkající se incidentu nebo testu

Název dokumentu	**Odkaz na dokument (URL**	**Dopady incidentu**	**Upřesnění části dokumentu**	**Poznámky**

6 ÚČASTNÍCI TESTU NEBO INCIDENTU

- seznam osob, které se na testu nebo incidentu podíleli. Obsahuje i určení jejich rolí a zodpovědností

Jméno a kontaktní informace	**Role**	**Zodpovědnost**

7 ZHOTOVITELÉ AAR

- seznam osob, které zhotovují tento ARR a jejich posudek testu nebo incidentu. Může obsahovat i nadřízené osoby

Jméno a kontaktní informace	**Role**	**Posudek**

8 ZJIŠTĚNÍ

- co se při testu nebo incidentu zjistilo a případné kroky k nápravě problému

Definování objektu zjištění/problému	**Reference nebo zdroj informací o problému**	**Doporučená opatření k nápravě**	**Osoba odpovědná za nápravu**	**Poznámky**

9 ZÁVĚR AAR

- sumarizace testu nebo bezpečnostního incidentu (Čeho se test týkal, jakých bylo dosaženo výsledků a jak mohou být aplikovány. Čeho se týkal bezpečnostní incident, k jakým škodám došlo a jak mají být škody napraveny.)