UNIVERZITA JANA AMOSE KOMENSKÉHO

Magisterské kombinované studium

2012 – 2014

DIPLOMOVÁ PRÁCE

Marta Gollová

Budování firemní kultury prostřednictvím vybraných bezpečnostních a IT procesů

Praha 2014

Vedoucí diplomové práce: PhDr. Jan Mattioli, Ph.D.

JAN AMOS KOMENSKY UNIVERSITY PRAGUE

Master Combined Studies

2012 – 2014

DIPLOMA THESIS

Marta Gollová

Building a corporate culture through selected security and IT processes

Prague 2014

The Diploma Thesis Work Supervisor: PhDr. Jan Mattioli, Ph.D.

Prohlášení

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

Souhlasím s prezenčním zpřístupněním své práce v univerzitní knihovně.

V Praze dne 1.1.2014 Marta Gollová

Poděkování

Chtěla bych poděkovat svému vedoucímu diplomové práce panu Doc. PhDr. Jiřímu Víškovi CSc., in memoriam, za odborné vedení, pomoc a cenné rady při zpracování této práce, které mi poskytoval do září roku 2013.

Dále bych chtěla poděkovat svému vedoucímu diplomové práce panu PhDr. Janu Mattiolimu Ph.D. a paní PhDr. Tereze Vacínové Ph.D. za jejich vstřícnost, pomoc a cenné rady při dokončení této diplomové práce.

Autorská anotace:

Tato diplomová práce poskytuje obecný rámec a definuje základní procesy systému řízení IT služeb z pohledu jejich efektivity a spokojenosti zaměstnanců společnosti People & Job, s.r.o.

Dále se tato práce zabývá implementací nástroje na ochranu citlivých dat, tj. Data Loss Prevention (DLP). Tento nástroj pomáhá zaměstnancům snadněji identifikovat citlivé informace společnosti.

Implementace IT procesů a technologie DLP vhodným způsobem podporuje budování firemní kultury společnosti People & Job, s.r.o.

Klíčové pojmy:

Data Loss Prevention, Change Management, Firemní kultura, Incident Management, Problem Management.

Annotation:

This thesis provides a general framework and defines the basic processes for an IT services management system from the perspective of its effectiveness and satisfaction of the employees of the company People & Job, s.r.o.

In addition, this paper deals with the implementation of the instruments for the protection of sensitive data, i.e. Data Loss Prevention (DLP). This tool helps employees to easily identify the more sensitive information of the company.

Implementation of these IT processes and of DLP in a suitable manner supports the building of the corporate culture of People & Job, s.r.o.

Key words:

Corporate Culture, Data Loss Prevention, Change Management, Incident Management, Problem Management.

OBSAH

ÚVOD

IT služby jsou v dnešní době integrální součástí fungování téměř každé společnosti.

Většina oborů je závislá na informacích pohybujících se ve virtuálním světě.

Společnost People & Job, s.r.o. se zaměřuje na psychologické a personální poradenství a je plně závislá na fungování IT prostředků a informačních systémů. Základním kamenem „výrobním prostředkem“ společnosti jsou informace o klientech společnosti a informace o lidech na trhu práce. Tyto informace dokáže tato společnost vhodně spojovat dohromady za účelem poskytování kvalitních služeb všem svým zákazníkům.

Tato společnost je vlastníkem citlivých informací. V rámci bakalářské práce, na kterou autorka navazuje, byl v této společnosti zaveden systém informační bezpečnosti podle rodiny norem ISO/IEC 27xxx. Zavedením informační bezpečnosti se sice zvýšila bezpečnost informací z pohledu důvěrnosti, dostupnosti a integrity těchto informací, ale nezvýšila se kvalita poskytovaných IT služeb.

Z tohoto důvodu vznikla potřeba zaměřit se na oblast kvality poskytovaných IT služeb a jejím prostřednictvím přímo pečovat o uživatele/zaměstnance informačních systémů. Poskytováním kvalitních IT služeb by měl být zvýšen komfort uživatelů, kteří každodenně k výkonu své práce tyto služby potřebují. Aspekty, na které je třeba se zaměřit, jsou následující:

- jak rychle a efektivně jsou řešeny problémy zaměstnanců s používáním informačních systémů a informačních prostředků;
- jak jsou zaměstnanci informováni o průběhu řešení svých požadavků na IT služby.

Termín IT služby definuje odborná literatura ITIL V3 (Information Technology Infrastructure Library) z jejichž obecného, procesního rámce pro poskytování IT služeb je v této práci vycházeno.

Vhodným řešením pro zvýšení komfortu a spokojenosti uživatelů je zavedení procesu Incident Management, který pomáhá zajistit dostupnost IT služeb. Samostatný proces Incident Management by nebyl plně funkční a efektivní bez podpory dalších procesů a to zejména procesů Problem Management a Change Management. Podle statistik uváděných v odborné literatuře je 60% nedostupnosti IT služeb způsobeno chybně provedenou změnou. Pokud by tyto procesy nebyly zavedeny, kontrolovány a měřena jejich efektivita, fungovaly by více méně náhodně a tím by způsobovaly pro společnost nárůst obchodních rizik.

Další oblastí, na kterou je nutné se zaměřit je podpora informační bezpečnosti. Každý zaměstnanec společnosti je odpovědný za nakládání s citlivými informacemi, které jsou obsaženy v informačních systémech společnosti. Zaměstnanci jsou v oblasti informační bezpečnosti průběžně a důkladně školeni, ale tuto oblast je potřeba doplnit a podpořit nástrojem, který zajistí monitoring možného úniku citlivých informací. Vhodným řešení je implementace technologie DLP (Data Loss Prevention), která je schopna monitorovat únik citlivých informací, klasifikovaných v rámci bakalářské práce autorky. Implementací tohoto nástroje je možné restriktivně bránit úniku citlivých informací vně společnost.

Teoretická část práce se prolíná s praktickou částí práce. Procesy Incident, Problem, Change Management a technologie DLP, navržené v teoretické části, jsou již prakticky přizpůsobeny implementaci do prostředí společnosti People & Job, jak z pohledu jejich efektivity, tak spokojenosti uživatelů.

V kapitole 3 je věnována pozornost firemní kultuře, protože ani ve firmě, která zaměstnává odborníky v dané oblasti a zajišťuje špičkovou technologii, není zaručeno, že prováděné činnosti, implementované procesy a technologie přinesou očekávaný přínos, pokud není věnována pozornost komplexu faktorů utvářejících firemní kulturu. Podcenění firemní kultury může zmařit mnohé z dobře naplánovaných záměrů. Tato kapitola nepopisuje firemní kulturu obšírně a ve všech jejích souvislostech, jelikož by byl značně překročen rozsah této práce. Pozornost je zaměřena zejména směrem k managementu společnosti, na efektivní leadership, který v konečném důsledku ovlivňuje vnímání, myšlení a jednání zaměstnanců. Pokud management zahrne firemní kulturu do svých úvah, měla by se firemní kultura stát velmi účinným nástrojem řízení.

Cílem práce je úspěšná implementace procesů Incident, Problem, Change Management a technologie DLP do prostředí společnosti People & Job, s.r.o.

Implementace uvedených procesů by měla přispět ke snížení výpadků IT služeb a ke zvýšení spokojenosti zaměstnanců v této oblasti. Technologie DLP by měla zaměstnancům pomoci snadněji identifikovat klasifikované citlivé informace společnosti a připomínat jim, jak s těmito informacemi při své práci zacházet.

Implementace těchto procesů a technologie by měla vhodným způsobem podpořit budování firemní kultury společnosti.

1 DEFINICE PROCESŮ A VZTAH MEZI DEFINOVANÝMI PROCESY

Incident Management, Problem Management a Change Management jsou samostatné procesy, které spolu úzce souvisejí. Incident Management zajišťuje rychlou reakci na vzniklý incident a následnou obnovu služeb pro uživatele služeb, zatímco Problem Management identifikuje a odstraňuje příčiny problémů, pro které není známo standardní řešení. Na tyto dva procesy, Incident Management a Problem Management, dále navazuje proces Change Management a proces Configuration Management, které zajistí bezpečné nasazení změn řešící problémy do produkčního prostředí tak, aby uživatel, který je odběratelem služby, nebyl omezen výpadky informačních systémů.

Tato kapitola definuje následující interní procesy:

- Incident Management;
- Problem Management;
- Change Management.

1.1 Charakteristika a cíl procesu Incident Management

Incident Management služeb odpovídá za řízení životního cyklu incidentů vzniklých během provozu služeb, přičemž Incident Management svou činností slouží jako podpůrný prostředek pro zajištění větší spolehlivosti, dostupnosti služeb a minimalizaci nežádoucího dopadu na obchodní aktivity společnosti a zároveň i větší spokojenosti uživatelů.

Incident je definován jako neplánované přerušení dodávky IT služeb nebo jejich úrovně kvality včetně všech událostí, které mohou ovlivnit IT službu.[1]

Incident Management je proces pro řešení událostí a poruch. Globálním cílem procesu je zajistit hlavní a výhradní komunikační linku uživatele směrem k Service Desku a na výstupu plně zabezpečit spokojenost uživatele s výsledným řešením jeho Incidentu.

Klíčovými cíli procesu Incident Management jsou:[2]

- nejrychlejší možná obnova normálního provozu IT služeb;
- minimalizace důsledků výpadku IT služeb na provoz společnosti;
- snížení nákladů na IT podporu společnosti;
- udržování nejlepší možné dostupnosti a kvality IT služeb.

Proces dále zajišťuje co nejrychlejší realizaci servisních požadavků, které nemají povahu incidentu a to například:

- obecné dotazy ke službám;
- požadavek na uživatelskou podporu;
- požadavek na přidělení přístupu do infrastruktury;
- další specifické požadavky.

Normálním provozem IT služeb rozumíme dostupnost fungování služeb tak, jak jsou definovány parametry dostupnosti pro jednotlivé IT služby společnosti.

---

[1] Více o této problematice: ITIL. *Service Operation: What are services.* 1. published. London: UK by TSO, 2007, s. 11-12. ISBN: 978 0 11 331046 3

[2] Tamtéž.Více In: ITIL. *Service Operation: Purpose/goal/objective, Scope,* s. 46-47.

1.1.1 Kontext a rozsah procesu

Proces Incident Management musí pokrýt klíčové principy Incident Managementu:[3]

- všechny požadavky jdou výhradně na IT Service Desku a to různými komunikačními prostředky;
- všechny požadavky a aktivity uživatele směrem k Service Desku jsou logovány a stejně tak jsou logovány všechny aktivity Service Desku určené k řešení incidentu;
- historie incidentů jsou logovány tj. incidenty, problémy, známé chyby a změny;
- jsou dohodnuté způsoby komunikace s partnery, kteří nemají přístup do systému Incident Management;
- jsou definovaná pravidla vnitřní komunikace Service Desku v případě incidentu, který se týká více uživatelů, tzn. sdružování Incidentů;
- jsou definovány cíle interní úrovně služeb a pravidla eskalace s podpůrnými týmy společnosti.

Incident potenciálně narušuje běh IT služeb.

Incident Management je proces, který operuje v kontextu procesů Problem Management a Change Management a komunikuje s jejich rozhraními.

V následující tabulce číslo 1 je názorně toto rozhraní popsáno.

[3] Více o této problematice: ITTIL. *Service Operation: Value to business.* 1. published. London: UK by TSO, 2007, s. 47. ISBN: 978 0 11 331046 3

Tabulka 1: Rozhraní mezi procesy

Aktivita	Vstupy	Výstupy	Popis
Change Management	Klasifikovaný incident – požadavek na změnu	Vyřešený požadavek na změnu	Za incidenty nejsou považovány požadavky na nové IT služby, nebo na změny stávajících IT služeb (např. instalace, reinstalace či upgrade SW, HW, konfigurace síťového prostředí apod.) z toho plyne, že požadavek na změnu nesmí být zadán jako incident, ale jako požadavek na změnu. Pokud je k problému nalezeno řešení, které vyžaduje změnu, je implementace takového řešení považována za změnu. Uzavření změny znamená současně uzavření souvisejícího problému.
Problem Management	Informace o incidentech	Známá chyba	V případě, že nelze implementovat trvalé řešení incidentu, vzniká problém a jeho řešení přebírá proces Problem Management.

Zdroj: autorka práce (vytvořeno na základě principů vycházejících z odborné literatury ITIL)

1.1.2 Klasifikace Incidentů

Dopad incidentů na výkonnost uživatele, respektive společnosti, je determinován dle rozsahu následků způsobených výpadkem služby:[4]

1. **Priorita: Very Heavy Impact**

   Dopad, nebo potenciální dopad na uživatele: Klíčové obchodní procesy, nebo uživatelské služby jsou nefunkční. Služba má kritický vliv na běh společnosti, výkonnost uživatelů, přístupnost ke klíčovým pracovním nástrojům. Dopad na všechny jednotky / služby / uživatele.

   Příklady: Důležitý software, který má klíčovou roli v doručení služby. Integrita aplikace nebo systému. Dostupnost hardwaru, který je klíčový pro funkčnost služeb nejméně v jedné lokalitě, nebo obchodní linii. Nefunkční kritický LAN Server nebo Gateway, která ovlivňuje mnoho uživatelů.

   Čas na odpověď: 1 hodina

2. **Priorita: Heavy Impact**

   Dopad, nebo potenciální dopad na uživatele: Klíčové obchodní procesy jsou oslabeny, ale jsou dostupné. Více jak jeden uživatel, nebo obchodní oddělení jsou schopni daný/é proces/y zpracovat. Dopad na některé služby uživatele.

   Příklady: Software problém, ale nejedná se o kritický problém, např.: přístup do počítačové sítě. Software problém, který ovlivňuje kritický monitorovací systém např. Call Centrum. Software problém, který ovlivňuje nedostupnost k hlavním databázím.

   Čas na odpověď: 2 hodiny

[4] Více o této problematice ITIL. *Service Operation: Value to business*. 1. published. London: UK by TSO, 2007, s. 50. ISBN: 978 0 11 331046 3

3. **Priorita**: **Moderate Impact**

   Dopad, nebo potenciální dopad na uživatele: Mírný obchodní dopad. Obchodní procesy jsou možná poškozeny, ale klientské služby nejsou ovlivněny. Problém se dotýká jednoho, nebo několika zaměstnanců, jejichž produktivita práce se významným způsobem nesníží. Dopad na jednu službu / jednoho uživatele.

   Příklady: Problém se softwarem potřebným pro podporu systému. Nefunkční MS office. Problém s tiskárnou, který má dopad na skupinu uživatelů. Reset hesla tzn.: bude zasláno provizorní heslo a následně provedena změna hesla uživatelem.

   Čas na odpověď: 8 hodin

4. **Priorita: Small Impact**

   Dopad, nebo potenciální dopad na uživatele: Minimální obchodní dopad. Nepříjemný dopad, který ale uživatel může nahradit jiným řešením. Spíše nepříjemnost.

   Příklady: Drobné problémy, které ovlivňují pouze jedince či jednotlivé služby.

   Čas na odpověď: 24 hodin

Výše uvedené priority 1 až 4 kvantifikují míru pozornosti věnované incidentům, které mají různou úroveň dopadu na business funkci (odlišení priorit v rámci dopadu). Proces je definovaný v rámci Service Desku společnosti People & Job. Definice jednotlivých typů a stavů incidentů je definována u Service Desku společnosti People & Job.

1.1.3 Vstupy a výstupy v procesu Incident Management

Vstupy do procesu Incident Management jsou:

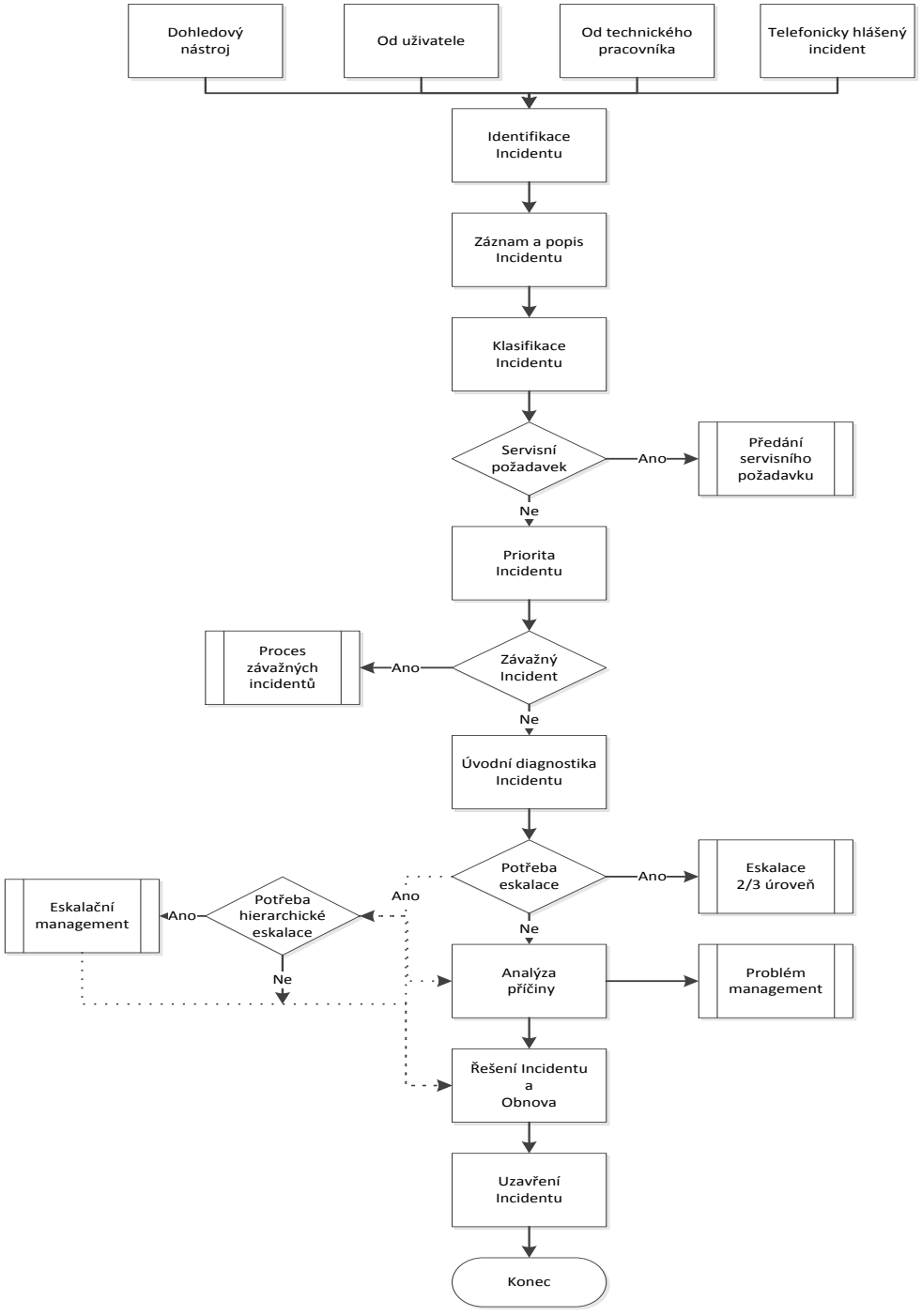
- incident zadaný uživatelem;
- incident zadaný technickým pracovníkem;
- incident identifikovaný dohledovým nástrojem;
- incident hlášený telefonem.

Výstupy z procesu Incident Management jsou:

- vyřešený a uzavřený incident, tedy implementováno trvalé řešení;
- problém řízený pomocí procesu Problem Management a následně uzavřený incident;
- požadavek na změnu řízený pomocí procesu Change Management a následně uzavřený incident.

Následující vývojový diagram číslo 1 přehledně zobrazuje proces Incident Management včetně vzájemných vazeb a souvislostí.

Diagram 1: Procesní tok Incident Management včetně vzájemných vazeb a souvislostí



Zdroj: ITIL. *Service Operation: Incident Models*, s. 48

Níže jsou popsány činnosti jednotlivých kroků, znázorněných v diagramu číslo 1.

Informace o jednotlivých aktivitách Incident Managementu.

1. **Aktivita**: Identifikace incidentu

   Vstup: Uživatel, nebo dohledový nástroj, nebo technický pracovník, nebo dodavatel detekoval incident

   Výstup: Identifikovaný incident

   Role: Service Desk

   Popis činnosti: Service Desk společnosti je jediné místo, kde uživatel hlásí incidenty prostřednictvím programu incidenty (prioritně program Incidenty, ve výjimečných případech telefon, e-mail). Uživatel je odpovědný za předání všech informací, které jsou nutné pro řešení incidentu. V rámci tohoto procesu jsou řešeny incidenty a servisní požadavky.

   V případě, že uživatel, nebo technický pracovník, nebo dodavatel detekuje incident, je povinen tuto skutečnost na Service Desk společnosti ohlásit.

2. **Aktivita:** Záznam a popis incidentu

   Vstup: Identifikovaný incident

   Výstup: Zaznamenaný incident

   Role: Service Desk

   Popis činností: Všechny incidenty musí být zaznamenány s uvedením data a času identifikace incidentu. Musí být zaznamenány všechny relevantní informace a okolnosti incidentu.

   Informace o incidentu jsou následující: Jednoznačné referenční číslo. Kategorie incidentu. Neodkladnost řešení incidentu. Dopad incidentu. Priorita incidentu. Datum a čas, do kterého má být incident vyřešen. Identifikace osoby, která incident nahlásila.

Způsob nahlášení incidentu (telefonem, automatickým systémem, e-mailem, osobně, atd.) Jméno, oddělení, kontaktní údaje o uživateli, který incident ohlásil. Metoda zpětné vazby pro uživatele (telefon, e-mail, osobně, atd.). Popis příznaků incidentu. Status incidentu (aktivní, čekající na vyřešení, uzavřený). Související informace o uživatelích. Osoby, kterým je řešení incidentu přiděleno. Související problémy a odkaz na známé chyby (uloženo v CMDB). Potřebné aktivity pro řešení incidentu. Datum a čas řešení Incidentu. Čas a datum uzavření incidentu. Zároveň se v tomto bodě vytváří vazba na související záznamy v CMDB (např. mateřský incident, nebo prvotní incident).

3. **Aktivita:** Klasifikace incidentu

   Vstup: Zaznamenaný incident

   Výstup: Klasifikovaný incident

   Role: Service Desk

   Popis činností: Operátor Service Desku společnosti v součinnosti s uživatelem, který oznámil incident, stanovuje typ incidentu, úroveň dopadu a naléhavosti incidentu a určuje kategorii incidentu dle parametrů definovaných pro danou službu.

   Klasifikace: Servisní požadavek tzn. požadavek uživatele na servisní zásah v případě např. instalaci uživatelského SW. Incident. Selhání HW. Nedostupnost služby. Bezpečnostní Incident.

   Operátor Service Desku společnosti v součinnosti s uživatelem, který oznámil incident, definuje časovou mez, do které má být daný incident vyřešen.Service Desk sdělí uživateli identifikátor incidentu, který slouží pro další komunikaci mezi uživatelem a Service Desk. Informuje uživatele o předpokládaném termínu vyřešení incidentu.

   Tyto informace pomáhají určit způsob zpracování incidentu a v některých případech i řešitelskou skupinu, které má být incident předán k řešení.

4. **Aktivita:** Předání servisního požadavku

   Vstup: Hlášený servisní požadavek

   Výstup: Předaný servisní požadavek

   Role: Service Desk

   Popis činností: Jestliže se jedná o servisní požadavek, předá pracovník Service Desku tento servisní požadavek příslušnému technickému zaměstnanci, který tento požadavek realizuje.

   V případě požadavku na pořízení nového HW či SW předá tento požadavek k odsouhlasení vedoucímu oddělení informatiky.

5. **Aktivita**: Priorita incidentu

   Vstup: Klasifikovaný incident

   Výstup: Stanovená priorita incidentu

   Role: Service Desk

   Popis činností: Priorita se stanovuje s ohledem na naléhavost incidentu. Určení priority je definováno tabulkou kódu priority, která jek dispozici na Servis Desku.

6. **Aktivita:** Úvodní diagnostika incidentu

   Vstup: Identifikovaný a klasifikovaný incident

   Výstup: Přidělení incidentu řešitelské skupině, nebo uzavřený incident

   Role: Service Desk

Popis činností: Cílem činnosti je nalézt řešení incidentu již na 1. úrovni podpory (více kapitola 2.1.6. Úrovně podpory). Service Desk se může pokusit použít dokumentované řešení v databázi znalostí, nebo se pokusí nalézt řešení na základě svých znalostí, nebo jiných informačních zdrojů.

Pokud Service Desk incident vyřeší, přechází proces přímo do uzavření incidentu.

Pokud není Service Desk schopen vyřešit incident na 1. úrovni podpory předá incident k řešení na 2. nebo 3. úroveň podpory tj. rozhodne o řešitelské skupině a zajistí co nejrychlejší předání incidentu této řešitelské skupině (více kapitola 2.1.4. Role v procesu Incident Management).

Předání incidentu se řídí potřebou hierarchické eskalace.

7. **Aktivita:** Šetření a diagnóza 2. nebo 3. úrovně podpory

   Vstup: Přidělený incident

   Výstup: Nalezené řešení incidentu

   Role: Specialista řešení incidentů

   Popis činností: Cílem je najít nejrychlejší možné řešení, které povede k odstranění incidentu. Specialista řešení incidentů v rámci 2. nebo 3. úrovně podpory najde nejrychlejší možné řešení obnovy služby. Při řešení využívají řešitelské skupiny svoje znalosti a čerpají informace z jiných záznamů.

8. **Aktivita:** Analýza příčiny incidentu

   Vstup: Nalezené řešení incidentu

   Výstup: Identifikována příčina incidentu

   Role: Specialista řešení incidentu

   Popis činností: Cílem je identifikovat příčinu incidentu a aplikovat vhodné preventivní opatření k zabránění opakovanému výskytu incidentu.

9. **Aktivita:** Řešení incidentu a obnova služby

   Vstup: Nalezené řešení incidentu

   Výstup: Vyřešený incident

   Role: Specialista řešení incidentů

   Popis činností: Vyřešit Incident dle nalezeného způsobu řešení

10. **Aktivita:** Uzavření incidentu

    Vstup: Vyřešený incident

    Výstup: Záznam o vyřešení incidentu

    Role: Specialista řešení incidentů

    Popis činností: V případě, že byl incident řešen externí řešitelskou skupinou (více kapitola 2.1.4. Role v procesu Incident Management) bude tato informovat Service Desk společnosti o tom, že incident byl vyřešen. Povinnou součástí zprávy o vyřešení incidentu je i informace o způsobu řešení Incidentu.

    Následně je povinností informovat uživatele o vyřešení incidentu a incident korektně uzavřít.

1.1.4 Role v procesu Incident Management

Operátor Service Desku

Operátor Service Desku společnosti má za úkol přijmout a zaevidovat incidenty a pokusit se jej vyřešit pomocí vědomostní báze. V případě, nemožnosti vyřešit tento incident je zodpovědný za jeho předání na další úroveň podpory. Tito pracovníci tvoří tzv. 1. úroveň podpory a většinou jsou vlastníky incidentu. Identifikují typy incidentů a související procedury, dokumentují všechny historické aktivity u incidentu, upravují priority nebo znovu-otevírají incidenty, uzavírají tickets.

Vlastník incidentu tedy operátor Service Desku je zodpovědný za vyřešení incidentu a informování uživatele. Operátor Service Desku je role s nejširším spektrem aktivit v procesu Incident Management.

Interní řešitelská skupina

Je skupina odborníků z řad zaměstnanců odpovědných za analýzu, návrh řešení a implementaci řešení incidentu.

Externí řešitelská skupina

Je skupina odborníků z externích zdrojů společnosti. Dodavatelé, kteří mají za úkol převzít incidenty od operátorů Service Desku společnosti a zajistit jejich vyřešení. Tito pracovníci tvoří 3. úroveň podpory.[5] V případě, že pracovník této skupiny detekuje incident, je povinen tuto skutečnost ohlásit na Service Desk společnosti.

[5] Poznámka autorky: Společnosti People & Job, s.r.o. nemá vlastní vysoce kvalifikované odborníky a z tohoto důvodu musí zajistit řešení prostřednictvím externích zdrojů, tzn.: skupiny odborníků, které nazývá dodavatelé.

Specialista řešení incidentů

Specialista řešení incidentů je obecně zodpovědný za analýzu, návrh řešení a implementaci řešení incidentu. Konkrétními zástupci této role jsou: Service Desk společnosti, interní a externí řešitelské skupiny.

Incident Manager

Incident Manager je zodpovědný za řízení pracovníků podílejících se na poskytování podpory, sledování výkonnosti a standardního průběhu procesu Incident Management. Dále je zodpovědný za přípravu podkladů pro reporting a předkládání návrhů na zlepšení. Zodpovídá za správu toků všech požadavků od uživatelů a zajišťuje jejich včasné vyřešení. Koordinuje oblasti procesů Problem Management a servisních požadavků. Identifikuje typy incidentů a související procedury, dokumentuje všechny historické aktivity u incidentu, vytváří Problem a Change tickets, upravuje priority nebo znovu-otevírá incidenty, zavírá tickets. Vytváří měsíční statistiky a reporty o úrovni služeb, datové a trendové analýzy dle definovaných metrik procesu.

1.1.5 RACI matice procesu Incident Management

Matice RACI slouží k identifikaci rolí a pro rozdělení a přiřazení individuálních odpovědností členů týmu v jednotlivých fázích procesu Incident Management. V modelu se používají zkratky R A C I.

Vysvětlení jednotlivých rolí:[6]

- **R = Responsible**
  Tato osoba vlastní danou aktivitu v procesu, je hlavním řešitelem, koordinátorem dané aktivy.

- **A = Accountability**
  Platí pravidlo, že celkovou odpovědnost k danému procesu má pouze jedna osoba. Tato osoba je vlastníkem celého procesu, je odpovědná za celý proces, ale nemusí fyzicky vykonávat aktivity procesu.

- **C = Consulted**
  Osoba, která se podílí na řešení formou konzultace nebo schválení.

- **I = Informed**
  Osoba, která má být informována o průběhu činnosti nebo výsledném rozhodnutí.

Následující tabulka číslo 2 názorně popisuje role a odpovědnosti procesu Incident Management.

[6] Více o této problematice: ITIL. *Service Design: Organization for Service Design*. 1st. published. London: UK by TSO, 2007, s. 189. ISBN: 978 0 11 331047 0

Tabulka 2: Role a odpovědnosti procesu Incident Management

	Incident Manager	Specialista Incidentu	Operátor Service Desku
Obdržení Incidentu v oddělení síťového perimetru a přiřazení odpovědnému řešitelskému týmu	**A**	**I**	**R**
Řešení Incidentu a obnova služby, aktualizace vědomostní báze	**I**	**R**	**I**
Nenalezeno řešení Incidentu, iniciace procesu Problem Management	**I**	**R**	**I**
Nenalezeno řešení problému, iniciace procesu Change Management	**C**	**R**	**I**
Uzavření Incidentu	**I**	**I**	**R**

Zdroj: autorka práce (vytvořeno na základě principů vycházejících z odborné literatury ITIL)

1.1.6 Úrovně podpory

Řešení incidentů je realizováno pomocí různých úrovní podpory a řešitelských skupin podle následující tabulky číslo 3. V této tabulce jsou uvedeny jednotlivé řešitelské skupiny a / nebo role, které dané úrovně zajišťují.[7]

Tabulka 3: Úrovně podpory

Úroveň podpory	Role
Uživatel	Společnosti, ostatní uživatelé
1. úroveň podpory	Service Desk společnosti
2. úroveň podpory	Interní řešitelské skupiny v rámci společnosti
3. úroveň podpory	Externí řešitelské skupiny

Zdroj: autorka práce (vytvořeno na základě principů vycházejících z odborné literatury ITIL)

Popis jednotlivých úrovní podpory:

První úroveň podpory

První úroveň podpory je řešena na Service Desku společnosti. Na této úrovni je zodpovědnost za průběžné sledování řešení všech evidovaných incidentů, z tohoto důvodu je také Service Desk vlastníkem všech incidentů. Incidenty, které není možno řešit ihned v rámci Service Desku jsou předávány na další úrovně podpory. Z této úrovně se definuje také klíčová metrika určující procento incidentů vyřešených na 1. úrovni podpory v rámci Service Desku.[8]

[7] Více o této problematice: ITIL. *Service Operation: Incident escalation*. 1. published. London: UK by TSO, 2007, s. 51-52. ISBN: 978 0 11 331046 3

[8] Poznámka autorky: Metriku definuje společnosti People & Job, s.r.o., aby byla schopna hodnotit efektivitu a tím i přínos procesu pro firmu.

Druhá úroveň podpory

Druhá úroveň podpory je zajišťována pomocí interních řešitelských skupin společnosti. Pokud není možné incident vyřešit v rámci 2. úrovně podpory, musí být co nejrychleji eskalován na 3. úroveň podpory.

Třetí úroveň podpory

Třetí úroveň podpory je zajišťována pomocí externích řešitelských skupin tj. dodavateli.

1.1.7 Nástroje procesu Incident Management

V následující tabulce číslo 4 jsou uvedeny nástroje sloužící pro podporu procesu Incident Management v rámci společnosti a jednotlivých úrovní podpory.

Tabulka 4: Nástroje procesu Incident Management

Nástroj	Role / úroveň podpory	Popis
Komunikační nástroje	Uživatel / 1. úroveň podpory	Service Desk společnosti. Rozhraní na Problem ticketing. Přístup do znalostní báze Service Desku.
Dohledové nástroje	2. úroveň podpory	Dohledový nástroj (Event Management) pro dohled nad IT službami společnosti. V případě, že tento nástroj detekuje incident v podobě nedostupnosti některé z částí IT služeb, zasílá automatické upozornění příslušnému oddělení.
Evidenční nástroje	1. úroveň podpory 2. úroveň podpory	Nástroj používaný pro evidenci kontaktů, incidentů, sledování životního cyklu incidentů a vytváření reportů o evidovaných incidentech.
Vyhodnocovací nástroje	1. úroveň podpory	Zpětná vazba pro uživatele o stavu incidentu, byl/nebyl vyřešen a uzavřen.
Kontakty na dodavatele IT služeb	1. úroveň podpory 2. úroveň podpory	Databáze všech dodavatelů, SLA, Smlouvy o podporách, kontaktů a eskalačních procedur
Online dokumentace a znalostní báze	1. úroveň podpory	Schopnost vyhledávat data o aktuálních problémech (dle komponenty, zprávy, příčiny)
Configuration Management nástroje	1. úroveň podpory 2. úroveň podpory	Nástroje pro sběr, ukládání a dohledávání dostupného inventáře servisních komponent a jejich konfiguračních dat, CMDB

Zdroj: autorka práce (vytvořeno na základě principů vycházejících z odborné literatury ITIL)

1.1.8 Výkonnost a metriky procesu Incident Management

Výkonnost a metriky procesu Incident Management.[9]

Přehled klíčových výkonnostních ukazatelů Key Performance Indicator dále jen KPI.

Pro posuzování výkonnosti procesu Incident Management jsou monitorovány a vyhodnocovány obecně následující hodnoty:

- počet incidentů dle jednotlivých kategorií;
- počet incidentů vyřízených v souladu s definovanou dobou reakce;
- počet incidentů vyřízených v souladu s dobou řešení externích dodavatelů, definovanou v jednotlivých smlouvách;
- počet incidentů vyřešených na 1. úrovni podpory z celkového počtu incidentů.

Pokud není určeno jinak, probíhá měření a vyhodnocování výkonnostních parametrů a jejich soulad s definovanými parametry na měsíční bázi.

Výčet konkrétních metrik KPI využitelných jako výkonnostní ukazatele je následující:

- % vyřešených incidentů na první úrovni podpory;
- celkový počet incidentů (kontrolní hodnota);
- rozpad incidentů v každé fázi (logované, uzavřené,…);
- objem nahromaděných incidentů čekajících na zpracování;
- střední doba nutná k vyřešení incidentu;
- % incidentů vypořádaných ve smluvním čase odezvy;
- % Incidentů vyřešených dle smluvní průměrné doby odezvy definované v Service Level Agreement dále jen SLA;

[9] Více o této problematice: ITIL. *Service Operation: Metrics.* 1. published. London: UK by TSO, 2007, s. 54-55. ISBN: 978 0 11 331046 3

- % a počet závažných Incidentů;
- % a počet správně přiřazených Incidentů;
- % chybně přiřazených incidentů odpovědnému řešitelskému týmu;
- průměrné náklady na vyřešení incidentu.

Incident Manager v součinnosti s operátory ze Service Desku vytváří podklady pro reporting v podobě záznamů o incidentech, přehledy dle kategorií, reakčních doby, doby řešení incidentu apod.

1.2 Charakteristika a cíl procesu Problem Management

Problém je jakákoliv situace, která má za následek ztrátu, nebo snížení dostupnosti, nebo výkonu služeb a/nebo prostředí. Problém může být identifikován buď automatickým anebo neautomatickým způsobem. [10]

Incident je ojedinělý výskyt problému, který ovlivňuje běžné uživatelské služby či prostředí. Služby musí být obnoveny v co nejkratší době a to s minimem přerušení těchto uživatelských služeb či prostředí.

V případě problému hovoříme o více jak jednom incidentu, které negativně ovlivňují více uživatelských služeb, které není možné obnovit v krátkém časovém horizontu a to bez dalšího uživatelského omezení.

Problem Management odpovídá za řízení životního cyklu problémů vzniklých během provozu IT služeb,

Přičemž Problem Management svou činností slouží jako podpůrný prostředek pro zajištění větší spolehlivosti IT služeb.

Cílem procesu Problem Management je:[11]

- minimalizovat nepříznivý dopad Incidentů a problémů na provoz;
- prevence opakovaného výskytu Incidentů souvisejících se stejnou chybou a to tím, že zjišťuje a následně odstraňuje příčinu těchto problémů.

Vstupy do procesu Problem Management:

- podrobnosti o incidentech z procesu Incident Management;
- podrobnosti o konfiguračních položkách z CMDB;

[10] Více o této problematice: ITIL. *Service Operation: Problem Management.* 1. published. London: UK by TSO, 2007, s. 58-68. ISBN: 978 0 11 331046 3
[11] Tamtéž. Více In: ITIL. *Service Operation: Purpose/goal/objective,* s. 58-59.

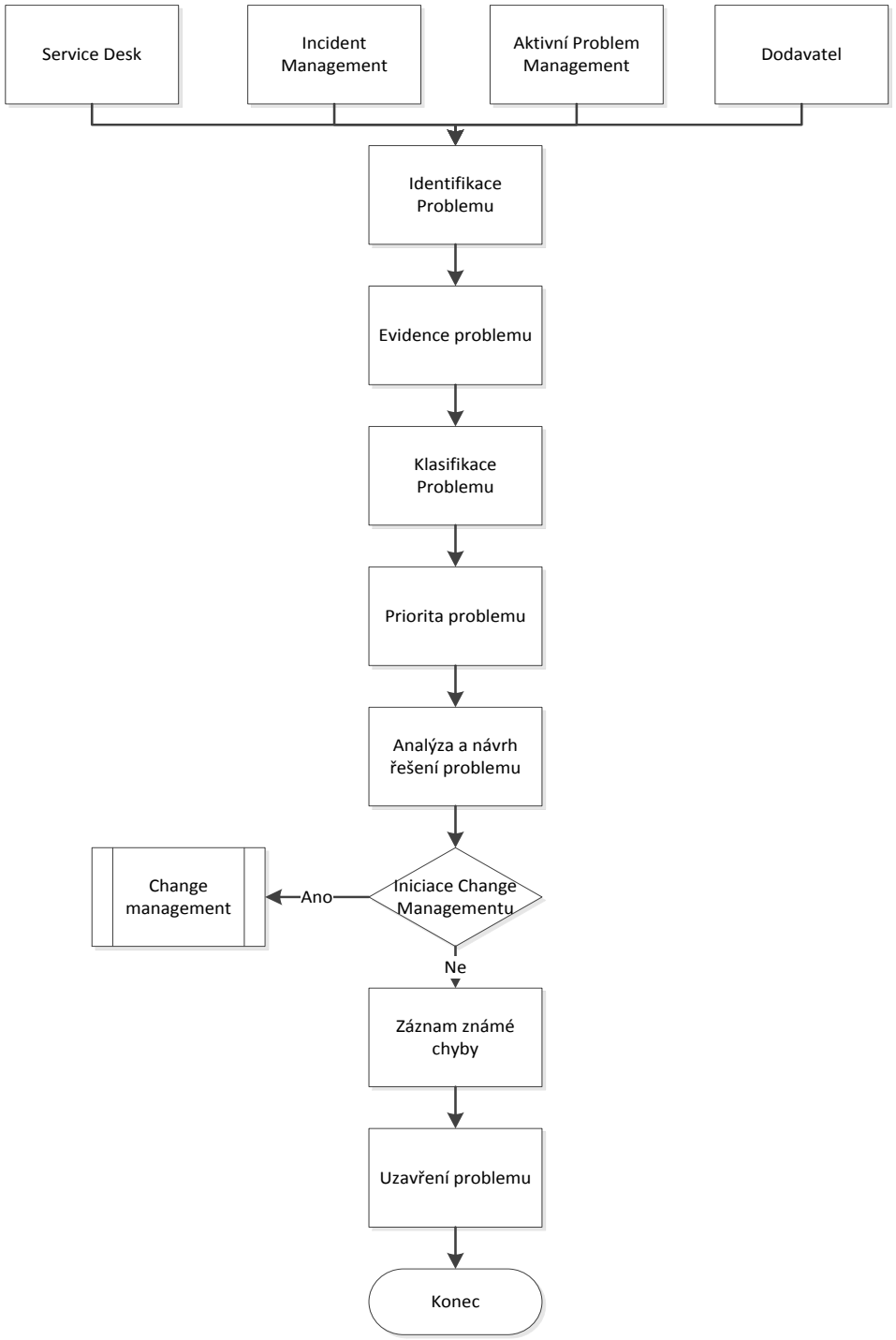
- způsob řešení Incidentů se stejnou chybou nebo opakujících se v procesu Incident Management;
- informace o změnách z procesu Change Management např. změna, která má za následek vznik incidentů.

Výstupy z procesu Problem Management:

- známé chyby;
- aktivace procesu Change Management;
- aktualizace záznamů o problémech;
- uzavřené problémy;
- reporty.

Následující vývojový diagram číslo 2 přehledně zobrazuje proces Problem Management, včetně vzájemných vazeb a souvislostí.

Diagram 2: Procesní tok Problem Management včetně vzájemných vazeb a souvislostí



Zdroj: ITIL. *Service Operation: Process activities, methods and techniques*, s. 60

Níže jsou popsány činnosti jednotlivých kroků, znázorněných v diagramu číslo 2.

Popis jednotlivých kroků vedoucích k řešení problému:

1. **Aktivita**: Identifikace a klasifikace problému

   Vstup: Problém je detekován a přednesen na jednání pracovního týmu. Možné příklady problému: opakující se incidenty, chyba v systému. Dodavatel detekuje ve svém systému chybu, která může být příčinnou incidentů.

   Výstup: Identifikovaný problém

   Role: Specialista Problem Management

   Popis činností: Problém může být detekován jako příčina opakujících se incidentů. Na jednání pracovního týmu je přiřazen řešitelské skupině. Je nutné identifikovat a zaznamenat základní údaje o problému, sloužící jako podklady pro následující analýzu. Identifikace řešitelské skupiny

2. **Aktivita:** Evidence problému

   Vstup: Identifikovaný problém

   Výstup: Zaznamenaný problém

   Role: Service Desku

   Popis činností: Identifikovaný problém je zaznamenaný v nástroji pro evidenci problémů a předán na relevantní řešitelskou skupinu.

3. **Aktivita:** Klasifikace problému

   Vstup: Zaznamenaný problém

   Výstup: Klasifikovaný problém

   Role: Řešitelská skupina problémů

Popis činností: Řešitelská skupina problémů stanoví typ problému, úroveň dopadu a naléhavosti problému a určuje kategorii problému dle parametrů definovaných pro danou službu.

Klasifikace: Incident. Selhání HW. Nedostupnost služby. Bezpečnostní incident

Řešitelská skupina definuje časový rámec pro vyřešení problému.

4. **Aktivita:** Priorita problému

   Vstup: Klasifikovaný problém

   Výstup: Stanovená priorita problému

   Role: Řešitelská skupina problémů

   Popis činností: Priorita se stanoví s ohledem na naléhavost problému. Určení priority je definováno úrovní priority (kapitola 2.2.1. Klasifikace problémů, tabulka 5: Úroveň priority).

5. **Aktivita:** Analýza a návrh řešení problému

   Vstup: Identifikovaný problém. Informace o konfiguračních položkách z CMDB

   Výstup: Návrh řešení problému

   Role: Specialista Problem Management

   Popis činností: Detailní analýza problému. Definice příčiny problému. Návrh řešení a odstranění příčiny problému.

6. **Aktivita:** Change Management

   Vstup: Návrh řešení problému

   Výstup: Implementace řešení

   Role: Change Manager

   Popis činností: Podle způsobu realizace řešení je návrh řešení problému zpracován v procesu Change Management.

7. **Aktivita:** Záznam známé chyby

   Vstup: Příčina problému nebyla odstraněna

   Výstup: Záznam v databázi znalostí

   Role: Service Desk

   Popis činností: V případě, že příčinu problému není možné odstranit, je problém, včetně aktivit vedoucích k jeho odstranění, zaznamenán do databáze znalostí.

8. **Aktivita:** Uzavření záznamu problému

   Vstup: Záznam v databázi znalostí. Příčina problému byla odstraněna

   Výstup: Uzavřený problém

   Role: Service Desk

   Popis činností: Korektní uzavření záznamu problému v podpůrných nástrojích.

1.2.1 Klasifikace Problémů

Dopad problémů na výkonnost uživatele, respektive společnosti, je determinován dle rozsahu následků způsobených výpadkem služby.[12]

Tabulka 5: Úrovně priority

Úroveň priority	Popis dopadu	Čas na odpověď
1 Very Heavy Impact	Kritický problém, ovlivňuje chod celé společnosti, která není schopna poskytovat své hlavní služby zákazníkům a zájemcům o zaměstnání.	4 Hodiny
2 Heavy Impact	Závažný problém, který ovlivňuje služby poskytované několika zákazníkům.	24 Hodin
3 Moderate Impact	Méně závažný problém, která má dopad na skupinu zájemců o zaměstnání a některé interní uživatele.	48 Hodin
4 Small Impact	Problém má dopad na malou skupinu interních uživatelů.	96 Hodin

Zdroj: autorka práce (vytvořeno na základě principů vycházejících z odborné literatury ITIL)

Úrovně priority 1 až 4 kvantifikují míru pozornosti věnované problémům, které mají dopad na business služby společnosti.

[12] Více o této problematice: ITIL. *Service Operation: Problem Prioritization.* 1. published. London: UK by TSO, 2007, s. 61. ISBN: 978 0 11 331046 3

1.2.2 Role a odpovědnosti procesu Problem Management

Specialista problému

Je odpovědný za analýzu, návrh řešení a případně i za implementaci řešení problému. Provádí počáteční evidenci a logování problému, dokončuje počáteční záznam problému, přiřazuje závažnost a prioritu problému.

Pracovní tým

V případě, že řešení problému vyžaduje iniciaci projektu, pak na tomto projektu spolupracuje pracovní tým složený z jednotlivých specialistů. Pracovní tým je dočasná či trvalá skupina odborníků z řad zaměstnanců s jasně přiděleným rozsahem úkolů od vedoucího projektu. Obsazení pracovního týmu je dáno náročností projektu, složení týmu se může v různých fázích projektu lišit.

Problem Coordinator

Problem Coordinator přebírá odpovědnost za veškerou komunikaci a za koordinaci aktivit vedoucích k vyřešení problému.Kontaktuje dodavatele v případě hardwarových problémů, sleduje životní cyklus problému a organizuje informační tok.

Problem Manager

Problem Manager je role Service Desku a je to osoba odpovědná za celý proces Problem Management.

Problem Manager, jako vlastník procesu Problem Management, je odpovědný za problém, za proces a za jeho efektivitu. Definuje co problém je, zadává úkoly a stanoví cíle procesu Problem Management.

1.2.3 RACI matice procesu Problem Management

Matice RACI slouží k identifikaci rolí a pro rozdělení a přiřazení individuálních odpovědností členů týmu v jednotlivých fázích procesu Problem Management. V modelu se používají písmenka R A C I.

Vysvětlení jednotlivých rolí:[13]

- **R = Responsible**
  Tato osoba vlastní danou aktivitu v procesu, je hlavním řešitel, koordinátorem dané aktivy.

- **A = Accountability**
  Platí pravidlo, že celkovou odpovědnost k danému procesu má pouze jedna osoba. Tato osoba je vlastníkem celého procesu, je odpovědná za celý proces, ale nemusí fyzicky vykonávat aktivity procesu.

- **C = Consulted**
  Osoba, která se podílí na řešení formou konzultace nebo schválení.

- **I = Informed**
  Osoba, která má být informována o průběhu činnosti nebo výsledném rozhodnutí

Následující tabulka číslo 6 názorně popisuje role a odpovědnosti procesu Problem Management.

[13] Více o této problematice: ITIL. *Service Design: Organization for Service Design*. 1st. published. London: UK by TSO, 2007, s. 189. ISBN: 978 0 11 331047 0

Tabulka 6: Role a odpovědnosti procesu Problem Management

	Specialista problému	Problem Coordinator	Problem Manager
Identifikace problému a přiřazení odpovědnému řešitelskému týmu	**I**	**I**	**A**
Nalezení řešení problému	**R**	**C**	**I**
Odsouhlasení problému a výběr řešení nebo zamítnutí problému	**I**	**R**	**R**
Řešení problému	**R**	**I**	**I**
Provedení kontroly a reportování	**I**	**R**	**I**
Uzavření problému	**R**	**I**	**I**

Zdroj: autorka práce (vytvořeno na základě principů vycházejících z odborné literatury ITIL)

1.2.4 Měření výkonnosti procesu Problem Management

Reporting procesu Problem Management umožňuje jeho řízení. Reporty na denní bázi identifikují problémy, které vznikly předešlý den či během dne. Týdenní reporting poskytuje shrnutí úspěchů, otevřených problémů a celkovou analýzu. Denní reporting je nutný především z technických důvodů, týdenní reporting je pak důležitý pro řízení procesu. Měsíční reporty umožňují IT zvýšit efektivitu systému Problem Management.[14]

Výčet konkrétních metrik využitelných jako výkonnostní ukazatele KPI je následující:

- % vyřešených problémů;
- celkový počet problémů;
- objem nahromaděných problémů čekajících na zpracování;
- střední doba nutná k vyřešení problému;
- % a počet závažných problémů;
- průměrné náklady na vyřešení problémů.

Problem Coordinator ve spolupráci se Service Desk vytváří podklady pro reporting problémů.

Problem Coordinator pak vytváří manažerské prezentace reportů a faktické interpretace.

[14] Více o této problematice: ITIL. *Service Operation: Metrics.* 1. published London: UK by TSO, 2007, s. 67. ISBN: 978 0 11 331046 3

1.3 Change Management charakteristika a kritéria procesu

Charakteristika procesu Change Management slouží k pochopení náročnosti procesu a jeho propojení na procesy Incident Management a Problem Management.

Proces Change Management IT služeb odpovídá za řízení životního cyklu požadavků na změny a jejich realizaci, které vzniknou během provozu IT služeb, přičemž Change Management svou činností slouží jako podpůrný prostředek pro zajištění větší spolehlivosti IT služeb.[15] 60% výpadků všech IT služeb je způsobeno špatně provedenou změnou.

Rizika plynoucí ze zjednodušené či nekvalitní implementace procesu Change Management mohou nastat v případě kdy:

- detailní evidence informací a dokumentů může být v kolektivu vnímána jako byrokracie a ne jako důležitý krok v procesu;
- nesprávné nastavení a dodržování jednotlivých rolí, tedy povinnosti a odpovědností v jednotlivých řešitelských týmech;
- nedostatečná frekvence kontrol, zhuštění více aktivit do jedné aktivity, je snížen počet kontrol / analýz informací, dokumentů.

Kritéria procesu Change Management:

- všechny podstatné změny v IT musí být v souladu s předpisem procesu Change Management. Podstatné změny mohou vzájemně ovlivnit schopnosti uživatelů nebo systémů;

[15]Více o této problematice: ITIL. *Service Transition: Purpose goals and objectives of the Change Management*. 1. published. London: UK by TSO, 2007, s. 43. ISBN: 978 0 11 331048 7

- všechny změny v produkčních systémech uvnitř IT jsou logovány a je vedena odpovídající dokumentace, ve které jsou uvedeny důvody provedení změny a povaha změny;
- riziko a/nebo dopad požadované změny určuje, která ze čtyř částí pracovního postupu změny (Analýza, Návrh, Testování a Implementace) je požadována k úspěšnému zavedení změny do produkce;
- oprávněná osoba, která může prostřednictvím Service Desku zadat žádost o změnu, ale pouze oprávněné osoby mohou tuto žádost akceptovat a tedy přijmout.

1.3.1 Stav žádosti o změny a druhy změn procesu Change Management

Všechny možné stavy žádosti o změnu jsou:[16]

- **Open**: žádost o změnu byla doručena a přijata, ale ještě nebyla přiřazena;
- **In–Progress**: žádost o změnu byla doručena, je srozumitelně popsána, z žádosti na změnu se stává návrh na změnu, který je zpracováván a je přiřazen odpovědné osobě;
- **Approved**: obchodní a technické vyhodnocení návrhu na změnu bylo dokončeno, návrh na změnu byl schválen a je plánována implementace;
- **Rejected**: návrh na změnu byl zamítnut a přesměrován zpět na servisní oddělení k zadavateli s vysvětlením a doporučením;
- **Hold**: alespoň jedna žádost o změnu je ve stavu Rejected, Failed nebo Delayed. Jedná se o chybový stav, který řeší koordinační skupina;
- **Implemented**: Všechny žádosti byly dokončeny a uzavřeny. Požadavek byl realizován;
- **Closed**: návrh na změnu byl uzavřen. Všechny návrhy na změnu byly dokončeny a uzavřeny;
- **Canceled**: návrh na změnu byl zrušen.

Níže je uveden popis jednotlivých druhů změn, které mohou nastat v procesu Change Management:[17]

- **Hardwarová změna**: jedná se o všechny změny v IT zařízeních;
- **Softwarové změny**: kritéria pro zadání softwarové změny do procesu Change Management jsou založena na předpokladu, že existují zdroje pro podporu IT; V případě, že potřeba takové změny nastane, uživatel nebo zaměstnanec v IT podpoře tuto žádost o změnu zadá;

[16]Více o této problematice: ITIL. *Service Transition: Design and planning considerations.* 1. published. London: UK by TSO, 2007, s. 45. ISBN: 978 0 11 331048 7
[17] Tamtéž. Více In: ITIL. *Service Transition: Types of Change request,* s. 46

- **Síťové změny**: všechny změny týkající se instalací, zařízení používaném pro IT komunikaci, jsou předmětem procesu Change Management;
- **Změny v dokumentech**: do této skupiny patří všechny procedurální změny týkající se operačních norem a politik.

1.3.2 Kategorie změn

Během plánovacího cyklu změny je nutné také stanovit výši rizika plynoucí z implementace této změny. Proto musí být jasně definováno minimum požadavků pro jednotlivé kategorie změn.[18] Odpovědná osoba za koordinaci procesu Change Management pak může naplánovat více času, zajistit potřebnou dokumentaci nebo zajistit přezkoumání, tak aby byl dodržen plán implementace.

Všechny změny jsou sledovány prostřednictvím Service Desku a jsou zahrnuty do manažerského reportování k identifikaci případné potřeby navýšení zdrojů.

Urgentní změna

Mezi urgentní změny patří životně důležité změny nutné k zajištění stanovené úrovně IT služeb a tak zvané výjimečné změny, které jsou výsledkem obchodních potřeb a musí být implementovány co nejrychleji. Rovněž se jedná o změny vynucené bezpečnostní zranitelností informačního systému. Tyto druhy změn postoupí do implementační fáze v momentě jejich schválení příslušnými manažery a to jen v případě, že nastala urgentní či výjimečná situace. Tyto změny jsou průběžně vyhodnocovány k zajištění úspěšné implementace, identifikují se externí dopady nebo nové požadavky.

[18] Více o této problematice: ITIL. *Service Transition: Process activities, methods and techniques.* 1. published. London: UK by TSO, 2007, s. 48. ISBN: 978 0 11 331048 7

Hlavním znakem urgentní změny je:

- nutnost okamžitě obnovit služby;
- potřeba opravit existující problém okamžitě;
- daná změna musí být implementována okamžitě, protože nebyla rozpoznána dostatečně brzo, aby byla zařazena do plánu implementace normálním způsobem;
- změna musí být okamžitě provedena za účelem odstranění problému pro zprovoznění on-line systému.

K provedení urgentní změny je zapotřebí schválení příslušným/i, odpovědným/i zaměstnanci (kapitola 2.3.5. Role v procesu Change Management).

Změny 4. Kategorie

Tyto změny mají zásadní dopad na IT služby, jestliže se problém objeví během instalace.[19] Čas instalace je dlouhý a proces instalace je velmi obtížný či nemožný zvrátit. Změny 4. kategorie jsou zadávány do procesu Change Management v dostatečném předstihu před plánovaným dnem implementace. Konkrétní den implementace je určen prostřednictvím Change Management kalendáře nebo SLA. Ačkoliv změny 4. kategorie musí být urychleny vzhledem ke kritické časové situaci, přesto musí být projednány za účasti zástupců oddělení, které mohou být změnou ovlivněny. Odpovědností žadatele o změnu je organizovat tuto schůzi a zajistit přítomnost požadovaných skupin či jednotlivců.

Hlavním znakem změny 4. kategorie je:

- změna je viditelná u všech uživatelů;
- změna je vysoce riziková;
- je to poprvé, kdy je tato změna provedena;
- změna je obtížná nebo je nemožné ji zvrátit;

[19] Více o této problematice: ITIL. *Service Transition: Process activities, methods and techniques.* 1. published. London: UK by TSO, 2007, s. 48. ISBN: 978 0 11 331048 7

- je velice obtížné implementovat tuto změnu;
- instalace změny potrvá velice dlouho;
- pokud změna nebude implementována, práce v aplikačním systému nebo na kritických souborech se zastaví.

K provedení změny 4. kategorie je zapotřebí schválení příslušným/i odpovědným/i zaměstnanci.

Změny 3. Kategorie

Změny 3 kategorie mají vliv na velké množství uživatelů. Změna je velice riziková a vyžaduje velké úsilí. Změny 3. kategorie jsou zadávány do procesu Change Management v dostatečném předstihu před plánovaným dnem implementace. Konkrétní den implementace je určen prostřednictvím termínového kalendáře nebo SLA.

Hlavním znakem změny 3. kategorie je:

- změna je viditelná u všech uživatelů;
- změna je vysoce riziková;
- změna je prováděna pouze zřídka;
- ke zvrácení změny je zapotřebí velkého úsilí;
- je obtížné změnu implementovat do prostředí společnosti;
- pokud změna nebude implementována, práce v aplikačním systému nebo na kritických souborech se zastaví.

K provedení změny 3. kategorie je zapotřebí schválení jednatelem společnosti. Tyto změny mají dopad na více oddělení či uživatelů, mají velký obchodní či technický dopad, jsou velmi rizikové a náročné na implementaci.

Změny 2. Kategorie

U změny 2. kategorie je minimální riziko dopadu změny na produkční systémy. Odpovědností žadatele o změnu je oznámit příslušným oddělením potenciální dopad změny. O změnu 2. kategorie se jedná v případě, že jde o restartování kritických komponent v produkčním systému.

Změny 2. kategorie jsou zadávány do databáze procesu Change Management prostřednictvím Service Desku společnosti, tak aby jejich implementace mohla být naplánována. Koordinátor změn je odpovědný za sledování a reportování změny 2. kategorie.
Hlavním znakem změny 2. kategorie je:

- změnu uvidí pouze malé množství koncových uživatelů;
- změna je málo riziková;
- změna je relativně snadno implementovatelná;
- změna byla úspěšně implementovaná již několikrát.

Změna 1. Kategorie

Změna první kategorie je málo nebo téměř viditelná, neexistují vnější závislosti, není potřeba intervencí. Není zde související riziko nebo dopad změny, ať již na produkční systémy či žadatele a to i v případě, že implementace změny je odložena. Změny 1. kategorie jsou evidovány v databázi změn, jsou komunikovány s odděleními, na které by změna mohla mít dopad nebo vliv.

Hlavním znakem změny 1. kategorie je:

- změna má minimální dopad na poskytované služby koncových uživatelů;
- změna je známá nebo běžná pro osobu (y), která (é) změnu implementuje;
- existuje již dříve navržený a odzkoušený postup pro implementaci změny;
- změna má minimální riziko;
- problém se dá snadno odstranit.

Následující tabulka číslo 7 názorně popisuje kategorie výše uvedených změn.

Tabulka 7: Shrnutí jednotlivých kategorií změn

Kategorie	1. Kategorie (zanedbatelné riziko)	2. Kategorie (malé riziko)	3. Kategorie (střední riziko)	4. Kategorie (vysoké riziko)
Organizačně viditelná změna nebo finanční dopad	Rutinní IT aktivita nebo minimální finanční dopad	Viditelná vedoucím pracovníkům, nebo s nízkým finančním dopadem	Viditelná na úrovni vrcholového managementu, nebo se středním finančním dopadem	Viditelná na úrovni vrcholového managementu, s vysokým finančním dopadem, nebo s negativní vnější publicitou
Dopad na ostatní systémy nebo aplikace	Žádný dopad	Jeden systém, nebo aplikace, která souvisí s touto změnou	2 až 3 systémy, nebo aplikace související s touto změnou	4 a více systémů nebo aplikací souvisejících s touto změnou, nebo hlavní obchodní aplikace
Úsilí nutné k zvrácení chyby	Minimální	Snadné	Možné, ale ne snadné	Složité a téměř nemožné
Procesní změna	Minimální	Je zapotřebí nízké změny	Je zapotřebí středně náročné změny ve spolupráci s IT, nebo/a uživateli	Je zapotřebí značné a komplexní změny ve spolupráci s IT nebo/a uživateli
Rozsah změny	Jeden komponent, např. hardware, software na jedné platformě	Dva komponenty na jedné platformě	Hardware, Software a síť na jedné platformě	Hardware, Software a síť napříč několika platformami
Stupeň viditelnosti pro IT zákazníky	Minimální	Nízký	Střední	Vysoký
Zkušenosti ohledně implementace změny	Existuje technologie a jsou značné zkušenosti pro implementaci	Existuje technologie a jsou nějaké zkušenosti pro implementaci	Nová technologie s omezenými zkušenostmi	Nová technologie bez zkušeností
Odhadovaný čas potřebný pro dokončení	Jeden měsíc a méně	Čtvrtletí nebo méně	Půl roku a méně	Více jak půl roku, nebo stanovený termín

Zdroj: autorka práce (vytvořeno na základě principů vycházejících z odborné literatury ITIL)

Pro stavení úrovně rizika může jednotlivým odpovědným osobám, posloužit níže uvedená, kategorizace rizikových faktorů, [20] pro přehlednost zobrazena v tabulkách 8a a 8b.

Tabulka 8a: Stanovení úrovně rizika

Faktory	**Body**
Organizačně viditelná změna nebo finanční dopad	
Viditelná na úrovni vrcholového managementu společnosti, s vysokým finančním dopadem nebo s negativní publicitou	1
Viditelná na úrovni vrcholového managementu společnosti nebo se středním finančním dopadem	2
Viditelná na manažerské úrovni nebo s nízkým finančním dopadem	3
Rutinní IT aktivita nebo minimální finanční dopad	4
Dopad na ostatní systémy nebo aplikace	
4 a více systémů nebo aplikací souvisí s touto změnou, nebo hlavní obchodní aplikací	1
2 až 3 systémy nebo aplikace souvisí s touto změnou	2
Jeden systém nebo aplikace souvisí s touto změnou	3
Žádný dopad	4
Úsilí nutné k zvrácení chyby	
Složité a téměř nemožné	1
Možné, ale ne snadné	2
Snadné	3
Minimální	4
Procesní změna	
Je zapotřebí značné a komplexní změny ve spolupráci s IT a/nebo s uživateli	1
Je zapotřebí středně náročné změny ve spolupráci s IT a/nebo s uživateli	2
Je zapotřebí nízké změny	3
Minimální	4

Zdroj: autorka práce (vytvořeno na základě principů vycházejících z odborné literatury ITIL)

[20] Více o této problematice: ITIL. *Service Transition: Assess and evaluate the Change.* 1. published. London: UK by TSO, 2007, s. 53. ISBN: 978 0 11 331048 7

Tabulka 8b: Stanovení úrovně rizika

Faktory	**Body**
Rozsah změny	
Hardware, Software a síť napříč několika platforem	1
Hardware, Software a síť na jedné platformě	2
Dvě komponenty na jedné platformě	3
Jedna komponenta, např. hardware, software na jedné platformě	4
Stupeň viditelnosti pro IT zákazníky	
Minimální	1
Nízký	2
Střední	3
Vysoký	4
Zkušenosti ohledně implementace změny	
Nová technologie bez zkušeností	1
Nová technologie s omezenými zkušenostmi	2
Existuje technologie a jsou nějaké zkušenosti pro implementaci	3
Existuje technologie a jsou značné zkušenosti pro implementaci	4
Odhadovaný čas potřebný pro dokončení	
Více jak půl roku nebo stanovený termín	1
Půl roku a méně	2
Čtvrtletí nebo méně	3
Jeden měsíc a méně	4

Zdroj: autorka práce (vytvořeno na základě principů vycházejících z odborné literatury ITIL)

Na základě součtu jednotlivých kategorií faktorů z tabulky číslo 8a, 8b je následně vyhodnocena celková míra rizika a náročnosti změny. Vyhodnocení celkové míry rizika a náročnosti změny je přehledně zobrazeno v následující tabulce číslo 9.

Tabulka 9: Vyhodnocení celkové míry rizika a náročnosti změny

Celkové bodové skóre je v rozmezí:	**Riziko a náročnosti změny**
8 – 14	4: kritické
15 – 20	3: střední
21 – 26	2: nízké
27 – 32	1: zanedbatelné

Zdroj: autorka práce

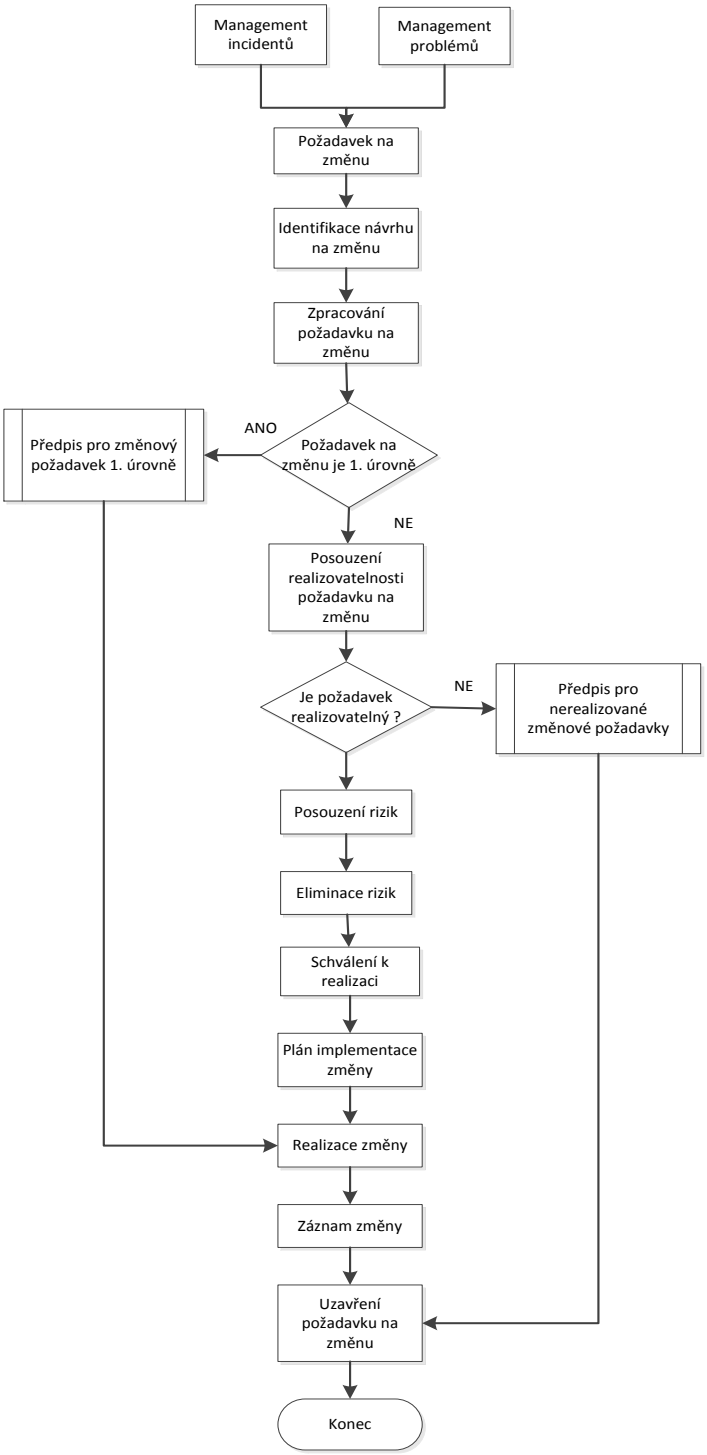
Kategorizace rizikových faktorů a vyhodnocení celkové míry rizika a náročnosti změny vychází z principu hodnocení analýzy rizik, které bylo popsáno v bakalářské práci autorky.[21]

1.3.3 Procesní tok procesu Change Management

Tato kapitola popisuje procesní tok Change Management, který je pro přehlednost znázorněn v diagramu číslo 3. Dále následuje podrobný popis jednotlivých kroků uvedených v diagramu číslo 3 včetně jednotlivých činností, vstupů a výstupů jednotlivých kroků.

[21] Více o této problematice. GOLLOVÁ, Marta. Budování systému bezpečnosti informací společnosti a zvyšování bezpečnostního povědomí zaměstnanců. Praha, 2012, s. 40. Bakalářská práce. UJAK, Katedra Andragogiky. Vedoucí práce: Jiří Víšek

Diagram 3: Procesní tok Change Management včetně vzájemných vazeb a souvislostí



Zdroj: autorka práce
(upraveno podle ITIL. *Service Transition: Process activities, methods and techniques*, s. 49-50)

Popis aktivity zadání požadavku na změnu, přidělení řešitelskému týmu, vyhodnocení dopadů a stanovení kategorie změn:

1. Identifikace návrhu na změnu

   Vstup: Požadavek na změnu

   Výstup: Relevantní nebo nerelevantní požadavek

   Role: Pracovní týmy

   Postup: Posoudit požadavek z hlediska věcného významu, vlivu na IT infrastrukturu a služby, popřípadě dle rámcových nákladů na tuto změnu.

2. Zpracování požadavku na změnu

   Vstup: Identifikovaný a zaznamenaný požadavek na změnu

   Výstup: Definovaný požadavek na změnu

   Role: Change Coordinator

   Postup: Zápis požadavku do databáze změn. Doplnit obecný harmonogram postupu prací. Definovat odpovědností za jednotlivé činnosti v rámci realizace změny. Definovat požadované dokumentace. Definovat schvalovací a akceptační orgán.

3. Schválení k realizaci

   Vstup: Definovaný požadavek na změnu

   Výstup: Schválený požadavek na změnu

   Role: Pracovní tým

   Postup: Schválení požadavku na změnu a předání požadavku k realizaci změny

4. Plán implementace změny

   Vstup: Schválený požadavek na změnu

   Výstup: Plán implementace změny

   Role: Change Coordinator

   Postup: Detailní harmonogram implementace změny. Definované odpovědnosti za implementaci jednotlivých dílčích kroků implementace změny. Definování akceptace změny.

5. Realizace změny

   Vstup: Plán implementace změny

   Výstup: Akceptovaná změna nasazená do produkčního prostředí

   Role: Change Specialista

   Postup: Doplnit číslo provozní změny dle databáze. Záznamy jednotlivých kroků implementace změny. Definovat požadované dokumentace

6. Záznam změny

   Vstup: Akceptovaná a nasazená změna do produkčního prostředí

   Výstup: Zapsaná změna do provozního deníku

   Role: Change Manager

   Postup: Aktualizace provozního deníku se zaznamenáním provedených změn v IT infrastruktuře a službách.

7. Uzavření požadavku na změnu

   Vstup: Změna implementovaná do produkčního prostředí

   Výstup: Uzavřený požadavek na změnu

   Role: Change Manager

   Postup: Korektně uzavřít požadavek na změnu. Zaznamenat informace o uzavření požadavku do zápisu z jednání pracovního týmu. Předat informace o případné změně konfigurační položky procesu. Konfigurační Management. Aktualizovat záznam v nástroji pro evidenci změn

8. Řízení průběhu životního cyklu požadavku, reporting

   Vstup: Informace o stavu požadavku

   Výstup: Report

   Role: Change Manager

   Postup: Sledovat životní cyklus změny. Průběžně aktualizovat databázi změn. Průběžně aktualizovat plán změn. Připravovat reporty.

1.3.4 Raci Matice procesu Change Management

Matice RACI slouží k identifikaci rolí a pro rozdělení a přiřazení individuálních odpovědností členů týmu v jednotlivých fázích procesu Change Management. V modelu se používají písmenka R A C I.

Vysvětlení jednotlivých rolí:[22]

- **R = Responsible**
  Tato osoba vlastní danou aktivitu v procesu, je hlavním řešitel, koordinátorem dané aktivy.

- **A = Accountability**
  Platí pravidlo, že celkovou odpovědnost k danému procesu má pouze jedna osoba. Tato osoba je vlastníkem celého procesu, je odpovědná za celý proces, ale nemusí fyzicky vykonávat aktivity procesu.

- **C = Consulted**
  Osoba, která se podílí na řešení formou konzultace nebo schválení.

- **I = Informed**
  Osoba, která má být informována o průběhu činnosti nebo výsledném rozhodnutí.

[22] Více o této problematice: ITIL. Service Design: Organization for Service Design. 1. published. London: UK by TSO, 2007, s. 189. ISBN: 978 0 11 331047 0

Tabulka 10: Role a odpovědnosti procesu Change Management

	Schvalovatel změny	Change Coordinator	Implementátor změny	Kontrolér změny
Přidělení požadavku na změnu řešitelskému týmu	**A**	**R**	**I**	**I**
Zadání požadavku na změnu	**R**	**I**	**I**	**I**
Vyhodnocení dopadů	**R**	**C**	**C**	**I**
Stanovení kategorie změny	**R**	**C**	**C**	**I**
Schválení nebo zamítnutí změny	**R**	**C**	**C**	**I**
Implementace změny	**I**	**C**	**R**	**I**
Kontrola implementace změny	**I**	**I**	**I**	**R**
Uzavření změny	**R**	**C**	**I**	**I**

Zdroj: autorka práce (vytvořeno na základě principů vycházejících z odborné literatury ITIL)

1.3.5 Role v procesu Change Management

Měla by zůstat zachována navrhovaná separace rolí v jednotlivých řešitelských týmech. Sloučením rolí mohou nastat rizika plynoucí z tohoto sloučení (vykonávání procesu a kontrola správnosti průběhu vykonávání procesu).

Change Coordinator

Change Coordinator je prvním vstupem do procesu Change Management. [23]

Mezi hlavní odpovědnosti Change Coordinator(a) změny patři:

- zajištění, že všechny změny jsou vhodně plánovány a prodiskutovány;
- přezkoumání návrhu změny z hlediska kvality informací a úplnosti, a zda jsou tyto v souladu s předpisy;
- zajišťuje, že je u změny uvedená správná priorita a jsou přiřazeny dopady změny;
- sleduje a eviduje životní cyklus změny a zároveň zajišťuje komunikace mezi jednotlivými subjekty, kterých se změna týká, nebo provedení změny spadá do jejich kompetence;
- zařizuje a účastní se všech meetingů ohledně prováděné změny;
- má odpovědnost za eskalaci a reportování výjimek vlastníkovi procesu Change Management;
- je odpovědný za koordinaci, konsolidaci procesu požadavku na změnu a za monitorování harmonogramu změn.

Implementátor změny

Implementátor změny má celkovou odpovědnost za pochopení návrhu na změnu, za dokumentování důsledků změny v IT prostředí, za implementaci samotné změny.

[23] Více o této problematice: ITIL. *Service Transition: Change Advisory Board.* 1. published. London: UK by TSO, 2007, s. 58-59. ISBN: 978 0 11 331048 7

Spolu s koordinátorem předkládají změnu ke schválení Schvalovateli/(ům) změny.
Mezi hlavní odpovědnosti Implementátora změny patři:

- posuzuje rizika a dopady změny a určuje vhodnou výši rizika;
- zajišťuje, že požadavek na změnu je úplný, s přesnými informacemi, které jsou dostačující k provedení rozhodnutí;
- komunikuje záměr změny se všemi potencionálními stranami, které mohou být změnou ovlivněny;

Kontrolor změny

Kontrolor změny je zodpovědný za harmonogram a dohled nad všemi změnami, které jsou implementovány do prostředí IT a do infrastruktury za účelem minimalizace rizikových dopadů změn. Je odpovědný za kontrolu implementace změny a to, zda implementace proběhla v dostatečné kvalitě.

Role Schvalovatele/ů změny

Je tvořen jedním schvalovatelem nebo ve výjimečných případech týmem, který je utvořen z odborníků pocházejících z řad IT Managementu, expertů, členů oddělení, dodavatelů a externích konzultantů. Tento tým je řízen Change koordinátorem.

Náplní této rady je plánovat a monitorovat požadavek na změnu a změny zaváděné do prostředí IT.

Odpovědnosti Schvalovatele změny je zajistit, že u každé změny:

- byly předloženy požadované informace;
- existuje bezpečnostní či funkční důvod implementace změny;
- existuje funkční plán změny;
- existuje funkční plán zotavení tj. návratu do původního stavu, který byl před změnou;
- bylo provedeno technické hodnocení změny;
- bylo provedeno hodnocení rizik změny;

- byl vytvořen komunikační plán mezi IT a uživatel;
- byly prodiskutovány možné dopady změny;
- byla provedena revize po instalaci, k zajištění řádné a úspěšné implementace.

1.3.6 Měření výkonnosti procesu Change Management

Cílem sledování, vyhodnocování a reportování Change Management procesu je zajistit:[24]

- snížení počtu neoprávněných změn;
- snížení počtu urgentních (nouzových) změn;
- snížení počtu Incidentů způsobených nesprávně provedenou změnou;

Pro zvýšení efektivity a účinnosti procesu jsou sledovány následující parametry:

- počet změn implementovaných během daného období členěných dle kategorií;
- počet změn realizovaných v plánovaném termínu za dané období;
- počet změn realizovaných později proti původně plánovanému termínu za dané období;
- procento úspěšně implementovaných změn, které naplnily všechny požadavky a očekávání od realizované změny;
- počet Incidentů způsobených implementovanou změnou za dané období.

[24]Více o této problematice: ITIL. *Service Transition: Key performance indicators and metrics.* 1. published. London: UK by TSO, 2007, s. 64. ISBN: 978 0 11 331048 7

2 NÁVRH IMPLEMENTACE NÁSTROJE DLP

Tato kapitola popisuje návrh implementace zajištění pro-aktivního řízení potencionálních rizik a následných dopadů plynoucích z úniku citlivých informací a dat mimo společnost People & Job prostřednictvím technologie Data Loss Prevention dále jen DLP.

Cílem je implementovat takovou technologii, která bude mít přímý vliv na uvědomění uživatelů o úmyslném či neúmyslném odesílání citlivých informací. Citlivé informace byly definovány v bakalářské práci autorky. Dále pak zajistit uživateli zpětnou vazbu o odesílání těchto citlivých informací.

2.1 Strategická hodnota informace aneb právní aspekty sledování zaměstnanců v oblasti ochrany informací

Každá společnost se potýká ve své praxi s rizikem, které představují její vlastní zaměstnanci pracující s informacemi společnosti a pohybující se na internetu. Monitorování firemní komunikace zaměstnanců, zejména elektronické komunikace je jednou z možností, jak chránit citlivá data, která společnost vlastní. Pravidla nakládání s citlivými informacemi v pracovní sféře se dotýká hlavně těchto zákonů:

- zákon č. 262/2006 Sb., Zákoník práce a s ním související pracovní řád a pokyny zaměstnavatele;
- zákon č. 513/1991 Sb., Obchodní zákoník;
- zákon č. 40/2009 Sb., Trestní zákoník.

Tyto zákony pravidla:

- určují;
- mohou být s odkazem na ně určena;
- chrání a v případě porušení pravidel umožňují stanovit sankce.

Podle § 301 Zákoníku práce jsou zaměstnanci povinni:

a) *„pracovat řádně podle svých sil, znalostí a schopností, plnit pokyny nadřízených vydané v souladu s právními předpisy a spolupracovat s ostatními zaměstnanci,*
c) *dodržovat právní předpisy vztahující se k práci jimi vykonávané;*
dodržovat ostatní předpisy vztahující se k práci jimi vykonávané, pokud s nimi byli řádně seznámeni,
d) *řádně hospodařit s prostředky svěřenými jim zaměstnavatelem a střežit a ochraňovat majetek zaměstnavatele před poškozením, ztrátou a zneužitím a nejednat v rozporu s oprávněnými zájmy zaměstnavatele*.“[25]

Podle § 306 Zákoníku práce je:

1) *„Pracovní řád zvláštním druhem vnitřního předpisu; rozvádí ustanovení tohoto zákona, popřípadě zvláštních právních předpisů podle zvláštních podmínek u zaměstnavatele, pokud jde o povinnosti zaměstnavatele a zaměstnance vyplývající z pracovněprávních vztahů.“*[26]

Zákon umožňuje firmám upravit své právní vztahy k zaměstnancům a to jednak v pracovní smlouvě, ale také formou vnitřních pracovněprávních předpisů. Vnitřními pracovněprávními předpisy se rozumí:

- pracovní řád, který upravuje vztahy k zaměstnancům komplexně;
- dílčí směrnice např.: IT směrnice, směrnice o ochraně obchodního tajemství specifikující definici tajemství, kategorizaci důvěrných informací aj.

[25] SCHMIED, Zdeněk., JAKUBKA, Jaroslav. *Zákoník práce 2012 s výkladem: Právní stav k 1.1.2012*. 13. vyd. Praha: Grada. 2012, s. 79-80. ISBN: 978-80-247-4031-7
[26] Tamtéž: SCHMIED, Zdeněk., JAKUBKA, Jaroslav. *Zákoník práce 2012 s výkladem: Právní stav k 1.1.2012*. s. 81

Výhodou těchto vnitřních předpisů je možnost jejich jednostranné změny ze strany zaměstnavatele, avšak za předpokladu, že jakoukoli změnu předpisů musí společnost zaměstnancům oznámit a musí umět doložit, že zaměstnanci byli se změnou seznámeni.

Podle zákoníku práce zaměstnavatel nesmí bez vážného důvodu, spočívajícího ve zvláštní povaze činnosti zaměstnavatele, narušovat soukromí zaměstnance na pracovištích tím, že podrobuje zaměstnance otevřenému či skrytému sledování. Tento výklad je také podpořen Listinou základních práv a svobod.

Podle článku 7 Listiny základních práv a svobod:

„*Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem“* [27]

Podle článku 13 Listiny základních práv a svobod:

„Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.“[28]

Na druhé straně ale stojí základní právo zaměstnavatele na ochranu jeho majetku a jeho právo na podnikání.

Podle § 17 Obchodního zákoníku:

„Předmětem práv náležejících k podniku je i obchodní tajemství. Obchodní tajemství tvoří veškeré skutečnosti obchodní, výrobní, či technické povahy související s podnikem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu, nejsou v příslušných obchodních kruzích běžně dostupné, mají být podle vůle podnikatele utajeny a podnikatel odpovídajícím způsobem jejich utajení zajišťuje.“[29]

---

[27] *LISTINA ZÁKLADNÍCH PRÁV A SVOBOD* [online]. [cit. 2013-07-16]. Dostupné z: http://www.psp.ct/docs/laws/listina.html
[28] *LISTINA ZÁKLADNÍCH PRÁV A SVOBOD* [online]. [cit. 2013-07-16]. Dostupné z: http://www.psp.ct/docs/laws/listina.html
[29] KOBLIHA, Ivan. et al. *Obchodní zákoník: úplný text zákona s komentářem: Podle stavu k 1.4.2006.* Praha: Linde, 2006, s. 41. ISBN: 80-7201-564-8

Podle §18 Obchodního zákoníku:

„Podnikatel provozující podnik, na který se obchodní tajemství vztahuje, má výlučné právo tímto tajemstvím nakládat, zejména udělit svolení k jeho užití a stanovit podmínky takového užití.“[30]

Podle § 51 Obchodního zákoníku:

„Porušováním obchodního tajemství je jednání, jímž jednající jiné osobě neoprávněně sdělí, zpřístupní, pro sebe nebo pro jiného využije obchodní tajemství (§17), které může být využito v soutěži a o němž se dověděl.“[31]

Z výše uvedeného vyplývá, že zákon určitý druh kontroly zaměstnavateli umožňuje. Klíčovým právem pro zaměstnavatele, které by mělo dodržování povinností stanovených vnitřními předpisy kontrolovat, je právo na přiměřený monitoring zaměstnance. Za přiměřenou kontrolu může být považováno sledování doby přístupů na internet a návštěvnost stránek v pracovní době, ale také e-mail komunikace, avšak za předpokladu, že se jedná o firemní způsob komunikace se zaměstnanci či zákazníky. V okamžiku, kdy by email komunikace měla mít soukromý charakter, je zaměstnavatel povinen kontrolu takové komunikace okamžitě ukončit a nijak nezneužít získané informace.

Společnost by neměla podceňovat úpravu vnitřních firemních předpisů. Vnitřní předpisy plní z jedné strany funkci preventivní tím, že zaměstnanci jsou srozuměni s konkrétními povinnostmi. Z druhé strany plní funkci významu, kdy zaměstnavatel, v případě porušení povinností zaměstnance, se o konkrétní úpravu vnitřního předpisu opře a vyvodí sankce z porušení povinností vyplývající. Stejně tak jsou vnitřní předpisy důkazně podstatné při soudním řízení o náhradě škody či ve sporu o neplatnost skončení pracovněprávního vztahu.

---

[30] KOBLIHA, Ivan. et al. *Obchodní zákoník: úplný text zákona s komentářem: Podle stavu k 1.4.2006. Praha: Linde, 2006, s. 41. ISBN: 80-7201-564-8*

[31] Tamtéž: KOBLIHA, Ivan. et al. *Obchodní zákoník: úplný text zákona s komentářem: Podle stavu k 1.4.2006. s. 121*

Podle § 221 Trestního zákoníku:

„Porušení povinnosti při správě cizího majetku z nedbalosti

1) *Kdo z hrubé nedbalosti poruší podle zákona mu uloženou nebo smluvně převzatou důležitou povinnost při opatrování nebo správě cizího majetku, a tím jinému způsobí značnou škodu, bude potrestán odnětím svobody až na šest měsíců nebo zákazem činnosti.“*[32]

Podle § 232 Trestního zákoníku:

„Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

a) Kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté

b) Data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo

c) Učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat, a tím způsobí na cizím majetku značnou škodu, bude potrestán odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.“[33]

[32] NAKLADATELSTVÍ SAGIT. *Úplné znění Trestní předpisy číslo 768: Podle stavu k 1.1.2010*. Ostrava: Sagit, 2010, s. 61. ISBN: 978-80-7208-782-2

[33] Tamtéž: NAKLADATELSTVÍ SAGIT. *Úplné znění Trestní předpisy číslo 768: Podle stavu k 1.1.2010,* s. 63-64.

2.2 Popis implementace DLP

Implementací technologie DLP se docílí efektivního propojení technologického s procesními celky a zabezpečení vybrané fáze životního cyklu informací. Implementované řešení zajistí zásadní posun v pro-aktivním řízení potenciálních rizik a následných dopadů plynoucích z úniku citlivých informací.

Oblasti klasifikace a ohodnocení informačních aktiv jsou součástí systému řízení bezpečnosti informací společnosti People & Job, s.r.o..[34] Implementované řešení vychází z těchto údajů a na základě již dříve realizované analýzy rizik[35] budou implementovány bezpečnostní mechanismy pro ochranu informačních aktiv s vysokou hodnotou.

Před započetím samotné implementace musí být pochopeny následující tři základní otázky:

1. Kdo je vlastníkem a správcem citlivých informací a dat?
2. Jaké jsou citlivé informace a data společnosti?
3. Kde se citlivé informace a data vyskytují a používají?

[34] Více o této problematice: GOLLOVÁ, Marta. *Budování systému bezpečnosti informací společnosti a zvyšování bezpečnostního povědomí zaměstnanců.* Praha, 2012. Bakalářská práce. UJAK, Katedra Andragogiky. Vedoucí práce: Jiří Víšek

[35] Více In: GOLLOVÁ, Marta. *Budování systému bezpečnosti informací společnosti a zvyšování bezpečnostního povědomí zaměstnanců.* Praha, 2012, s. 31-35. Bakalářská práce. UJAK, Katedra Andragogiky. Vedoucí práce: Jiří Víšek

2.2.1 Společné příčiny ztráty dat

Nejčastější příčiny ztráty dat, dle zkušeností z fungování společnosti, jsou obvykle neúmyslné způsobené chybami uživatelů.

Příčiny ztráty dat lze rozdělit do následujících oblastí:

- Lidský faktor:
    - nedostatečná zodpovědnost uživatelů;
    - nedostatečné pochopení obsahu a souvislostí odesílaných dat;
    - uživatelé neodpovídají za své činy.
- Procesy:
    - nedefinované procedury výměny dat;
    - nedostatečné sledování oběhu dat.
- Technologie:
    - nedostatečné zabezpečení vzdáleného připojení do společnosti;
    - nedostatečné pochopení obsahu a souvislostí odesílaných dat;
    - nezabezpečené komunikační kanály.

2.2.2 Řešení rizik plynoucích z úniku dat a informací

Pro efektivní ošetření rizik plynoucích ze ztráty dat je nutné definovat jasné firemní cíle pro implementaci technologie DLP.

Tyto cíle musí zahrnovat následující oblasti:

- zabránění úmyslnému či neúmyslnému zveřejnění citlivých dat směrem k neoprávněným třetím stranám;
- ochrana dat klientů a firemní reputace;

- ochrana osobních údajů a duševního vlastnictví;
- snížení rizika na dodržování shody s regulatorními požadavky.

Řízení rizik úniku dat prostřednictvím technologie DLP musí být zaměřeno na ochranu nejcitlivějších údajů, kterými společnost disponuje.

Efektivní implementace technologie DLP vyžaduje znalost o následujících tématech:

- jaká data společnost vlastní;
- jaká je hodnota těchto dat;
- jaké máme zákonné povinnosti při ochraně dat;
- kde jsou naše data uložena;
- kdo má k datům přistup;
- kam jsou data zasílána;
- jak jsou naše data v současnosti chráněna;
- jaké jsou nedostatky při ochraně dat;
- jak reagovat na bezpečnostní Incidenty způsobené únikem dat.

Odpovědi a znalosti o výše uvedených tématech jsou zapracovány v bakalářské práce autorky. Z tohoto důvodu není nutné, aby byly v této práci podrobněji rozebírány.

2.2.3 Postup implementace DLP

Postup implementace vychází z technické dokumentace technologie RSA DLP, která popisuje technické možnosti implementované technologie, včetně doporučení pro implementaci této technologie.[36]

Implementaci technologie DLP je možné rozčlenit následujícím způsobem:

- Integrační vrstva:
    - zajišťuje efektivní integraci nového řešení do stávajících procesů a mechanismů informační bezpečnosti.
- Procesní a procedurální vrstva:
    - zajišťuje translaci požadavků na ochranu informačních aktiv z relevantních organizačních zdrojů do politiky řešení a identifikuje (upravuje) procedury reakce na incidenty.
- Technologická vrstva:
    - technologické řešení zajišťující detekci incidentů a vynucení definované politiky bezpečnosti ochrany údajů.

V rámci přípravné fáze jsou shromážděny informace potřebné k iniciaci technologie, sestavení prvotních konfiguračních politik a spuštění testovacího provozu.

[36] Dostupnost technické dokumentace a více o této problematice: RSA. *RSA Customer Profiles: Data Loss Prevention (DLP).* [online]. [cit. 2013-04-06]. Dostupné z: http://www.emc.com/collateral/customer-profiles/h12158-rsa-dlp-cp.pdf

2.3 Popis vstupních parametrů, proces a popis reakce na bezpečnostní incidenty

Na základě požadavků společnosti a možnostech implementované technologie RSA DLP a technické dokumentace technologie DLP byla stanovena základní sada parametrů pro identifikaci informačních aktiv, které budou touto technologií sledovány.

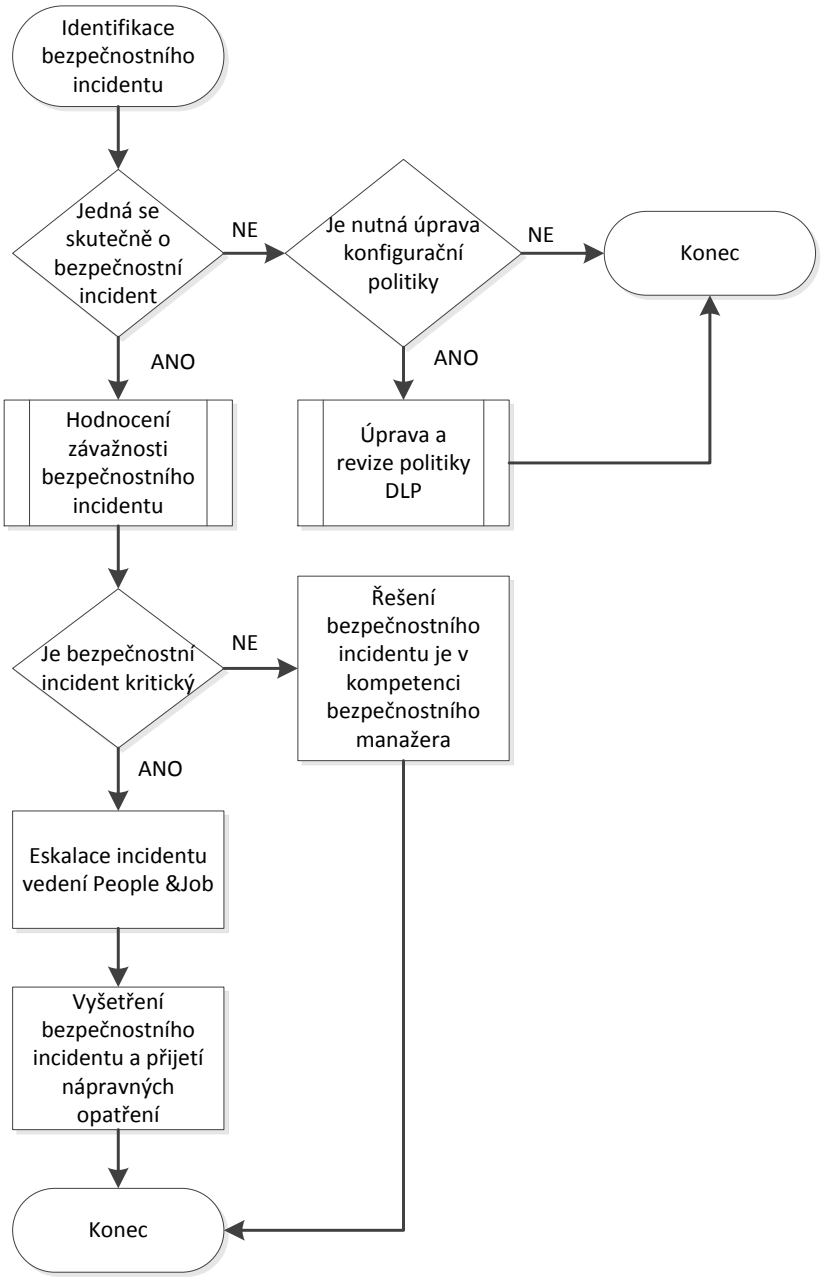
Tabulka 11: Základní možnosti DLP

	Technologické řešení
Detekce typů dat	
Fragmenty databází	Technologie automaticky detekuje komunikaci na databázové úrovni (SQL) a dále je registruje v rámci DLP workflow. Přidělené výkonné role potom mohou vytvářet pravidla v konfiguračních politikách.
Fragmenty Souborů	Technologie detekuje souborové typy na bázi „otisků prstů – fingerprint“. Ty dokážou s určitou přesností určit typ přenášeného souboru v rámci datové komunikace. Tato detekce rovněž pracuje v předávaných archivech. Jednotlivé typy souborů je možné následně zařadit do konfiguračních politik a uzpůsobit jim reakční workflow.
Vyjmenované soubory	V rámci vytváření konfigurační politiky je možné specifikovat typy souborů a následně pro ně vytvářet specifické reakční kroky. Technologie zároveň umožňuje vytvářet otisky prstů z již existujících dokumentů. Jejich pohyb v rámci firemní komunikace může být následně detekován.
Klíčová slova v dokumentech	Technologie umožňuje vyhledávat klíčová slova v dokumentech dle dodaných slovníků (často užívané výrazy v dokumentech s vyšším profilem ochrany), případně je možné definovat vlastní slovníky, které jsou upraveny přímo pro užití v organizaci.
Data definovaná jako Regular Expression	V rámci definování pravidel konfiguračních politik pro detekci a následnou reakci je možné vytvářet „Regular Expression“ výrazy dle tržního standardu.
Metadata souborů	Souborová metadata je možné zahrnout do detekčních konfiguračních politik jako možné parametry pro identifikaci a sledování pohybu dokumentů.

Zdroj: autorka práce (vytvořeno podle technické dokumentace RSA: *RSA. Data Loss Prevention (DLP).* [online]. [cit. 2013-04-06]. Dostupné z: http://www.emc.com/security/rsa-data-loss-prevention.htm-resources

V rámci implementace je nutné definovat proces reakce na vzniklé bezpečnostní incidenty. Celý proces reakce na vzniklé bezpečnostní incidenty přehledně zobrazuje následující diagram.

Diagram 4: Proces reakce na vzniklé bezpečnostní Incidenty



Zdroj: autorka práce

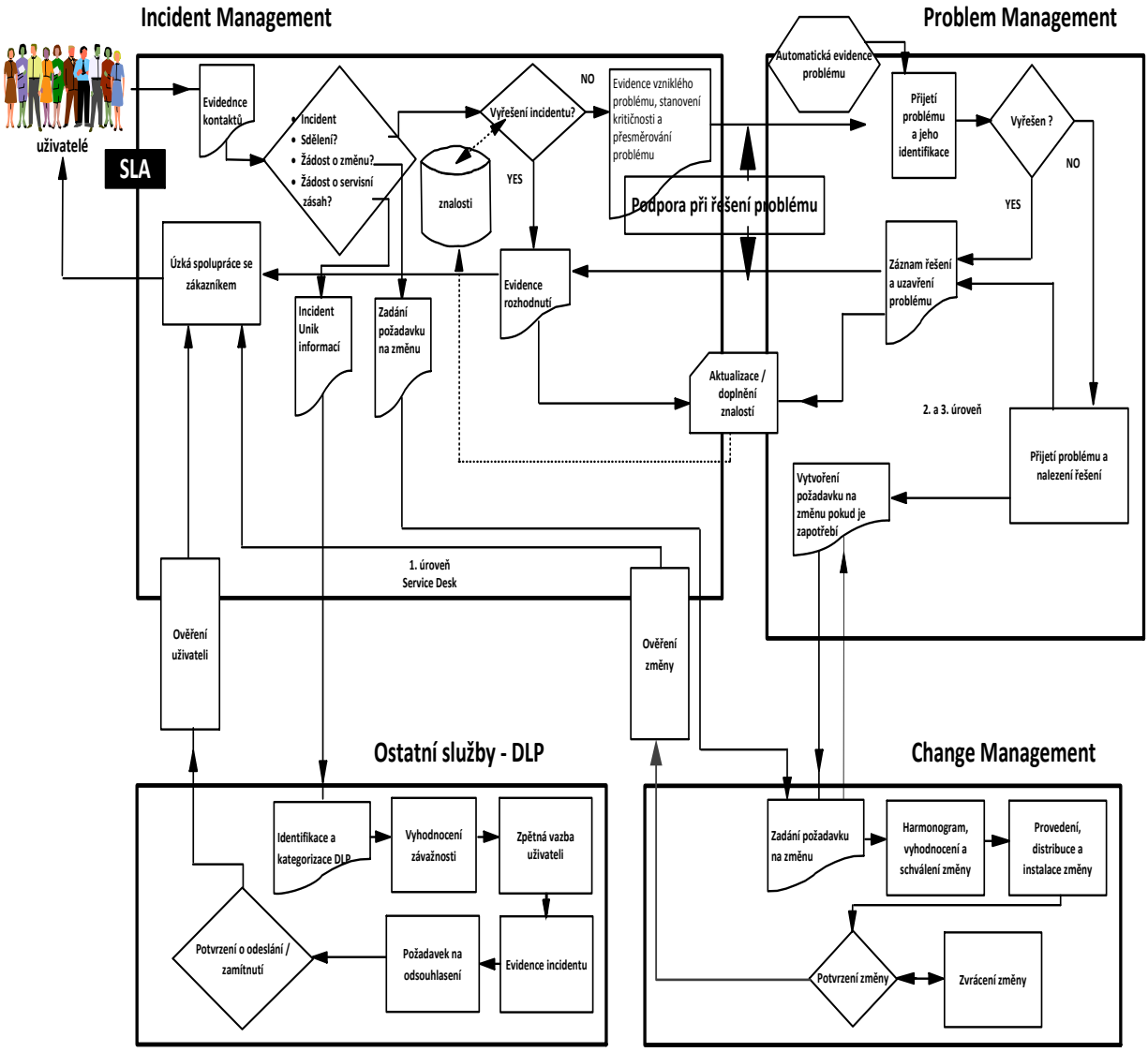
Popis procesu reakce na bezpečnostní incidenty:

- Bezpečnostní manažer na základě reportů z implementované technologie DLP identifikuje potencionální vznik bezpečnostního Incidentu;
- Bezpečnostní manažer provede prvotní hodnocení, jedná-li se skutečně o bezpečnostní incident;
    - jestli-že se nejedná o bezpečnostní incident, provede hodnocení nutnosti úpravy konfiguračních politik DLP;
    - jestli-že se jedná o bezpečnostní incident, pokračuje hodnocením závažnosti bezpečnostního incidentu.
- Úprava a revize politiky DLP:
    - Bezpečnostní manažer, společně s Bezpečnostním poradcem provede úpravu konfiguračních politik implementované technologie DLP.
- Hodnocení závažnosti bezpečnostních incidentů:
    - kritičnost Incidentu hodnocena jako **nízká (low)**, řešení bezpečnostního incidentu je plně v kompetenci Bezpečnostního manažera, který rozhodne o způsobu řešení incidentu a jeho následné eskalaci;
    - kritičnost incidentu hodnocena jako **střední (medium),** řešení bezpečnostního incidentu je plně v kompetenci Bezpečnostního manažera, který rozhodne o způsobu řešení incidentu a jeho následné eskalaci;
    - kritičnost incidentu hodnocena jako **kritická (critical)**, Bezpečnostní manažer je povinen eskalovat bezpečnostní incident vedení společnosti. Společně s pracovníkem vedení rozhodne o způsobu a postupu řešení bezpečnostního incidentu.
- Jednatel společnosti u kritických incidentů určí odpovědné osoby, odpovídající za vyšetření bezpečnostního incidentu. Dále zajistí a zkontroluje přijetí příslušných nápravných opatření.
- Bezpečnostní manažer aktivně spolupracuje s bezpečnostním fórem a pracovní skupinou informační bezpečnosti při řešení jednotlivých bezpečnostních incidentů.

2.4 Vztah mezi jednotlivými interními procesy a jejich interakce

Následující diagram názorně popisuje vztah mezi jednotlivými interními procesy, které byly popsány v kapitole 1 a 2 této práce a jejich vzájemnou interakci.

Diagram 5: Vzájemné vazby mezi popisovanými interními procesy



Zdroj: autorka práce (vytvořeno na základě definovaných procesů v kapitole 1 a 2)

Diagram 5 názorně zachycuje vztah mezi jednotlivými procesy a to, jak se tyto procesy vzájemně ovlivňují, přičemž Incident Management má za úkol vyřešit co nejrychlejší obnovu IT služeb. V okamžiku, kdy se stejný incident opakuje či není známo řešení vzniklého incidentu, přebírá toto řešení proces Problem Management. Po nalezení řešení je tento problém většinou řešen změnou v procesu Change Management a zároveň jsou aktualizovány záznamy v Configuration Management Database. Digram rovněž znázorňuje vazbu implementované DLP technologie na definované procesy z kapitoly 1 této práce.

3 FIREMNÍ KULTURA

Ani ve firmě, která zaměstnává odborníky v dané oblasti a zajišťuje špičkovou technologii, není zaručeno, že prováděné činnosti, implementované procesy a technologie přinesou očekávaný přínos, pokud není věnována pozornost komplexu faktorů utvářejících firemní kulturu. Vrcholový management nesmí zapomínat na význam firemní kultury, která pokud je podceňována, může zmařit mnohé z dobře naplánovaných záměrů.

Každá společnost má svou vlastní firemní kulturu, která v sobě zahrnuje soubor hmotných a duchovních hodnot vytvářených činností lidí/zaměstnanců.

Firemní kultura ovlivňuje nejen vnitro-firemní vztahy mezi zaměstnanci, jejich systém komunikace, myšlení, zvyklostí, rituálů, postojů a uznávaných hodnot, ale také způsob prezentace společnosti ve vztahu k vnějšímu okolí. Společnost, která je na trhu konkurenceschopná, je vnějším okolím, ale i samotnými zaměstnanci vnímána jako perspektivní a má z hlediska utváření firemní kultury velkou výhodu.

Definic firemní kultury existuje v odborné literatuře nespočet.

„*Kultura společnosti neboli podniková kultura představuje soustavu hodnot, norem, přesvědčení, postojů a domněnek, která sice nebyla nikde výslovně zformulována, ale určuje způsob chování a jednání lidí a způsoby vykonávání práce.*“[37]

„Kulturu společnosti lze charakterizovat z hlediska hodnot, norem a artefaktů (lidských výtvorů) a stylu vedení, nebo řízení.“[38]

Mezi viditelné artefakty materiální povahy, tak zvané hmatatelné patří architektura budov, propagační materiály, vybavení společnosti, produkty, nebo služby společností vytvářené. Mezi artefakty nemateriální povahy patří zvyky, rituály, firemní řeč, kterou může tvořit odborný slang a různá slovní spojení, nebo styl oblékání

[37] AMSTRONG, Michael. *Řízení lidských zdrojů. Nejnovější trendy a postupy*. 10. vyd. Praha: Grada, 2010, s. 257. ISBN: 978-80-247-1407-3

[38] Tamtéž: AMSTRONG, Michael. *Řízení lidských zdrojů. Nejnovější trendy a postupy*, s. 259.

Dále je firemní kultura tvořena historií společnosti, zejména předávanými informacemi o historii společnosti a udržováním některých tradic a rituálů.

Firemní kultura je vlastní jen členům dané společnosti, kteří hodnoty a normy, vytvářené a uznávané vrcholovým managementem, přijmou za své a uznávají je.

Jak uvádí Šigut, *„Podniková kultura se projevuje v myšlenkových procesech a určuje lidské myšlení, cítění, chování v podniku. Z toho vyplývá, že každý podnik má svoji specifickou podnikovou kulturu.“* [39]

Kultura společnosti je těžko uchopitelným fenoménem. Podle Lukášové, Nového a kol., by měl ve firmách existovat fyzicky existující dokument, který obsahuje explicitně formulované parametry žádoucí kultury. Jde například o etický kodex, kodex zaměstnance společnosti nebo dokonce některé pracovní normy ISO.[40] Existence těchto dokumentů je významným pomocníkem při prosazování žádoucí kultury do běžného pracovního života společnosti.

„Normy ISO/IEC 27xxx Informační bezpečnost, byly ve společnosti People & Job, zavedeny v rámci bakalářské práce autorky, kdy přínosy pro společnost People & Job byly spatřeny zejména v oblasti, "…*zavedení systémového a systematického přístupu v administrativních procesech. Trvalé monitorování a následné zlepšování systému řízení bezpečnosti informací. Zvýšení povědomí a odpovědnosti zaměstnanců při práci s citlivými daty. Začlenění informační bezpečnosti do firemní kultury společnosti.“*[41] (Příloha C „Politika kvality a bezpečnosti informací společnosti People & Job“).

[39] ŠIGUT, Zdenek. *Firemní kultura a lidské zdroje*. Praha: ASPI Publishing, 2004, s. 11. ISBN: 80-7357-046-7
[40] LUKÁŠOVÁ, Růžena., NOVÝ, Ivan. a kol. *Organizační kultura*. *Od sdílených hodnot k vyšší výkonnosti podniku.* Praha: Grada, 2004, s. 116. ISBN: 80-247-0648-2
[41] Poznámka autorky a více o této problematice: GOLLOVÁ, Marta. *Budování systému bezpečnosti informací společnosti a zvyšování bezpečnostního povědomí zaměstnanců.* Praha, 2012, s. 64. Bakalářská práce. UJAK, Katedra Andragogiky. Vedoucí práce: Jiří Víšek

Podle Šiguta, by měla být firemní kultura čitelná nejen pro zaměstnance dané společnosti, ale také pro vnější subjekty, kteří s firmou spolupracují. Zaměstnanci vědí, co jim je tolerováno. Vnější subjekty vědí, které kulturní normy společnost uznává a co by nikdy nedovolila a netolerovala. Díky stabilní firemní kultuře je řada věcí jasnějších a srozumitelnějších. Stabilní firemní kultura tak vytváří předpoklad úspěšnosti společnosti.[42]

Jak dále uvádí Šigut, *„…kultura podniku je také silně ovlivněna hlavním předmětem činnosti, užívanými technologiemi a technikou. Jinou kulturu si pravděpodobně bude vytvářet společnost zabývající se obchodní činností, jinou kulturu bude mít podnik zabývající se strojní výrobou.“*[43]

[42] Více o této problematice: ŠIGUT, Zdenek. *Firemní kultura a lidské zdroje*. Praha: ASPI Publishing, 2004, s. 18. ISBN: 80-7357-046-7
[43] Tamtéž: ŠIGUT, Zdenek. *Firemní kultura a lidské zdroje*, s. 18.

3.1 Znaky a formování firemní kultury

Znaky firemní kultury, na kterých se shodují autoři zabývající se firemní kulturou, jsou převážně následující:[44]

- vzniká, rozvíjí se a zaniká v určitém čase a na určitém místě;
- představuje společné hodnoty a normy;
- její obsah je upravován podle aktuálních firemních cílů;
- je zprostředkována v adaptačním procesu, kdy nově příchozím zaměstnancům osvětluje, jak jednat v souladu s kulturními tradicemi společnosti.

Firemní kultura značně ovlivňuje firemní procesy. Nacházíme ji v různých oblastech života společnosti.

Je formována procesy, které jsou:

- Na kulturu přímo zaměřené:
    - vytvoření etického kodexu společnosti (Příloha B „Etický kodex“);
    - vytvoření strategií, politik (Příloha C „Politika kvality a bezpečnosti….“), vizí a cílů společnosti;
    - vytvoření kodexu chování zaměstnance.

- Působením nepřímých procesů, kterými jsou děje a aktivity všech zaměstnanců společnosti:
    - komunikace se zaměstnanci;
    - koncept „Učící se společnosti“;
    - přidělování odpovědnosti, pravomocí aj.

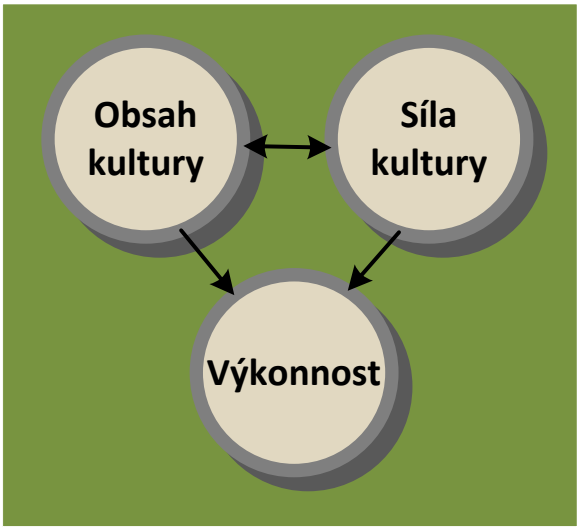
[44]Více o této problematice: NOVÝ, Ivan., BEDRNOVÁ, Eva. In: ŠIGUT, Zdenek. *Firemní kultura a lidské zdroje*. Praha: ASPI Publishing, 2004, s. 15-16. ISBN: 80-7357-046-7

3.2 Vliv obsahu a síly kultury na výkonnost společnosti

Obsah kultury představuje základní předpoklady, hodnoty a normy chování sdílené v konkrétním sociálním celku a navenek manifestované chováním a artefakty. Síla kultury vyjadřuje, nakolik jsou dané předpoklady, hodnoty, normy a vzorce chování v daném sociálním celku sdíleny.

Obsah kultury je upravován v souladu s aktuálními firemními cíli. Obsah a síla firemní kultury, ve vzájemné kombinaci, má značný vliv na výkonnost společnosti, kdy její účinek je dvojí. Podle Lukášové, Nového a kol., jednak pracovníky aktivuje a to v závislosti na konkrétních hodnotách a normách chování, jednak pracovníky směruje k naplňování hodnot a cílů společnosti.[45]

Obrázek 1: Vliv organizační kultury na fungování a výkonnost společnosti



Zdroj: Lukášová, Nový a kolektiv, *Organizační kultura*, s. 57

[45]Více o této problematice: LUKÁŠOVÁ, Růžena., NOVÝ, Ivan. a kol. *Organizační kultura. Od sdílených hodnot a cílů k vyšší výkonnosti podniku.* Praha: Grada, 2004, s. 53. ISBN: 80-247-0648-2

Výkonnost společnosti ovlivňuje funkce angažovanosti a participace zaměstnanců společnosti. Pokud je angažovanost a participace zaměstnanců obsahem kultury, dá se předpokládat, že zaměstnanci se budou chovat následovně:

- *„aktivně, iniciativně, angažovaně ve prospěch cílů společnosti;*
- *samostatně a operativně řeší vzniklé problémy a přijímají odpovědnost za svou práci;*
- *vůči firmě se chovají loajálně*.“[46]

Silná kultura se vyznačuje vysokou mírou sdílení a respektování hodnot a norem v rámci společnosti.

Výhoda silné kultury spočívá především v tom, že:[47]

- **Silná kultura vytváří soulad ve vnímání pracovníků:**
    - to usnadňuje komunikaci a redukuje konflikty mezi zaměstnanci uvnitř společnosti;
    - zaměstnanci mluví stejným jazykem a používaným pojmům přikládají stejný obsah;
    - shodují se v tom, co je důležité a nedůležité;
    - pozitivním důsledkem je urychlení rozhodování a realizace přijatých rozhodnutí.

- **Silná kultura usměrňuje chování zaměstnanců:**
    - zaměstnanci sdílejí společné hodnoty a normy;
    - díky tomu směřují stejným směrem a dodržují určité způsoby chování;
    - zaměstnanci pociťují sounáležitost s firmou, jsou k ní loajální a mají pozitivní postoj ke spolupráci.

[46] LUKÁŠOVÁ, Růžena., NOVÝ, Ivan. a kol. *Organizační kultura. Od sdílených hodnot a cílů k vyšší výkonnosti podniku.* Praha: Grada, 2004, s. 53. ISBN: 80-247-0648-2
[47] Tamtéž. Více o této problematice: LUKÁŠOVÁ, Růžena., NOVÝ, Ivan. a kol. *Organizační kultura. Od sdílených hodnot a cílů k vyšší výkonnosti podniku,* s. 52.

Znaky, kterými se vyznačuje silná kultura a na kterých se s Šigutem shoduji, jsou: [48]

- **Jasnost a zřetelnost:**
    - management musí dávat zaměstnancům zřetelně najevo jaké jednání je od zaměstnanců požadované a jaké aktivity jsou nutné, žádoucí a akceptovatelné a které jsou zcela vyloučené a nepřijatelné;
    - toto lze splnit pouze za předpokladu, že firemní kultura se opírá o rozsáhlý soubor hodnot, standardů a symbolů, které utvářejí vnitřní logicky uspořádaný celek a jsou snadno sdělitelné všem pracovníkům příslušné společnosti.

- **Rozšířenost:**
    - zaměstnanci musí být s jednotlivými prvky dostatečně seznámeni a musejí se s nimi setkávat v každé situaci, v každém okamžiku a na každém místě;

- **Zakotvenost:**
    - teprve tehdy, když se stane firemní kultura nedílnou součástí každodenního jednání většiny, nejlépe však všech zaměstnanců, je možné hovořit o tom, že je silná.

Silná firemní kultura se stává výrazným zdrojem soudržnosti společnosti a nezanedbatelným zdrojem motivace zaměstnanců.

[48] Více o této problematice: ŠIGUT, Zdenek. *Firemní kultura a lidské zdroje*. Praha: ASPI Publishing, 2004, s. 16. ISBN: 80-7357-046-7

3.3 Firemní kultura a lidské zdroje

Z hlediska lidských zdrojů existují podle Jiráska dva pojmy firemní kultury: *„První podniková kultura je soubor určitých metod, procedur, dovedností, jež se rozvíjejí na podkladě praxe a jimž se normálně inteligentní člověk může naučit. Druhá podniková kultura zahrnuje postojové, osobnostní a hodnotové schopnosti, jimž se nedá naučit knižním způsobem, např.: vstřícné chování, návyk na týmovou práci, osobní iniciativa, odpovědnost, loajalita, oddanost práci aj.“*[49]

Podle Šiguta, vystupuje v současné době podnik jako útvar kvalifikovaných lidí, kteří jsou sjednoceni ke společnému výkonu. Zaměstnanec již není pouhou pracovní silou, ale stává se členem pracovní skupiny se všemi nároky, odpovědnostmi, riziky a neúspěchy. Význam osobnosti zaměstnance vzrostl natolik, že si vynucuje změnu orientace a první podniková kultura by měla tvořit symbiózu s druhou podnikovou kulturou.[50]

Management by si měl být vědom významu firemní kultury a jejího využití pro ovlivňování postojů, hodnot, myšlení a jednání zaměstnanců. Kultura společnosti má přímý vliv na to, s čím se zaměstnanci ztotožňují a co naopak odmítají či ignorují. Bezprostředně ovlivňuje jednání a myšlení zaměstnanců a jejich ochotu angažovat se.

[49] JIRÁSEK, Jaroslav. In: ŠIGUT, Zdenek. *Firemní kultura a lidské zdroje*. Praha: ASPI Publishing, 2004, s. 52-53. ISBN: 80-7357-046-7

[50] Tamtéž. Více o této problematice: ŠIGUT, Zdenek. *Firemní kultura a lidské zdroje*, s. 52.

3.4 Leadership a jeho vliv na firemní kulturu

Firemní kulturu ovlivňuje chování managementu, jeho postoje a aktivity např.: k rizikům, k dosaženým úspěchům, k budoucnosti společnosti. Management svým chováním a vedením dává zaměstnancům jasně najevo, co je pro něj důležité a jaké má priority.

Management péčí o zaměstnance, o jejich pracovní podmínky, vhodným motivačním systémem a přímou komunikací sděluje zaměstnancům, co se od nich očekává a jaké chování bude oceňováno a tím významně ovlivňuje převládající postoje zaměstnanců. Postoje zaměstnanců následně ovlivňují to, jak odpovědně zaměstnanci plní své povinnosti a jak se v pracovním procesu angažují.

Jak uvádí Šigut: *„Management společnosti je tím, kdo vytváří podnikovou kulturu. Manažeři se sami musí chovat tak, aby byli pozitivním příkladem svým zaměstnancům, neboť jim jsou skutečně příkladem, ať již pozitivním, nebo negativním. Všechno to, co sdělují svému okolí, partnerům, investorům, tisku, zákazníkům, zaměstnancům atd. se odráží uvnitř společnosti, spoluutváří vlastní podnikovou kulturu.“*[51]

Management společnosti by měl působit na zaměstnance s cílem dosáhnout, aby jejich činnosti optimálním způsobem přispívaly k plnění cílů společnosti. Firemní leadership zahrnuje veškeré jednání vedoucích pracovníků a jejich angažovanost v procesech řízení lidských zdrojů.

Jak uvádí Amstrong: *„Leadership, schopnost vést, je inspirování lidí k tomu, aby vynaložili své nejlepší síly a schopnosti k dosažení žádoucích výsledků, získávání jejich oddanosti dané věci a jejich motivování k dosažení stanovených cílů.“*[52] .

Leadership zahrnuje širokou škálu činností, mezi které se řadí formulace strategií, vizí a politik, aktivní komunikování s podřízenými zaměstnanci, vytváření podmínek pro týmovou spolupráci, vytváření efektivních informačních toků, soustavné utváření postojů a motivace zaměstnanců. Všechny tyto činnosti vytvářejí ve společnosti příznivé psychosociální klima a pomáhají rozvíjet firemní kulturu.

Znaky efektivního leadershipu:

---

[51] ŠIGUT, Zdenek. *Firemní kultura a lidské zdroje*. Praha: ASPI Publishing, 2004, s. 34. ISBN: 80-7357-046-7
[52] AMSTRONG, Michael. *Management a leadership.* Praha: Grada, 2008, s. 28. ISBN: 978-80-247-2177-4

- zaměstnanci mají pocit, že jsou respektování, je jim důvěřováno a jsou předmětem zájmu svých vedoucích pracovníků.;
- management vytváří obraz, kam společnost směřuje a zajistí, aby každý zaměstnanec si byl vědom svého významu pro společnost, kdy zaměstnanec zřetelně „vidí“ svou roli, chápe své uplatnění v této společnosti a je si vědom faktu, jak přispívá a působí svou prací na konečný výsledek práce a hlavně, jaký z toho má/může mít prospěch.

Nedostatky v procesech řízení lidských zdrojů mají přímý dopad na chování zaměstnanců ve společnosti a tím negativně ovlivňují firemní kulturu.

Pokud se společnost ocitne v mimořádné situaci např. při řešení krize, která vyústí v organizační změny, dá se předpokládat, že vliv managementu na firemní kulturu bude ještě narůstat. Otázkou je, zda postoje v této mimořádné situaci ovlivní firemní kulturu pozitivně či negativně. Negativní vliv na vývoj firemní kultury nastane tehdy, pokud vznikne rozpor mezi tím, co bude management v krizové situaci proklamovat a kam budou skutečně směrovat jeho aktivity.

3.4.1 Styly vedení

Každý manažer uplatňuje určitý styl leadership(u), kterým spoluvytváří firemní kulturu.

Styl vedení:

- **Autoritativní/autokratický styl řízení** je založen spíše na přikazování a kontrole, jehož důsledkem bývá fakt, že je u zaměstnanců podceňována potřeba seberealizace a respektu. Tento styl řízení bude mít zřejmě za následek rozvoj pasivních postojů zaměstnanců, kdy každý jednotlivý zaměstnance bude dělat jen to, co mu je přikázáno a co musí.

- **Demokratický styl řízení** klade důraz na zapojování zaměstnanců do firemních procesů. Manažer vede se zaměstnanci otevřený dialog a povzbuzuje zaměstnance,

aby se podíleli na rozhodování a angažovali se v něm. Tento styl vedení může podporovat soulad individuálních zájmů zaměstnance s potřebami společnosti.

Další možné styly vedení a řízení podle Amstronga:[53]

- **Charismatický versus Necharismatický: Charismatičtí lídři** spoléhají na svou osobnost, jsou orientováni na úspěch a jsou dobří komunikátoři. **Necharismatičtí lídři** spoléhají na své znalosti a know-how. K problémům zaujímají analytický a chladný přistup.

- **Umožňovatel versus kontrolor**: **Umožňovatel** inspiruje své zaměstnance svou vizí o budoucnosti a podporuje je při plnění týmových cílů. **Kontrolor** manipuluje se zaměstnanci, aby získal jejich ochotu vyhovět.

- **Transakční versus Transformační**: **Transakční lídři** nabízejí za ochotu vyhovět peníze a jistotu práce. **Transformační lídři** motivují zaměstnance k tomu, aby usilovali o náročnější cíle.

Je otázkou, jaký styl vedení zaměstnanců je optimální. Styl vedení bude ovlivňovat povaha úkolu, okolnosti a v neposlední řadě samotní zaměstnanci, které je třeba vést. Z tohoto důvodu se mohou styly vedení prolínat či střídat.

[53] Více o této Problematice: AMSTRONG, Michael. *Management a leadership.* Praha: Grada, 2008, s. 28. ISBN: 978-80-247-2177-4

3.4.2 Leader: požadavky na chování leadera

Leader má vize, určuje směr, zná cestu kudy jít, vede zaměstnance a stará se o jejich potřeby. Dobrý leader je příkladem hodným následování. Jedním z důležitých aspektů, pro vytváření pozitivní firemní kultury, je chování leadera.

Amstrong uvádí tyto požadavky na chování leadera:

- *„projevuje nadšení;*
- *podporuje ostatní lidí a pomáhá jim;*
- *uznává a oceňuje úsilí jednotlivců;*
- *naslouchá nápadům a problémům lidí;*
- *udává směr;*
- *demonstruje svou osobní čestnost a poctivost;*
- *dělá to, co říká;*
- *povzbuzuje k týmové práci;*
- *aktivně povzbuzuje lidi k poskytování zpětné vazby;*
- *rozvíjí ostatní lidi.“*[54]

Dobrý leader by měl u zaměstnanců budit důvěryhodnost, zaměstnance respektovat a projevovat zájem o pracovní podmínky na pracovišti. Měl by být schopen se orientovat ve svých vlastních pocitech, ale i pocitech druhých, dobře zvládat své emoce a jednat se zaměstnanci podle jejich emočních reakcí, znát své silné a slabé stránky. V neposlední řadě by měl být motivován, zanícen pro práci a vytrvale sledovat cíle. Mezi důležité kompetence leadera patří také umění a ochota vést otevřený dialog a delegování odpovědností a pravomocí.

[54] AMSTRONG, Michael. *Management a leadership.* Praha: Grada, 2008, s. 32. ISBN: 978-80-247-2177-4

3.5 Vliv managementu na utváření postojů zaměstnanců

Postoje zaměstnanců ovlivňuje chování managementu, které zahrnuje postupy, způsoby a procesy, kterými management vytváří ve firmě prostředí, které následně významně ovlivňuje firemní kulturu.

„Termín postoj je užíván ve vztahu k pozitivním, nebo negativním pocitům, které se týkají nějaké osoby, věci, události či problému. Jsou produktem hodnocení, v němž jsou integrovány kognitivní, emotivní a konaktivní složky psychiky. Kognitivní procesy přinášejí člověku poznatky, v emocích prožívá jejich význam a v postojích zaujímá vůči objektům hodnotící vztah – objekt hodnocení se mu pak jeví jako žádoucí či nežádoucí, dobrý či špatný".[55]

Myšlení a jednání každého člověka je řízeno komplexem vnitřních a vnějších vlivů, které odrážejí jeho aktuální nastavení psychiky. Výslednicí tohoto procesu jsou postoje.

Mezi vnitřní vlivy, které ovlivňují postoje, se řadí individuální dispozice, které v sobě zahrnují zvyky či automatické reflexi, osobnostní vlastnosti a schopnosti. Z hlediska formování postojů jsou relativně neměnné. Tyto dispozice jsou dány věkem, zdravotní stavem, vzděláním, výchovou, pohlavím či dědičnými faktory.

Mezi vnější vlivy ovlivňující postoje se řadí pracovní prostředí, jeho klima, technické vybavení či přístup světla. Dalšími faktory jsou interpersonální a skupinové vztahy, náplň práce, její charakter a celkové požadavky na zaměstnance. V neposlední řadě jednání managementu, systém kontroly, odměňování a motivace.

Postoje určují a přímo řídí chování zaměstnanců jak obecně, tak v konkrétních situacích a mohou hrát velmi důležitou roli při případném vzniku rizik.

---

[55] LUKÁŠOVÁ, Růžena., NOVÝ, Ivan. a kol. *Organizační kultura*. *Od sdílených hodnot a cílů k vyšší výkonnosti podniku.* Praha: Grada, 2004, s. 23. ISBN: 80-247-0648-2

Z tohoto důvodu nesmí být opomenuty faktory, které mohou zapříčinit vznik bezpečnostního incidentu:

- momentální psychická únava;
- nemoc; [56]
- rozčilení;
- interpersonální konflikty;
- averze k některým činnostem, nebo zaměstnancům aj.

Postoje jsou souhrnem potřeb, motivů a uznávaných hodnot. Projevují se tím, co zaměstnanec dělá, čemu dává přednost, co považuje za důležité, s čím je spokojen, co odmítá či co ho nutí ke změnám. Právě tyto aspekty psychického prožívání jsou intenzivně formovány aktuální firemní kulturou, chováním managementu a jeho politikou (povyšování, uznání, kvalita pracovního života).
Postoje určují míru pracovní disciplíny, rozhodnosti, pečlivosti, systematičnosti, důslednosti aj. Převládající postoje zaměstnanců ovlivní, jak odpovědně plní zaměstnanci své povinnosti, jak se individuálně angažují a zapojují do procesů neustálého zlepšování.

Postoje patří k nejvýznamnějším pilířům, na kterých firemní kultura stojí. Utváření pozitivních postojů každého zaměstnance k pracovním činnostem, ke kvalitě odvedené práce, k pracovní disciplíně, ke klientům je hlavním účelem formování pozitivně laděné firemní kultury. Významnou oblastí ovlivňující postoje zaměstnanců jsou vhodné pracovní podmínky, mající bezprostřední vliv na postoje zaměstnanců k firmě a k její kultuře. Dobré pracovní podmínky jsou viditelným důkazem zájmu managementu o své zaměstnance.

Změna postojů zaměstnanců patří k velmi složitým a časově náročným procesům.
Management a především pak linioví manažeři musí na zaměstnance působit komplexně a dlouhodobě za využití vhodné argumentace, vysvětlování, projevované důvěry, respektu a vhodné motivace, neboť motivace zaměstnance bývá propojena s postoji zaměstnance.

[56] Poznámka autorky této práce: zaměstnanci společnosti mají nárok 3 dny v roce na Sick Leave „necítěnku“

Se změnou postojů dochází i ke změně pracovních návyků zaměstnance.

Správné návyky pomáhají zaměstnanci lépe analyzovat nestandardní pracovní situace a šetří mu čas při rozhodování. V konečném důsledku je zaměstnanec spokojen se svou pracovní činností. Spokojenost zaměstnance významně ovlivní v pozitivním směru jeho sounáležitost s firmou.

3.6 Motivace

Dalším významným faktorem, kterým jsou ve firmách formovány postoje, je působení motivačních stimulů.

Podle Amstronga*: „Teorie motivace zkoumá proces motivování, proces utváření motivací. Vysvětluje, proč se lidé při práci určitým způsobem chovají, proč vyvíjejí určité úsilí v konkrétním směru. Popisuje, co mohou společnosti udělat pro povzbuzování lidí, aby uplatnili své schopnosti a vyvinuli úsilí způsobem, který podpoří splnění cílů společnosti i uspokojení jejich vlastních potřeb. Zabývá se rovněž spokojeností s prací – faktory, které ji vytvářejí, a jejím vlivem na pracovní výkon.“*[57]

Aby zaměstnanci naplňovaly firemní cíle, měly by ve firmě fungovat procesy řízení motivace vedoucí ke kvalitní práci při naplňování přidělených odpovědností a povinností a to za předpokladu striktního dodržování všech parametrů činností, které mohou ovlivnit výslednou kvalitu.

Amstrong dále uvádí dva typy motivace:

- ***„Vnitřní motivace:*** *faktory, které si zaměstnanci sami vytvářejí a které ovlivňují, aby se určitým způsobem chovali. Tyto faktory tvoří odpovědnost (pocit, že práce je důležitá a že máme kontrolu nad svými vlastními možnostmi) a autonomie (příležitost využívat a rozvíjet dovednosti a schopnosti směřující k postupu v hierarchii pracovních funkcí).*
- ***Vnější motivace****: motivace managementu, kterou tvoří odměny, povýšení, ale také tresty, odepření platu, nebo kritika*.“[58]

[57] AMSTRONG, Michael. *Řízení lidských zdrojů. Nejnovější trendy a postupy*. 10. vyd. Praha: Grada, 2010, s. 219. ISBN: 978-80-247-1407-3

[58] Tamtéž: AMSTRONG, Michael. *Řízení lidských zdrojů. Nejnovější trendy a postupy*, s. 221.

O skutečném působení motivačních stimulů rozhodují vnitřní osobností, ale i situační motivační dispozice zaměstnanců.

Vnější motivační faktory mohou mít bezprostřední a výrazný účinek, ale nemusejí nutně působit dlouhodobě. Zatímco vnitřní motivační faktory jsou součástí jedince, nikoli vynucené zvnějšku a proto účinek bude hlubší a dlouhodobější.

Podle Amstronga, vnitřně motivovaní lidé jsou motivovaní sami za sebe a chtějí jít ve správném směru toho, čeho mají dosáhnout.[59]

3.6.1 Motivační systém a jeho faktory

Jednání managementu výrazně ovlivňuje to, jak se zaměstnanci ve firmě cítí a jak jsou ochotni pro firmu nasazovat své síly. Motivační systém je pozitivním účinným prostředkem při budování firemní kultury. Motivační systém napomáhá formovat žádoucí postoje a chování zaměstnanců

Mezi faktory, které mohou mít značný motivační efekt a nejsou pro firmu nijak nákladově náročné, můžeme řadit:

- úprava pracoviště: pracovní podmínky a prostředí ovlivňují nejen výkonnost, ale i spokojenost zaměstnance a jeho vztah k firmě;
- flexibilní pracovní doba;
- pozitivní leadership zahrnující:
    - nadstandardní informovanost;
    - respektování názorů a podnětů;
    - spontánní uznání ze strany přímých nadřízených aj.

[59] Více o této problematice: AMSTRONG, Michael. *Management a leadership.* Praha: Grada, 2008, s. 70. ISBN: 978-80-247-2177-4

Autorka této práce se ve své pracovní praxi přesvědčila, že významným motivačním faktorem mohou být krátké neformální návštěvy pracovišť přímo podřízených zaměstnanců. Projevením zájmu o podřízené, o jejich starosti, radosti, trápení, získáním podnětů co by chtěli zlepšit a naopak s čím jsou spokojení, narůstá motivace zaměstnanců pracovat co nejlépe. Na druhou stranu nadřízený získává bezprostřední informace z pracovišť, které pak pozitivně ovlivňují jeho řídící činnosti.

Manažeři mohou také zaměstnance motivovat svým osobním příkladem:

- jak vyjadřují své postoje;
- jak mezi sebou komunikují;
- jak se pro firmu angažují;
- jak se chovají v mimořádných situacích.

Mezi nákladnější motivační faktory patří systém benefitů:

- programy péče o zaměstnance, které přispívají k harmonizaci potřeb zaměstnanců společnosti (příspěvek na letní a zimní rekreace, hrazené vzdělávací kurzy za účelem zvýšení klíčových kompetencí aj.);
- automobil i pro soukromé účely;
- stravenky;
- notebook, telefon aj.

Má-li být motivace účinná, musí být zaměřena na podporu uvědomění si závažnosti vlastních pracovních činností zaměstnance při plnění konkrétních cílů. Zde můžeme hovořit o zvyšování subjektivní odpovědnosti zaměstnance v případě kvalitně odvedené práce. Naopak za opakované nesplnění úkolů, bude následovat pro zaměstnance sankce.

Sankce by měla být udělena v případě, pokud zaměstnanec opakovaně porušuje pracovní povinnosti a předchozí prostředky, zejména ve formě domluvy, selhaly. Management si musí být vědom skutečnosti, že udělení sankce je posledním prostředkem jak zaměstnance, který neplní a porušuje pracovní povinnosti napravit. Sankce se většinou vztahuje k finančnímu postihu pro zaměstnance např. nepřiznání prémií.

V případě opakované nekázně by měl management zvážit, zda se zaměstnancem rozváže pracovní poměr.

3.7 Firemní komunikace a její procesy

Dalším tématem, kterému se musí management společnosti soustavně věnovat, jsou komunikační procesy. Komunikace uvnitř společnosti je velmi důležitá a patří k účinným prostředkům rozvoje zaměstnanců, k formování jejich postojů a přispívá k vytváření pozitivní firemní kultury

Jak zdůrazňuje Šigut: *„…bez komunikace nemůže existovat žádný podnik. Na komunikaci a plynulém toku informací do jisté míry závisí, zda bude podnik dosahovat svých cílů. Komunikace v organizaci je součástí řízení, je rovněž součástí podnikové kultury.“*[60]

Podle Amstronga: *„…je nezbytné, aby management průběžně pracovníky informoval o záležitostech, které se jich týkají, a zajistil jim cesty, jejichž prostřednictvím mohou vyslovit své názory. Zvlášť nezbytné je to v případech, kdy se zavádějí nové kroky a efektivní řízení změny je do značné míry záležitostí poskytování informací pracovníkům o záměrech managementu a následného ověření, že změnám, které se jich budou týkat, porozuměli.“*[61]

Existují dva základní typy firemních komunikačních procesů:

- komunikace vertikální, která probíhá shora dolů a zdola nahoru a to mezi různými úrovněmi firemní hierarchie;
- komunikace horizontální, která probíhá mezi jednotlivými spolupracovníky, uvnitř pracovních týmů a mezi útvary.

Kvalita vertikální a horizontální komunikace závisí zejména na těchto procesech:

- kvalita komunikačních kanálů: komunikační šumy (zkreslení, prostupnost);
- přístup a dostupnost informací: informování podřízených zaměstnanců (včasnost, pravdivost, věrohodnost, transparentnost);

[60] ŠIGUT, Zdenek. *Firemní kultura a lidské zdroje*. Praha: ASPI Publishing, 2004, s. 68. ISBN: 80-7357-046-7
[61] AMSTRONG, Michael. *Řízení lidských zdrojů. Nejnovější trend a postupy*. 10. vyd. Praha: Grada, 2001, s. 662. ISBN: 978-80-247-1407-3

- forma, rozsah a obsah předávaných informací: srozumitelnost, přehlednost, způsoby prezentace, timing (časovaní);
- formální a neformální procesy předávání a sdílení informací: uvnitř týmů a útvarů;
- soulad informací s dalším jednáním managementu.

Kromě vertikální a horizontální komunikace můžeme rozlišit komunikace podle zúčastněných subjektů následovně:

- uvnitř managementu;
- uvnitř pracovních týmů;
- mezi vlastníky procesů;
- v rámci technické podpory komunikačních procesů – informační systémy;
- komunikace s externími klienty a zákazníky.

3.7.1 Neefektivní komunikace

Absence efektivní komunikace navozuje u zaměstnanců skepsi, pasivitu, obavy, bývá značně demotivující a může vyvolat negativní postoje, které mohou vyústit ze strany zaměstnanců k odporu ke změnám.

Odpor ke změnám může mít za následek/lze očekávat zvýšený výskyt významných procesních a bezpečnostních rizik.[62]

Neefektivní komunikace bývá velmi úzce spojena se stylem vedení a řízení zaměstnanců. Neefektivní komunikace se bude pravděpodobně omezovat na jednosměrné přenášení příkazů shora dolů a bude postrádat informační otevřenost, což znamená, že bude kladen malý důraz na význam sdílení informací a znalostí.

[62] Více o této problematice. GOLLOVÁ, Marta. *Budování systému bezpečnosti informací společnosti a zvyšování bezpečnostního povědomí zaměstnanců.* Praha, 2012. Bakalářská práce. UJAK, Katedra Andragogiky. Vedoucí práce: Jiří Víšek

V prostředí, kde nejsou zaměstnanci zapojováni do komunikačních procesů a není s nimi ze strany managementu veden efektivní dialog s možností zpětné vazby, vznikají komunikační bariéry, které nepříznivě ovlivňují firemní kulturu.

Neefektivní komunikace může vyvolat negativní důsledky v oblasti informačních toků a to zejména v těchto oblastech:

- omezený přístup zaměstnanců k potřebným informacím zejména nevyhovující adresnost a dostupnost;
- nespolehlivé toky informací, což znamená, že není zaručena včasnost, správnost, pravdivost, úplnost, aktuálnost informací;
- zkreslení či ztráta informací tj. nedoručení správným adresátům;
- zvýšený výskyt procesních selhání, což muže mít za následek malou výkonnost a produktivitu práce zaměstnance v návaznosti na špatná rozhodnutí, nedodržení termínu, vznik negativních postojů a s tím spojené snížení motivace zaměstnance;
- podcenění rizik.

3.7.2 Cesta k efektivní komunikaci

Dobře komunikovat, sdílet, využívat a vyhledávat informace by mělo být předmětem stálého zájmu managementu.

Manažeři by měli rozlišovat 3 roviny firemní komunikace:[63]

- první rovina zahrnuje obsah a předmět komunikace;
- v druhé rovině se prolínají procesy a to jak je komunikace realizována, organizována, časována a jakými prostředky se komunikuje;

[63] Více o této problematice: AMSTRONG, Michael. *Řízení lidských zdrojů: Nejnovější trendy a postupy*. 10. vyd. Praha: Grada, 2010, s. 661-667. ISBN: 978-80-247-1407-3

- třetí rovina je osobní rovina, do které vstupují zaměstnanci se svými postoji, dovednostmi, zkušenostmi, motivy, osobnostními vlastnostmi aj.

Úkolem managementu je, aby spolu zaměstnanci z jednotlivých útvarů společnosti efektivně spolupracovali. Klíčem k efektivní spolupráci je efektivní komunikace, jejímž prostřednictvím se mohou stereotypy, nebo předsudky ve vnímání zaměstnanců měnit.

Pro většinu pracovních činností je důležité informacím správně porozumět a správně interpretovat jejich obsah. Velmi důležité je umění naslouchat, dobře argumentovat, potlačit negativní emoce v komunikaci, zaujmout, získat a udržet si důvěru.

Je třeba, aby management podporoval zájem zaměstnanců informovat a být informován. Tento zájem podřízených si management získá svou otevřeností, příležitostí k dialogům a zpětnovazební reakcí na informace z pracovišť podřízených.

Klíčovou roli k efektivní komunikaci zde hraje setkávání zaměstnanců. Společnost může uspořádat pro své zaměstnance výjezdní zasedání, vzdělávací workshopy, briefingy. V rámci těchto akcí je možné zlepšovat úroveň komunikace uvnitř společnosti.[64]

3.7.2.1 Technika Johariho okna, využití komunikace ke změně vnímání

Efektivní komunikace může měnit předsudky ve vnímání jednotlivých kolegů/zaměstnanců společnosti. Efektivní komunikace pomáhá pochopit naše myšlenky, názory a chování.

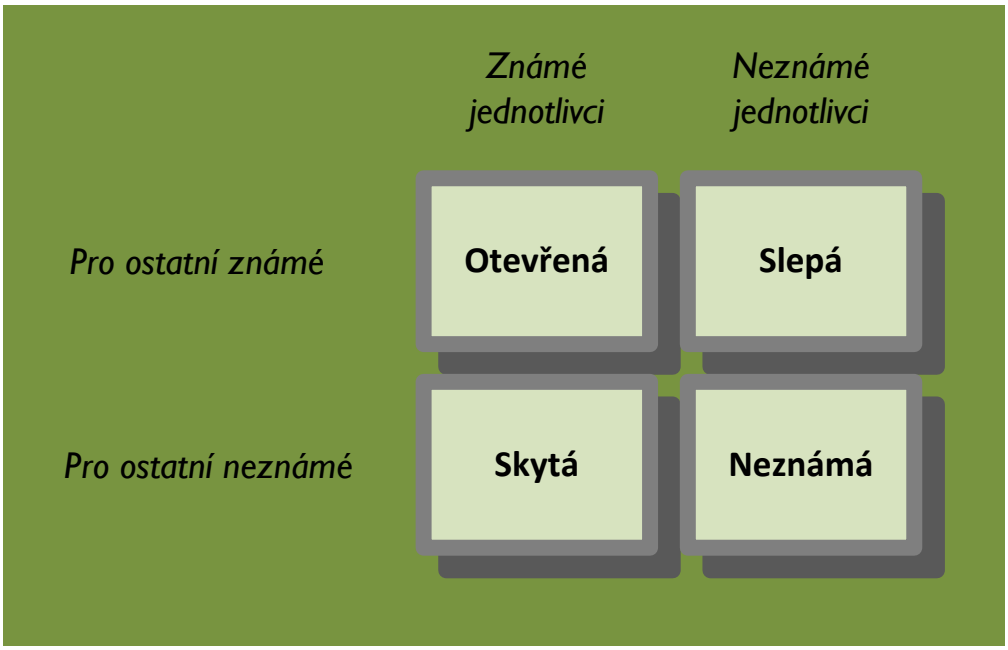
Nástroj, který umožňuje popsat náš vztah k ostatním, se nazývá model oken Johari, neboli Johariho okno.

[64] Poznámka autorky: Zkušenost ukázala, že zaměstnanci jsou na těchto akcích uvolněnější a přístupnější komunikaci. Výsledkem je odbourání komunikačních bariér mezi jednotlivými útvary a zlepšení úrovně komunikace uvnitř celé společnosti.

Model oken Johari vytvořili autoři Joseph Luft a Harry Ingham ve 20. století v USA. Tento model slouží pro zlepšení sebeuvědomění skupiny. Komunikace umožňuje měnit velikost jednoho okna na úkor druhých oken.

Obrázek číslo 2 názorně zobrazuje okno se čtyřmi kvadranty, které jsou rozděleny na otevřenou, skrytou, slepou a neznámou oblast. V rámci tohoto modelu má každý jedinec své okno.

Obrázek 2: Johariho okno



Zdroj: Lukášová, Nový a kolektiv, Firemní kultura, s. 37

Existují čtyři oblasti povědomí o jednotlivci.

Otevřená oblast, neboli veřejná: představuje to, co o sobě jednotlivec ví a chce, aby to o něm věděli i ostatní. Jsou to způsoby chování či motivace. Tato oblast zahrnuje veřejně prezentované názory, postoje, motivy. Projevuje se zcela spontánně. Čím více informací bude o sobě schopen jedinec sdělit, tím lépe ho budou ostatní znát a budou mu lépe rozumět. Čím je okno otevřené oblasti větší, tím jsou ostatní okna menší. Rozšíření okna otevřené oblasti brání strach z neznámého či nízké sebevědomí.

Slepá oblast: představuje aspekty chování jednotlivce, které jsou známy jiným lidem, ale on sám si jich není vědom např. zlozvyk či povahový rys. Poznání této oblasti je možné jen za pomoci jiných osob. V praxi to znamená, že jednotlivec pozoruje reakce jiných osob na své chování. Tyto reakce vyhodnocuje a v případě negativních reakcí se snaží své chování měnit.

Skrytá oblast: představuje to, co jednotlivec ví sám o sobě, ale před ostatními to z různých příčin skrývá. Může se jednat o skutečnosti, jejichž prozrazení by jednotlivce ohrožovalo, poškozovalo či by mu jinak škodilo.

Neznámá oblast: spočívá v podvědomí, vyjadřuje to, co o sobě nevíme a neví to ani ostatní. Tato oblast bývá poznávána až v konkrétních, vyhraněných situacích, které jednotlivec dosud nezažil např.: při ohrožení života jednotlivce.

3.7.3 Komunikace při prevenci procesních rizik

Efektivní, kvalitní komunikace je nezbytným předpokladem řízení prevence a analýzy rizik. V oblasti řízení rizik má efektivní komunikace klíčový význam a to zejména v těchto oblastech informačních toků a znalostí:[65]

- o rizicích;
- o možných důsledcích selhání;
- o nastalých mimořádných a nežádoucích událostech;
- o příčinách a způsobech zvládání rizik;
- o cílech, procesech a činnostech potřebných pro integrovaný systém řízení rizik.

[65] Více o této problematice. GOLLOVÁ, Marta. *Budování systému bezpečnosti informací společnosti a zvyšování bezpečnostního povědomí zaměstnanců.* Praha, 2012. Bakalářská práce. UJAK, Katedra Andragogiky. Vedoucí práce: Jiří Víšek

3.8 Kultura bezpečnosti

Kultura bezpečnosti tvoří podstatnou součást firemní kultury. Zhuravlyov považuje kulturu bezpečnosti za: *„…mentalitu nebo stav mysli společnosti nebo jednotlivce při činnosti v organizaci. Představuje kulturu bezpečnosti jako sdílený vzorec chování a jednání, který ovlivňuje veškerou činnost a interakce. Všudypřítomnost kultury bezpečnosti je způsob, kterým lidé myslí a pracují.“*[66]

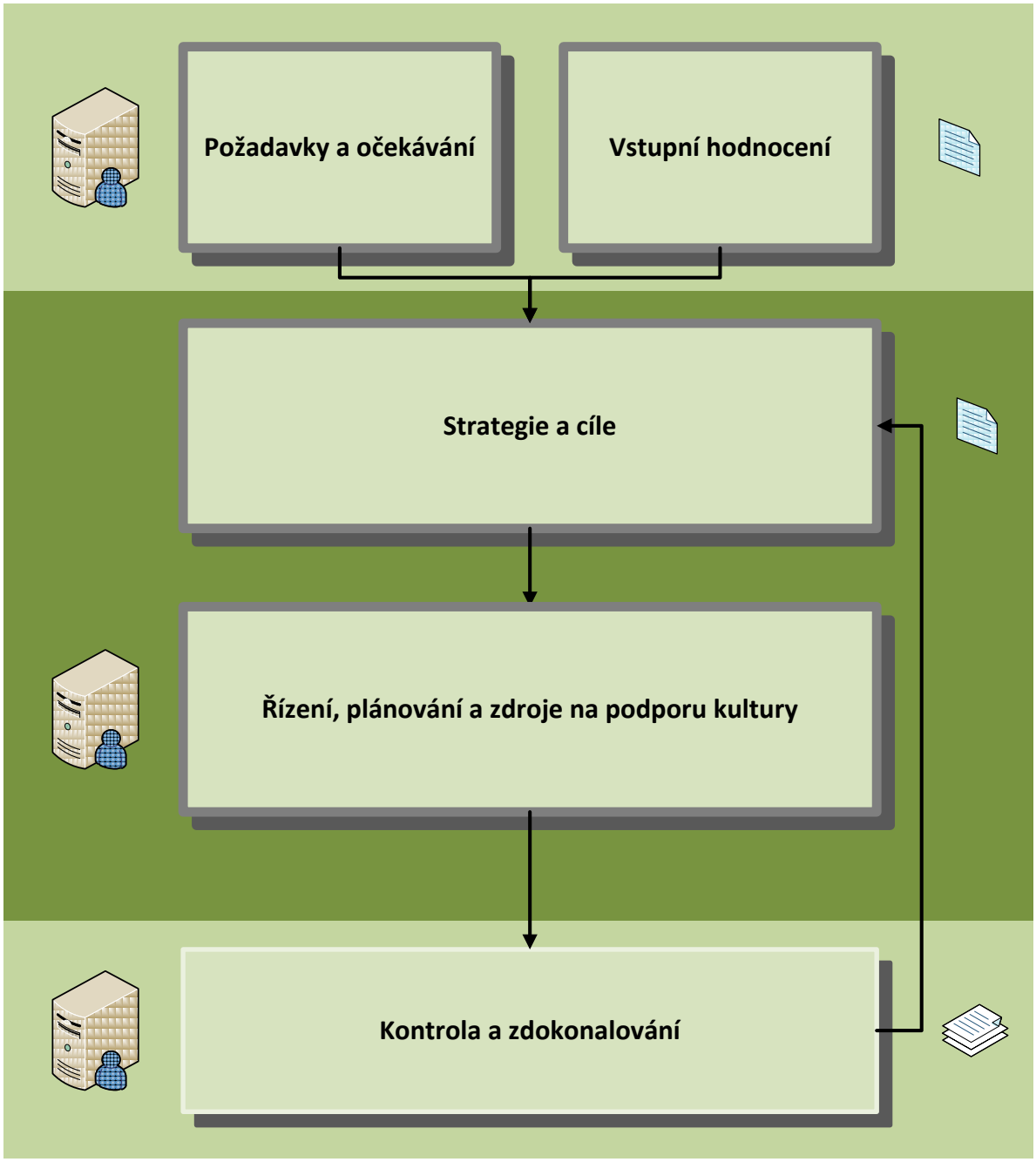
Kultura bezpečnosti omezuje rizika provozních chyb za pomoci sdíleného uvažování, při účasti, zapojení a předvídavém myšlení všech zaměstnanců společnosti.

Jak uvádí Michalík a Paleček: *„Efektivní kulturu bezpečnosti je třeba chápat jako vhodné sladění chování, hodnot a postojů pracovníků společnosti s očekáváním zainteresovaných subjektů. Jak se mohou měnit očekávání, tak by se mělo měnit i chování, hodnoty a postoje společnosti. Z toho plyne, že efektivní kultura bezpečnosti není něčím statickým, nýbrž se jedná o neustále se vyvíjející a zdokonalující soubor chování, hodnot a postojů.“*[67]

Následující obrázek číslo 3 zobrazuje jednotlivé kroky a jejich vzájemnou provázanost pro zvyšování kultury bezpečnosti

[66] ZHURAVLYOV, In: MICHALÍK, David. a PALEČEK, Miloš. *Kultura bezpečnosti. Metodická příručka*. Praha: Výzkumný ústav bezpečnosti práce, 2010, s. 7. ISBN: 978-80-86973-05-0
[67] MICHALÍK, David. a PALEČEK, Miloš. *Kultura bezpečnosti. Metodická příručka*, s. 28.

Obrázek 3: Pohled na kroky ke zvyšování úrovně kultury bezpečnosti



Zdroj: Michalík D., Paleček M., *Kultura bezpečnosti. Metodická příručka*, s. 28

3.8.1 Funkce kultury bezpečnosti

Kultura bezpečnosti podporuje dosahování co nejvyšší spolehlivosti lidského činitele.[68]

Funkcí kultury bezpečnosti je:

- shodné vnímání hodnot a norem chování zaměstnanců zajišťuje žádoucí chování a disciplínu;
- pocit smysluplnosti práce dává zaměstnanci pocit, že je důležitou součástí společnosti a podporuje tak jeho motivaci k dobrému pracovnímu výkonu;
- podporuje konkurenční výhodu společnosti.

3.8.1.1 Silná kultura bezpečnosti

Silnou kulturu bezpečnosti ve firmě zajistíme tehdy, pokud budou ve firmě znatelné následující indikátory.[69]

- Bezpečnost informací je ve firmě jasně uznávanou hodnotou, je integrována do všech činností zaměstnanců a jsou jasně stanovené odpovědnosti zaměstnanců:[70]
    - bezpečnost informací je prokazována v dokumentaci, která je na kvalitní úrovni;
    - postupy pro implementaci a prověřování informační bezpečnosti jsou dobře a srozumitelně zpracovány;

[68] Více o této problematice: MICHALÍK, David. PALEČEK, Miloš. *Kultura bezpečnosti. Metodická příručka*. Praha: Výzkumný ústav bezpečnosti práce, 2010, s. 7. ISBN: 978-80-86973-05-0

[69] Tamtéž: Více o této problematice: MICHALÍK, David. PALEČEK, Miloš. *Kultura bezpečnosti. Metodická příručka*, s. 15-17.

[70] Více o této problematice. GOLLOVÁ, Marta. *Budování systému bezpečnosti informací společnosti a zvyšování bezpečnostního povědomí zaměstnanců.* Praha, 2012. Bakalářská práce. UJAK, Katedra Andragogiky. Vedoucí práce: Jiří Víšek

- při každodenních činnostech zaměstnanců je zřetelný pro-aktivní přístup k bezpečnosti informací, který se projevuje v jejich rozhodování, chování a přístupu k pracovním činnostem; zaměstnanci mají potřebné znalosti pro pochopení pracovního procesu;
- ve firmě je vysoká kompatibilita s předpisy a postupy;
- ownership, kdy zaměstnanci berou odpovědnost za vlastní, tato odpovědnost je evidentní u všech zaměstnanců společnosti a projevuje se na všech úrovních společnosti.

- Je zřetelně projevován leadership orientovaný na informační bezpečnost:
  - management zajišťuje dostatečně odborně schopné pracovníky;
  - management zapojuje jednotlivce do aktivního zlepšování informační bezpečnosti;
  - management podporuje otevřenou a efektivní komunikaci v celé organizaci;
  - vztahy mezi managementem a podřízenými zaměstnanci jsou postaveny na důvěře.

- Bezpečnost je prosazována učením:
  - existuje systematický rozvoj odbornosti každého zaměstnance;
  - na základě rozvoje odbornosti jsou zaměstnanci schopni lépe diagnostikovat a monitorovat odchylky a následně přijímat účinky nápravných opatření.

3.8.1.2 Slabá kultura bezpečnosti

Společnost musí zajistit, aby v kultuře bezpečnosti nebyla slabá místa, která mohou zapříčinit výskyt bezpečnostních Incidentů.[71]

Indikátory slabé kultury bezpečnosti mohou být následující:[72]

- **Nedostatek systematického přístupu:** přítomnost tohoto nedostatku zapříčiní takový leadership, který se projevuje špatným rozhodovacím procesem managementu. Dále je zřetelná absence vizí a strategií společnosti, nedostatek adekvátních a ucelených informací směrem k zaměstnancům a nejsou předem stanoveny odpovědnosti zaměstnanců jednotlivých zaměstnanců.

- **Nesprávně udržované postupy**: postupy, které nejsou pravidelně prověřovány a udržovány mohou zapříčinit nesprávné používání postupu, což bude mít za následek zvyšující se počet porušení předem stanovených postupů a bude znamením, že informační bezpečnost nemá prioritu, kterou si zasluhuje.

- **Neshoda zdrojů:**
    - nedostatek zkušených zaměstnanců s vhodnou kvalifikací a praxí;
    - množství práce přes čas;
    - neodpovídající hodnocení rizik;
    - společnost nemá dostatečnou kulturu učení se.

[71] Více o této problematice. GOLLOVÁ, Marta. *Budování systému bezpečnosti informací společnosti a zvyšování bezpečnostního povědomí zaměstnanců.* Praha, 2012. Bakalářská práce. UJAK, Katedra Andragogiky. Vedoucí práce: Jiří Víšek

[72] Více o této problematice: MICHALÍK, David. PALEČEK, Miloš. *Kultura bezpečnosti. Metodická příručka*. Praha: Výzkumný ústav bezpečnosti práce, 2010, s. 19-21. ISBN: 978-80-86973-05-0

- **Chybějící proces sebehodnocení:** společnost s absencí tohoto procesu bude slepá k nedostatkům v postojích, v chování svých zaměstnanců a v otázkách informační bezpečnosti, což může mít za následek neuvědomění si prvotní příčiny mnoha událostí. Absence sebehodnocení společnosti bude mít za následek absenci filozofie „trvalého zlepšování“ společnosti.

- **Pracovní podmínky:** špatně větrané, osvětlené a v nečistotě udržované pracoviště, management bez zájmu o pracovní podmínky zaměstnanců bude mít za následek špatně motivovanou pracovní sílu, bez hrdosti na prostředí a firmu, ve které pracuje. Tato slabost ovlivní nejen firemní kulturu jako celek, ale projeví se také v kultuře bezpečnosti.

4 IMPLEMENTACE NÁSTROJE DLP A JEHO VLIV NA FIREMNÍ KULTURU

Praktická část se věnuje implementaci technologie DLP, jako způsobu vzdělávání zaměstnanců společnosti v oblasti informační bezpečnosti.

Na základě teoretické analýzy poznatků, definice procesů a požadavků na firemní kulturu je v této části práce popsána implementace technologie DLP do prostředí společnosti People & Job, s.r.o.

Cílem praktické části je rozpracovat zásady budování bezpečnostního povědomí v systému řízení bezpečnosti informací společnosti prostřednictvím implementované technologie DLP.

Dalším cílem praktické části je budování firemní kultury této společnosti prostřednictvím definovaných procesů a implementované technologie a následné celkové zhodnocení vlivu implementované technologie a definovaných procesů na firemní kulturu společnosti.

4.1 Identifikace variant zapojení technologie DLP do provozního prostředí

Tato kapitola popisuje způsob, který byl zvolen pro zapojení technologie DLP do prostředí společnosti:

První zvolenou fází byl pasivní způsob sledování za účelem vyladění technologie DLP. V druhé navazující fázi byla technologie DLP aktivně zapojena a po určité době byla pře-nastavena do režimu restriktivního blokování nežádoucí odchozí komunikace

Možností jak zařízení zapojit do sítě je několik, v zásadě ale existují 2 základní modely a to pasivní, nebo aktivní sledování.

Model 1. Pasivní sledování

V tomto modelu se jedná o zapojení určené pouze k pasivnímu monitorování a zaznamenávání s možností pozdějšího vyhodnocení uložených akcí. Takto implementovaná technologie DLP nemá žádný vliv na přenos dat a jeho rychlost, přičemž žádným způsobem neovlivňuje technické parametry. Jedná se pouze o pasivní sledování obsahu prostřednictvím sondy, která je schopna identifikovat odesílaná data vně společnost dle jejich obsahu, dále vytvořit záznam v logu incidentů a případně informovat Bezpečnostního manažera.

Model 2. Aktivní reakce

Druhým modelem je aktivní zapojení. V tomto případě je možné konfigurovat technologii DLP tak, aby byla schopna aktivně reagovat na aktuální situaci v síťovém provozu při odesílání dat vně společnost. V extrémním případě může ukončit spojení a tak znemožnit odeslání dat, např. vyhodnocených jako data „zakázaná pro přenos mimo společnost“.

Model 2 zahrnuje také **Restriktivní blokování nežádoucí odchozí komunikace** tj. napojení na server, který zajišťuje komunikaci společnosti. To přináší možnost monitorovat tok dat přímo na proxy serveru a poskytovat tak zpětně serveru informace o „čistotě“ dat.

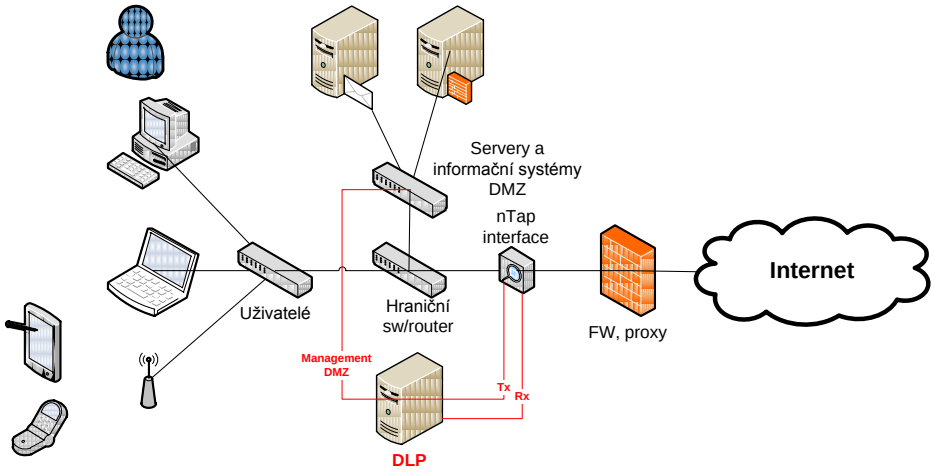
V případě identifikace citlivých dat je přenos ukončen na proxy serveru. Tímto způsobem je možné implementovat také monitoring šifrovaného provozu a zabránit, aby nedocházelo k únikům citlivých informací prostřednictvím šifrovaných souborů nebo šifrovaného komunikačního kanálu.

Technologie provozovaná na základě druhého modelu má možnost aktivně zasahovat do spojení v reálném čase. Může mít i přímý vliv na vlastnosti přenosového media, což znamená, že u některých e-mailů může zpozdit jejich odeslání, nebo v některých případech může pozorovatelně zpomalit prohlížení internetu a komunikaci s proxy serverem.

Místem zapojení technologie DLP a umístění jeho sondy je okraj sítě tzn. hranice mezi LAN/WAN a internetem.

Níže uvedený obrázek číslo 3 a následné schéma číslo 1 přehledně naznačují popsaný způsob, jak lze technologii efektivně používat.

Obrázek 4: Zapojení, pro aktivní on-line monitoring a možnost aktivního zasahování do spojení v reálném čase



Zdroj: *Technická dokumentace RSA. Data Loss Prevention (DLP).* [online]. [cit. 2013-04-06]. Dostupné z: http://www.emc.com/security/rsa-data-loss-prevention.htm#!resources

Schéma 1: Funkce DLP

Zdroj: autorka práce

4.2 Iniciační konfigurační politika

Iniciační konfigurační politika vychází z klasifikace informací systému informační bezpečnosti, která byla vypracována v rámci bakalářské práce autorky.[73] Tato kapitola je věnována pouze definici pravidel pro nastavení technologie DLP, která vycházejí z této klasifikace informací

V rámci technologie DLP jsou definovány tři úrovně možného porušení bezpečnostní politiky o úniku informací, která vychází z klasifikace informací a dělící se na následující tři úrovně:

1. Kritický: kritické porušení bezpečnostní politiky, kdy mail zpráva nemůže být odeslána. Jedná se o závažný bezpečnostní incident. Technologie DLP zastaví komunikaci a případ je hlášen bezodkladně Bezpečnostnímu manažerovi.
2. Střední: je zde velký potenciál způsobit bezpečnostní incident, odesílání zprávy je pozastaveno a čeká na odsouhlasení či zamítnutí nadřízeného zaměstnance.
3. Nízký: mohlo by se jednat o bezpečnostní incident, odesílání zprávy je pozastaveno a čeká na odsouhlasení zaměstnance, který zprávu odeslal.

V rámci technických možností DLP byla vytvořena následující pravidla/konfigurační politika identifikující odchozí komunikaci vně společnost. Tato politika vyhledává klíčová slova, případně řetězce v dokumentech. Výskyt následujících slov či řetězců má potenciál způsobit bezpečnostní incident.

Jedná se o výstupy, které generují následující programy:

- Ekonomický systém;
- Evidence zájemců o zaměstnání;
- Evidence klientů;
- Personální informační systém (dále jen PIS);
- Psychodiagnostické výstupy.

[73] Více o této problematice.: GOLLOVÁ, Marta. *Budování systému bezpečnosti informací společnosti a zvyšování bezpečnostního povědomí zaměstnanců.* Praha, 2012, s. 26-28. s. V, Příloha A. Bakalářská práce. UJAK, Katedra Andragogiky. Vedoucí práce: Jiří Víšek

Hodnocení kritičnosti výskytu dle klasifikace informací:

- **Kritický (Critical)**: výskyt následujících slov či řetězců je nutné hodnotit jako kritický, může zapříčinit vznik kritického incidentu;
    - **STRIKTNĚ INTERNÍ:** např. výstupy z psychodiagnostiky, PIS;
- **Střední (Medium)**: výskyt následujících slov či řetězců má potenciál způsobit bezpečnostní incident;
    - **INTERNÍ:** evidence klientů/zájemců o zaměstnání, ekonomický systém;
- **Nízký (Low)**: výskyt následujících slov či řetězců samostatně nemá potenciál způsobit bezpečnostní Incident. K výskytu bezpečnostního incidentu může dojít při kumulaci informací;
    - **TATO KATEGORIE NENÍ ZACHYTÁVÁNA.**

Fragmenty databází: detekuje komunikaci na databázové úrovni a dále ji registruje v rámci DLP postupu/workflow. Zajišťuje ochranu před odesláním části, či celé databáze mimo společnost.

Fragmenty souborů: detekuje souborové typy na bázi tzv. „Otisků prstů – fingerprint“, které umějí s určitou přesností určit typ přenášeného souboru v rámci datové komunikace. Tato detekce rovněž pracuje v předávaných archivech. Jednotlivé typy souborů jsou zařazeny do konfiguračních politik dle průběžně identifikovaných typů souborů.

Regulární výrazy: s jejich pomocí detekuje četnost výskytu výrazů definovaných jako „Regular Expression“ tzv. regulární výrazy a na základě četnosti výskytu vyhodnocuje kritičnost datové komunikace (např.: e-mail adresy, rodná čísla, čísla dokladů, čísla účtů apod.).

Výskyt následujících slov či řetězců má potenciál způsobit bezpečnostní incident. Jedná se zejména o charakteristiky osobních údajů:

- adresy;
- čísla dokladů;
- čísla účtů;
- e-mail;
- charakteristika zdravotního stavu;
- jména;
- rodná čísla aj.

Hodnocení kritičnosti výskytu z klasifikace informací a četnosti jejich výskytu:

- **Kritický** výskyt více než 100 výskytů;
- **Střední** výskyt více než 10 výskytů;
- **Nízký** výskyt více než 1 výskyt.

4.3 Revize a optimalizace

Po prvotním nastavení pravidel v implementované technologii DLP je nutné fungování těchto pravidel sledovat a vyhodnocovat jejich relevantnost. V případě že prvotní nastavení pravidel je hodně restriktivní dochází ke vzniku falešných poplachů a značnému počtu notifikací, které mohou zbytečně zatěžovat jednotlivé uživatele a Bezpečnostního manažera. Na druhou stranu, když jsou pravidla příliš měkká (neúplná) může docházet k neidentifikovanému úniku citlivých dat a informací. Z těchto důvodů je nutné průběžně optimalizovat nastavení pravidel technologie DLP.

Za optimalizací politik se skrývá zpřesňování a zaměřování jednotlivých bezpečnostních politik, které má za cíl maximální možnou měrou eliminovat výskyt falešných poplachů tak, aby nedocházelo, těmito falešnými poplachy, ke zbytečnému zatěžování uživatelů.

Konkrétní opatření:

- zpřesňování politik a pravidel, zejména pak tvorba a zpřesňování regulárních výrazů a kombinace vícero pravidel v rámci politiky anebo určení minimálního počtu výskytů před zaznamenáním nového incidentu a vyvoláním příslušné akce např. politika hlídající výskyt několika e-mail adres je aplikována až po dosažení minimálního počtu 10, poté je vyvolána související akce a to logování incidentu a případně jeho notifikace;

- kombinace klíčových slov, řetězců a regulárních výrazů, např. výskyt rodného čísla bude nejspíše někde poblíže následovat nebo předcházet jméno či příjmení osoby, nebo obojí, z tohoto důvodu se optimální zdá být právě kombinace regulárního výrazu, vyhledávajícího rodné číslo a seznam v ČR používaných jmen a příjmení;

- na základě požadavku, byla provedena implementace výjimek, kdy ke každé definované bezpečnostní politice byla přiřazena a tím zřetězena politika výjimek. Výjimka je aplikována ve chvíli, kdy je zachycen incident standardní politikou. Následně dochází k vyhodnocení politiky výjimek. Pokud je výsledek vyhodnocení kladný tzn., v případě, kdy jsou zachycena a identifikována data týkající se výjimky, je provedena pouze akce týkající se výjimek, nikoliv akce nadřazené politiky. Definice akce v politikách zachycujících výjimky je definována a není vytvořen záznam a tudíž nedochází ani k notifikacím jak Bezpečnostního manažera, tak např. konkrétního uživatele, jehož se výjimka týká.

4.3.1 Definice priorit a vztažených akcí

Nedílnou součástí definice pravidel a konfigurace DLP technologie je vyhodnocování vzniklých incidentů. Již při tvorbě bezpečnostních politik je zároveň definováno jakou míru kritičnosti, nebo váhu bude mít případně vzniklý incident (low, medium, critical) a kdo o něm bude nebo nebude informován.

Toto hodnocení kritičnosti incidentů vychází z definice incidentů z bakalářské práce autorky.[74]

Definice priorit a reakce:

- Bezpečnostní manažer je notifikován e-mailem o vniklém incidentu s vážností kritický (critical);
- kontrola "běžných" incidentů probíhá online;
- je možné a velmi efektivní předdefinovat a uložit dotazy do báze incidentů a pak rychle a cíleně vyhledávat pouze data, která mohou být aktuálně zajímavá.

[74] Více o této problematice. GOLLOVÁ, Marta. Budování systému bezpečnosti informací společnosti a zvyšování bezpečnostního povědomí zaměstnanců. Praha, 2012, s. 40. Bakalářská práce. UJAK, Katedra Andragogiky. Vedoucí práce: Jiří Víšek

5 VYHODNOCENÍ PŘÍNOSU IMPLEMENTOVANÝCH PROCESŮ A TECHNOLOGIE DLP

5.1 Vyhodnocení přínosu implementované technologie DLP

Hodnocení přínosu implementované technologie probíhalo v několika fázích tak, aby bylo možné vyhodnotit přínos implementované technologie pro společnost a její přímý vliv na firemní kulturu, prostřednictvím vybudovaného bezpečnostního povědomí uživatelů. Vyhodnocovány byly následující fáze, jejichž jednotlivé hodnocení probíhalo v týdenních cyklech:

1. Fáze „Prvotní nastavení“: doba trvání 4 týdny. Implementovaná technologie RSA DLP s prvotně nastavenými pravidly bez upozornění uživateli, že odesílá citlivá data. Po ukončení první fáze proběhla revize politik, jejich následná úprava a zpřesnění.
2. Fáze „Revize nastavených politik“: doba trvání 4 týdny. Celková doba od „Prvotního nastavení“ 8 týdnů. Implementovaná technologie DLP nyní již s upravenými a optimalizovanými pravidly na základě analýzy 1. fáze „Prvotní nastavení“, stále bez upozornění uživateli, že odesílá citlivá data. V průběhu 2. fáze probíhá neustálé sledování a zpřesňování politik.
3. Fáze „Zkušební, plný provoz“: doba trvání 15 týdnů. Celková doba od „Prvotního nastavení“ 23 týdnů. Implementovaná technologie DLP s upravenými a optimalizovanými pravidly na základě analýzy 2. fáze, již s upozorněním uživateli, že odesílá citlivá data. Na základě zpětné vazby od Bezpečnostního manažera a uživatelů, jsou politiky během 3. fáze neustále zpřesňovány.

Následující tabulka číslo 12 přehledně zobrazuje počty identifikovaných událostí a incidentů pro jednotlivé vyhodnocované fáze za sledované období 23 týdnů.

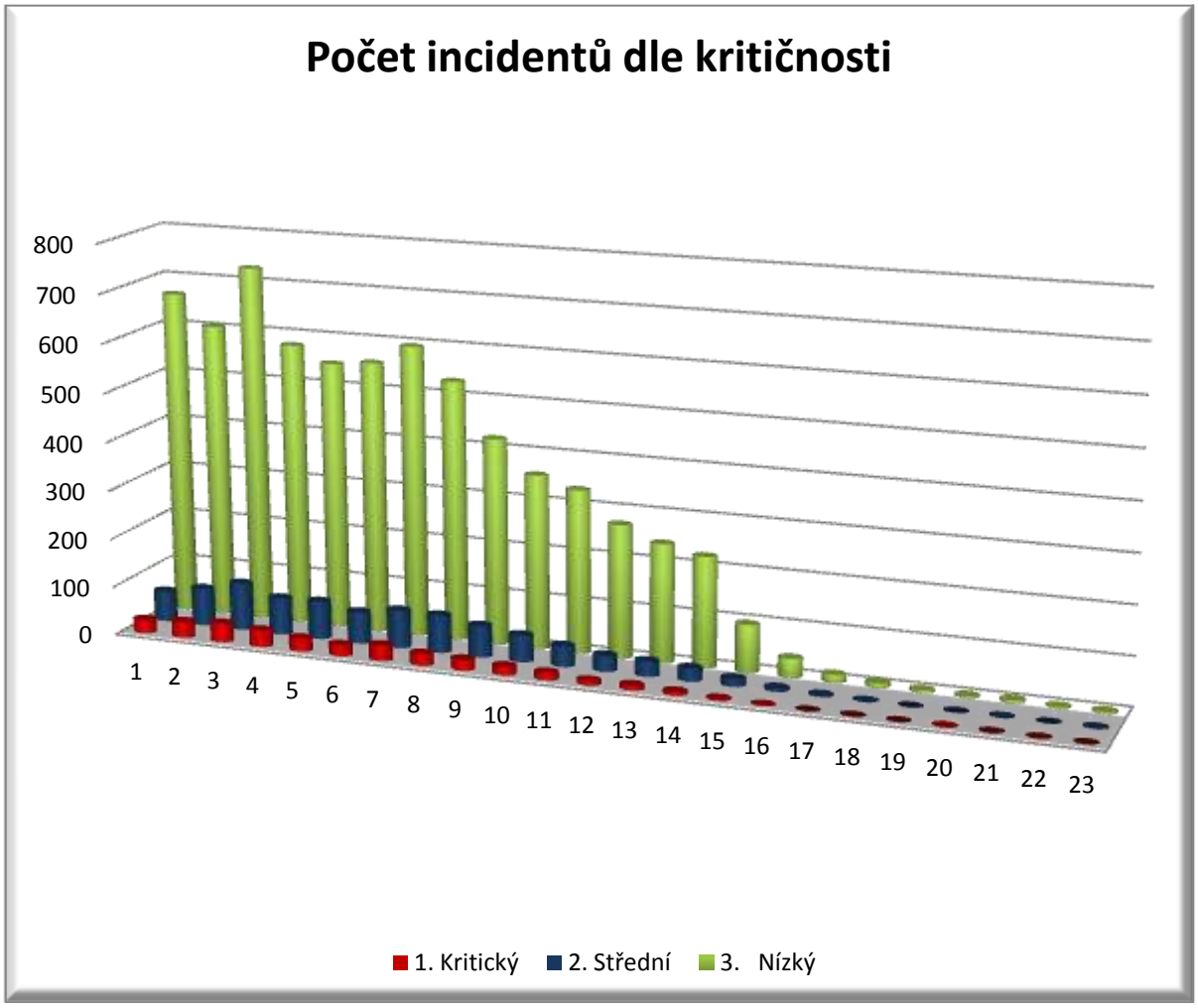
Tabulka 12: Identifikované incidenty

		Celkově identifikované incidenty				Skutečné incidenty			
	Týden	1. Kritický	2. Střední	3. Nízký	Celkově	1. Kritický	2. Střední	3. Nízký	Pozitivně
Prvotní nastavení	1	35	83	756	874	28	63	666	757
	2	39	96	686	821	33	78	605	716
	3	86	198	983	1267	39	98	730	867
	4	37	89	653	779	34	76	579	689
Revize nastavených politik	5	27	76	525	628	27	78	548	653
	6	23	64	547	634	23	65	556	644
	7	32	77	598	707	32	78	596	706
	8	29	82	568	679	24	77	532	633
Zkušební, plný provoz	9	22	66	430	518	22	65	423	510
	10	18	56	360	434	18	55	357	430
	11	15	43	336	394	15	43	335	393
	12	9	33	276	318	9	33	273	315
	13	11	31	243	285	10	31	243	284
	14	7	28	193	228	7	27	226	260
	15	3	16	98	117	3	16	98	117
	16	1	7	43	51	1	7	39	47
	17	0	3	16	19	0	3	16	19
	18	0	1	9	10	0	1	9	10
	19	0	0	5	5	0	0	5	5
	20	1	0	4	5	1	0	4	5
	21	0	1	7	8	0	1	6	7
	22	0	0	3	3	0	0	3	3
	23	0	1	4	5	0	1	4	5

Zdroj: autorka práce (vlastní výzkum)

Pro přehlednost byly tyto údaje znázorněny v následujícím grafu číslo 1, jehož údaje vychází z uvedené tabulky číslo 12. Graf názorně zobrazuje vývoj počtu incidentů v sledovaném čase tj. 23 týdnů z celkových skutečných/pozitivních incidentů a člení incidenty dle jednotlivých kategorií incidentů a to kritický, střední a nízký.

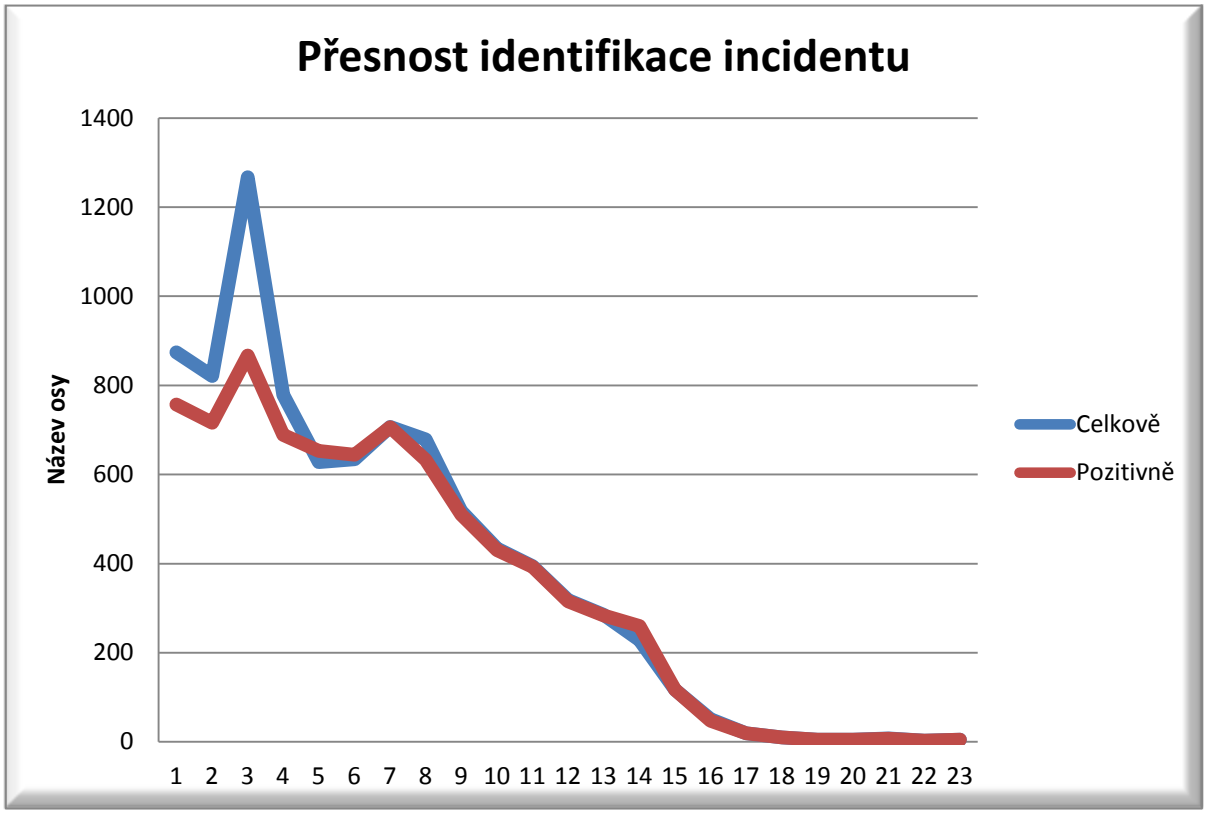
Graf 1: Počet skutečných incidentů dle kritičnosti za sledované období



Zdroj: autorka práce (vlastní výzkum)

Následující graf číslo 2 vychází také z tabulky číslo 12 a přehledně znázorňuje vývoj zpřesňování identifikace incidentů a to mezi celkově identifikovanými incidenty a skutečně/pozitivně identifikovanými incidenty. Celkově identifikované incidenty patří do skupiny všech incidentů, které technologie DLP zachytila. Na základě průběžné revize politik z celkově identifikovaných incidentů byly vybrány pozitivně identifikované incidenty. Po celkové optimalizaci politik pracuje technologie DLP mnohem přesněji.

Graf 2: Počet celkových a skutečných incidentů za sledované období



Zdroj: autorka práce (vlastní výzkum)

Jak bylo řečeno výše, po celkové optimalizaci politik pracovala technologie DLP mnohem přesněji. Po 23 týdnech zkušebního provozu byla technologie DLP, s upravenými a optimalizovanými pravidly, uvedena do ostrého provozu a to s nastaveným blokováním při odesílání citlivých dat a upozorněním uživateli, že odesílá citlivá data s vynucením odsouhlasení přímým nadřízeným.

5.2 Vyhodnocení přínosu definovaných IT služeb a jeho vliv na spokojenost zaměstnanců s pracovním prostředím

Hodnocení přínosu definovaných IT služeb a spokojenost zaměstnanců s pracovním prostředím probíhalo anonymním hodnocením spokojenosti uživatelů, na základě jednoduchého on line dotazníku, „Dotazník hodnocení spokojenosti zaměstnanců s pracovním prostředím a s IT službami“ (Příloha D), a to ve dvou fázích. Dotazník byl poskytnut zaměstnancům k vyplnění v září roku 2012, před zavedením definovaných IT procesů a následně po zavedení definovaných IT procesů do praxe v září roku 2013. Cílem bylo vyhodnotit, zda zavedení definovaných procesů do praxe přineslo žádoucí změnu s následným ovlivněním firemní kultury.

Tabulka číslo 13 zobrazuje počet odpovědí zaměstnanců na jednotlivé otázky, dle jednotlivých možností z dotazníku v roce 2012 (Příloha D), kdy zeleně jsou vyznačeny odpovědi související s pracovním prostředím a modře jsou vyznačeny odpovědi související s IT službami. V roce 2012 vyplnilo dotazník 64 zaměstnanců.

Tabulka 13: Odpovědi podle jednotlivých otázek a jejich variant (rok2012)

	č. otázky	1. URČITĚ ANO	2. SPÍŠE ANO	3. SPÍŠE NE	4. URČITĚ NE
Spokojenost s pracovním prostředím	1	12	15	33	4
	2	16	22	18	8
	3	16	25	17	6
	4	15	13	26	10
	5	16	15	25	8
	6	15	10	24	15
	7	18	16	20	10
Spokojenost s IT Službami	8	9	14	32	9
	9	8	10	30	16
	10	2	8	35	19
	11	0	8	40	16
	12	0	10	34	20
	13	0	15	39	10
	14	0	13	40	11

Zdroj: autorka práce (vlastní výzkum)

Následující tabulka číslo 14 zobrazuje počet odpovědí zaměstnanců na jednotlivé otázky, dle jednotlivých možností z dotazníku v roce 2013 (Příloha D), kdy zeleně jsou vyznačeny odpovědi související s pracovním prostředím a modře jsou vyznačeny odpovědi související s IT službami. V roce 2013 vyplnilo dotazník taktéž 64 zaměstnanců.

Tabulka 14: Odpovědi podle jednotlivých otázek a jejich variant (rok 2013)

	č. otázky	1. URČITĚ ANO	2. SPÍŠE ANO	3. SPÍŠE NE	4. URČITĚ NE
Spokojenost s pracovním prostředím	1	28	36	0	0
	2	25	30	9	0
	3	22	30	10	2
	4	25	30	7	2
	5	25	29	8	2
	6	25	33	4	2
	7	23	28	7	6
Spokojenost s IT Službami	8	20	39	5	0
	9	20	42	2	0
	10	30	33	1	0
	11	39	25	0	0
	12	20	42	2	0
	13	35	29	0	0
	14	25	39	0	0

Zdroj: Vlastní výzkum

Pro přehlednost byly údaje z tabulek č. 13 a č. 14 znázorněny v následujících grafech č. 3 a č. 4.

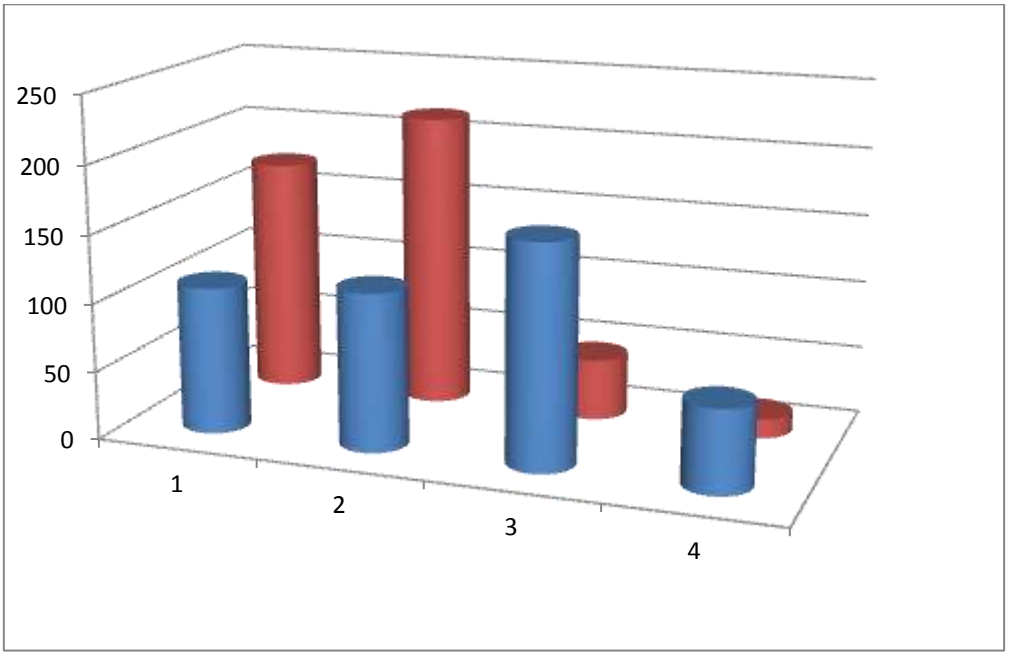
Graf č. 3 názorně porovnává spokojenost s pracovním prostředím mezi rokem 2012 a 2013, kdy modře jsou označeny výsledné údaje z roku 2012 a červeně jsou označeny výsledné údaje z roku 2013.

Spodní osa znázorňuje variantu odpovědí:

1. Určitě ano
2. Spíše ano
3. Spíše ne
4. Určitě ne

Levá osa znázorňuje celkové počty odpovědí k jednotlivým variantám 1 až 4.

Graf 3: Porovnání spokojenosti s pracovním prostředím rok 2012 a rok 2013



Zdroj: autorka práce (vlastní výzkum)

Z grafu č. 3 je patrné, že spokojenost zaměstnanců s pracovním prostředím v roce 2013 je vyšší, než v roce 2012.

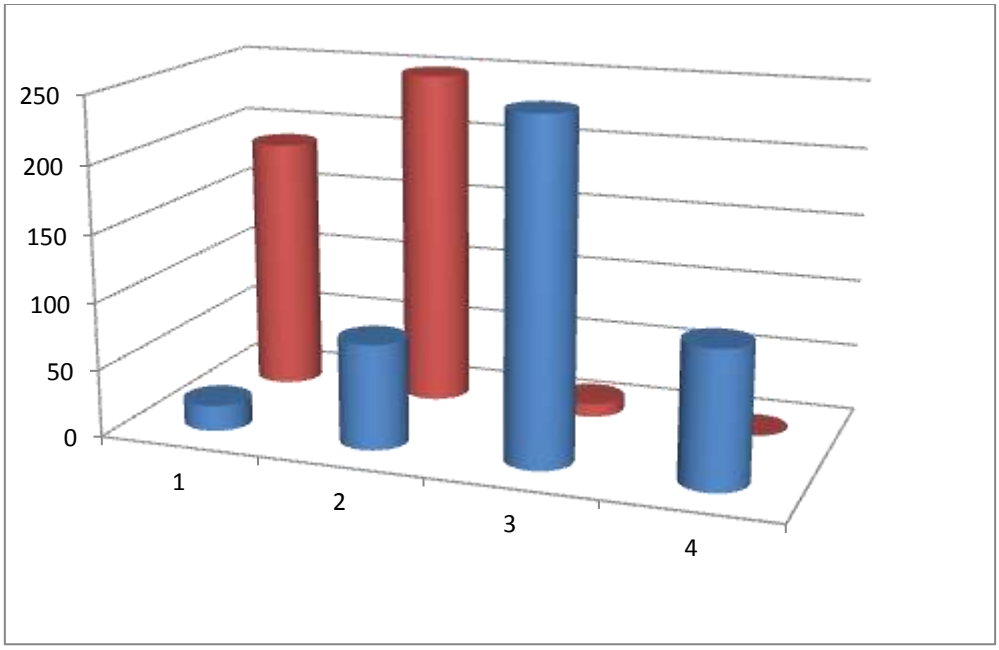
Graf č. 4 názorně porovnává spokojenost s IT službami mezi rokem 2012 a 2013, kdy modře jsou označeny výsledné údaje z roku 2012 a červeně jsou označeny výsledné údaje z roku 2013.

Spodní osa znázorňuje variantu odpovědí:

1. Určitě ano
2. Spíše ano
3. Spíše ne
4. Určitě ne

Levá osa znázorňuje celkové počty odpovědí k jednotlivým variantám 1 až 4.

Graf 4: Porovnání spokojenosti s IT službami rok 2012 a rok 2013



Zdroj: autorka práce (vlastní výzkum)

Z grafu č. 4 je patrné, že se úroveň IT služeb zvýšila, což se promítlo do celkové spokojenosti zaměstnanců v pracovním procesu.

5.3 Vyhodnocení dopadu zavedených opatření na firemní kulturu

Zavedením IT procesů bylo zaměstnancům dáno najevo, že managementu společnosti nejsou lhostejné pracovní podmínky zaměstnanců. Je jasným a viditelným důkazem péče a zájmu managementu o své zaměstnance a o jejich následnou spokojenost v pracovním procesu. Tato péče se stala významným faktorem, který pozitivně ovlivnil chování zaměstnanců s následným promítnutím do firemní kultury společnosti.

Zavedení technologie DLP napomáhá zaměstnancům lépe identifikovat, co jsou citlivé informace společnosti. S pomocí této technologie si zaměstnanci neustále opakují předepsané postupy při práci s citlivými informacemi společnosti. S těmito postupy byli zaměstnanci důkladně seznámeni na školení informační bezpečnosti, která byla zavedena v rámci bakalářské práce autorky, ale byl zde reálný předpoklad, že zaměstnanci některé postupy zapomenou, nebo je postupem času začnou úmyslně opomíjet. Technologie DLP pomáhá zaměstnancům snadněji identifikovat klasifikované citlivé informace společnosti. V případě, že by některý ze zaměstnanců porušil při práci s citlivými informacemi předepsané postupy, je technologií DLP na svou chybu upozorněn a je vyžadováno uplatnění předepsaného postupu. Implementovaná technologie DLP zaměstnance učí, jak správně zacházet s citlivými informacemi společnosti.

Implementací IT procesů a DLP technologie byl učiněn další krok k vytvoření příznivé firemní kultury společnosti. Implementace těchto procesů a technologie se stala součástí cílů, strategií a politik společnosti. Zaměstnanci se lépe orientují v otázkách „kam společnost směruje, o co usiluje a co od každého svého zaměstnance očekává“.

Zároveň byly zlepšeny pracovní podmínky zaměstnanců, což mělo bezprostřední, kladný vliv na jejich postoje k práci. Účinným způsobem se zvýšila důvěra v management společnosti, což přispělo k pozitivní firemní atmosféře ovlivňující v konečném důsledku firemní kulturu společnosti.

Bylo přispěno k vytvoření příznivé image společnosti a to jak ve vztahu k zaměstnancům společnosti, tak ve vztahu k vnějšímu okolí, zejména pak směrem ke klientům společnosti v oblasti odpovědnějšího přístupu k ochraně citlivých informací klientů. Jen takový management společnosti, který projevuje odpovědný přístup ke svým zaměstnancům a klientům vytváří pozitivně laděnou firemním kulturu.

ZÁVĚR

Otázka informační bezpečnosti, IT technologií a firemní kultury je v dnešní době významným tématem.

V kapitole 1 byla pozornost zaměřena na procesy Incident, Problem a Change Management. V rámci těchto procesů byly definovány jednotlivé role a odpovědnosti zaměstnanců společnosti a to na základě doporučení z odborné literatury ITIL V3: Information Technology Infrastructure Library. Tato literatura poskytuje kvalitní, doporučené postupy pro správu IT služeb, avšak univerzální řešení pro správu IT služeb tato literatura nenabízí. Vždy bude záležet na vrcholovém managementu společnosti, jaké doporučení si z této literatury vybere a jak bude následně tato doporučení implementovat do pracovního prostředí společnosti.

Přínosy pro společnost People & Job, s.r.o. v souvislosti se zavedením těchto procesů do pracovního prostředí jsou následující.

Proces Incident Management

Největší riziko bylo v nedokonalé evidenci vědomostní báze, která je vedena u Service Desk společnosti. Vědomostní báze byla vedena nedůsledně a neúplně a to zejména v oblasti kvality informací ukládaných do této vědomostní báze, bez možnosti sdílení a případné korekce informací z řad odborníků. Tím docházelo k opětovné eskalaci incidentů, které již mohly být vyřešeny na 1. úrovni podpory v rámci Service Desk společnosti. Tato skutečnost měla za následek navýšení prodloužení doby řešení jednotlivých incidentů a nárůst požadavků na kapacity odborníků na 2. a 3. úrovni podpory.

Po zavedení procesu Incident Management byla významně zkrácena doba řešení incidentu, včetně jeho nápravy. Uživatelé jsou nyní průběžně informování o průběhu řešení incidentu, což přispělo k pozitivní náladě uživatelů. Uživatelé si uvědomují, že je o ně náležitě pečováno.

Proces Problem Management

Před zavedením tohoto procesu docházelo k opětovné evidenci incidentů se stejným kořenovým problémem. V důsledku toho docházelo ke zbytečnému prodloužení doby řešení incidentů a zatížení kapacity z řad odborníků, kteří neměli dostatek času a kapacit na řešení skutečně naléhavých problémů uživatelů, protože několik z nich řešilo stejný incident, na místo tohoto, aby bylo iniciováno řešení kořenového problému.

Prodloužená doba řešení vzniklých problémů měla rovněž neblahý vliv na spokojenost uživatelů a tím nepříznivě ovlivňovala firemní kulturu společnosti.

Po zavedení procesu Problem Management byla významně zkrácena doba řešení jednotlivých problémů a bylo zamezeno opakování stejných typů incidentů. Tyto aspekty přispěly ke komfortu uživatelů, kteří již nejsou zdržování výpadky IT služeb, což výrazně přispívá k pozitivnímu pracovnímu prostředí.

Proces Change Management

Proces Change Management usnadňuje implementaci změn, které jsou vyvolány požadavky procesů Incident Management a Problem Management. Change Management velkou měrou přispívá k zajištění bezpečnosti pro vedení těchto změn, čímž se snižují rizika plynoucí z implementace změn. Snížení těchto rizik má za následek snížení počtu neplánovaných výpadků informačních systémů, což významně redukuje omezování uživatelů v práci, které bylo způsobováno v důsledku nedostupnosti služeb informačních systémů. Tento fakt má výrazný vliv na spokojenost uživatelů v pracovním procesu a významně ovlivňuje, v pozitivním směru, firemní kulturu.

Rozsah a kvalita těchto procesů vedla k tomu, že IT oddělení je schopno poskytovat svým uživatelům to, co chtějí, ve chvíli, kdy to potřebují. Tyto procesy podpořily otevřenou a vstřícnou komunikaci mezi uživateli a oddělením IT.

Data Loss Prevention

Kapitola 2 a 4 se zabývala implementací technologie Data Loss Prevention (DLP). S pomocí této technologie bylo zajištěno efektivní a koncepční řešení problematiky úniku citlivých informací.

Přínosy implementace technologie DLP pro společnost jsou spatřovány zejména v těchto aspektech. Informační toky v rámci společnosti jsou efektivně identifikovány, označovány a následně řízeny, čímž jsou významně podporovány procesy spojené s řízením informačních aktiv. Byla zajištěna vysoká míra zabezpečení informací se speciálními ochrannými profily a monitoring jejich toků v rámci společnosti. Společnost má tak možnost pro-aktivně chránit svá vysoce důležitá informační aktiva a rychle a efektivně reagovat na detekované narušení bezpečnostní politiky. Implementací technologie DLP si zaměstnanci neustále připomínají, co jsou citlivé informace společnosti, čímž je v této oblasti budováno bezpečnostní povědomí zaměstnanců a dále je budována firemní kultura při nakládání s citlivými informacemi.

Zavedení procesů Incident, Problem, Change Management a implementace DLP technologie významně ovlivňuje firemní kulturu společnosti, která je jedním z účinných nástrojů řízení. Tyto procesy a technologie se staly součástí firemní strategie, cílů a politik společnosti. Zaměstnanci vědí, kam společnost směřuje, o co usiluje a co od každého svého zaměstnance očekává, což pozitivně ovlivňuje vnímání, myšlení, jednání a emoce zaměstnanců.

Zavedené procesy a implementovaná technologie změnily pracovní návyky zaměstnanců a tím se staly jedním z činitelů formování změny postojů zaměstnanců. Postoje zaměstnanců patří mezi významné pilíře firemní kultury. Zaměstnanci přistupují ke svým pracovním činnostem zodpovědněji, což má za následek zvýšení jejich pracovní výkonnosti.

Kromě výše uvedených výstupů bylo z poznatků této práce vrcholovému managementu společnosti doporučeno následující.

- Pokud management identifikuje potřebu změn ve společnosti, je nutné, aby tyto změny byly prosazovány a bylo důsledně řízeno jejich zavádění. Proces změn musí být účinný a neustále viditelný, protože důležité pro úspěch procesu změn je získání zaměstnanců pro změny s následnou realizací změn.

- Jednání managementu má velký vliv na utváření firemní kultury a z tohoto důvodu musí být firemní kultuře věnována každodenní pozornost.

- Management musí podporovat vytvoření příznivého pracovní prostředí a vytvoření pocitu sounáležitosti, protože zaměstnanci musí být hrdi na to, kde pracují.

- Na pozice liniových manažerů by měli být dosazováni zaměstnanci, kteří mají profesionální respekt a jsou schopni naslouchat. Je důležité, aby tito zaměstnanci se svými podřízenými mluvili a byli schopni nejen poradit, ale také zachytit náznaky a signály počátku nějakého problému.

- Management by měl podporovat otevřenou, jasnou komunikaci a nazývat věci pravými jmény. Nejasná a nedostatečná komunikace vede k desinformacím a v konečném důsledku se negativně projeví v oblastech ovlivňujících firemní kulturu.

- Je nutné pečlivě vybírat zaměstnance, zejména pro práci s rizikovými informacemi. Jedná se o velmi efektivní cestu, jak snížit nebezpečí úmyslného či neúmyslného úniku informací.

- Příznivé postoje k úniku informací musí být podporovány vhodnými stimuly a rozvíjením příznivé firemní kultury. Klíčovým postojem se stává vědomí významu bezpečnosti a vědomí odpovědnosti ve vztahu k rizikům. Musí být podporováno vědomí odpovědnosti každého zaměstnance, které se může promítat v procesech hodnocení a odměňování zaměstnance a to podle toho do jaké míry se jeho odpovědnosti naplňují.

Charakteristické pro firemní kulturu je to, že její projevy nelze nařídit. Pozitivně laděná firemní kultura bývá doprovázena otevřeností a vzájemnou důvěrou mezi zaměstnanci, což je předpokladem pro spolupráci, sdílení informací a ochotu zaměstnanců pracovat a využívat svých schopností ve prospěch společných zájmů a cílů společnosti, ve které pracují.

Pokud management zahrne firemní kulturu do svých úvah, stane se firemní kultura velmi účinným nástrojem řízení.

SEZNAM POUŽITÝCH ZDROJŮ

Seznam použitých českých zdrojů

AMSTRONG, Michael. *Management a leadership*. 1. vyd. Praha: Grada, 2008. ISBN: 978-80-247-2177-4

AMSTRONG, Michael. *Řízení lidských zdrojů. Nejnovější trendy*. 10. vyd. Praha: Grada, 2007. ISBN: 978-80-247-1407-3

BROOKS, Ian. *Firemní kultura: jedinci, skupiny, organizace a jejich chování*. 1. vyd. Brno: Computer Press, 2003. ISBN: 80-7226-763-9

BARTÁK, Jan. *Skryté bohatství firmy.* 1. vyd. Praha: Alfa, 2006. ISBN: 80-86851-17-6

DYTRT, Zdenek. *Dobré jméno společnosti*. 1. vyd. Praha: Alfa, 2006. ISBN: 80-86851-45-1

GOLLOVÁ, Marta. *Budování systému bezpečnosti informací společnosti a zvyšování bezpečnostního povědomí zaměstnanců.* Praha, 2012. Bakalářská práce. UJAK, Katedra Andragogiky. Vedoucí práce: Jiří Víšek

HENDL, Jan. *Kvalitativní výzkum: základní metody a aplikace.* 1. vyd. Praha: Portál, 2005. ISBN: 80-7367-040-2

KOBLIHA, Ivan. et al. *Obchodní zákoník: úplný text zákona s komentářem: Podle stavu k 1.4.2006.* Praha: Linde, 2006. ISBN: 80-7201-564-8

KOUBEK, Josef. *Řízení lidských zdrojů. Základy moderní personalistiky*. 4. vyd. Praha: Management Press, 2012. ISBN: 978-80-7264-168-3

LUKÁŠOVÁ, Růžena., NOVÝ, Ivan. a kol. *Organizační kultura. Od sdílených hodnot a cílů k vyšší výkonnosti podniku.* 1. vyd. Praha: Grada, 2004. ISBN: 80-247-0648-2

MICHALÍK, David., PALEČEK, Miloš. *Kultura bezpečnosti. Metodická příručka.* 1. vyd. Praha: Výzkumný ústav bezpečnosti práce, 2010. ISBN: 978-80-86973-05-0

NAKLADATELSTVÍ SAGIT. *Úplné znění Trestní předpisy číslo 768: Podle stavu k 1.1.2010*. Ostrava: Sagit, 2010. ISBN: 978-80-7208-782-2

PFEIFER, Luděk., UMLAUFOVÁ, Miloslava. *Firemní kultura. Konkurenční síla sdílených cílů, hodnot a priorit.* 1. vyd. Praha: Grada Publishing, 1993. ISBN: 80-7169-018-X

SCHMIED, Zdeněk., JAKUBKA, Jaroslav. *Zákoník práce 2012 s výkladem: Právní stav k 1.1.2012*. 13. vyd. Praha: Grada. 2012. ISBN: 978-80-247-4031-7

SILVESTER, Joanne. et al. *Psychologie práce pro manažery a personalisty*. 1. vyd. Brno: Computer Press, 2007. ISBN: 978-80-251-1518-3

ŠIGUT, Zdeněk. *Firemní kultura a lidské zdroje*. 1. vyd. Praha: ASPI Publishing, 2004. ISBN: 80-7357-046-7

UZEL, Jaroslav. *Firemní kultura-její význam pro management, bezpečnost a ochranu zdraví při práci.* 1. vyd. Praha: Výzkumný ústav bezpečnosti práce, 2006. ISBN: 80-86973-03-4

Seznam použitých zahraničních zdrojů

HARRIS, Shon. ALL IN ONE CISSP EXAM GUIDE Sixth Edition. USA: Copyright by McGraw-Hill Companies, 2013. ISBN: 978-0-07-178173-2

ITIL. *Continual Service Improvement.*1st. published. London, UK: by TSO, 2007. ISBN: 978 0 11 331049 4

ITIL. *Service Design*. 1st.published. London, UK: by TSO, 2007. ISBN: 978 0 11 331047 0

ITIL. *Service Operation*. 1st.published. London, UK: by TSO, 2007. ISBN: 978 0 11 331046 3

ITIL. *Service Strategy*. 1st.published. London, UK: by TSO, 2007. ISBN: 978 0 11 331045 6

ITIL. *Service Transition*. 1st.published. London, UK: by TSO, 2007. ISBN: 978 0 11 331048 7

ITIL. *The Official Introduction to the ITIL Service Lifecycle*.1st. published. London: by TSO, 2007. ISBN: 9780113310616

LONG, John. O. *ITIL Version 3 at a Glance: Information Quick Reference*. New York, USA: by Springer Science+Business Media, LLC, 2008. ISBN: 978-0-387-77392-6

Seznam použitých internetových zdrojů

RSA. *RSA Customer Profiles:Data Loss Prevention (DLP).* [online]. [cit. 2013-04-06]. Dostupné z: http://www.emc.com/collateral/customer-profiles/h12158-rsa-dlp-cp.pdf

LISTINA ZÁKLADNÍCH PRÁV A SVOBOD [online]. [cit. 2013-07-16]. Dostupné z: http://www.psp.ct/docs/laws/listina.html

Zákony

Zákon č. 101/2000 Sb., o Ochraně osobních údajů a o změně některých zákonů ve znění pozdějších předpisů

Zákon č. 121/2000 Sb., o Právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)

Zákon č. 513/1991 Sb., Obchodní zákoník ve znění pozdějších předpisů

Zákon č. 262/2006 Sb., Zákoník práce ve znění pozdějších předpisů

Zákon č. 40/2009 Sb., Trestní zákoník ve znění pozdějších předpisů

SEZNAM OBRÁZKŮ, TABULEK, GRAFŮ, DIAGRAMŮ A SCHÉMAT

Seznam obrázků

Seznam tabulek

Seznam grafů

Seznam diagramů

Seznam schémat

SEZNAM PŘÍLOH

Příloha A - Termíny a definice

Aktivum: cokoli, co má pro organizaci hodnotu/význam (informace; služby; software/počítačový program; lidé a jejich kvalifikace/dovednosti/praxe; pověst/image společnosti)

Analýza rizik: systematické použití informací k identifikaci zdrojů a k odhadu rizika

Bezpečnostní Incident: jednotlivá nechtěná a neočekávaná událost, nebo série nechtěných a neočekávaných bezpečnostních událostí, které mají významnou pravděpodobnost kompromitování obchodních operací a ohrožení bezpečnosti informací

Bezpečnost informací: ochrana Integrity; Dostupnosti; Důvěrnosti

Change Management (Řízení změn): proces přecházení ze stávajícího stavu do požadovaného stavu tak, aby byla minimalizována rizika plynoucí z této změny

Change Coordinator (Koordinátor změny): koordinuje činnosti a zaměstnance v rámci procesu Change Management

Change ticket: souhrnný záznam změny tzn. záznam požadavku na změnu, řešení změny, ukončení změny

Configuration Management (CM): řídí záznamy v databázi konfigurací (CMDB)

Configuration Management Database (CMDB): Databáze stávajících konfigurací, kde je zaznamenán stávající stav IT infrastruktury a softwaru

Dostupnost – vlastnosti přístupnosti a použitelnosti na žádost autorizované entity

Důvěrnost – vlastnost, že informace není dostupná, nebo není odhalena neautorizovaným jednotlivcům nebo procesům

Data Loss Prevention (DLP): ochrana před únikem dat

Gateway: brána do počítačové sítě

Hodnocení rizika: proces odhadnutého rizika s danými kritérii rizika = určení významnosti rizika

Hrozba: potenciální příčina nechtěného Incidentu, jehož výsledkem může být poškození systému nebo společnosti

Information Technology (IT): Informační technologie

ID: identifikační číslo

Incident Management (Řízení Incidentů): řeší obnovu služeb pro uživatele služeb

Incident Manager: je vlastníkem procesu Incident Management

ISMS: část celého systému řízení, založená na přístupu k bezpečnostním rizikům, k ustanovení, implementování, provozování, monitorování, přezkoumávání, spravování a zlepšování bezpečnosti informací

Ticket: záznam v informačním systému

Key Performance Indicator (KPI): klíčový ukazatel výkonnosti definovaných procesů

Leadership: styl vedení a motivace jednotlivých podřízených zaměstnanců a týmů

Local Area Network (LAN): v informatice počítačová síť, která pokrývá malé geografické území, jedná se o sítě uvnitř místností, areálů či budov

Požadavek na změnu: požadavek na malou změnu

Problem Management (Řízení problémů): identifikace a odstraňování příčin problémů pro které není známo standardní řešení

Problem Manager: je vlastníkem procesu Problem Management

Problem Coordinator: koordinuje činnosti a zaměstnance v rámci procesu Problem Management

Problem ticket: záznam problému

Proxy server: odděluje vnitřní síť od internetu, tzn.: zajišťuje komunikaci lokální počítačové sítě s internetem

Personální informační systém (PIS): systém odpovídající potřebám moderního řízení společnosti tj. uchovává, zpracovává a poskytuje informace o personální práci společnosti

Riziko: kombinace pravděpodobnosti události a jejího následků

Řízení rizik: koordinované činnosti sloužící k řízení a kontrole společnosti vzhledem k riziku

Service Desk (SD): je primárním centrálním bodem moderní společnosti pro kontakt se všemi uživateli IT. Jsou zde spravovány a řešeny veškeré IT Incidenty (něco nefunguje, jak má) a požadavky na změnu (přístup do databáze, žádost o nový notebook aj.)

Software (SW): sada všech počítačových programů používaných v počítači, taktéž programové vybavení

Hardware (HW): technické vybavení počítače (monitor, klávesnice, myš aj.)

Service Level Agreement (SLA): dohoda o úrovni, rozsahu a požadované kvalitě dodávky služeb

Wide Area Network (WAN): je v informatice počítačová síť, která pokrývá rozlehlé geografické území překračující hranice měst, regionu či státu. Sítě WAN jsou využívány pro spojení sítí LAN, což umožní, že uživatelé z jednoho místa mohou komunikovat s uživateli a počítači na jiném, vzdáleném místě.

Příloha B – Etický kodex společnosti

Etický kodex

- **Náš cíl**

Naším cílem je snaha vybudovat osobní vztah založený na vzájemné důvěře a otevřenosti mezi námi, klientem a kandidátem.

- **Transparentnost**

Všem zúčastněným stranám poskytujeme vždy maximum relevantních informací.

- **Reference**

Reference ověříme diskrétně, zpracujeme pečlivě a objektivně.

- **Diskrétnost**

S důvěrnými informacemi a materiály, které nám jsou svěřeny, zacházíme vždy s nejvyšší možnou opatrností a nikdy je neposkytneme třetí straně bez předchozího souhlasu, a to ani po ukončení spolupráce.

- **Kvalita**

Doporučíme pouze ty kandidáty, kteří nejlépe vyhovují požadavkům příslušného pracovního místa. Při výběru posuzujeme nejen odborné, ale i osobnostní charakteristiky uchazeče.

- **Odpovědnost**

Jsme si vědomi, že neseme odpovědnost za průběh a výsledek procesu výběru vhodných kandidátů, a proto máme snahu se neustále rozvíjet a zdokonalovat k maximální spokojenosti našich klientů.

Příloha C – Politika kvality a bezpečnosti informací společnosti People & Job, s.r.o.

People & Job s.r.o. je spolehlivá a profesionálně vedená společnosti. Stěžejním předmětem činnosti společnosti je personální poradenství, služby psychologů a školení.

Základním cílem je uspokojování požadavků klienta, a to hlavně trvalým zvyšováním kvality našich služeb, flexibilním přístupem k požadavkům klienta a ochraně informací jak vlastních, tak informací klientů.

Jako nejdůležitější požadavky klienta vidíme:

- vysokou spokojenost s kvalitou námi poskytovaných služeb;
- dodržování sjednaných termínů;
- péči o klienta, v průběhu celého životního cyklu;
- systematické řízení bezpečnosti informací vlastních i svěřených klienty s cílem eliminovat, či snížit rizika související s možným narušením důvěrnosti, integrity, nebo dostupnosti informací a dat;
- poskytování kvalitních služeb, které přinesou klientům další přidanou hodnotu.

Vedení společnosti a zaměstnanci se pro splnění požadavků klienta zavazují k:

- neustálému zvyšování odborné kvalifikace a zvyšování povědomí o zásadách ochrany informací;
- motivování všech svých kolegů k zajištění ochrany vlastních i svěřených informací, týmové práci a realizaci procesů zlepšování kvality a informační bezpečnosti;
- vedení společnosti se zavazuje zajistit podporu a koordinaci a zajištění zdrojů pro zavádění principů kvality a bezpečnosti informací;
- spolupráci s kvalitními partnery;
- dodržování relevantních právních předpisů a smluvních závazků;
- osobní angažovanosti, vysokému pracovnímu nasazení a odpovědnosti za kvalitu odvedené práce;
- dodržování požadavků systému řízení kvality a bezpečnosti informací.

Integrovaný přístup k řízení:

• na základě požadavků zákazníka stanovovat a přezkoumávat cíle kvality a bezpečnosti informací;

• identifikovat procesy z hlediska jejich efektivity a výkonnosti, systematicky měřit způsobilost a výkonnost procesů a analyzovat výsledky z měření jednotlivých procesů a tyto výsledky zpětně využívat k řízení a zlepšování procesů;

• monitorovat a řídit bezpečnostní rizika, přijímat bezpečnostní opatření pro snížení jejich vlivu;

• systematicky, objektivně a pravidelné hodnotit výkonnost integrovaného systému řízení;

• neustále zlepšovat integrovaný systém řízení Management jakosti (QMS) dle požadavků normy ČSN EN ISO 9001:2009 a systému řízení bezpečnosti informací (ISMS) dle požadavků normy ČSN ISO/IEC 27001:2006;

• identifikovat strategické záměry společnosti a seznamovat s nimi všechny zaměstnance;

• definovat činnosti a prostředky pro dosažení cílů kvality a ochrany informací se zřetelem na neustálé zlepšování.

Společnosti se tímto zavazuje k dodržování platných právních předpisů v oblasti integrovaného systému řízení (QMS a ISMS) a k zajištění potřebných finančních a dalších zdrojů pro splnění stanovených zásad.

Výše uvedená politika a její zásady jsou závazné pro všechny zaměstnance společnosti People & Job, s.r.o.

Příloha D - Dotazník hodnocení spokojenosti zaměstnanců s pracovním prostředím a s IT službami

Vážení zaměstnanci vyplněním dotazníku nám pomůžete získat objektivní pohled na spokojenost vás, zaměstnanců v naší společnosti, čímž výrazně přispějete k následnému zlepšení pracovních podmínek. Odpovědi, které uvedete, jsou zcela anonymní.

1. **JSTE DOBŘE INFORMOVÁN/A O CÍLECH A POSLÁNÍCH SPOLEČNOSTI VE KTERÉ PRACUJETE?**

- Určitě ano
- Spíše ano
- Spíše ne
- Určitě ne

2. **JSTE SPOKOJEN S PRACOVNÍM PROSTŘEDÍM SPOLEČNOSTI, VE KTERÉ PRACUJETE?**

- Určitě ano
- Spíše ano
- Spíše ne
- Určitě ne

3. **JSTE SPOKOJEN S ATMOSFÉROU NA PRACOVIŠTI?**

- Určitě ano
- Spíše ano
- Spíše ne
- Určitě ne

4. **JSOU VAŠI KOLEGOVÉ OCHOTNI VÁM V PRACOVNÍCH ZÁLEŽITOSTECH POMOCI, POKUD TO POTŘEBUJETE, NEBO O TO POŽÁDÁTE?**

- Určitě ano
- Spíše ano
- Spíše ne
- Určitě ne

5. **JSTE SPOKOJEN/A S TÍM, JAK PRACOVNÍ TÝM FUNGUJE?**

- Určitě ano
- Spíše ano
- Spíše ne
- Určitě ne

6. **JSOU VAŠI PŘÍMÍ NADŘÍZENÍ PŘIPRAVENI VYSLECHNOUT VÁS, KDYŽ TO POTŘEBUJETE?**

- Určitě ano
- Spíše ano
- Spíše ne
- Určitě ne

7. **MÁTE MOŽNOST PŘI PRÁCI V TÉTO SPOLEČNOSTI ROZVÍJET SVÉ PROFESNÍ SCHOPNOSTI?**

- Určitě ano
- Spíše ano
- Spíše ne
- Určitě ne

8. **JSTE SPOKOJEN/A S PROFESIIONALITOU PACOVNÍKŮODDĚLENÍ IT SLUŽEB (ZNALOST A SCHOPNOST OPODVĚDĚT NA TECHNICKÉ PROBLÉMY)?**

- Určitě ano
- Spíše ano
- Spíše ne
- Určitě ne

9. **JSTE SPOKOJEN/A SE VSTŘÍCNOSTÍ PRACOVNÍKŮODDĚLENÍ IT SLUŽEB PŘI ŘEŠENÍ VAŠICH POŽADAVKŮ (OCHOTA VYHOVĚT, PŘÍJEMNÉ JEDNÁNÍ AJ.)?**

- Určitě ano
- Spíše ano
- Spíše ne
- Určitě ne

10. **JSTE SPOKOJEN/A S REČAKČNÍ DOBOU ODDĚLENÍ IT SLUŽEB NA VAŠE POŽADAVKY (KDY SE S VAŠÍM POŽADAVKEM ZAČNE ODDĚLENÍ IT SLUŽEB ZABÝVAT)?**

- Určitě ano
- Spíše ano
- Spíše ne
- Určitě ne

11. JSTE PRŮBĚŽNĚ INFORMOVÁNI ODDĚLENÍM IT SLUŽEB O ŘEŠENÍ VAŠEHO POŽADAVKU?

- Určitě ano
- Spíše ano
- Spíše ne
- Určitě ne

12. JE VÁŠ POŽADAVEK NA ZMĚNU IT SLUŽBY ŘEŠEN DOSTATEČNĚ RYCHLE?

- Určitě ano
- Spíše ano
- Spíše ne
- Určitě ne

13. JE VÁM POSKYTNUTA Z ODDĚLENÍ IT SLUŽEB ZPĚTNÁ VAZBA Z NAHLÁŠENÝCH INCIDENTŮ?

- Určitě ano
- Spíše ano
- Spíše ne
- Určitě ne

14. JSTE CELKOVĚ SPOKOJEN/A S POSKYTOVYNÝMI IT SLUŽBAMI?

- Určitě ano
- Spíše ano
- Spíše ne
- Určitě ne

15. CO BYSTE SI PŘÁL/A ZLEPŠIT NA FUNGOVÁNÍ ODDĚLENÍ IT SLUŽEB?

16. PROSTOR PRO VLASTNÍ POSTŘEHY A NÁMĚTY.

BIBLIOGRAFICKÉ ÚDAJE

Jméno autora: Marta Gollová

Obor: Andragogika

Forma studia: Kombinovaná

Název práce: Budování firemní kultury prostřednictvím vybraných bezpečnostních a IT procesů

Rok: 2014

Počet stran: 125

Celkový počet stran příloh: 9

Počet titulů české literatury a pramenů: 22

Počet titulů zahraniční literatury a pramenů: 8

Počet internetových zdrojů: 2

Vedoucí práce: PhDr. Jan Mattioli, Ph.D.