Vysoká škola regionálního rozvoje a Bankovní institut – AMBIS

Katedra ekonomie a managementu

Informační bezpečnost a ochrana informací v podniku

Diplomová práce

Autor: **Bc. Josef Novotný**

Management, Strategický management

Vedoucí práce: **doc. RNDr. Juraj Pančík, CSc.**

Praha **2020**

Prohlášení

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a v seznamu uvedl veškerou použitou literaturu.

Svým podpisem stvrzuji, že odevzdaná elektronická podoba práce je identická s její tištěnou verzí, a jsem seznámen se skutečností, že se práce bude archivovat v knihovně VŠ AMBIS a dále bude zpřístupněna třetím osobám prostřednictvím interní databáze elektronických vysokoškolských prací.

V Jesenici, dne 30. dubna 2020 *Josef Novotný*

Poděkování

Velmi děkuji vedoucímu mé diplomové práce doc. RNDr. Juraji Pančíkovi, CSc. za vstřícné vedení, cenné rady a inspirativní podněty při psaní diplomové práce.

Moje díky patří také mé manželce za to, že mi byla během přípravy této práce a v průběhu celého studia velkou oporou.

Ambis. VYSOKÁ ŠKOLA REGIONÁLNÍHO ROZVOJE A BANKOVNÍ INSTITUT – AMBIS

ZADÁNÍ DIPLOMOVÉ PRÁCE

Akademický rok: 2018/2019

Student: Josef Novotný

UČO: 23994

Program:	Ekonomika a management
Studijní obor:	Management
Téma:	Informační bezpečnost a ochrana informací v podniku
Topic:	Information security and information protection in the company
Vedoucí diplomové práce:	doc. RNDr. Juraj Pančík, CSc.
Cíl práce:	TÉMA DIPLOMOVÉ PRÁCE: Informační bezpečnost a ochrana informací v podniku HLAVNÍ CÍL: Návrh řídících dokumentů a školících dokumentů pro uplatnění zákona o kybernetické bezpečnosti v prostředí konkrétní firmy. Návrh interního projektu pro zabezpečení uplatnění zákona. ÚVOD 1. TEORETICKÁ ČÁST: Vymezení základních pojmů v předmětné oblasti. 2. ANALYTICKÁ ČÁST: Přehled výsledků průzkumu stavu informační bezpečnosti v podnicích. Analýza dopadu uplatňování GDPR v prostředí firmy. 3. NAVRHOVĚ-REALIZAČNÍ ČÁST: Návrh řídích dokumentů a školících dokumentů pro uplatnění zákona o kybernetické bezpečnosti v prostředí konkrétní firmy. Návrh interního projektu pro zabezpečení uplatnění zákona. ZÁVĚR
Základní prameny a odborná literatura:	NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4. GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi. 3., aktualizované vydání. Praha: Grada Publishing, 2015. Management v informační společnosti. ISBN 978-80-247-5457-4. DOHNAL, Jan a Jan POUR. IT v řízení podniku: MBI. Praha: Professional Publishing, 2016. ISBN 978-80-7431-160-4. ÚZ č.1320 Svobodný přístup k informacím, Informatika, eGovernment. Ostrava: Sagit, 2019. ISBN 978-80-7488-354-5. LAUDON, Kenneth C. a Jane P. LAUDON. Essentials of management information systems. 10th ed. Boston: Pearson, c2013. ISBN 978-0-13-266855-2.

Souhlasím se zadáním (podpis, datum): 30.8.2019

.....
Josef Novotný
student

.....
doc. RNDr. Juraj Pančík, CSc.
Vedoucí diplomové práce

Anotace

Diplomová práce se zabývá problematikou ochrany bezpečnosti informací a s ní souvisejících zákonů a jejich implementací do podnikových procesů.

Práce je rozdělena na tři části: teoretickou, analytickou a návrhovou. V první části se autor zabývá vysvětlením základních pojmů a legislativních dokumentů, v analytické části zkoumá publikované výzkumy od EY, NÚKIB a PwC týkající se bezpečnosti informací a popisuje interní projekt na zajištění souladu s GDPR, včetně nápravných opatření. Ve třetí části autor navrhuje řídící dokumenty – směrnici pro Organizaci a řízení bezpečnosti informací. Navrhuje školící materiály včetně testů a interní projekt pro certifikaci firmy na normu ISO/IEC 27000:2013. Vzor směrnice a prezentace pro školení jsou uvedeny jako přílohy.

Klíčová slova

Bezpečnost, informace, aktiva, zranitelnosti, hrozby, rizika, školení.

Annotation

The diploma thesis deals with the issue of the information security protection and related laws and their implementation into the business processes.

The study is divided into three parts: theoretical, analytical and design. In the first part, author explains the basic concepts and legislative documents, in the analytical part examines published research from EY, NÚKIB and PwC on information security and describes an internal project to ensure compliance with GDPR, including corrective measures. In the third part author proposes governing documents - a directive for the Organization and Management of Information Security. It designs training materials including tests and an internal project for the company's certification to the standard ISO / IEC 27000: 2013. A sample guideline and a presentation for the training are provided as annexes.

Keywords

Security, information, assets, vulnerabilities, threats, risks, training.

Obsah

Úvod

Cílem práce je návrh řídících a školících dokumentů pro uplatnění kybernetického zákona a návrh interního projektu pro zabezpečení uplatnění zákona. Práce je rozdělená do třech hlavních kapitol.

V první kapitole autor vymezuje základní pojmy z předmětné oblasti, zabývá se tématy jako informační bezpečnost, ochrana informací v podniku, standard GDPR a zákon o kybernetické bezpečnosti. Tyto pojmy spolu dohromady tvoří rámec, ve kterém se autor v dalších kapitolách pohybuje.

V druhé kapitole, nazvané Analytická část, nejprve autor analyzuje již existující průzkumy stavu informační bezpečnosti z veřejně dostupných zdrojů, konkrétně jsou to průzkumy EY, NÚKIB a PwC. V druhé části je pak popsán projekt na řešení dopadu uplatňování GDPR v prostředí konkrétní firmy, autor zde představuje projekt rozfázovaný do třech etap, včetně možných nápravných opatření.

Hlavnímu cíli práce je věnována třetí kapitola. Autor zde navrhuje řídící dokumenty, kdy detailně rozpracovává směrnici „Organizace a řízení bezpečnosti informací“ a připravuje školící materiály včetně testů ve dvou variantách. Jako interní projekt pro zabezpečení uplatnění zákona navrhuje projekt na certifikaci firmy na normu ISO/IEC 27000:2013.

1 Vymezení základních pojmů v předmětné oblasti

Žijeme ve společnosti, která se spoléhá na informační systémy a začíná na nich být ve velké míře závislá. Ohrožení jejich funkčnosti může způsobit ohrožení fungování základní infrastruktury potřebné pro život.

Informační bezpečnost, počítačová nebo kybernetická bezpečnost, jsou pojmy, které vymezují velkou oblast, týkající se ochrany moderních systémů a jejich využívání, a zahrnují pod sebe téměř vše, co se dá pro bezpečnost a ochranu takových systémů využít. Nasazení počítačů nebo speciálních, počítačem řízených strojů, je dnes naprosto běžnou věcí, která nepotřebuje žádnou další popularizaci. V oblasti bezpečnosti a ochrany těchto systémů je ale stále ještě mnoho otevřených otázek a problémů k řešení. Roste význam jak technické, tak organizační ochrany, přičemž je potřeba konstatovat, že funkční celek představuje pouze naprosté vyvážení a kvalitní řešení každého z těchto obou bodů. Zde více, než kdy jindy, platí klasické rčení, že řetěz je právě tak silný, jako jeho nejslabší článek. Počítačové systémy a sítě mohou představovat velmi rozlehlý, a i víceméně autonomní organismus, jehož ochrana je náročná, jak z hlediska technických prostředků, tak i z hlediska organizačních prvků, procesů a návyků, včetně ošetření hrozby lidského faktoru. Velmi výstižně tuto problematiku vystihl Kevin Mitnick ve své knize Umění klamu (Mitnick, 2003), kde popisuje, jak sofistikované systémy a zábrany překonal pomocí technik sociálního inženýrství. Tato kniha byla napsána v roce 2001, což je z hlediska vývoje počítačových technologií již velmi dávno, ale její platnost přetrvává v nezměněné podobě i do dnešní doby.

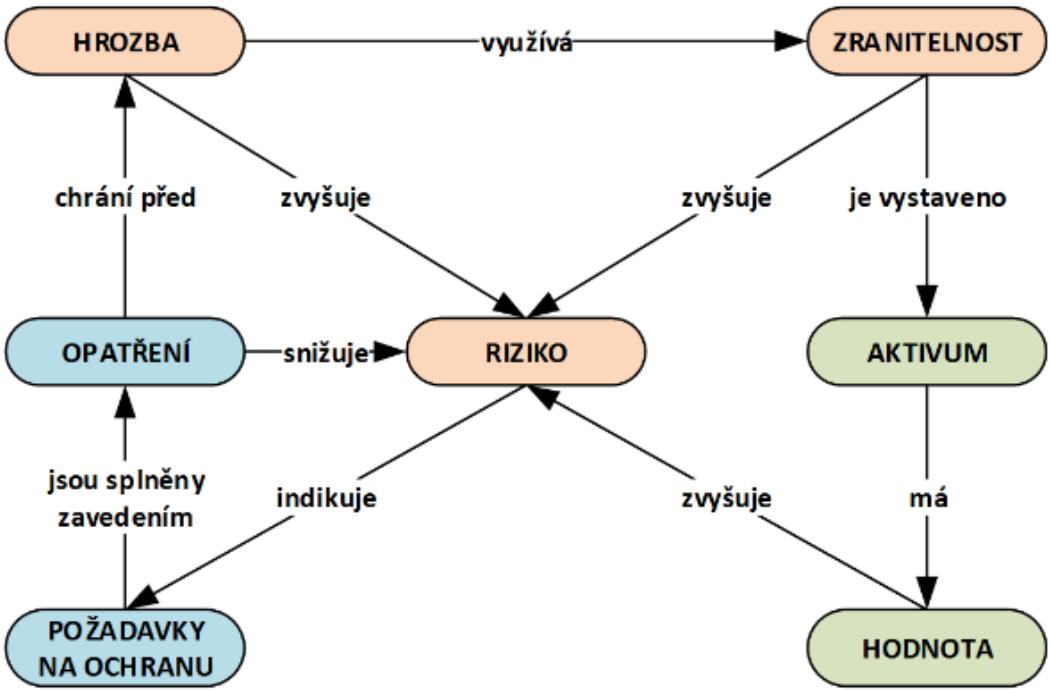
V oblasti informační bezpečnosti se v českém právním prostředí opíráme zejména o dva stěžejní prvky. Prvním z nich je zákon č. 181/2014 Sb., což je „Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů“, ke kterému patří vyhláška o kybernetické bezpečnosti č. 82/2018 Sb., celým názvem „Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat“, a druhým je „Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů“, vžitým názvem tohoto nařízení je i v Česku používaná zkratka anglického názvu GDPR (General Data Protection Regulation). S tímto nařízením souvisí i zákon č. 110/2019 Sb. o zpracování osobních údajů, jenž je prováděcím zákonem GDPR pro Českou republiku.

Řízením informační bezpečnosti se rovněž zabývají mezinárodní normy ISO/IEC, kde základní normou je norma ČSN ISO/IEC 27001 – Systémy řízení bezpečnosti informací – Požadavky.

1.1 Informační bezpečnost

Bezpečnost informačního systému je nutné vnímat jako samostatnou a vysoce specializovanou vlastnost informačního systému. Aby bylo možné dosáhnout uspokojivého stavu, je potřeba mít ošetřené všechny aspekty, které ji mohou nějak ovlivňovat nebo jsou s ní přímo provázány, přičemž tento stav není stálý a je nezbytné neustále pracovat na jeho udržení, protože zajištění informační bezpečnosti je kontinuální proces, a protože i jednotlivé hrozby se stále vyvíjejí.

Pro potřeby jednotného pojmenování při řešení bezpečnosti, případně jejím auditování, se ustálily některé základní pojmy, které jsou, včetně jejich vzájemných vazeb, znázorněny na obrázku 1.



Obrázek 1: Přehledové schéma k řízení rizik. Zdroj: (SMEJKAL, RAIS, 2013)

1.1.1 Informace

Výklad tohoto pojmu může být velmi široký a subjektivní. Slovníková definice uvádí: „*Ve světě počítačů slouží informace ke zpracování, skladování nebo přenášení dat. V běžném životě je akt informování chápán jako komunikace za účelem získání nebo sdělení nových skutečností.*“ (IT SLOVNÍK, 2020). Z pohledu počítačových systémů je informace

nespecifikovaný soubor dat a proto není rozdílu, mluvíme-li o ochraně informací nebo ochraně dat zpracovávaných v rámci počítačových systémů. Nicméně, z pohledu využití mimo počítačovou terminologii, vnímáme informaci jako nějaké sdělení nebo zprávu. Oba tyto pohledy je potřeba v rámci ochrany informací řešit. *„Informace je pojmenování pro obsah toho, co se vymění s vnějším světem, když se mu přizpůsobujeme a působíme na něj svým přizpůsobováním.“* (Gála, 2015, s. 13).

1.1.2 Informační aktiva

Aktiva jsou jednotlivé části informačního systému a jsou charakterizovány svou hodnotou a také zranitelností. Dle vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb., máme jejich rozdělení do třech skupin:

a) Primární aktiva

   Primární aktiva jsou informace nebo služba, kterou zpracovává nebo poskytuje informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém.

b) Podpůrná aktiva

   Podpůrná aktiva jsou technická aktiva, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.

c) Technická aktiva

   Technickými aktivy rozumíme technické vybavení, komunikační prostředky a programové vybavení informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému a objekty, ve kterých jsou tyto systémy umístěny.

Kritická informační infrastruktura je klíčová pro chod firmy a její ochrana je důležitá pro eliminaci možnosti, že jejím poškozením nebo zneužitím dojde ke krizové situaci.

1.1.3 Hodnota aktiva

Tento pojem je relativní a určuje se např. podle nákladů na pořízení, nákladů na vývoj, nebo nákladů na znovuobnovení konkrétního aktiva.

1.1.4 Zranitelnosti

Vyhláška o kybernetické bezpečnosti č. 82/2018 Sb. definuje zranitelnost jako slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.

Zranitelnost rozeznáváme (Gála, 2015, s. 214) v několika kategoriích:

a) Fyzickou – riziko poškození, zničení nebo ztráty.

b) Přírodní – riziko živelních pohrom.

c) Technologickou – zde se jedná o skutečnost, že tato jedna konkrétní část informačního systému je již z podstaty navržena tak, že není schopna vyhovět např. nepřetržitému provozu bez nutnosti pravidelných servisních odstávek. Toto riziko lze eliminovat zdvojením systému nebo jinou formou redundance, která následně umožní bez-výpadkový provoz.

d) Fyzikální – riziko fyzikálních principů, např. elektromagnetické vyzařování monitorů nebo kabelů.

e) Lidskou – riziko ohrožení vlivem lidských omylů.

Zranitelnost aktiva je ovlivněna jeho citlivostí (riziko, že bude poškozeno) a kritičností, tedy jeho kritičností pro daný informační systém (Gála, 2015, s. 215).

1.1.5 Hrozby

Hrozbou rozumíme potenciální příčinu nežádoucího stavu nebo jevu, který je způsobilý poškodit nebo jinak nežádoucím způsobem ovlivnit chráněná primární nebo podpůrná aktiva.

Hrozby jsou možnosti, jak využít zranitelného místa k samotnému útoku na dané aktivum. Kybernetické útoky mohou být cílené, kdy je daná organizace středem zájmu útočníka nebo necílené, kdy robot plošně zkouší skenovat známé zranitelnosti na celém rozsahu sítě, aby následně identifikoval neošetřenou zranitelnost a tato pak byla využita k útoku na konkrétní aktivum nebo celou lokální síť.

1.1.6 Analýza rizik

Analýza rizik je nezbytnou součástí řízení rizik, jejímž prostřednictvím se na základě hrozeb a zranitelností zjišťuje míra nebezpečí, resp. úroveň hrozby, které je organizace vystavena. Na základě zpracované a schválené metodiky určuje také hodnotu aktiv a míru rizika

pro jednotlivá aktiva, jak jsou její aktiva zranitelná, jaká je pravděpodobnost zranitelnosti a jaký dopad to může mít na organizaci.

1.1.7 Riziko

Ve vyhlášce o kybernetické bezpečnosti je uvedeno, že rizikem rozumíme *„možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu"*(Vyhláška č. 82/2018 Sb.). Platí, že riziko přiměřeně vzrůstá s identifikací hrozeb a zranitelností. „*Velikost rizika je vyjádřena jeho úrovní, přičemž úroveň rizika je určena hodnotou aktiva, zranitelností aktiva a úrovní hrozby*" (Gála, 2015, s. 216). Existuje-li pojmenované riziko, lze k němu přijmout protiopatření, kterým úroveň rizika snížíme. Výsledné riziko hrozby působící na identifikované aktivum společnosti se vyjadřuje Mírou rizika (MR).

1.1.8 Opatření

Opatření vůči riziku stanovujeme úměrně podle míry rizika a nákladů na jeho eliminaci. Obvykle se po zpracování analýzy rizik zpracuje „Plán zvládání rizik" pro následující rizikové skupiny:

Tabulka 1: Stupnice rizikových skupin. Vlastní práce autora

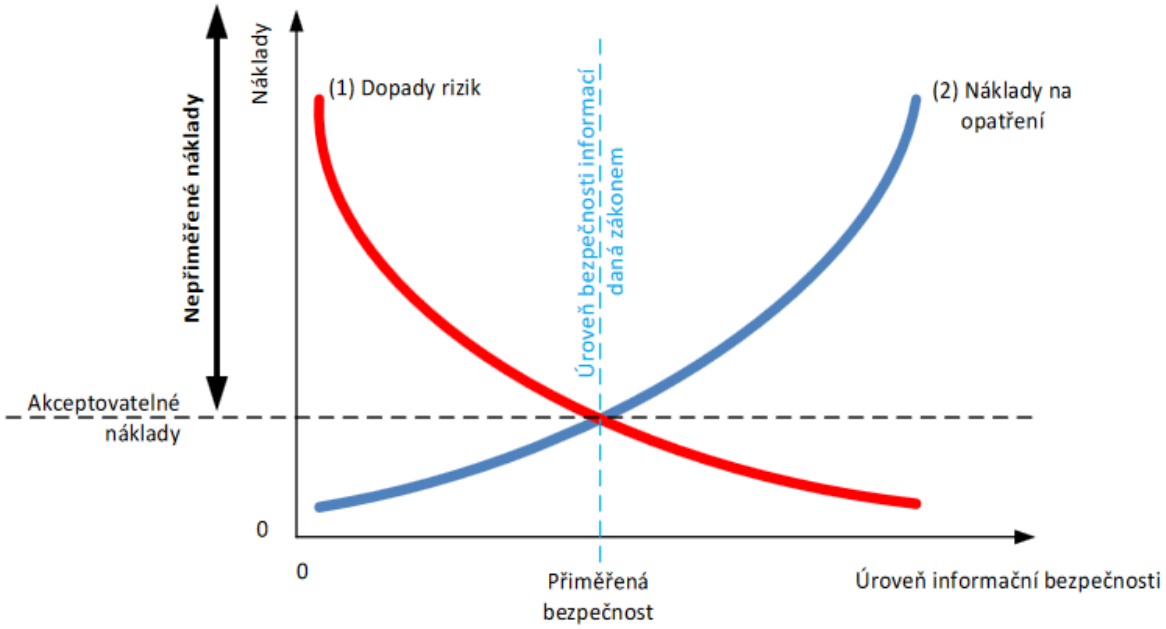
4 - Kritická
3 - Vysoká
2 - Střední
1 - Nízká

V praxi se hledá kompromisní řešení, přičemž ve výsledku riziko není úplně eliminováno, ale je sníženo na zanedbatelnou úroveň. Je potřeba vzít v úvahu fakt, že ideální univerzální řešení bezpečnosti je nereálné, ale její přijatelnou úroveň je potřeba stále udržovat. Protiopatření lze rozdělit podle vztahu vůči průběhu bezpečnostního incidentu na preventivní, dynamická (proaktivní) a následná (reaktivní), přičemž každá z těchto třech kategorií se dále dělí dle formy opatření na administrativní, fyzické, technologické (Gála, 2015, s. 221). Pokud je zvládnutí rizika nad možnostmi firmy, je nutné riziko akceptovat.

1.1.9 Akceptovatelné náklady

Informační bezpečnost je současně významnou položkou v nákladech na informační systém, proto se lze setkat s pojmy „přiměřená bezpečnost" a „akceptovatelné náklady". V podstatě jde

o kompromisní stav mezi náklady a úrovní informační bezpečnosti, při zohlednění dopadů rizik a nákladů na případná bezpečnostní opatření, viz obrázek 2.



Obrázek 2: Akceptovatelné náklady na přiměřenou bezpečnost. Zdroj: NCKB

1.1.10 Zbytková rizika

Akceptace zbytkového rizika se volí především v situacích, kdy se to jeví jako ekonomicky nejvýhodnější varianta. Je to v případech, kdy je dopad tak malý, nebo je výskyt hrozby tak málo pravděpodobný, že je efektivnější riziko podstoupit, a také v případech, kdy by se náklady na snížení rizika přiblížily k výši možných škod, které může toto riziko způsobit. Do zbytkových rizik většinou spadají rizika z rizikových skupin 2 a 1, tedy riziková skupina střední a nízká. Navržená zbytková rizika, která vyplynou ze zpracování analýzy rizik, schvaluje vedení společnosti.

1.1.11 Nejčastěji používané pojmy v oblasti škodlivých kódů

Počítačový virus

Je to škodlivý program, který má za cíl poškozovat nebo úplně zničit sobě dostupná data. Vývoj počítačových virů velmi rychle kopíruje vývoj IT technologií, takže jich existuje mnoho různých druhů, většinou specializovaných na určitou oblast. Mezi jejich základní vlastnosti počítačových virů schopnost rozšiřovat se svépomocí a také schopnost ochrany před detekcí antivirovými programy nebo snaha o eliminaci této detekce.

Malware

V praxi takto označujeme škodlivý kód, který prvoplánově neničí data, ale vykonává aktivity, které umožní útočníkovi získat data či informace, případně otevře možnost pro instalaci dalšího škodlivého software.

Ransomware

Jedná se o agresívní škodlivý počítačový kód, který po instalaci zašifruje dostupná data a znepřístupní je uživateli, případně nastavením hesla znepřístupní celý počítač. Za šifrovací klíč, kterým by bylo možné data opět zpřístupnit, je obvykle vyžadováno výkupné. S rozvojem kryptoměn je požadavek většinou na takovou platbu právě v kryptoměně (např. Bitcoin), protože příjemce je prakticky nedohledatelný. Nicméně ani po zaplacení výkupného nemá postižený žádnou jistotu, že se ke svým datům skutečně dostane.

Phishing

Jde o podvodný útok prostřednictvím e-mailu, kdy je uživatel uváděn v omyl pomocí falešné zdrojové adresy nebo odkazem na falešnou webovou adresu. Využívá se podobnosti slov, záměny písmen apod. Pokud uživatel použije takový podvržený odkaz, je na falešné webové stránce, která věrně kopíruje jeho originální verzi, požadováno zadání privátních údajů, které jsou v tu chvíli kompromitovány a zneužity (typicky internetové bankovnictví). Základní ochranou je dvou-faktorová autentifikace. V praxi na phishingový útok navazuje pokračování ve formě sociálního inženýrství nebo pokusu o instalaci malware.

1.1.12 Národní úřad pro kybernetickou a informační bezpečnost

Bezpečnost a ochrana informací se týká úplně každé firmy a podniku, bez ohledu na velikost, týká se samozřejmě i státních organizací. Moderní systémy jsou navzájem propojeny, soukromé podniky komunikují se státní správou a naopak a i stát používá pro svou správu počítačové systémy. Pro Českou republiku je ústředním správním orgánem pro kybernetickou bezpečnost Národní úřad pro kybernetickou a informační bezpečnost (dále jen NÚKIB). Ředitel tohoto úřadu se účastní jednání Bezpečnostní rady státu a je členem Výboru pro kybernetickou bezpečnost, což je orgán Bezpečnostní rady státu řešící kybernetickou bezpečnost České republiky (NÚKIB, 2020).

Výkonnou sekcí NÚKIB je Národní centrum kybernetické bezpečnosti (dále jen NCKB), které zajišťuje mimo jiné i činnost vládního CERT týmu České republiky.

CERT je zkratka z anglického názvu Computer Emergency Response Team. Jeho náplní je zveřejňování bezpečnostních rad a tím šíření informací o možných zranitelnostech jednotlivých systémů.

CSIRT je zkratka anglického názvu Computer Security Incident Response Team, jehož náplní je koordinace řešení a prevence proti bezpečnostním incidentům v počítačových sítích.

V praxi se činnost těchto dvou týmů tak velmi přiblížila, že se tyto dva názvy zaměňují nebo se používají současně (CERT/CSIRT) a můžeme za těmito zkratkami chápat stejný typ týmu „*…který je ve svém jasně definovaném poli působnosti zodpovědný za řešení bezpečnostních incidentů, z pohledu uživatelů nebo jiných týmů, tedy místo, na které se mohou obrátit se zjištěným bezpečnostním incidentem nebo i jen s podezřením*“ (ROOT.CZ, 2013).

Vládní CERT tedy zajišťuje NÚKIB a Národní SCIRT České republiky dle veřejnoprávní smlouvy a zákona o kybernetické bezpečnosti provozuje zájmové sdružení právnických osob CZ.NIC.

NCKB vydává průběžně bezpečnostní doporučení, která se týkají bezpečnosti infrastruktury, bezpečnosti stanic a serverů a bezpečnosti uživatelů, která jsou nastavena tak, aby by je bylo možné aplikovat v každé organizaci, viz Příloha č. 1.

1.2 Ochrana informací v podniku

Ochrana informací je pro každou organizaci velmi důležité téma, protože informace a data jsou obvykle ty největší hodnoty, které firma má a jejich ztráta ji může dostat do významných existenčních potíži nebo vést až ke krachu. Nejedná se přitom pouze o ekonomické riziko, ale dle typu zaměření činnosti organizace, se může jednat i o celospolečenské ohrožení, a to při zneužití ukradených dat, případně neoprávněné manipulaci s nimi. Namátkou lze uvést například nemocnice spravující zdravotní data pacientů, telekomunikační operátory a jejich databáze a infrastrukturu anebo společnosti dodávající energie. Útoky na tyto organizace jsou dnes běžné a nezřídka se můžeme setkat s pojmem *kybernetická válka*. Lze konstatovat, že pojem válka není v tomto použití nijak nadsazený, neboť jak uvádí Laudon, tak: „*Kybernetická válka představuje vážnou hrozbu pro infrastrukturu moderních společností, protože jejich hlavní finanční, zdravotní, vládní a průmyslové instituce se při každodenním provozu spoléhají na internet. Kybernetická válka také zahrnuje obranu proti těmto typům útoků.*“ (LAUDON, 2013, s. 232) (překlad autora).

1.2.1 Organizační opatření

Mezi tyto prvky pasivní ochrany se řadí veškeré směrnice, normy, metodiky a interní politiky, které nějak vymezují chování uživatelů ve firemní počítačové síti, a třeba i konkrétně specifikují konkrétní situace nebo činnosti, definují ověřování identity uživatele, nastavují minimální požadavek na kvalitu přístupového hesla, vyjmenovávají povolené mailové přílohy, definují nakládání s datovými nosiči (typicky USB klíč nebo přenosný disk). Součástí jsou také různé formy školení.

Normy ISO

Řízení informační bezpečnosti v organizacích je řešeno Mezinárodní organizací pro normalizaci (anglický název je International Organization for Standardization), známou též pod názvem ISO, což je světová federace národních organizací se sídlem v Ženevě. Tato organizace vydává mezinárodní normy pod označením ISO s přidáním čísla označujícího konkrétní sadu norem. V České republice zajišťuje vydávání norem Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ), v případě, že se jedná o převzaté normy, přidává se před název normy zkratka ČSN.

Dalším typem zkratky, se kterou se v označení norem setkáváme, je ČSN EN a znamená českou verzi normy Evropské unie. Pokud je v označení zkratka IEC znamená to, že norma byla vydaná Mezinárodní organizací pro normalizaci v elektrotechnice, spojené zkratky ČSN IEC značí její českou verzi. Složením výše uvedených zkratek dostaneme označení norem ČSN EN ISO, což značí českou verzi mezinárodní normy převzaté evropskou komisí pro normalizaci.

Řízením informační bezpečnosti se pak konkrétně zabývá rodina norem ČSN ISO/IEC 27000, přičemž klíčová a nejpoužívanější je norma ISMS (zkratka anglického názvu Information Security Management Systems). Do češtiny je tato norma překládaná jako Systém řízení bezpečnosti informací, s označením ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Požadavky. Tato norma poskytuje požadavky na ustavení, implementování, udržování a neustálé zlepšování systému řízení bezpečnosti informací. Přijetí takového systému se považuje za strategické rozhodnutí organizace, přičemž respektuje potřeby a cíle organizace a zohledňuje její strukturu a velikost (ČSN ISO/IEC 27001, 2014).

Tato norma je založena na třech základních principech informační bezpečnosti: důvěrnosti, celistvosti, dostupnosti. Principem důvěrnosti je poskytování informací k dispozici pouze těm, kteří mají k takové informaci povolený přístup. Princip celistvosti zaručuje, že existuje

správnost a úplnost informací, princip dostupnosti říká, že informace je k dispozici v okamžiku, kdy je jí potřeba.

Norma je určena pro všechny organizace bez rozdílu velikosti nebo typu firmy a je standardně používána pro získání certifikace. Je uznávána zejména pro svůj komplexní charakter (ManagementMania, 2015).

V rámci podnikových procesů bývá oblast normy ISMS řešena sadou souvisejících dokumentů, které obsahují obvykle sadu Instrukcí a sadu Směrnic.

V sadě Instrukcí se nacházejí *Havarijní plány* zpracované pro jednotlivá aktiva a současně *Plány obnovy* pro tato aktiva, ve kterých jsou popsány kroky nezbytné k obnově provozu, ať už jednoho konkrétního systému, nebo kompletního prostředí včetně případného přesunu provozu do jiné lokality. Někdy se také označují jako *Plány kontinuity*.

Směrnice pak obsahují dokumenty, které definují pravidla pro řízení jednotlivých oblastí a odpovědnosti jednotlivých rolí.

Řídící dokumenty

Jsou to dokumenty, které definují základní pravidla pro fungování organizace.

Řídicí dokumenty firmy jsou sada principů, postupů, doporučení nebo nařízení, pomáhající při řízení organizace a usměrňování chování pracovníků. Typicky jsou to organizační řád, směrnice, instrukce, normy, pracovní postupy atd. Normy kvality ISO požadují, aby existoval zdokumentovaný proces životního cyklu těchto dokumentů, ze kterého by bylo možné zjistit, jak konkrétní směrnice nebo instrukce vznikla, kdo je jejím autorem, resp. vlastníkem, schvalovatelem, či případné připomínky a také jakým způsobem byla zveřejněna její platná verze a jak s ní byli prokazatelně seznámeni pracovníci firmy.

Školení

Školení jsou již nezbytnou součástí průběžného vzdělávání zaměstnanců, bývají periodicky opakována a jejich absolvování je často podle interních směrnic předpokladem pro samotný výkon činnosti. V moderním pojetí jsou realizována prostřednictvím e-learningu, kdy zaměstnanec projde interaktivní prezentací na počítači a následně vyplňuje zkušební test. Jeho úspěšné absolvování je současně potvrzením o proběhlém školení. Tato forma umožňuje pružné reagování na aktuální bezpečnostní trendy a zaměstnance nezatěžuje ani z časových ani z logistických důvodů. Její celkový efekt je ale diskutabilní, protože praktické ukázky a diskuse mají větší vzdělávací efekt a jsou snáze přenositelné do reálného života.

Součástí edukace, v návaznosti na takové školení může být i testování v praxi, kdy jsou uživatelé testováni na proškolené znalosti promítnutím do reálné situace, je např. testováno reagování na podvržený mail nebo nalezený USB disk.

1.2.2 Technická opatření

Fyzická bezpečnost

Technická opatření ochrany informací nutně musí začínat u fyzické bezpečnosti. Je to základní prvek ochrany aktiv, kdy je potřeba mít zajištěnu ochranu na úrovni objektů a případně i celé vymezené oblasti. Musí existovat ochrana proti neoprávněnému vstupu, a tím i proti možnosti fyzického poškození nebo neoprávněným zásahům do firemního systému.

Fyzické bezpečnosti se věnuje i jedna z norem rodiny ISO 27000, konkrétně je to ČSN ISO/IEC 27002:2014 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací. Tato norma obsahuje 14 kapitol týkajících se bezpečnosti, 35 hlavních kategorií bezpečnosti a 114 kontrol pro zvýšení bezpečnosti informací:

Tabulka 2: Fyzická bezpečnost. Zdroj: ČSN ISO/IEC 27002:2014

Kapitola	Opatření bezpečnosti
5	Politiky bezpečnosti informací
6	Organizace bezpečnosti informací
7	Bezpečnost lidských zdrojů
8	Řízení aktiv
9	Řízení přístupu
10	Kryptografie
11	Fyzická bezpečnost a bezpečnost prostředí
12	Bezpečnost provozu
13	Bezpečnost komunikací
14	Akvizice, vývoj a údržba systému
15	Vztahy s dodavateli
16	Řízení incidentů bezpečnosti informací
17	Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací
18	Soulad s požadavky

Jednotlivé kapitoly jsou dále rozpracovány do podkapitol. Např. kapitola 11 má dvě podkapitoly, kde se řeší zajištění fyzické bezpečnosti a které jsou vždy vysvětleny svým cílem:

Tabulka 3: Fyzická bezpečnost, kapitola 11. Zdroj: ČSN ISO/IEC 27002:2014

Kapitola 11	**Fyzická bezpečnost a bezpečnost prostředí**
11.1	Bezpečné oblasti Cíl: Předcházet neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací organizace.
11.2	Zařízení Cíl: Zabránit ztrátě, poškození, odcizení nebo kompromitaci aktiv a přerušení provozu organizace.

Členění pak postupuje dál, např. v podkapitole 11.2 je bod 11.2.9 který říká, že by měla být přijata zásada prázdného stolu a prázdné obrazovky. Tu lze naplnit např. opatřením: *„Musí být přijata zásada prázdného stolu ve vztahu k dokumentům a výměnným paměťovým médiím a zásada prázdné obrazovky monitoru u vybavení pro zpracování informací“* (ČSN ISO/IEC 27002, 2014).

Prvky aktivní ochrany

Dalším technickým opatřením pro každou počítačovou síť jsou prvky aktivní ochrany, které ji chrání před útoky nebo neoprávněnými zásahy. Tyto prvky fungují autonomně a v reálném čase reagují na situace dle naprogramovaných algoritmů a vlastní logiky. V ideálním případě bychom měli mít pod kontrolou jak vnější provoz, tak vnitřní provoz v síti. Následkem interního útoku, kdy útočník buď zneužije nebo kompromituje interní zdroj, bývá velká škoda, protože pachatel postupuje se znalostí interních systémů a pokud není odhalen bezprostředně, může k takovému jednání docházet po poměrně dlouhou dobu.

Mezi prvky aktivní ochrany patří zejména firewall, webová a mailová proxy a antivirová řešení, v kombinaci například se zařízením pokoušejícím se detekovat nové typy útoků na základě vyhodnocování odchylek v chování požadavků systémů (např. různé anti-ransomware techniky).

Autor v této části textu používá anglické názvy systémů, protože buď neexistuje alternativní překlad pojmu do češtiny nebo je původní pojem tak zažitý, že se ani nepřekládá.

Firewall je zařízení, které tvoří rozhraní mezi interní počítačovou sítí a internetem. Pojem by se dal volně přeložit jako „bezpečnostní brána“, protože toto zařízení na základě definovaných pravidel a své logiky rozhoduje, která komunikace může skrz něj projít,

jak směrem dovnitř, tak směrem ven. Princip firewalu se postupně vyvíjí, první generace uměla pouze filtrovat packety a porovnávala základní informace s předdefinovaným seznamem pravidel. Druhá generace navíc uměla rozeznat, kdo komunikaci zahájil a za jakým účelem. Třetí generace firewallu přidala možnost filtrování informací a tím rozpoznávat aplikace a často používané protokoly, s tím souvisí schopnost detekce útoků, pokud se definovaný typ operace pokouší o něco jiného, než je jeho standardní chování. Poslední generace se označuje jako „nextgen“, ve které se při kombinaci všech výše zmíněných metod dále rozvíjí schopnost kontroly filtrovaného obsahu a demaskování případných anomálií požadavků (ESET, 2019).

Webový proxy server neboli webová brána je zařízení, které stojí v cestě klientskému počítači při snaze zobrazit webové stránky z prostředí internetu. Jeho úkolem je inspekce obsahu a požadavků stránky a eliminace škodlivých kódů. Používá se také pro vymezení povolených kategorií webových stránek, kdy stránky s nepovoleným obsahem jsou automaticky blokovány a prostřednictvím této brány znepřístupněny pro zobrazení z chráněné sítě. Typicky patří mezi takový blokovaný obsah stránky propagující násilí, zbraně, alkohol, gamblerství.

E-mailový proxy server neboli e-mailová brána je zařízení sloužící ke kontrole příchozích a odchozích e-mailů organizace. E-mail je velmi rozšířený komunikační prostředek a jako takový je jedním z hlavních způsobů, pomocí kterých lze dostat škodlivý kód do interního prostředí organizace, proto je kvalitní a dostatečně robustní řešení této oblasti firemní komunikace důrazně doporučováno. Lze provádět inspekci obsahu na přítomnost škodlivých kódů, eliminaci některých typů přiložených souborů. Typicky se jedná o soubory s příponou EXE, které jsou jako příloha e-mailu rovnou považovány za nebezpečné a většinou automaticky blokovány. V konfiguraci e-mailového proxy serveru lze také rovnou zakázat příjem z určitých poštovních domén, které už jsou evidovány jako nebezpečné. Používají se k tomu tzv. black listy, tedy černé listiny, které někteří poskytovatelé bezpečnostních prvků zpřístupňují k veřejnému použití právě pro tyto účely.

Antivirové programy jsou základem každého bezpečnostního řešení. Ochrana koncové stanice, tedy obvykle klientského počítače, tabletu nebo mobilu, je nezbytným prvkem při řešení počítačové bezpečnosti. Dochází zde k permanentní kontrole zpracovávaných informací, jsou chráněny lokální prostředky, např. při použití externího disku je tento automaticky zkontrolován na přítomnost nějakého škodlivého kódu. Při pokusu o spuštění škodlivého kódu ze sítě je takový pokus blokován a automaticky je odeslána informace správci systému o tomto incidentu na konkrétním počítači.

Klasifikace dokumentů je již pokročilejší technika při ochraně informací a vyžaduje určitou úroveň bezpečnostní politiky a existenci procesů v dané organizaci. Jedná se o nastavení procesu, kdy již při vzniku dokumentu je tento označen dle definované kategorie, obvykle se používají tři kategorie: „veřejná“, „interní“, „chráněná“, ale není to podmínkou. Mohou být kategorie kopírující potřeby organizace a jejich definice může vycházet přímo z účelu používání dokumentů. Podle dané kategorie je pak na příslušný dokument aplikována ochrana, resp. pravidla pro povolenou manipulaci. V praxi se to může projevit např. tak, že dokumenty z kategorie „interní a „chráněná“ nemohou být poslány prostřednictvím e-mailu na adresu mimo organizaci a dokument v kategorii „chráněná“ nemůže být uložen na firemní disk v cloudovém prostředí. Souvisí s tím i automatické nastavení oprávnění přístupu pro určené skupiny uživatelů.

Fyzické prvky sledující tok dat v interní síti jsou vyspělým bezpečnostním řešením, které umožňuje monitoring datových toků v interní síti a na základě jeho vyhodnocení detekci anomálií. Lze takto identifikovat napadenou stanici, která vyvíjí neobvyklou aktivitu při snaze infikovat další stroje v síti nebo stahování velkých objemů dat, které nemá opodstatnění. Na základě statistiky lze vysledovat i neobvyklá krátkodobá spojení, která provoz v síti nijak neomezují, ale již jejich samotná existence znamená problém, např. periodické kontaktování firemního e-mailového serveru nebo serveru zajišťující adresářové služby.

Všechna výše zmiňovaná zařízení jsou a musí být neustále aktualizována na nejnovější verze svých bezpečnostních databází, protože jen v takovém případě je výrobce schopen garantovat jejich správnou činnost. Není neobvyklé, že v případě zvýšené aktivity probíhajících útoků v prostředí internetu, jsou tyto databáze aktualizovány několikrát denně. Je třeba si uvědomit, že tyto ochranné prvky vždy reagují na nějaký reálný incident nebo známou zranitelnost, a proto je nezbytné mít nejaktuálnější možnou verzi, kterou jednotliví výrobci poskytují.

1.3 Standard GDPR

Kompletní název tohoto nařízení je: „NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)“. Jak je již z názvu patrné, toto nařízení vychází z původní směrnice EU o ochraně osobních údajů, která platila od roku 1995.

Dnem schválení GDPR, tedy 27. dubnem 2016, bylo odstartováno období, během kterého museli všichni, jichž se nařízení týká, udělat revizi svých systémů a postupů pro nakládání s osobními údaji. Je nutné zdůraznit, že se nejedná o směrnici nebo doporučení, ale o nařízení EU, které je platné v rámci členských zemí EU bez možnosti zásadních úprav. Nařízení GDPR vstoupilo v platnost 25. května 2018.

V České republice je dozorovým úřadem pro dodržování a uplatňování GDPR určen Úřad pro ochranu osobních údajů. Působnost tohoto úřadu není omezena pouze na GDPR, ale má i další úkoly:

- Působnost v oblasti ochrany osobních údajů;
- Dozor nad dodržováním povinností při zpracováním osobních údajů v oblasti elektronických komunikací;
- Dozor nad dodržováním povinností při šíření obchodních sdělení;
- Projednávání správních deliktů v oblastech zvláštních zpracování osobních údajů;
- Vytváření a převod elektronických identifikátorů pro státní registry.

Jednotlivé členské státy měly také povinnost přijmout prováděcí zákon, kterým upřesní více než 50 bodů, které jsou v rámci GDPR svěřeny do jejich moci. V České republice se tak stalo s téměř ročním zpožděním, konkrétně 24. dubna 2019, kdy vstoupil v účinnost nový zákon č. 110/2019 Sb. o zpracování osobních údajů a byl aktualizován zákon č. 181/2014 Sb. o kybernetické bezpečnosti, který platí s aktualizovanou vyhláškou č. 82/2018 Sb. o bezpečnostních opatřeních.

V českém právním prostředí je významně zmírněna hrozba pokut pro orgány veřejné moci a veřejné subjekty (pokud jsou zpracovateli osobních údajů) a to tak, že je nulová. Autor se domnívá, že existuje velká pravděpodobnost pro budoucí revidování tohoto diskriminačního přístupu, protože se tím stanovily výrazně rozdílné podmínky mezi subjekty veřejného a soukromého práva. Soukromé podniky zpracovávající osobní údaje, typicky banky nebo distribuční společnosti, musely investovat značné prostředky do analýzy svých systémů, ve kterých se takové údaje zpracovávají. Není přitom neobvyklé, že konkrétně banky mají takových systémů řádově stovky a jejich analýza byla časově i personálně velmi náročná. Jako problém se ukázaly hlavně ty nejstarší systémy, které dokonce ani nemusely být původně určeny pro danou organizaci, ale které byly v historii získány, například prostřednictvím

akvizice. Jako takové pak z nějakého důvodu neprošly integrací a byly zakonzervovány v původním stavu, nebyly dále rozvíjeny a aktualizovány.

Podstata GDPR

Smyslem GDPR je hájit práva občanů Evropské Unie proti neoprávněnému zacházení s jejich daty včetně osobních údajů, týká se všech firem a institucí, ale i jednotlivců a online služeb, které zpracovávají data uživatelů (GDPR.CZ, 2016).

GDPR je unikátní, nejen z důvodu, že podobně komplexní a detailní typ ochrany osobních údajů zde dosud nebyl, ale také, že neřeší ochranu pouze v EU. GDPR se týká kohokoliv, kdo by chtěl zpracovávat osobní údaje občanů EU. Lze také konstatovat, že vzniklo jako reakce na rychlou digitalizaci a kybernetizaci veřejného prostoru, které při své rychlosti nebraly ochranu osobních dat v potaz, a pokud ano, tak jen velmi okrajově. Zároveň umožnily, že se balíky osobních údajů spotřebitelů staly běžnou komoditou na trhu a jejich sofistikované využití následně dokázalo ovlivňovat nejen ekonomiky jednotlivých států, ale i jejich policko u situaci. Jako příklad je možné uvést problém Facebooku a poradenské společnosti Cambridge Analytica v roce 2018 (LUPA.CZ, 2018).

Pro zajištění uplatňování GDPR, jeho monitorováním a pro vydávání pokynů a doporučení byl ke dni 25.5.2018 ustanoven Evropský sbor pro ochranu osobních údajů (dříve Pracovní skupina 29). Je to nejvyšší dozorový orgán a je tvořen vedoucími dozorových úřadů z jednotlivých členských zemí EU a evropským inspektorem ochrany údajů.

1.3.1 Pověřenec pro ochranu osobních údajů

Nově GDPR definovalo kontrolní funkci, kterou musí mít obsazenou někteří zpracovatelé a správci osobních údajů. Týká se to těch, kteří systematicky a rozsáhle zpracovávají údaje jednotlivců. Tato funkce se jmenuje Pověřenec pro ochranu osobních údajů, anglický název je Data Protection Officer, zkráceně DPO. Tato zkratka se vžila i do používání v českém prostředí.

Role pověřence v rámci organizace musí být nezávislá, samostatná a vyčleněná mimo standardní firemní struktury, ale současně musí mít tento pověřenec přímý přístup k nejvyššímu vedení organizace (Nezmar, 2017, s. 168). Hlavní úkoly DPO jsou vyjmenovány přímo v GDPR nařízení, konkrétně v čl. 39, je jich celkem 5, zkráceně je lze popsat takto: (GDPR, 2016)

a) poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům;

b) monitorování souladu s tímto nařízením;

c) poskytování poradenství na požádání;

d) spolupráce s dozorovým úřadem;

e) působení jako kontaktní místo pro dozorový úřad.

V praxi se ale mohou tyto povinnosti střetávat s povinnostmi správce nebo zpracovatele a pověřenec se může octnout pod tlakem ze dvou stran, kdy na jedné straně je jeho úkolem pomáhat organizaci, a na druhé straně zajišťovat práva subjektů údajů (Nezmar, 2017, s. 168).

Zajištění DPO se stalo ze strany právně vzdělaných osob běžně nabízenou komerční službou, protože obsazení této pozice sice vyžaduje profesní kvality, ale současně, z důvodu nezávislosti a kvůli případnému konfliktu zájmů, zmenšuje možnosti využití kompetence takového zaměstnance pro jiné využití v rámci organizace.

1.3.2 Další vybrané důležité pojmy

Nařízení GDPR ve svém textu (GDPR, 2016) definuje i několik dalších pojmů, se kterými je nutné pracovat:

Osobní údaj

V definici pojmu „osobní údaj" je obsaženo v zásadě vše, čeho se nařízení týká, jsou zde vyjmenovány varianty, jak identifikovat fyzickou osobu a které informace spadají pod tento pojem. Konkrétně je zde řečeno, že: *„Osobními údaji jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů"); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby."* (GDPR, 2016).

Udělení a odebrání souhlasu

GDPR nově zavedlo pojmy a pravidla pro získání výslovného souhlasu, doložení souhlasu a odvolání souhlasu. Samotný souhlas ke zpracování osobních údajů dle obecného nařízení o ochraně osobních údajů je definován takto: „*jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů*" (Pracovní skupina 29, 2018).

Odvolání souhlasu musí být stejně snadné jako jeho poskytnutí. Pokud je tedy poskytnutí souhlasu možné například prostřednictvím stisknutí tlačítka „Ano“ na webové stránce, tak odvolání souhlasu nemůže být realizováno pouze voláním na infolinku v pracovních dnech v určených hodinách, ale musí být opět realizovatelné kliknutím na tlačítko. (Pracovní skupina 29, 2018).

Právo na výmaz

Dalším novým podstatným prvkem je „právo na výmaz“ někdy také „právo být zapomenut“. V případě, že pomine důvod pro uchovávání a další zpracovávání osobních údajů a jednotlivec odvolá souhlas se zpracováním, případně byly-li osobní údaje zpracovávány neoprávněně, je právo na vymazání osobních údajů a zabránění jejich dalšímu zpracovávání. Toto je důležitý prvek pro společnosti pracující v online prostředí, protože jejich systémy musí obsahovat mechanismy, které takovou operaci umožní a také jsou schopny její provedení doložit.

Pseudonymizace

Dalším důležitým pojmem, který je v GDPR definován, je „pseudonymizace“. Jedná se o způsob ochrany zpracovávaných dat, nařízení to vykládá takto: *“Pseudonymizace je zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;“* (GDPR, 2016). V praxi je to obvykle postup, při kterém se doplňují umělé identifikátory místo konkrétních významných údajů, které nejsou pro dané zpracování důležité, ale jsou součástí datového celku. Dochází tím sice ke snížení možnosti statistického využití dat, ale bez přístupu k pseudonymizačnímu identifikátoru jsou data zpětně nespojitelná.

Správce a zpracovatel

Nařízení GDPR také definovalo role a odpovědnosti, kdy vedle role správce osobních údajů klade důraz i na povinnosti zpracovatele a na jejich společnou odpovědnost vůči subjektům údajů (Nezmar, 2017, s. 150).

Roli správce pak GDPR definuje takto: *„Správcem je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho jmenování;“* (GDPR, 2016) a roli zpracovatele takto: *„Zpracovatelem je fyzická nebo*

právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;" (GDPR, 2016). Vyplývá z toho, že správce specifikuje činnosti spojené se zpracováním osobních údajů a zpracovatel je jeho subbdodavatelem. Na základě výše uvedené citace článku 4, odstavce 8, kde je zmíněno, že zpracovatel zpracovává osobní údaje pro správce, se pod tento pojem musí zahrnout například i provozovatel datového úložiště, na kterém jsou předmětná data uložena, i když se samotným zpracováním nemusí mít nic společného. Celý průběh zpracování musí být detailně zdokumentován, aby bylo zajištěno, že správce má celý proces pod kontrolou. Bez vědomí správce není možné zpracování delegovat na další subjekt: „*Zpracovatel nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce."* (GDPR, 2016). Na základě poměrně široké definice zpracování nebo odstraňování osobních údajů je v praxi ale poměrně obvyklá situace správce jako zpracovatele (Nezmar, 2017, s. 152).

1.3.3 Pokuty

GDPR zavedlo značné pokuty za porušení nařízení a tyto jsou na české poměry až abstraktní, neboť mohou ve své druhé variantě dosahovat až do výše 20 000 000 eur nebo 4 % celkového ročního celosvětového obratu organizace (první varianta je trochu mírnější, je nastavena na 10 000 000 eur nebo 2 % celkového ročního celosvětového obratu organizace). Zvolená varianta pokuty se odvíjí závažnosti porušení povinností ke kterému došlo. Nařízení vychází z premisy, že ukládání správních pokut musí být účinné, přiměřené, ale zároveň odrazující. Každý případ je posuzován individuálně a správci může být uděleno jen napomenutí nebo uloženo uvést zpracování dat do souladu s nařízením. Český prováděcí zákon č. 110/2019 Sb. sice v §63 čl. 3 zastropoval maximální výši pokuty na 10 000 000 Kč, ale také v §61 čl. 3 současně konstatuje, že: *„…Úřad upustí od uložení správního trestu také tehdy, jde-li o subjekty uvedené v čl. 83 odst. 7 nařízení Evropského parlamentu a Rady (EU) 2016//679*" (Zákon č. 110/2019 Sb.), přičemž v tomto zmiňovaném čl. 83 je definováno, že každý členský stát si může stanovit pravidla pro správní pokuty orgánům veřejné moci a veřejným subjektům.

1.4 Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), zkráceně ZoKB, upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Současně zpracovává

příslušné předpisy Evropské unie (s odkazem na Směrnici Evropského parlamentu a Rady EU 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii) a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů (Zákon č. 181/2014 Sb.). Doplňuje ho Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

Vedle GDPR je tento zákon druhý klíčový prvek legislativní opory při řešení bezpečnosti a ochrany informací. Zákon vymezuje pojmy jako je kybernetický prostor, kritická informační infrastruktura a jsou v něm popsány bezpečnostní opatření vyžadované pro zajištění bezpečnosti. Vyjmenovává i situace, jako je kybernetická bezpečnostní událost a kybernetický bezpečnostní incident. V zákonu jsou také popsány role národního a vládního CERT týmu. Současně ZoKB definuje pravomoci a povinnosti Národního bezpečnostního úřadu (dále jen NBÚ), přičemž v §22, který se týká výkonu státní správy, stanovuje, že NBÚ zajišťuje také činnost Národního centra kybernetické bezpečnosti.

Kybernetický prostor

V §2 ZoKB je definován jako *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací“* (Zákon č. 181/2014 Sb.).

Kritická informační infrastruktura

Toto je velmi důležitý pojem, protože se k němu váže mnoho povinností, resp. se podle něj hodnotí úroveň nutné ochrany aktiv podniku, kdy na základě pozitivní klasifikace je na aktivum a jeho ochranu nahlíženo právě z pohledu vyhovění tomuto zákonu. Vykládán je jako *„prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti“* (Zákon č. 181/2014 Sb.).

Významný informační systém

Vyhláška č. 317/2014 Sb., resp. její aktualizace č. 205/2016 Sb. o významných informačních systémech a jejich určujících kritériích, se týká orgánů veřejné moci a krajů s přenesenou působností a definuje parametry, na základě kterých se informační systém řadí mezi významné. Hodnocené faktory jsou jednak možnost negativního vlivu případné nefunkčnosti informačního systému na fungování služeb a provozu orgánů veřejné moci a jednak ohrožení kritické infrastruktury, oběti na životech nebo významné materiální ztráty. Ve své Příloze č. 1 pak

vyhláška obsahuje 153 vyjmenovaných významných informačních systémů, vždy je definován správce a název systému (Vyhláška č. 205/2016 Sb.).

Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident

Definice v §7 ZoKB uvádí, že kybernetická bezpečnostní událost je taková událost, která může způsobit narušení bezpečnosti informací a kybernetický bezpečnostní incident je již narušení bezpečnosti informací. Detekované události a incidenty jsou povinni správci jednotlivých systémů hlásit, a to podle úrovně významnosti systému buď NBÚ nebo provozovateli národního CERT, což je CZ.NIC, které bylo NBÚ vybráno jako provozovatel národního CERT (Zákon č. 181/2014 Sb.).

Evidence

Všechny bezpečnostní incidenty jsou evidovány prostřednictvím NBÚ a je s nimi nakládáno dle §9 ZoKB. Evidence obsahuje vždy samotné hlášení kybernetického incidentu, identifikační údaje systému, ve kterém se incident vyskytl, údaje o zdroji incidentu, postup při řešení a jeho výsledek (Zákon č. 181/2014 Sb.).

Stav kybernetického ohrožení

Zákon popisuje i případ, kdy je ve velkém rozsahu ohrožena bezpečnost informací a je riziko, že může dojít k poškození zájmu České republiky. Takový stav nazývá jako *Stavem kybernetického ohrožení* a zákon taktéž stanovuje pravidla pro jeho vyhlášení a speciální pravomoci, kdy je například provozovatel celoplošného rozhlasového a televizního vysílání povinen okamžitě zveřejnit informaci o vyhlášení tohoto stavu.

1.4.1 Vyhláška o kybernetické bezpečnosti

Celým název vyhlášky č. 82/2018 Sb. je „Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat“. Zapracovává směrnici Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, a upravuje některé stávající prvky ochrany bezpečnosti informací. Současně mění a upřesňuje požadavky na povinné osoby. Hlavní změnou je, povinnost implementovat požadavky zákona a vyhlášky do jednoho roku od zveřejnění zákona, resp. vyhlášky.

Povinná osoba

Dle §2 je tímto pojmem označován orgán nebo osoba *„které jsou povinny zavést bezpečnostní opatření podle zákona“*, v důsledku to znamená, že za každou ve vyhlášce popsanou činnost nebo rozhodnutí je podle vyjmenovaných kritérií někdo zodpovědný a tomuto jsou určeny konkrétní povinnosti a úkoly (Vyhláška č. 82/2018 Sb.).

Hodnocení rizik

Součástí vyhlášky je i několik příloh, kdy například konkrétně příloha č. 2 přibližuje hodnocení rizik a stanovuje pro hodnocení rizik funkci:

Riziko = dopad x hrozba x zranitelnost

Pokud se při hodnocení rizik používá metoda, která nerozlišuje hodnocení hrozby a zranitelnosti, lze tyto dvě stupnice sloučit. Součástí přílohy jsou vzorové stupnice pro hodnocení hrozeb, zranitelností a rizik. Úroveň rizika zobrazuje tabulka 4:

Tabulka 4: Hodnocení rizik. Zdroj: Vyhláška o kybernetické bezpečnosti

Úroveň	**Popis**
Nízké	Riziko je považováno za akceptovatelné.
Střední	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.
Vysoké	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické krok k jeho odstranění.
Kritické	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

2 Analytická část

2.1 Průzkum stavu informační bezpečnosti v podniku

Autor pro přiblížení stavu informační bezpečnosti v podnicích použil již existující průzkumy, Protože se oblast informační bezpečnosti velmi rychle vyvíjí, bylo jeho záměrem bylo pracovat s materiálem obsahujícím, pokud možno, nejaktuálnější dostupné výsledky.

Jako první se věnuje analýze „Mezinárodního průzkumu informační bezpečnosti 2017-2018“ (Global Information Security Survey), který realizovala společnost EY.

Jako druhý materiál, který navíc umožnil meziroční srovnání stejných dat, autor použil výroční zprávy od NÚKIB za roky 2016, 2017 a 2018, doplněné o průzkum NÚKIB, kterým bylo zjišťováno, jaká byla reakce na bezpečnostní varování, vydané NÚKIB v roce 2018.

Třetím materiálem, kterému se autor věnuje, je průzkum od společností Pricewaterhouse Coopers Audit a TATE International z roku 2017 s názvem „Kyberbezpečnost a my“ na téma „Průzkum na téma aspekty vzdělávání zaměstnanců v oblasti kyberbezpečnosti“.

2.1.1 Global Information Security Survey 2017-2018 (EY)

Tento reprezentativní mezinárodní průzkum realizovala společnost EY metodou dotazování a v jeho rámci poskytli odpovědi manažeři odpovědní za oblast informační bezpečnosti a IT. Bylo dotazováno 1200 firem z celého světa ve více než dvaceti různých odvětvích. Výzkum probíhal v období června až září 2017 (EY, 2017).

Z výzkumu vyplynulo, že navzdory tomu, že k obraně bezpečnosti se používá stále sofistikovanějších nástrojů a získává se více informací o tom, co se v sledované oblasti děje, tak mnoho firem deklaruje, že se potencionální bezpečnostní hrozby obává stále více.

Z průzkumu také vyplynulo, že pouze 4 % dotazovaných organizací jsou přesvědčena, že plně zvážila důsledky a potřeby informační bezpečnosti vzhledem k jejich aktuální strategii, a že pro jejich rizikové prostředí zahrnují a sledují relevantní počítačové hrozby, zranitelnosti a rizika.

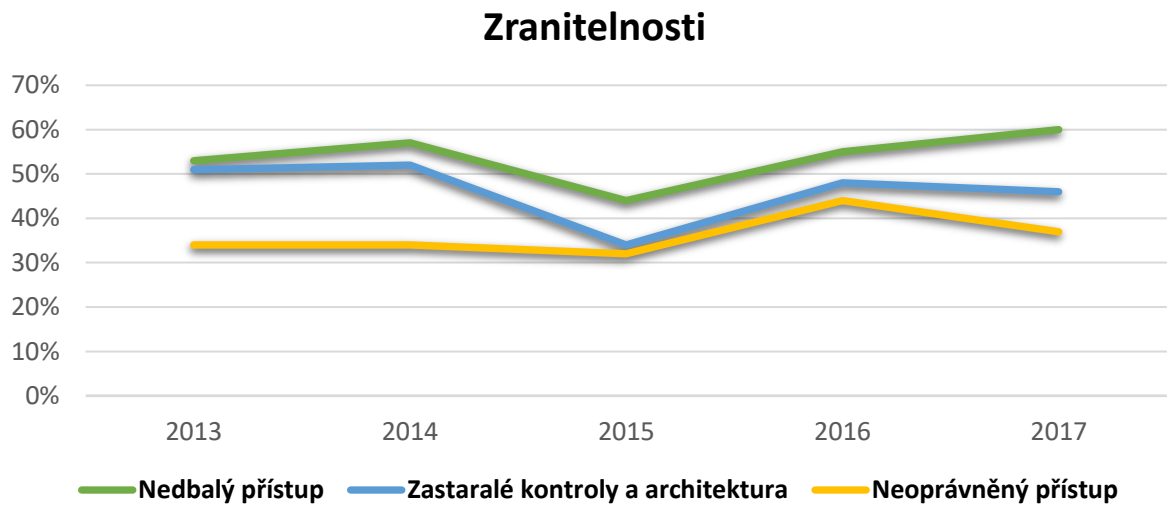
Přehled zranitelností a bezpečnostních hrozeb s nejvýraznějším podílem na expozici respondentů vůči rizikům za období 2013-2017

Zranitelnosti

Podíl dotazovaných organizací (v %), jež daný faktor považují za jeden ze dvou nejzásadnějších vzhledem k míře souvisejících rizik

Tabulka 5: Zranitelnosti. Zdroj: EY

Rok	2013	2014	2015	2016	2017
Nevědomý či nedbalý přístup	53 %	57 %	44 %	55 %	60 %
Zastaralé kontroly či bezpečnostní architektura	51 %	52 %	34 %	48 %	46 %
Neoprávněný přístup	34 %	34 %	32 %	44 %	37 %



Graf 1: Zranitelnosti. Zdroj: EY

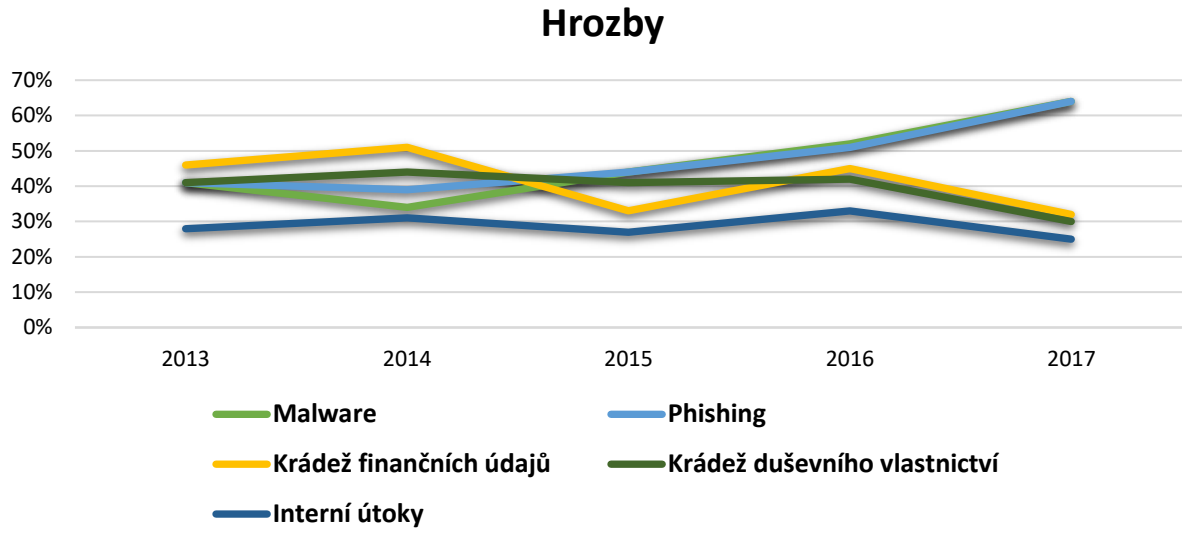
Za povšimnutí stojí, že jedinou křivkou, která mezi roky 2013 a 2017 klesla, je křivka zobrazující zranitelnost vlivem zastaralých kontrol nebo architektury. Ze třech hodnocených oblastí je tato jediná, kterou lze vztáhnout na úroveň technického vybavení nebo investic obecně, ostatní dvě, tedy riziko zranitelnosti kvůli nevědomému či nedbalému přístupu a riziko zranitelnosti kvůli neoprávněnému přístupu jsou oblasti, ve kterých hlavní roli hraje lidský faktor. A jak je z grafu zřejmé, tak i přes mírný pokles během sledovaného období, se finální hodnota obou těchto ukazatelů dostala za rok 2017 na vyšší hodnotu, než byla v roce 2013. Je to potvrzením toho, že ochrana a bezpečnost informací je nikdy nekončící proces a vlivem lidského faktoru je zde stále obrovský potenciál pro zlepšení. Ani sebelepší procesní příručky, směrnice a nařízení nejsou samy o sobě schopny zajistit a vynutit bezpečnost na úrovni, jakou lze považovat za ideální, bez toho, aniž by bylo současně pracováno s vlivem lidského faktoru.

Hrozby

Podíl dotazovaných organizací (v %), které daný faktor považují za jeden ze dvou nejzásadnějších vzhledem k míře souvisejících rizik.

Tabulka 6: Hrozby. Zdroj: EY

Rok	2013	2014	2015	2016	2017
Malware	41 %	34 %	44 %	52 %	64 %
Phishing	41 %	39 %	44 %	51 %	64 %
Útoky zaměřené na krádež finančních údajů	46 %	51 %	33 %	45 %	32 %
Útoky zaměřené na krádež duševního vlastnictví	41 %	44 %	41 %	42 %	30 %
Interní útoky	28 %	31 %	27 %	33 %	25 %



Graf 2: Hrozby. Zdroj: EY

Z graficky vyjádřených hodnot je zřetelně vidět trvalý nárůst malware a phishingu, přičemž tyto dvě hrozby jsou považovány za téměř shodné. V praxi je obvykle pokračováním phishingového útoku buď nějaká realizace sociálního inženýrství (podvržené stránky a získání citlivých údajů), nebo pokus o malware či ransomware útok. Právě rok 2016 byl ve znamení masívního nástupu těchto škodlivých kódů, je tedy pravděpodobné, že právě tyto souvislosti jsou prezentovány stoupající křivkou grafu phishingu a malware, a také výrazným vzestupem obavy z krádeže finančních údajů v roce 2016. Interní útoky se přes drobné výkyvy drží na víceméně stálé pozici okolo 30 % a mírně sestupnou tendenci vykazuje riziko krádeže duševního vlastnictví. Lze se domnívat, že tento trend je důsledkem zvyšující se ochrany bezpečnosti údajů a používání moderních nástrojů k jejich ochraně (klasifikace dokumentů, DLP apod.).

Shrnutí klíčových trendů zjištěných průzkumem:

Tabulka 7: Klíčové trendy. Zdroj: EY

87 %	respondentů poukazuje na nutnost navýšit až o polovinu firemní výdaje na kybernetickou bezpečnost.
77 %	respondentů považuje za nejpravděpodobnější příčinu kybernetického útoku nedbalý přístup zaměstnanců.
12 %	organizací je přesvědčeno, že by patrně dokázaly odhalit sofistikovaný počítačový útok.
63 %	podniků svěřilo zajištění počítačové bezpečnosti téměř výhradně na bedra IT oddělení.
48 %	firem nemá specializované centrum bezpečnostního provozu (SOC), ačkoliv se tato pracoviště stávají stále rozšířenějšími.
17 %	zástupců a členů vrcholového vedení společností má o kybernetické bezpečnosti dostatečné povědomí.
57 %	zúčastněných podniků nedisponuje žádným programem na analýzu relevantních hrozeb, případně uplatňují pouze dílčí opatření.
89 %	podniků pokládá vlastní bezpečnostní opatření uplatňovaná proti kybernetickým útokům za ne zcela postačující.

2.1.2 Zprávy o stavu kybernetické bezpečnosti za roky 2016-2018 (NÚKIB)

NÚKIB každoročně předkládá zprávu o stavu kybernetické bezpečnosti České republiky, ve které hodnotí stav kybernetické bezpečnosti v naší zemi, rekapituluje hodnocený rok a upozorňuje na potenciální rizika blízké budoucnosti. Součástí této zprávy jsou také statistické údaje o incidentech řešených NCKB.

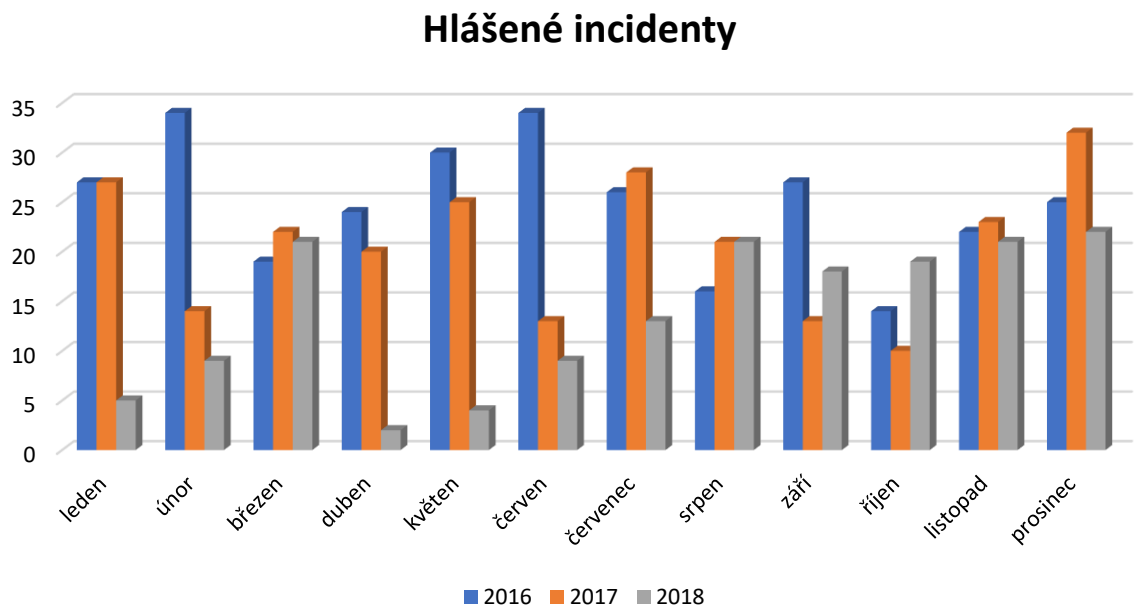
Jedná se o zpracování dat získaných reportováním stavu, který, na základě povinnosti hlásit kybernetické bezpečnostní incidenty, poskytují organizace, kterých se tato povinnost týká. Reporting probíhá prostřednictvím formuláře pro hlášení incidentů.

Autor použil data ze zpráv za roky 2016, 2017 a 2018 (NÚKIB, 2020), aby bylo možné sledovat vývoj hlášení a incidentů. Počty těchto zpráv jsou vyneseny do tabulky 8:

Tabulka 8: Incidenty. Zdroj: NÚKIB

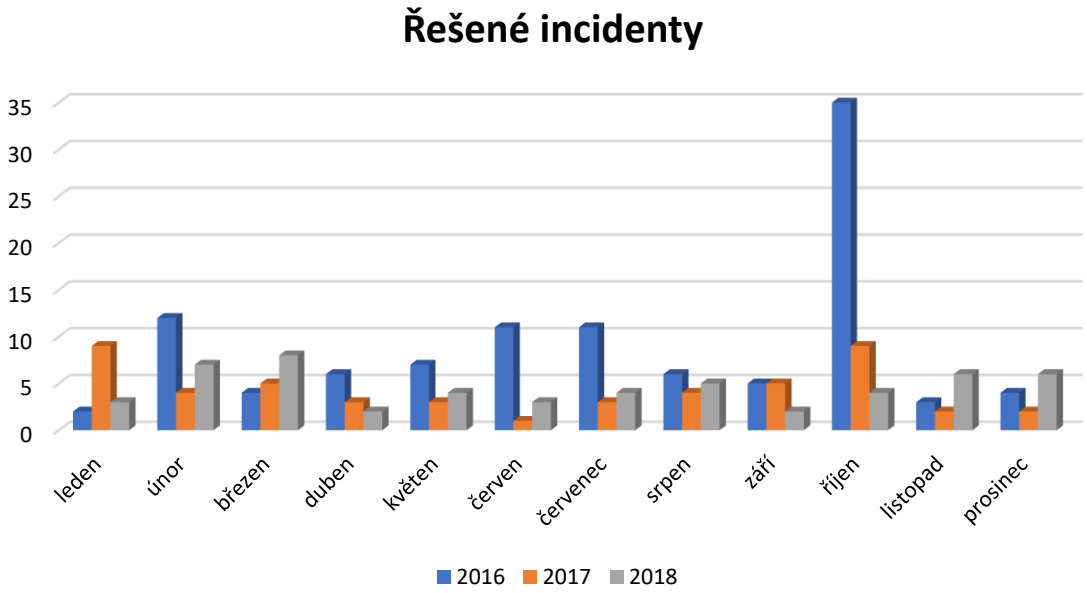
Měsíc		01	02	03	04	05	06	07	08	09	10	11	12
Hlášené incidenty	2016	27	34	19	24	30	34	26	16	27	14	22	25
	2017	27	14	22	20	25	13	28	21	13	10	23	32
	2018	5	9	21	2	4	9	13	21	18	19	21	22
Řešené incidenty	2016	2	12	4	6	7	11	11	6	5	35	3	4
	2017	9	4	5	3	3	1	3	4	5	9	2	2
	2018	3	7	8	2	4	3	4	5	2	4	6	6

Grafické znázornění hlášených incidentů v letech 2016-2018:



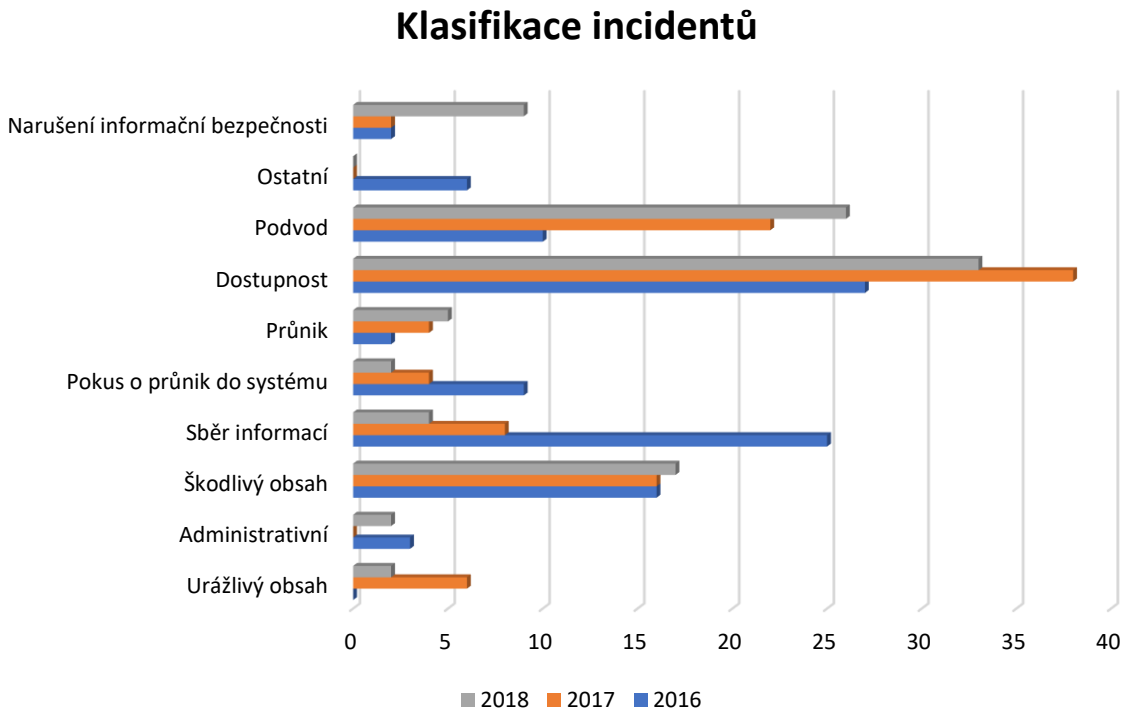
Graf 3: Hlášené incidenty. Zdroj: NÚKIB

Grafické znázornění řešených incidentů v letech 2016-2018



Graf 4: Řešené incidenty. Zdroj: NÚKIB

Incidenty se dle formuláře pro hlášení incidentů dělí do různých kategorií:



Graf 5: Klasifikace dokumentů. Zdroj: NÚKIB

Z poskytnutých údajů lze odvodit, že poměr mezi nahlašovanými a řešenými incidenty se po analýze incidentu pohybuje mezi 20 % až 35 % a největší podíl na počtu řešených incidentů mají kategorie Dostupnost, Podvod a Škodlivý kód.

Kategorie Dostupnost, které patří třetina všech řešených bezpečnostních incidentů, zahrnuje např. narušení dostupnosti způsobené DoS/DDoS útokem nebo sabotáží. Reálně to znamená, že každý měsíc jsou prostřednictvím NÚKIB řešeny zhruba tři tyto incidenty. Je třeba vzít v úvahu, že toto relativně nízké číslo ale zohledňuje pouze organizace, které jsou povinny tuto skutečnost nahlásit, tedy jsou to povinné subjekty dle zákona o kybernetické bezpečnosti.

Ze zpráv vyplývá, že nejčastěji NCKB, resp. pracovníci CSIRT.CZ řešili ransomware a phishingové útoky (2016), a vyděračské maily hrozící DDoS útoky při nezaplacení požadované částky v Bitcoinech (2017), přičemž je zdokumentováno, že síla DDoS útoků meziročně roste téměř exponenciálně. V roce 2018 byl nejčastěji řešeným problémem malware na těžbu kryptoměny, který posiluje na úkor ransomware.

Autor doplňuje, že nebezpečí infikace ransomware ale stále nelze podceňovat. Na konci roku 2019 byla identifikována kampaň namířená na organizace v celé republice napříč různými odvětvími. Útok byl složen z phishingového podvržení škodlivého makra, následně stažením malware a nainstalováním ransomware. V rámci této útočné kampaně jsou známy dva úspěšné útoky, a to na Nemocnici Rudolfa a Stefanie v Benešově a na těžební společnost OKD. V obou případech došlo k paralyzování chodu organizace a bylo nutné zcela obnovit poškozenou infrastrukturu.

Průzkum s cílem zjistit rozsah používání technologií Huawei a ZTE (NÚKIB)

V prosinci roku 2018 vydal NÚKIB varování, že používání technických nebo programových prostředků společností Huawei Technologies Co., Ltd. (dále Huawei) a ZTE Corporation (dále ZTE) představuje hrozbu v oblasti kybernetické bezpečnosti. Součástí tohoto varování bylo upozornění, že subjekty podléhající zákonu o kybernetické bezpečnosti musí zohlednit toto bezpečnostní opatření při výběru řešení a potenciálního dodavatele, a u již provozovaných řešení toto zohlednit při hodnocení rizik a plánu zvládání rizik. (NÚKIB, 2018)

V červnu roku 2019 byla vydána tisková zpráva, že NÚKIB následně provedl průzkum, jehož cílem bylo zjistit rozsah používání technologií Huawei a ZTE mezi povinnými subjekty a vliv varování z prosince 2018 (NÚKIB, 2019).

Metodou dotazování bylo osloveno 126 organizací provozujících 472 systémů kritické informační infrastruktury, významných informačních systémů a informačních systémů základních služeb. Z těchto 126 oslovených organizací jich 75 uvedlo, že technologie Huawei a ZTE nepoužívá, 49 je používá a dvě nedodaly podklady.

Technické a programové prostředky Huawei a ZTE byly hodnoceny z pohledu rizikovosti na škále nízká, střední, vysoká, kritická.

Tabulka 9 zobrazuje poměr zařízení z pohledu rizikovosti před vydáním varování, po jeho vydání a po následném přijetí opatření.

Tabulka 9: Hodnoty rizika (Huawei, ZTE). Zdroj: NÚKIB

Hodnota rizika	Před varováním	Po varování	Po přijetí opatření
Nízká	56,87 %	18,88 %	46,93 %
Střední	7,50 %	19,18 %	38,81 %
Vysoká	0,68 %	52,25 %	1,52 %
Kritická	1,14 %	9,53 %	1,14 %
Nebylo zjištěno	33,82 %	0,16 %	2,63 %
Nebylo zaváděno opatření (riziko akceptováno)	-	-	8,97 %

Tisková zpráva obsahuje pouze zjištěné souhrnné informace, přičemž doplňuje, že bližší informace či konkrétní výsledky průzkumu není možné sdělovat či komentovat.

Z tabulky je přitom zřejmé, že u zkoumaných organizací došlo při aktualizaci analýzy rizik k zohlednění varování a identifikaci rizik spojených s technologiemi Huawei a ZTE, aby následně po přijetí opatření došlo ke korekci hodnoty rizika. Autor se domnívá, že opatření byla realizována vyřazením nebo naplánováním vyřazení zmiňovaných technologií a jejich nahrazení technologiemi jiných výrobců. Autor bez bližších údajů neumí interpretovat pouze finální zvýšení rizika v kategorii Středního rizika. Domnívá se, že by se mohlo jednat o nově identifikované riziko, u kterého je akceptován provoz po zbývající dobu životnosti prostředků a tím hodnota rizika, která jako původně neidentifikovaná byla poměrně nízká, vyskočila na hodnotu výrazně vyšší.

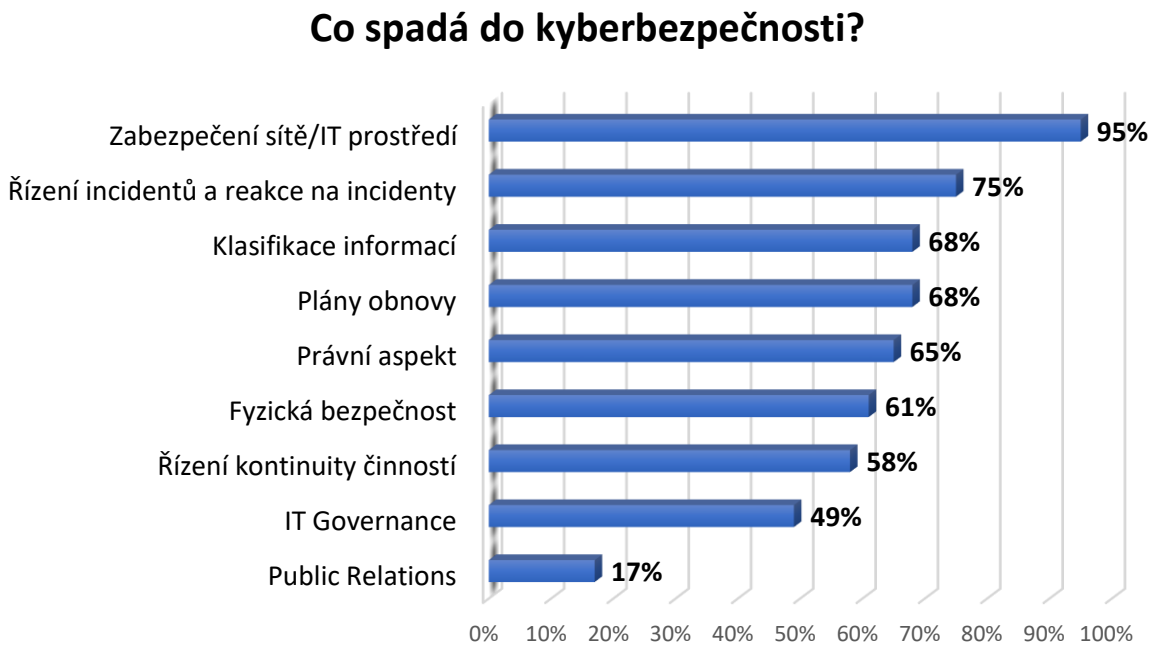
2.1.3 Kyberbezpečnost a my (PwC a TATE)

V červenci 2017 realizovaly společnosti PricewaterhouseCoopers Audit a TATE International průzkum na téma „Průzkum na téma aspekty vzdělávání zaměstnanců v oblasti kyberbezpečnosti“. Součástí výzkumu byly i otázky na spolupráci dotazovaných s NÚKIB (PwC, 2018).

Průzkum byl formou dotazníkového šetření a zúčastnilo se ho 104 osob, přičemž 87 % z nich pracuje na manažerské pozici.

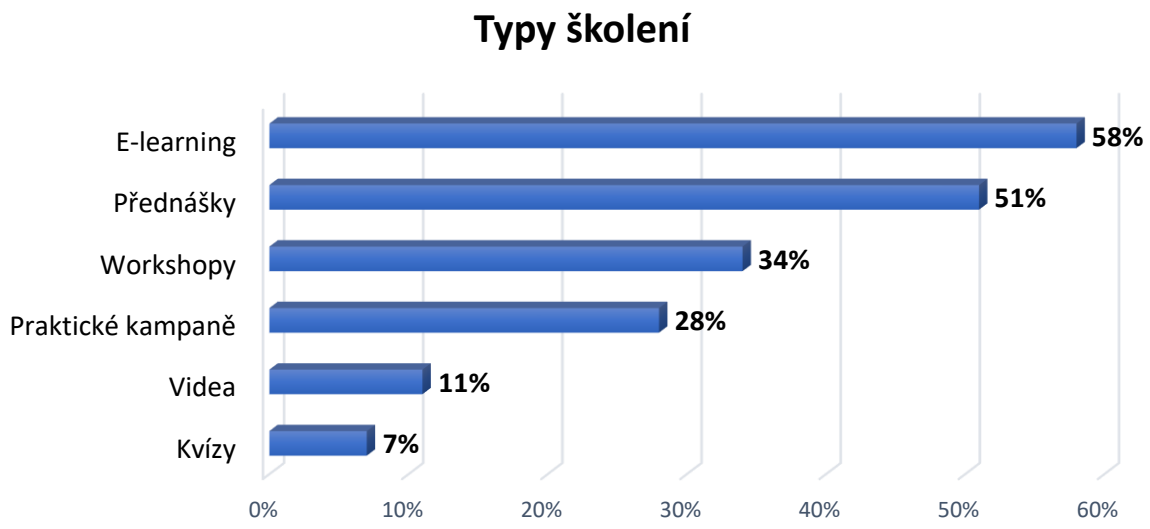
Graf 6: Rozdělení respondentů. Zdroj: PwC

Dotazník byl sestaven z otázek přibližujících prostředí dotazované firmy, její povědomí o možnostech kybernetických rizik a úrovně školení. Na otázku „Co všechno podle vás spadá do kyberbezpečnosti?“ byly získány odpovědi, ze kterých je patrné, že je preferován technický aspekt ochrany bezpečnosti ICT prostředí.



Graf 7: Kyberbezpečnost. Zdroj: PwC

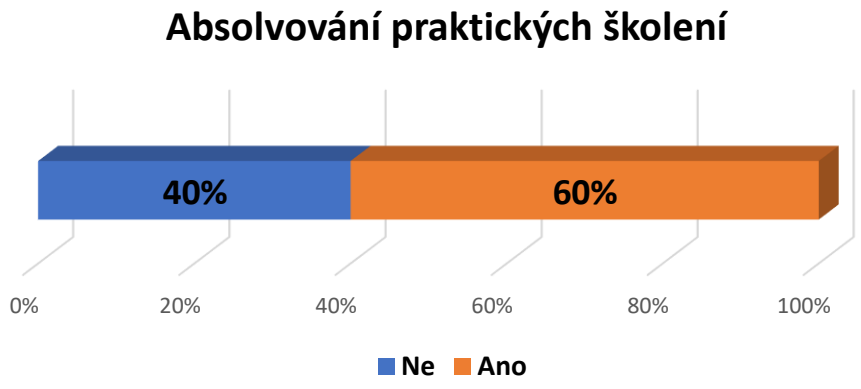
Průzkum potvrdil, že je v organizacích praktikováno školení a vzdělávání zaměstnanců v oblasti kyberbezpečnosti, přičemž z výzkumu vyplynulo, že minimálně jednu nějakou formu školení používá 81 % organizací.



Graf 8: Typy školení. Zdroj: PwC

Nicméně, propojení praktických školení souvisejících s kyberbezpečností si vybavilo pouze 60 % dotazovaných.

Z průzkumu mj. také vyplynulo, že ačkoliv je management firem nejméně proškolenou skupinou, má největší povědomí o možných bezpečnostních rizicích. Lze to vysvětlit skutečností, že je zapojován do rozhodovacích procesů týkajících se rizik a na základě toho jeho informovanost roste.

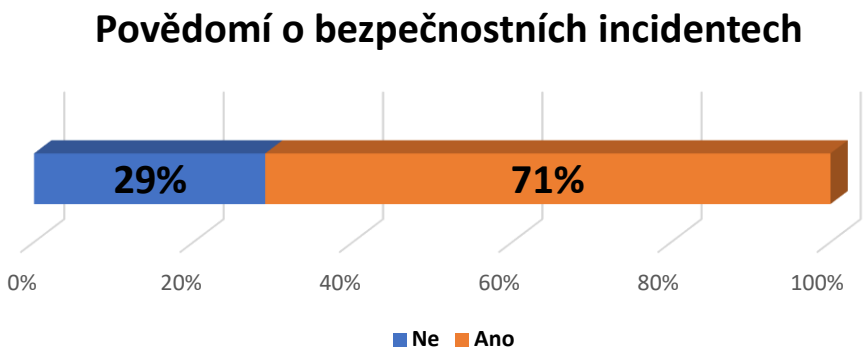


Graf 9: Praktická školení. Zdroj: PwC

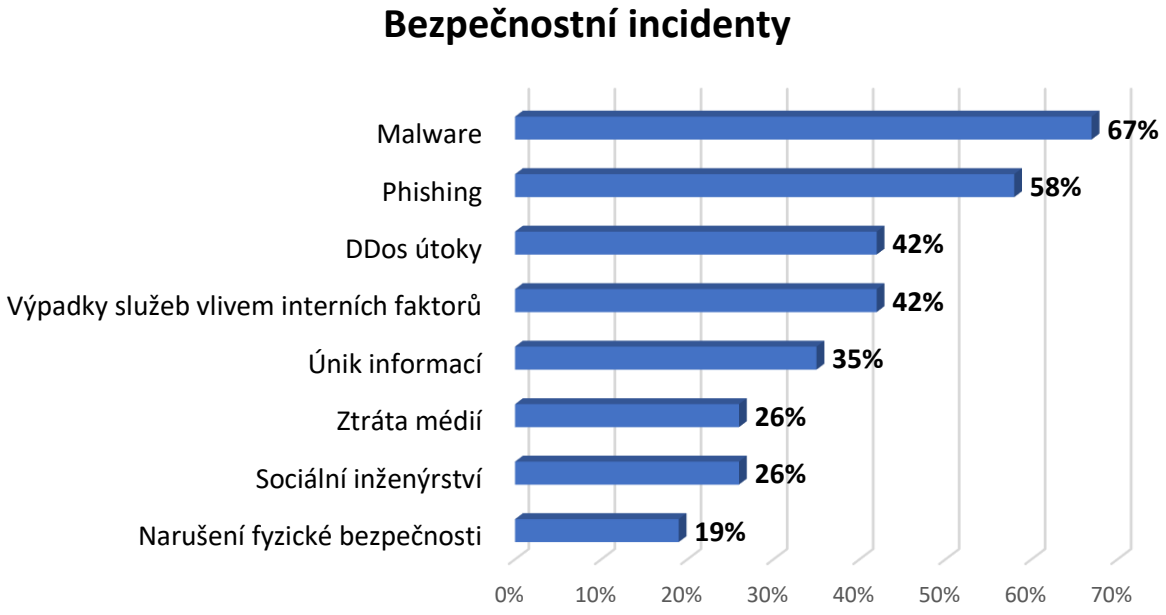
Jako významné hrozby respondenti vnímají nebezpečí útoku na cloudové služby a zneužití kryptoměn. V reakci na globální útoky nového typu (ransomware) vnímají nutnost chránit

firemní počítačovou síť komplexně, tedy nikoliv pouze počítače, ale i tiskárny, kamery, mobilní zařízení a všechny ostatní prvky, které se do sítě připojují nebo v ní nějak fungují.

Na otázku, zda mají dotazovaní povědomí o tom, jaké typy bezpečnostních incidentů se v jejich organizaci objevují odpovědělo pozitivně 71 % účastníků a tito také byli schopni je konkrétně pojmenovat, viz graf 11.

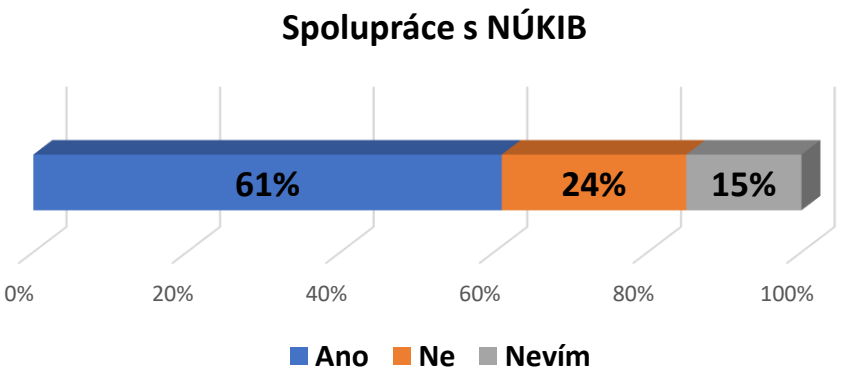


Graf 10: Povědomí o incidentech. Zdroj: PwC



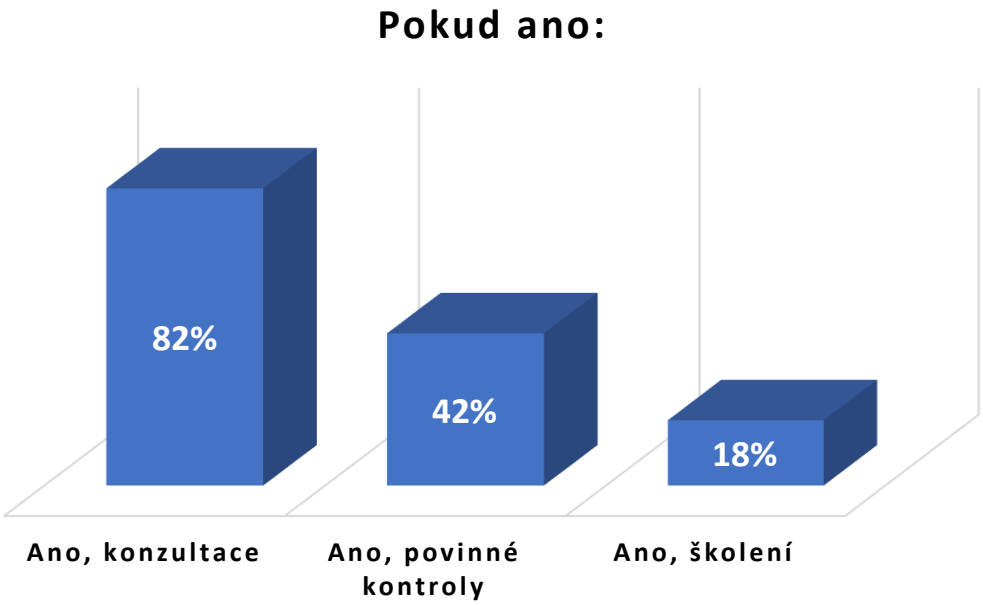
Graf 11: Bezpečnostní incidenty. Zdroj: PwC

V průzkumu bylo také zjištěno, že nadpoloviční většina dotazovaných organizací nějakou formou spolupracuje v otázce kyberbezpečnosti s NÚKIB.



Graf 12: Spolupráce s NÚKIB. Zdroj: PwC

Z výsledků vyplynulo, že se značná část spolupráce odehrává na dobrovolné bázi prostřednictvím aktivit připravovaných NÚKIB.



Graf 13: Spolupráce s NÚKIB – ano. Zdroj: PwC

2.2 Analýza dopadu uplatňování GDPR v prostředí firmy

Jak již bylo v bodu 1.3 uvedeno, GDPR, celým názvem Nařízení Evropského parlamentu a Rady (EU), bylo schváleno 27. dubna 2016 a v platnost vstoupilo 25. května 2018.

Přibližně od posledního čtvrtletí roku 2016 bylo možné v České republice zaznamenat začátky diskusí na téma problematiky jeho analýzy a implementace. Po prvotním seznámení se s obsahem nařízení, začaly organizace, kterých se to týkalo, postupně spouštět projekty na analýzu stavu a přizpůsobovat svoje prostředí a procesy tak, aby dokázaly vyhovět nařízení GDPR. Složitost tohoto procesu se odvíjela od velikosti organizace a také od účelu a způsobu

nakládání s osobními údaji, případně i od počtu systémů, kterými organizace disponovala. Například bankovní instituce běžně uváděly, že musejí analyzovat systémy v počtu vyšších stovek. Z podstaty věci tedy vyplývá, že tento proces byl značně zdlouhavý, náročný na alokování dostatečného počtu kvalifikovaných odborníků, a tím také i finančně náročný.

V červnu 2019 vydala EU tiskovou zprávu s výsledky zvláštního průzkumu v rámci programu Eurobarometr, v němž zjišťovala povědomí Evropanů o nových právech, které GDPR přineslo. Průzkum se uskutečnil formou dotazování a bylo do něj zapojeno 27 000 Evropanů (Evropská komise, 2019).

Přinesl zajímavé informace, například tu, že sice 60 % Evropanů čte prohlášení o ochraně soukromí, ale pouze 13 % je dočte až do konce. Průzkumem bylo současně potvrzeno, že ochrana údajů je zdrojem znepokojení, neboť 62 % respondentů uvedlo, že se obává zneužití údajů, které poskytnou prostřednictvím internetu.

Protože se nařízení GDPR týká ochrany v zásadě jakéhokoliv zpracování osobních údajů fyzických osob EU, dopadá jeho účinnost prakticky na všechny firmy. Pro soulad s novými pravidly musely firmy, na základě přechozí analýzy, udělat změny v nakládání s osobními údaji a jejich zpracováním. Z vnějšího pohledu jsou tyto změny zaznamenatelné zejména ve dvou oblastech. První z nich znamenala nutnost získat nový souhlas se zpracováním osobních údajů od každého subjektu, a to pro každou činnost, pro kterou je zamýšleno jeho údajů použít. V praxi to znamená, že např. souhlas s posíláním pravidelného vyúčtování e-mailem je jedna činnost a zasílání reklamních e-mailů nebo newsletterů je činnost druhá. Pro každou z nich je vyžadován explicitní souhlas a každá z nich může být samostatně odvolána.

Druhý dopad, jenž je zaznamenatelný vnějším pohledem, je uvádění informace o nakládání s osobními údaji na webové stránce každé firmy. Obvykle jsou k dispozici informace o tom, proč a jaké osobní údaje daná firma zpracovává, přičemž rozsah se může výrazně lišit podle potřeby a důvodu zpracovávání. Dále zde bývá informace, jak dlouho jsou tyto osobní údaje zpracovávány a také jakým způsobem lze dosáhnout opravy nebo vymazání osobních údajů.

Už jen splnění těchto dvou zmíněných dopadů nutně znamenalo změny v rámci interních procesů, a to jak v oblasti získávání kontaktních informací, tak v jejich zpracování a nakládání s nimi. Je snadno představitelné, že firmy typu telekomunikačních operátorů nebo utilitní společnosti mohou zpracovávat osobní údaje několika miliónů subjektů a realizace opatření pro soulad s GDPR znamenala revizi procesů a technologií napříč celým ekosystémem firmy.

Praktický dopad GDPR na různé oblasti lze dle PwC shrnout přibližně takto: (PwC, 2017)

Tabulka 10: Dopady GDPR. Zdroj: PwC

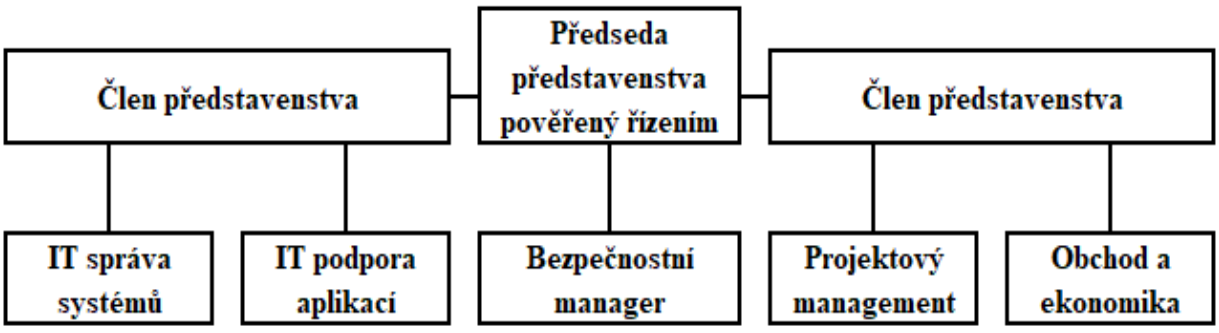
Interní směrnice	Koncepční rámec interních směrnic a pravidel
Procesy	Soubor procesů pro správu dat a informací
Role	Organizační struktura, definice rolí a odpovědností
Kultura	Přístup lidí k otázce ochrany osobních údajů
Informační toky	Kvalita datových toků a přístup k řešení problémů
Lidé a dovednosti	Dovednosti lidí vztahující se ke správě dat
Infrastruktura	Technická infrastruktura, klasifikace a katalog dat

2.2.1 První výpočetní a.s.

Na příkladu firmy První výpočetní a.s. autor demonstruje konkrétní dopad na jednotlivé procesy a činnosti, včetně vzorových dokumentů potřebných k realizaci změn.

Společnost První výpočetní a.s. je firma zaměřující se na poskytování IT služeb se zaměřením na systémovou integraci a podporu zákaznických řešení. Má 60 zaměstnanců a aktuálně přibližně 15 dlouhodobých kontraktů na podporu prostředí zákazníka nebo realizaci konkrétního projektu. Firma také poskytuje školení a pořádá tematické akce zaměřené na konkrétní technologie a možnosti jejich využití.

Struktura firmy se snaží optimálně kopírovat potřeby firmy. Společnost řídí předseda představenstva pověřený řízením spolu s dalšími dvěma členy představenstva zodpovědnými za konkrétně vymezené oblasti. Ve firmě jsou celkem čtyři týmy, každý má svého vedoucího. Týmy jsou rozděleny podle zaměření činnosti na: IT správa systémů, IT podpora aplikací, Projektový management, Obchod a ekonomika. Samostatnou pozici pak má bezpečnostní manager, který je zodpovědný přímo představenstvu.



Obrázek 3: Organizační schéma. Vlastní práce autora.

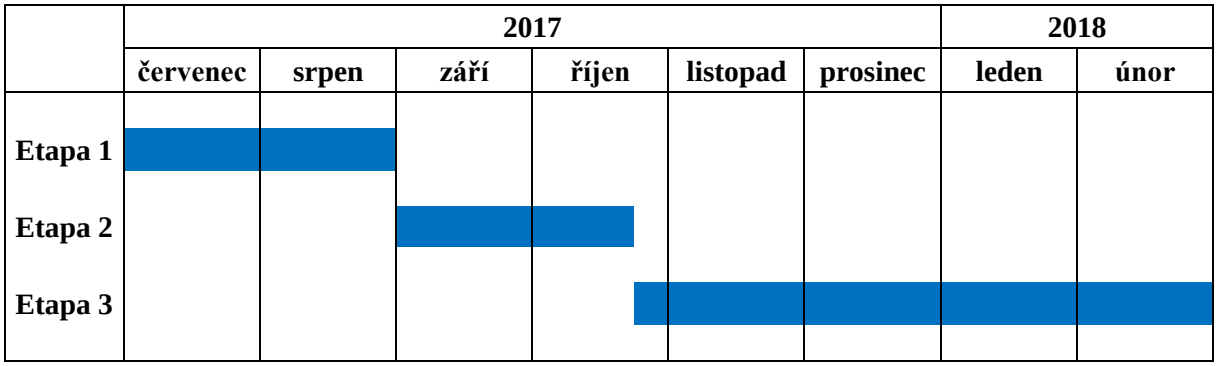
Firma svou přípravu na aplikaci změn nutných pro soulad s GDPR pojala jako projekt, jehož vedení svěřila auditorské firmě. Ještě před začátkem projektu bylo rozhodnuto, že role DPO bude pro společnost zajišťována externě, vybranou právní kanceláří, na základě uzavřené smlouvy o poskytování těchto služeb.

2.2.2 Projekt pro zajištění souladu s GDPR

Projekt byl rozložen do tří etap a byl rozplánován na dobu osmi měsíců tak, aby s dostatečnou rezervou skončil před vstoupením nařízení v platnost.

1. Etapa – Analýza, co všechno se bude muset pro soulad s GDPR řešit.
2. Etapa – Návrhy, jak zjištění z první etapy vyřešit.
3. Etapa – Implementace řešení

V grafu 14 je pomocí zjednodušeného Ganttova diagramu prezentován harmonogram jednotlivých etap projektu.



Graf 14: Zjednodušený Ganttův diagram harmonogramu prací. Vlastní práce autora.

Etapa č. 1: ve své první části obsahovala zmapování systémů a jejich využívání, protože společnost pracuje s daty klientů, dodavatelů, zaměstnanců a také zájemců o zaměstnání. Konkrétním naplněním etapy č. 1 se tak staly čtyři samostatné analýzy, ve kterých se detailní pozornost věnovala těmto oblastem:

a) jaké osobní údaje jsou sbírány a za jakým účelem, v jakých systémech jsou ukládány a zpracovávány, a jak je tato činnost zdokumentována.

b) právní analýze rozdílu mezi požadavky GDPR a zákona na ochranu osobních údajů, identifikaci nových nebo aktualizovaných požadavků.

c) rozdílovému porovnání současného stavu oproti stavu požadovanému pro soulad s GDPR v jednotlivých oblastech činnosti firmy První výpočetní.

d) dopadům právních změn a jejich řešení.

Etapa č. 2: byla rozdělena na dvě části. V první části se diskutovaly návrhy a ohodnocení vybraných variant řešení na základě nalezených nedostatků z etapy č. 1. Součástí byla jejich prioritizace s ohledem na vyčíslení nákladů, časovou a technickou náročnost implementace. Výstupem druhé části byly již konkrétní dopadové karty, ve kterých byl specifikován problém a na jeho základě definovaný projekt nápravy. Vzor dopadové karty je přiložen jako Příloha č. 2.

Etapa č. 3: v jejím rámci probíhala samotná implementace změn, ve které bylo velmi důležité precizní projektové řízení a koordinace všech zúčastněných. Součástí této etapy byly také změny a aktualizace podnikových směrnic a procesů.

Nápravná opatření

V rámci etapy č. 2 byly jako výstup z analýz zpracovány dopadové karty pro pět oblastí, u kterých byl identifikován výrazný nesoulad se zněním GDPR:

1) způsob získání osobních údajů a jejich rozsah
2) způsob zpracovávání a uchovávání získaných osobních údajů
3) bezpečnost úložišť osobních údajů, jak technických, tak technologických
4) obsah smluv se zákazníky
5) způsob nakládání s osobními údaji uchazečů o zaměstnání

Pro všechna tato zjištění bylo nutno udělat nápravná opatření.

Nápravné opatření č. 1 – zajištění souladu s GDPR při získávání osobních údajů a definování nezbytně nutného rozsahu.

Všechny zpracovávané osobní údaje klientů musely projít revizí a očištěním o zbytné položky, a to pro plánovanou akci na znovuzískání souhlasu se zpracováním konkrétních osobních údajů za vyjmenovaným účelem. Bylo naplánováno, že znovuzískání souhlasu bude spojeno se sérií tematických pracovních akcí tak, aby to bylo pro stávající klienty zajímavé a měli důvod a motivaci souhlas poskytnout. Společnost pro tuto potřebu vytvořila nový formulář nazvaný „Souhlas se zpracováním osobních údajů“, jehož součástí byla i informace o možnosti odvolání tohoto souhlasu a návod jak toho dosáhnout. Odvolání souhlasu musí být stejně snadné jako jeho poskytnutí.

Součástí tohoto opatření byla i změna v používání kamerového systému na firemním parkovišti a u vstupu do budovy. Byla vydána nová směrnice o provozu kamerového systému, ve které bylo definováno, kdo má přístup k zobrazení záznamu, jak dlouho a kde jsou tyto záznamy uchovávány.

Nápravné opatření č. 2 – revize způsobu zpracovávání a uchovávání osobních údajů.

Aby byl detailně zmapován celý životní cyklus používaných osobních údajů, bylo nutné zkontrolovat všechny firemní systémy, jako je např. CRM, e-mailové adresáře pro oslovení klientů, finanční databáze apod. Pro zajištění souladu bylo rozhodnuto o vytvoření nové centrální databáze, u které byla použita pseudonymizace tak, aby jednotlivé části osobních údajů samostatně neumožňovaly identifikaci subjektu. Součástí bylo i upravení procesu, aby bylo v budoucnu možné realizovat a dokladovat smazání a „zapomenutí“ osobních údajů.

Nápravné opatření č. 3 – zajištění bezpečnosti úložišť osobních údajů.

Nařízení GDPR doporučuje jako jeden z klíčových postupů pro ochranu citlivých osobních informací šifrování. Realizace a nasazení tohoto způsobu ochrany vyžaduje detailní naplánování architektury systémů a použitých technologií, protože zabezpečený by měl být celý proces práce s citlivými údaji, včetně jejich případného přenosu mezi systémy. V praxi to znamená, že by mělo být šifrované datové pole, kde jsou dala uložena (tedy minimálně ta oblast pole, obsahující tato data). Pokud jsou data zpracovávána v rámci nějaké databáze, měla by mít zapnuto šifrování i tato databáze. Přenos mezi datovým úložištěm a samotnou databází by měl být také šifrován. Proces samozřejmě musí zohledňovat aspekty, kdy například při zpracování dat v tabulkovém procesoru a úpravě uživatelem musí být data nejprve dešifrována. (Nezmar, 2017, s. 245). Nápravné opatření společnosti První výpočetní tedy znamenalo instalaci nového centrálního databázového serveru, postaveného na technologii Microsoft SQL Server 2016, a na jím spravovaných databázích bylo zapnuto šifrování. Do těchto nově vytvořených databází byla postupně přesouvána zrevidovaná data. Dále bylo na poštovním serveru zapnuto šifrování e-mailů a kontrolou bylo potvrzeno již dříve aplikované používání šifrovaného spojení i v rámci interních webů a intranetu.

Nápravné opatření č. 4 - zajištění souladu ve smlouvách.

Toto nápravné opatření se týkalo již uzavřených smluv se zákazníky a dodavateli a bylo nutné doplnění definice rozsahu, účelu a časového ohraničení zpracování dat, případně, pokud se jednalo o zpracovatele dat, doplnění práv a povinností správce a zpracovatele. Zvažována byla varianta doplnění smluv o dodatek, to se však ukázalo jako zdlouhavý proces, který by

znamenal další administrativní práci navíc. Bylo rozhodnuto, že pro každou dotčenou smlouvu bude podepsána aktualizovaná verze firemní Smlouvy o ochraně důvěrných informací (NDA), jež je stejně součástí každého smluvního vztahu, který má společnost navázán.

Aktualizací tohoto dokumentu a zapracováním změny do interních procesů bylo zajištěno, že nové smlouvy a kontrakty budou uzavírány již v souladu s novými pravidly.

Nápravné opatření č. 5 – změna nakládání s životopisy uchazečů o zaměstnání

Řešení tohoto nesouladu bylo rozděleno do třech bodů:

V rámci prvního bodu byl upraven webový formulář na stránkách společnosti, který umožňuje uchazečům o zaměstnání zaslání životopisu. Nově obsahuje informaci o zpracování osobních dat s povinným potvrzením udělení souhlasu se zpracováním. Stejnou verzi formuláře uchazeč vyplňuje při případném osobním jednání, pokud byl například na pohovor pozván na základě telefonického rozhovoru.

Vzor formuláře „Souhlas se zpracováním osobních údajů a poučení“ je přiložen jako Příloha č. 3.

Druhým bodem byla úprava automatické odpovědi od poštovního systému pro případ, že uchazeč poslal životopis e-mailem. Odpověď byla rozšířena o informaci, jak bude s jeho údaji nakládáno.

Třetí bod znamenal úpravu procesů samotného zpracovávání již získaných životopisů. Bylo rozhodnuto, že se tyto dokumenty nebudou uchovávat pro další zpracování a budou automaticky mazány, nejpozději do třech měsíců od ukončení předmětného výběrového řízení, na jehož základě byly získány. Pro transparentní kontrolu a eliminaci možných opomenutí byl na firemním dokumentovém serveru zřízen speciální adresář, jako jediné místo, kam se smějí životopisy ukládat.

Všeobecná informace o zpracování osobních údajů

Na zápatí své hlavní webové stránky společnost umístila odkaz na dokument „Informace o zpracování osobních údajů“ ve kterém jsou popsány zásady zpracování osobních údajů, jejich rozsah a způsob získávání, účel zpracování a vyjmenována práva subjektu na přístup, opravu a doplnění nebo výmaz osobních údajů. V dokumentu je také uveden kontakt na pověřence pro ochranu osobních údajů (DPO).

3 Návrh řídících a školících dokumentů

3.1 Návrh řídících dokumentů

Řídící dokumenty firmy jsou nezbytnou součástí řízení organizace. Je to sada dokumentů, mezi které patří organizační řád, organizační směrnice, instrukce, předpisy, normy, případně sdělení vedení firmy. Pokud je ve firmě zaveden systém řízení kvality podle ČSN EN ISO 9001, je vydán ještě završující dokument Příručka kvality, který stanoví základní pravidla pro tvorbu a obsah všech řídících aktů, tak aby pokrývaly celou činnost firmy.

Uvedené dokumenty obsahují definice procesů a postupů, nařízení a doporučení, a spolu dohromady stanovují závazná pravidla a postupy při řízení organizace. Příručka kvality pak obsahuje mapu procesů organizace. Svým obsahem mapuje celou škálu možných činností důležitých pro chod organizace.

Podle portálu MBI mezi organizační a řídící dokumenty podniku patří zejména:

- Status podniku;
- Organizační řád;
- Funkční náplň pracovních pozic;
- Pracovní řád;
- Podpisový řád;
- Spisový řád;
- Všechny podnikové organizační směrnice a nařízení;
- Předpisy ve vztahu k IT;
- Další specializované předpisy a pokyny, podle odvětví a charakteru podniku.

Účelem těchto dokumentů je „*definovat základní pravidla fungování podniku (organizaci, schvalování dokumentů atd.), a tím zvyšovat a zkvalitňovat celkovou úroveň řízení a následně i výkonnost a úspěšnost podniku*“ (MBI, 2014).

Směrnice

Řídící dokumenty jsou schvalovány na nejvyšší úrovni vedení společnosti a jako takové jsou obvykle závazné pro celou společnost, nebo její vyjmenovanou část. Jak již bylo zmíněno, tyto

dokumenty by měly mapovat celou škálu činností ve společnosti, proto obvykle mají organizací definovanou pevně stanovenou strukturu, která umožňuje jejich přehledné použití.

V záhlaví dokumentu se uvádějí základní údaje týkající se vytvoření dokumentu, kdo a kdy materiál zpracoval (vlastník dokumentu), kdo a kdy jej schválil, od kdy nabývá účinnosti, a který dokument je tímto zneplatněn. Uvádí se také rozdělovník, komu je dokument distribuován a jakou formou.

Každá směrnice obsahuje tyto nezbytné náležitosti:

1. **Účel a cíl**

   V tomto bodu se stručně popisuje účel směrnice a důvod jejího vydání. Důvodem může být např. ustanovení vyplývající ze zákona nebo z technické normy, změna v předmětu činnosti organizace, změna smluvních vztahů nebo jakákoliv jiná změna kontextu organizace. Pokud je firma součástí koncernu, mohou to být např. požadavky mateřské společnosti.

2. **Rozsah působnosti**

   Tento bod vymezuje platnost v rámci společnosti, obvykle je na této úrovni dokumentu platnost stanovena na všechny zaměstnance. Stanovuje také rozsah odpovědnosti jednotlivých zaměstnanců při uplatnění uvedených povinností a pravidel. Pokud je to uvedeno, mohou některá konkrétní ustanovení nabýt účinnosti později nebo mohou být pouze přechodná. Dokument může stanovovat povinnosti pouze pro zaměstnance podřízené schvalovateli.

3. **Pojmy a použité zkratky**

   Vymezení pojmů je důležité pro správné pochopení, protože se terminologie může odkazovat na názvy úřadů nebo k zákonem stanoveným pojmům, a nemusí odpovídat jejich běžně používanému významu.

   Přehledné uvedení použitých zkratek je důležité rozlišení interních a externích pojmů. V textu směrnice se mohou používat jak obecně známé zkratky, tak zkratky platné jen pro konkrétní společnost, obvykle zkratky názvů oddělení nebo odborných útvarů. Zákonem stanovené zkratky se neuvádějí.

4. **Obecná ustanovení**

Zde jsou uvedena pravidla pro použití směrnice a pro nakládání s ní, stejně tak povinnosti, které z ní vyplývají pro pracovníky na určité úrovni řízení.

5. **Vlastní obsah směrnice**

   Tento bod obsahuje konkrétní rozpracování směrnice, definice pravidel, postupů a povinností z nich vyplývajících.

6. **Závěrečná ustanovení**

   V této kapitole se popisuje způsob, resp. zodpovědnost za plnění směrnice, stanovují se kontrolní mechanismy včetně možných kroků při zjištění nesouladu. Mohou zde být stanovena také pravidla pro revizi této směrnice v budoucnu. Například u směrnice pro určení cestovních náhrad dochází každoročně k očekávané novelizaci odpovídajícího zákona.

7. **Související dokumentace**

   Zde se uvádějí zdroje informací související s danou směrnicí, a to jak interní, tj. jiné směrnice nebo instrukce, tak i externí, obvykle zákony nebo směrnice.

8. **Přílohy**

   Přikládají se přílohy, např. vzory formulářů, případně odkazy na elektronické dokumenty nebo formuláře. Ve vlastním obsahu směrnice musí vždy existovat odkaz na přílohy, které jsou závazné.

Směrnic patřících mezi řídící dokumenty může mít podnik několik desítek a tématu „Informační bezpečnost a ochrana informací v podniku“ se bude v praxi věnovat několik z nich, záleží vždy na pojetí formátu řídících dokumentů v daném podniku. Autor zde vyjmenovává návrh devíti směrnic, které mohou obsahovat základní součásti týkající se informační bezpečnosti:

- Směrnice S01 - Ochrana osobních údajů
- Směrnice S02 - Organizace a řízení bezpečnosti informací
- Směrnice S03 - Politika bezpečnosti informací
- Směrnice S04 - Systémová bezpečnostní politika
- Směrnice S05 - Řízení aktiv informačních systémů
- Směrnice S06 - Řízení bezpečnostních incidentů informačních systémů
- Směrnice S07 - Řízení komunikace a provozu informačních systémů

- Směrnice S08 - Řízení přístupu k informačním systémům
- Směrnice S09 - Přístupová práva v systémech ITSM a ISMS

Každá z těchto směrnic zpracovává konkrétní oblast, aby společně postihly celou oblast.

Obvykle jsou směrnice zpracovány pro každou oblast podle přílohy A normy ISO/IEC 27001, případně podle Vyhlášky č. 82/2018 Sb. vydané k zákonu o kybernetické bezpečnosti.

Vzor směrnice „Organizace a řízení bezpečnosti informací“ je přiložen jako Příloha č. 4.

Pracovní instrukce

Na rozdíl od směrnic obsahují pracovní instrukce ještě podrobný postup (algoritmus) předepsané činnosti, který má většinou formát tabulky se sloupci, ve kterých je uvedeno pořadové číslo kroku, odpovědná osoba, činnost a záznamy, které se v daném kroku provádějí, a také další dokumenty, na které se činnost odkazuje.

Příručka kvality

Stanovuje základní pravidla pro tvorbu a obsah všech řídících aktů tak, aby pokrývaly celou činnost firmy a vždy také určovaly odpovědnost zaměstnanců zařazených v odpovídajících funkcích. Příručka kvality obsahuje strategii společnosti, organizaci společnosti, podrobný popis systému managementu kvality a podřízených dokumentů, strategii chování společnosti. Nedílnou součástí je určení postupu při plánování jednotlivých činností, postup při ověřování shody, pravidla pro hodnocení kvality, požadavky na informování, způsob provádění změn. V Příručce je uvedena mapa procesů v organizaci, která umožňuje snadno prověřit, zda jsou skutečně popsány všechny procesy. Je také uveden rozsah systému kvality, ke každé kapitole normy 9001 jsou vyjmenovány příslušné řídící akty, které na ní navazují.

Příručka kvality je minimálně jednou ročně aktualizována.

3.2 Návrh školících dokumentů

V kapitole 1.2.1 autor uvádí, že školení je nezbytnou součástí průběžného vzdělávání zaměstnanců. Obvykle musí projít školením zaměstnanec krátce po nástupu do zaměstnání, nezřídka to bývá i součástí podmínek pro výkon činnosti. Školení se organizuje pro každou potřebnou oblast, takže nový zaměstnanec v krátkém časovém sledu absolvuje např. školení bezpečnosti práce, protipožární školení, školení řidičů, školení firemních hodnot, školení pro práci s počítačovou technikou, a také školení pro bezpečné nakládání s informacemi.

Poslední dvě jmenovaná školení mohou být spojena v jedno, protože se tyto dvě oblasti úzce prolínají a vzájemně doplňují. Tato vstupní školení probíhají formou krátké prezentace a následně podpisem protokolu o proškolení nebo formou e-learningu, kdy po shlédnutí prezentace nebo výukového videa následuje elektronický test na ověření získaných informací.

Mnoho firem si ale uvědomuje nedostatečnost tohoto způsobu vzdělávání a organizuje pro své zaměstnance pravidelné doplňkové proškolení o ochraně informací a počítačové bezpečnosti obecně, zaměřené např. na identifikace základních forem sociálního inženýrství, případně praktickou demonstraci phishingu. Pro praktické využití je tato forma samozřejmě vhodnější a účinnější, protože pro člověka, který nepracuje s počítačem nad rámec svých pracovních povinností, jsou tyto praktické ukázky a zkušenosti velmi cenné a lépe zapamatovatelné.

Navržené školící dokumenty sestávají z prezentace ve formátu PowerPoint a následného testování prostřednictvím e-learningového systému. Testovací program umožňuje stanovit časový limit pro zodpovězení otázky a lze nechat náhodně kombinovat pořadí nabízených odpovědí vždy s náhodně vybranou podmnožinou otázek.

Pro školení infomační bezpečnosti existují tři verze prezentace i testu. První varianta je určena pro nově nastupující zaměstnance a je více zaměřena na osvojení základních pojmů a pravidel používaných ve společnosti. Druhá varianta je určena pro stávající zaměstnance a jejich pravidelné přezkušování. Třetí varianta je doplňková a je určena pro vedoucí pracovníky, protože se v oblasti informační bezpečnosti mohou setkávat s jinými problémy než řadoví zaměstnanci. Vedoucí pracovníci mají také delegovánu větší odpovědnost a jsou na ně kladeny jiné nároky z pohledu ochrany informační bezpečnosti, jejich proškolování může probíhat v odlišných lhůtách a cyklech.

Všechny tři varianty testů jsou pravidelně aktualizovány, přičemž varianty 2 a 3 ale doznávají při aktualizaci alespoň 50 % obměny, aby se otázky při pravidelném přezkušování, pokud možno neopakovaly a uživatelé se museli soustředit na nové téma.

Cílem školení je obsáhnout všechny oblasti informační bezpečnosti a to hlavně z praktického hlediska tak, aby si zaměstnanci dokázali v průběhu školení představit reálné situace z běžného života.

3.2.1 Školení pro koncové uživatele informačních systémů

Školení se ve variantě 1 a 2 zaměřuje na témata, která jsou obsažena v příslušných směrnicích. V rámci online prezentace jsou tyto oblasti podrobně vysvětlovány a následný test obsahuje

náhodně vybranou kontrolní otázku z každého tématu. Otázky jsou uzavřené a u každé jsou v nabídce tři odpovědi, přičemž jen jedna je správná. Pro úspěšné absolvování testu je zapotřebí zodpovědět správně alespoň 8 z 10 náhodně do testu vybraných otázek.

Uživatel v testu tedy dostane deset otázek náhodně zkombinovaných z padesáti dostupných. Tímto je zaručeno, že se testy budou lišit a uživatelé budou nuceni se na jejich splnění soustředit.

Uvedená struktura školících materiálů a navazujících testů je zde uvedena jako příklad a může se v jednotlivých společnostech podle jejich zaměření lišit.

Témata pro variantu 1 a 2:

1. Informační bezpečnost – co si představit pod pojmem informační aktivum, jeho dostupnost, důvěrnost a integrita
2. Fyzická bezpečnost – jak souvisí s ochranou informací, základní zásady ochrany fyzických aktiv a řízení přístupů k těmto aktivům
3. Osobní údaje – co to je, a proč to je potřeba chránit, GDPR
4. Používání hesel a certifikátů – základní informace o bezpečnosti a pravidla pro jejich tvorbu a obnovu, digitální podpis
5. Používání elektronické pošty – SPAM, základní pravidla firemní etikety
6. Používání webu – zakázané stránky a témata, sociální sítě, stahování souborů
7. Licence – rizika porušování autorských práv, softwarová čistota
8. Malware, ransomware, phishing – informace o nových typech možných útoků
9. Používání Wifi – rozdíl mezi firemní, domácí a veřejnou, rizika
10. Zabezpečený vzdálený přístup k firemní síti – VPN, šifrování, pravidla pro práci
11. Žádání o přidělení přístupových práv a schvalování rozsahu přístupových práv k informačním systémům
12. Postup chování uživatelů při obdržení podezřelých E – mailů
13. Pravidla pro nakládání s výpočetní technikou a přístupovými právy přidělenými zaměstnanci při odchodu zaměstnance ze společnosti
14. Postup při likvidaci komponent výpočetní techniky

Vzor školení je ve formě PowerPoint prezentace přiložen jako Příloha č. 5. Prezentace předpokládá výklad lektora a souběžné vysvětlování konkrétních bodů, které se mohou jevit jako příliš složité, jako je např. problematika šifrování.

Vzor odpovědního formuláře pro závěrečný test je přiložen jako Příloha č. 6. Pokud zaměstnanec v tomto testu vyplní alespoň 8 správných odpovědí, bude mu toto potvrzeno školitelem a poslouží jako doklad o úspěšně absolvovaném školení.

Z důvodů evidence účasti na školeních se vyhotovuje Prezenční listina, kde každý účastník školení vyplní svoje jméno, vnitrofiremní identifikační a podepíše se. Vzor formuláře „Prezenční listina pro účastníky školení“ je přiložen jako Příloha č. 7.

Vzorový test z informační bezpečnosti pro uživatele informačních systémů

(Správné odpovědi jsou označeny šedou barvou.)

1. Pravidla pro práci s uživatelskými hesly:

a) hesla musí být minimálně sedmimístná a musí obsahovat pouze malá a velká písmena.
b) hesla musí být minimálně osmimístná a musí obsahovat malá a velká písmena, číslice, případně i zvláštní znaky.
c) hesla musí být minimálně osmimístná a nesmí obsahovat číslice.

2. Pokud je uživatel s přenosným počítačem na cestách, musí zajistit, aby:

a) byly v přenosném počítači vždy nabité baterie, nebo aby měl zajištěný přístup ke zdroji elektrické energie.
b) byl přenosný počítač vždy umístěn v k tomu určené brašně.
c) měl svůj přenosný počítač neustále pod kontrolou. Nesmí zůstat v automobilu nebo na hotelovém pokoji, pokud není uzavřen v hotelovém trezoru.

3. Pokud má uživatel podezření na výskyt škodícího programu:

a) musí tento výskyt okamžitě nahlásit na IT helpdesk společnosti a nesmí pokračovat v práci, dokud nedojde k prověření počítače odbornými pracovníky odboru IT.
b) musí nahlásit tento výskyt na IT helpdesk společnosti, na svém počítači však může nadále pracovat.
c) sám se pokusí tento škodlivý program odstranit a teprve v případě neúspěchu nahlásí tento stav na IT helpdesk společnosti.

4. V čem spočívá princip „Sociálního inženýrství“?

a) V oklamání oběti za účelem získání přístupů například do počítače nebo systému.
b) Sociálního inženýrství je vědní obor, zabývající se vzděláváním sociálních skupin.
c) Sociální inženýrství je vědní obor, zabývající se studiem lidského chování na sociálních sítích.

5. Je povoleno používat pouze schválené a řádně licencované standardní a aplikační počítačové vybavení, které uživatelům nainstalovali pracovníci IT odboru. Je zakázáno:

a) kopírovat firemní data z přenosných nosičů dat do počítače uživatele.
b) kopírovat firemní data z počítače uživatele na přenosné nosiče dat pro služební účely.
c) používat jakékoli neoprávněné kopie licencovaných programů a stahovat jakékoliv nelegální programové vybavení.

6. Vzdálené připojení do počítačové sítě společnosti (zpravidla přes veřejnou síť) představuje značné riziko pro případný průnik do systému:

a) uživatel nesmí za žádných okolností nedovoleným jednáním přispět k tomu, aby se otevřela vnitrofiremní síť společnosti pro nežádoucí přístupy zvenčí.
b) uživatel nesmí pro vzdálený přístup do počítačové sítě společnosti využívat bezpečnostní systémy SSL VPN.
c) uživatel může pro vzdálený přístup do počítačové sítě společnosti využít nástroje doporučené externí firmou, pokud si je dokáže sám nainstalovat.

7. Který z následujících příspěvků je pro mě potenciálním rizikem, pokud jej vystavím na sociální síť?

a) Právě jsme se vrátili z dovolené, uteklo to jako voda, klidně bychom tam mohli být o týden déle.
b) Zítra odjíždíme celá rodina na 14 dní na dovolenou k moři. Chudáci kytky, asi doma uschnou, po celou dobu je nikdo nezaleje.
c) Příští léto bychom chtěli jet zase k moři, ale uvidíme, jak na tom budeme se zdravím a penězi.

8. Klasifikované informace jsou:

a) takové informace, u nichž není potřebné zajistit dostupnost, důvěrnost ani integritu.

b) takové informace, u nichž je nutné zabezpečit alespoň jeden z atributů: dostupnost, důvěrnost a integritu.

c) takové informace, které podléhají zvláštním předpisům.

9. Pro přístup na internet je možné využívat pouze přístupové cesty nastavené odborem IT, které jsou zajištěny odpovídajícími ochrannými prvky (Firewall apod.):

a) uživatelé si mohou sami zřídit přístup na internet ze svého firemního počítače prostřednictvím soukromých přenosových zařízení.

b) uživatelům je zakázáno používat a instalovat jakékoliv zařízení pro přístup na internet, a to i v kombinaci se stávajícím přístupem do sítě.

c) uživatelé mohou svou firemní internetovou adresu používat i pro své podnikání.

10. Na které tři údaje bych se měl zaměřit při kontrole důvěryhodnosti certifikátu, kterým je podepsána chráněná HTTPS stránka?

a) Kde je certifikát uložen, z jaké je země, jestli je určen pro systém Windows.

b) Vystaveno pro, vystavitel, platnost od do.

c) Jakou barvu textu, jakou barvu pozadí a jakou barvu tlačítek má webová stránka certifikační autority, která certifikát vydala.

3.2.2 Školení pro vedoucí pracovníky

Školení ve variantě 3 je doplňkové pro vedoucí pracovníky a věnuje se těmto tématům:

1. Odpovědnost v oblasti ochrany osobních údajů
2. Povinnosti týkající se přístupových práv a oprávnění do konkrétních informačních systémů pro jeho podřízené
3. Zajištění plnění Bezpečnostní politiky IS
4. Požadavky a kritéria pro rozvoj IS nebo pořízení nových součástí
5. Způsob klasifikace a zajištění dostupnosti, důvěrnosti a integrity informací

Závěrečný test obsahuje dvě náhodně vybrané otázky z každého tématu, opět se vybírá ze třech možností, přičemž jen jedna odpověď je správná.

Vzorový test z informační bezpečnosti pro vedoucí zaměstnance

(Správné odpovědi jsou označeny šedou barvou.)

1. **V oblasti ochrany osobních údajů jsou vedoucí zaměstnanci, v jejichž úseku mají zaměstnanci přístup k osobním údajům, povinni:**

   a) zajistit těmto zaměstnancům dostatečné prostory pro ukládání dokumentů obsahující osobní údaje. Tyto prostory nemusí být chráněny proti fyzickému přístupu.
   b) přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití.
   c) přijmout taková opatření, aby nemohlo dojít k neoprávněnému, nebo nahodilému přístupu k osobním údajům, zničení či ztrátě, neoprávněným přenosům, jinému neoprávněnému zpracování, jakož i k jinému zneužití. Ke změně osobních údajů může dojít.

2. **V případě, že uživatel ukončil ve společnosti pracovní poměr, je nadřízený tohoto uživatele povinen:**

   a) zajistit prostřednictvím žádosti na Helpdesk odebrání přístupových oprávnění odchozího zaměstnance do IS/ICT.
   b) provést zálohu všech souborů, které byly uloženy na pracovní stanici odchozího zaměstnance.
   c) zabezpečit pracovní stanici odchozího zaměstnance proti zneužití uložením této stanice do uzamykatelného prostoru.

3. **Vedoucí zaměstnanci jsou povinni zajistit:**

   a) aby požadavky a kritéria pro přejímání nových počítačových a informačních systémů byly jednoznačně stanoveny.
   b) aby požadavky a kritéria pro přejímání nových počítačových a informačních systémů byly jednoznačně stanoveny, schváleny, zdokumentovány a otestovány.
   c) aby požadavky a kritéria pro přejímání nových počítačových a informačních systémů byly jednoznačně zdokumentovány.

4. **Cílem společnosti je vyvarovat se porušení smluvních povinností a bezpečnostních požadavků. Za dodržování smluvních vztahů je odpovědný:**

a) vedoucí zaměstnanec, jehož útvar smluvní vztah připravuje, který je kontaktní osobou / iniciátorem tohoto konkrétního smluvního vztahu.
b) ředitel společnosti.
c) obchodní útvar.

5. Vlastníka aktiva jmenuje:

a) ředitel společnosti nebo jeho zástupce.
b) bezpečnostní manažer.
c) vedoucí zaměstnanec příslušného organizačního útvaru.

6. Pominou-li důvody přidělení přístupových práv, například odchodem zaměstnance ze společnosti nebo přeřazením na jiné funkční místo, musí být neprodleně přístupová práva zrušena nebo změněna. Za včasné zrušení nebo změnu přístupových práv zodpovídají:

a) vedoucí zaměstnanci příslušných organizačních útvarů.
b) klíčoví uživatelé informačních systémů.
c) správci informačních systémů.

7. Vedoucí zaměstnanci dbají:

a) na nakládání s informacemi v souladu s jejich klasifikací a zajištění dostupnosti, důvěrnosti a integrity informací používaných v procesu rozhodování.
b) zabezpečení provozu informačních systémů z hlediska fyzické bezpečnosti a dostatečného příkonu elektrické energie.
c) dodržování pravidel pro uskladnění provozního materiálu.

8. O přidělení individuálních přístupových práv žádá:

a) uživatel informačního systému.
b) ředitel společnosti.
c) vedoucí zaměstnanec příslušného organizačního útvaru.

9. Plnění Bezpečnostní politiky IS je soustavně a cílevědomě kontrolováno. Za provádění této kontroly zodpovídají:

a) správci informačních systémů.
b) všichni vedoucí zaměstnanci.

c) klíčoví uživatelé informačních systémů.

10. Vedoucí organizačních útvarů, kteří připravují (schvalují) smluvní ujednání se třetími stranami:

a) musí zajistit, tato ujednání byla zpracována v souladu s Obchodním zákoníkem.
b) musí zajistit, aby tato ujednání odrážela požadavky informační bezpečnosti vycházející z Bezpečnostní politiky IS, vnitřních norem, standardů a dalších dokumentů vyjadřujících povinnosti, práva a zájmy společnosti.
c) musí zajistit, tato ujednání obsahovala reálný časový harmonogram, definici poskytovaných služeb a specifikaci ceny.

3.3 Návrh interního projektu pro zabezpečení uplatnění zákona

Jako návrh interního projektu autor navrhl projekt na certifikaci firmy na normu ISO/IEC 27001:2013. Návrh projektu obsahuje veškeré činnosti od přípravy, přes implementaci a uvedení do provozu.

Úvod do problematiky

Před zahájením projektu implementace systému řízení bezpečnosti informací (ISMS) je v každé společnosti nutné přezkoumat východiska a vstupy pro tento projekt. Do těchto vstupů zejména patří:

- požadavky mezinárodní bezpečnostní normy ISO/IEC 27001:2013 (ČSN ISO/IEC 27001:2014), ISO/IEC 27005:2011 (ČSN ISO/IEC 27005:2013);
- požadavky zákona č. 181/2014 Sb. a vyhlášky č. 82/2018 Sb.;
- Nařízení Evropské komise – GDPR;
- smlouvy dané společnosti o službách v oblasti informačních a komunikačních technologií (ICT), kterými může být daná společnost stanovena jako provozovatel informačního systému kritické informační infrastruktury (významného informačního systému), nebo jako významný dodavatel dle ZoKB;
- došlá varování Národního úřadu pro kybernetickou a informační bezpečnost, pokud je daná společnost vázána ZoKB;

- vývoj situace v informačních a komunikačních technologiích, zejména v mobilních technologiích, které přinášejí mnoho výhod, ale disponují řadou bezpečnostních zranitelností;
- nutnost zajistit dostatečnou dostupnost a kontinuitu informačních aktiv nebo agend;
- důraz na ochranu dobrého jména společnosti.

Projekt na certifikaci firmy na normu ISO/IEC 27001:2013

Projekt je rozdělen do devíti etap, každá z nich má definovány hlavní výstupy a konkrétní činnosti.

3.3.1 Etapa 1 – Stanovení rozsahu a plánu ISMS, základní zaškolení

Hlavní výstupy:

- Stanovený rozsah chráněných aktiv ISMS (Základ pro Politiku ISMS)
- Stanovený (definovaný) rozsah systému – ISMS
- Harmonogram implementace ISMS
- Školicí materiály
- Zaškolený management a implementační tým
- Stanovené základní role pro ISMS

Činnosti v rámci etapy:

- Navržení základního rámce ISMS
- Projednání, oponentura a odsouhlasení rozsahu chráněných aktiv ISMS
- Projednání a odsouhlasení harmonogramu implementace ISMS
- Navržení a projednání základních rolí pro ISMS
- Přizpůsobení školení dle požadavků a dodání manuálů pro zaškolení managementu a implementačního týmu ISMS
- Realizace základního školení ISMS určeného pracovníkům managementu a členům pracovního implementačního týmu
- Rozhodnutí o formě bezpečnostní dokumentace, o konvenci pro popis procesů

3.3.2 Etapa 2 - Metodika, Identifikace a hodnocení aktiv

Hlavní výstupy

- Metodika pro analýzu rizik
- Registr aktiv, ohodnocená aktiva, stanovení vlastníci
- Stanovený základní rámec přípustného použití aktiv v organizaci
- Rozhodnutí o výběru aktiv pro detailní analýzu rizik

Činnosti v rámci etapy:

- Navržení, projednání a schválení Metodiky pro analýzu rizik
- Provedení inventarizace aktiv, jejich seskupení
- Provedení hodnocení aktiv dle Metodiky
- Stanovení vlastníků aktiv
- Vymezení základního přípustného použití aktiv v organizaci, pravidla pro klasifikaci informací
- Přezkoumání registru aktiv
- Rozhodnutí o výběru aktiv pro detailní analýzu rizik
- Provedení detailní analýzy rizik pro identifikovaná a hodnocená aktiva:
    - identifikace a ohodnocené hrozby,
    - identifikace a ohodnocené zranitelnosti,
    - stanovení rizik

3.3.3 Etapa 3 - Detailní analýza rizik

Hlavní výstupy:

- Registr rizik, identifikované a vyhodnocené hrozby a zranitelnosti, stanovená rizika
- Zpráva o hodnocení rizik
- Prohlášení o aplikovatelnosti bezpečnostních opatření (dokumentuje stávající a nová potřebná bezpečnostní opatření)
- Stanovená míra akceptovatelného rizika
- Plán zvládání rizik

Činnosti v rámci etapy:

- Identifikace stávajících a vytipování nových potřebných bezpečnostních opatření ve vztahu k rizikům (způsob zvládání rizik)
- Přezkoumání nasazení nástrojů pro zvýšení informační bezpečnosti v rámci technických opatření
- Přezkoumání registru rizik a opatření
- Vypracování Zprávy o hodnocení rizik (včetně informačních aktiv a opatření)
- Rozhodnutí o míře akceptovatelného rizika
- Vypracování Prohlášení o aplikovatelnosti
- Vypracování Plánu zvládání rizik – RTP

3.3.4 Etapa 4 - Tvorba a implementace dokumentů a plánů ISMS

Hlavní výstupy:

- Bezpečnostní dokumentace
- Revidovaná stávající dokumentace IMS
- Stanovené záznamy
- Plán kontinuity
- Plán budování bezpečnostního povědomí

Činnosti v rámci etapy:

- Tvorba metodiky pro analýzu rizik
- Vytvoření registru aktiv, ohodnocení aktiv, stanovení vlastníci aktiv
- Stanovení základního rámce přípustného použití aktiv v organizaci
- Vytvoření návrhů bezpečnostní dokumentace, eventuálně revize stávající dokumentace pro tyto oblasti řízení bezpečnosti v souladu s normou ISO27001 a zákonem o kybernetické bezpečnosti:
  - A.5 Politiky bezpečnosti informací
  - A.6 Organizace bezpečnosti informací
  - A.7 Bezpečnost lidských zdrojů
  - A.8 Řízení aktiv
  - A.9 Řízení přístupu a bezpečné chování uživatelů

- A.10 Kryptografie
- A.11 Fyzická bezpečnost a bezpečnost prostředí
- A.12 Bezpečnost provozu
- A.13 Bezpečnost komunikací
- A.14 Akvizice, vývoj a údržba systémů
- A.15 Dodavatelské vztahy, stanovení bezpečnostních požadavků pro dodavatele
- A.16 Řízení incidentů bezpečnosti informací, zvládání bezpečnostních a kybernetických bezpečnostních událostí a incidentů
- A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací
- A.18 Soulad s požadavky
- Kontrola a audit kritické informační infrastruktury a významných informačních systémů

3.3.5 Etapa 5 – Proškolení personálu a Ověřovací provoz systému

Hlavní výstupy:

- Školicí materiály
- Zaškolený střední a vyšší management
- Záznamy pořízené o provozu

Činnosti v rámci etapy:

- Customizace školení a dodání manuálů pro výcvik personálu ISMS
- Provedení výcviku středního a vyššího managementu v rozsahu 1 dne s cílem seznámení s implementovaným ISMS
- Provedení zaškolení uživatelů / zaměstnanců
- Činnosti klienta dle Plánu zvládání rizik, dle stanovených procesů, případné doplňkové a korektivní konzultace
- Běžné provozní činnosti klienta
- Identifikace příležitostí ke zlepšení ISMS
- Průběžné shromažďování faktů o ISMS na základě stanovených záznamů (např. o incidentech a událostech, …)

3.3.6 Etapa 6 - Interní audity a přezkoumání systému vedením

Hlavní výstupy:

- Školicí materiály
- Zaškolení interní auditoři
- Výstupy z interních auditů
- Realizovaná opatření

Činnosti v rámci etapy:

- Customizace školení a dodání manuálů pro výcvik interních auditorů ISMS
- Zaškolení interních auditorů pro ISMS s cílem osvojit si techniky auditování
- Provedení interních auditů ISMS - metodická podpora konzultantem
- Vyhodnocení a uzavření interních auditů
- Zahájení realizace nápravných opatření
- Dopracování systému
- Vytvoření rámce pro řízení souladu ISMS s legislativou a s požadavky
- Vytvoření podkladů a moderování přezkoumání z pohledu ISMS

3.3.7 Etapa 7- Certifikace

Hlavní výstupy:

- Zpráva z prvního stupně auditu
- Zpráva z druhého stupně auditu
- Odstraněné neshody
- Vydaný certifikát

Činnosti v rámci etapy:

- První stupeň certifikačního auditu - přezkoumání dokumentace ISMS
- Odstranění neshod
- Druhý stupeň certifikačního auditu – provedení auditu implementace ISMS
- Odstranění neshod

3.3.8 Etapa 8 - Vyhodnocení projektu implementace ISMS

Hlavní výstupy:

- Celková akceptace projektu

Činnosti v rámci etapy:

- Společné vyhodnocení projektu implementace ISMS

3.3.9 Etapa 9 - Rutinní provoz ISMS

Hlavní výstupy:

- Záznamy pořízené o provozu

Činnosti v rámci etapy:

- Běžné provozní činnosti

Hlavním výstupem projektu tedy bude certifikace na bezpečnostní normu ISO/IEC 27001:2013, která bude obsahovat:

a) popis rozsahu systému řízení bezpečnosti informací,

b) prohlášení politiky a cílů systému řízení bezpečnosti informací,

c) popis použité metody hodnocení rizik a zprávu o hodnocení rizik,

d) prohlášení o aplikovatelnosti,

e) certifikát systému řízení bezpečnosti informací podle ISO/IEC 27001:2013,

f) záznam o přezkoumání systému řízení bezpečnosti informací včetně souvisejících vstupů a výstupů přezkoumání a zprávu z auditů provedených certifikačním orgánem včetně příslušných záznamů o nápravě zjištěných neshod s příslušnou normou a s konstatováním, že společnost splňuje požadavky na zavedení bezpečnostních opatření podle zákona a této vyhlášky.

4 Výsledky

Hlavní cíle této diplomové práce byly definovány jako „Návrh řídících dokumentů a školících dokumentů pro uplatnění zákona o kybernetické bezpečnosti v prostředí konkrétní firmy. Návrh interního projektu pro zabezpečení uplatnění zákona.“. Autor se těmto cílům věnuje v několika částech.

V první části autor navrhl sadu řídících dokumentů, týkajících se této oblasti, včetně vzoru směrnice definující „Organizaci a řízení bezpečnosti informací“ v prostředí konkrétní organizace. Autor si je vědom rozsáhlosti tématu, která značně přesahuje rozsah daný k dispozici v rámci této práce. Bezpečnost informací, pakliže má být řešena v rámci firmy komplexně, vyžaduje mnoho definic a procesů tak, aby společně s technickými prostředky zajistí odpovídající ochranu a kontrolu.

Současně je potřeba vzít v úvahu specifikum každé jednotlivé firmy, protože sice informace, resp. informační aktiva, jsou základní hodnotou každé firmy, ale dle zaměření působnosti společnosti může být jejich kompromitace rozdílně hodnocena, a následně tímto i ovlivněna ochota firmy pro ochranu a bezpečnost těchto informačních aktiv něco aktivně dělat. Platí zde úměra, že čím jsou pro firmu její informační aktiva důležitější, tím je také ohroženější a její ochrana je nákladnější. Tento aspekt se prolíná do všech vrstev ochrany, ať už se jedná o technická nebo organizační opatření.

Technická opatření jsou nezbytnou součástí každé ochrany a generují jak investiční, tak provozní náklady. Obvyklý problém k jejich prosazení je skutečnost, že jejich přínos není na první pohled viditelný. Nezvýší se kapacita ani rychlost, informační systémy nemají nové funkcionality. Dokonce se může stát, že některé stávající systémy mohou být ve své činnosti nasazením moderních prvků ochrany omezeny, protože například používají staré verze komunikačních protokolů nebo zastaralé metody ověřování a při řešení takových situací vznikají vícenáklady, které jsou neplánované.

Poměrně nákladnou položkou je kvalitně řešené organizační opatření. Precizně sepsaná sada řídících dokumentů a směrnic vyžaduje osobu legislativně zdatnou, nejlépe s právnickým vzděláním. Pokud firma ke své činnosti potřebuje např. certifikaci ISO, znamená to opět náklady, jak do interních kapacit, tak do auditorské firmy. Zde se v praxi jako zcela pravdivé potvrzuje pragmatické heslo, že bezpečnost není zadarmo.

V druhé části stanoveného cíle se autor věnoval školení informační bezpečnosti, kde navrhl tři typy školení - pro nově nastupující zaměstnance, pravidelné udržovací proškolení pro stávající zaměstnance a doplňkové školení pro vedoucí pracovníky. Autor se domnívá, že ve společnosti, kde informační technologie nejsou primárním prvkem jejího podnikání, by měla fungovat pravidelná a řízená osvěta, tak aby byli zaměstnanci informováni o aktuálních trendech na poli informační bezpečnosti a aktuálních typech útoků, které se v čase vyvíjejí a jsou stále sofistikovanější. Součástí textu diplomové práce jsou vzorové testy pro zaměstnance a pro vedoucí pracovníky, jako přílohy pak prezentace pro školení, formulář pro testy a prezenční listina.

V textu diplomové práce autor zmiňuje i skutečnost, že zejména ve velkých firmách se stává trendem řešit školení prostřednictvím e-learningových prezentací, stejně tak i následné kontrolní testy. Je to rychlé a operativní, a z toho důvodu méně nákladné na organizaci a čas zaměstnanců. Lze se však domnívat, že školení, při kterém mohou zaměstnanci nad danou tématikou, která jim nemusí být úplně blízká, diskutovat a probírat jednotlivé body na konkrétních příkladech s erudovaným školitelem, mohou mít větší účinnost při přenosu získaných informací do praxe.

Ve třetí části cíle se autor věnoval návrhu interního projektu, ve kterém řešil certifikaci firmy na normu ISO/IEC 27001:2013 a procesy s ní spojené. Jednotlivé kroky a činnosti jsou rozepsány do etap. Lze konstatovat, že každá z etap klade poměrně značné nároky na kompetence interních pracovníků, nebo počítá se zapojením externích konzultantů či auditorů, kteří jsou schopni dané úkoly provést. Ze seznamu těchto činností je zřejmé, že certifikace je nákladná záležitost, která navíc vyžaduje další náklady v budoucnu, protože musí být pravidelně kontrolována a opětovně potvrzována. Jako protihodnotu za tyto náklady lze považovat fakt, že po získání certifikace firma disponuje uznávaným potvrzením kvality, které jejím partnerům nebo zákazníkům zaručuje, že má svá data zabezpečena, umí je řídit a chránit.

Závěr

Cílem diplomové práce bylo naplnění hlavního cíle a dílčích cílů, které byly pro práci stanoveny.

Dílčí cíle byly řešeny v analytické části, ve které byly nejprve jako první dílčí cíl zpracovány průzkumy stavu informační bezpečnosti v podnicích, konkrétně byly použity tři existující výzkumy: od EY, NÚKIB a PwC.

Druhým dílčím cílem pak byla analýza dopadu uplatňování GDPR v prostředí firmy, tento cíl autor řeší návrhem interního projektu ve společnosti První výpočetní, související formulář pro dopadovou kartu a vzor souhlasu se zpracováním osobních údajů jsou přiloženy jako přílohy práce.

První částí hlavního cíle bylo navrhnout řídící dokumenty a školící dokumenty pro uplatnění zákona o kybernetické bezpečnosti v prostředí konkrétní firmy. Toto je zpracováno návrhem směrnice „Organizace a řízení bezpečnosti informací zařazené“ a návrhem školících dokumentů, včetně formuláře pro testy a prezenci.

Druhou částí hlavního cíle bylo vypracovat návrh interního projektu pro zabezpečení uplatnění zákona, tento je řešen návrhem projektu certifikace firmy na normu ISO/IEC 270001:2013.

Na závěr si autor dovoluje uvést, že se vzhledem k tomu, že dílčí cíle i hlavní cíl byly splněny, domnívá, že zadání diplomové práce splnil.

Seznam použité literatury

Monografie

ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Třídící znak 36 9797.

ČSN ISO/IEC 27002. *Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Třídící znak 36 9798.

GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi*. 3., aktualizované vydání. Praha: Grada Publishing, 2015. Management v informační společnosti. ISBN 978-80-247-5457-4.

LAUDON, Kenneth a Jane LAUDON. *Essentials of management information systems*. 10th. Boston: Pearson, 2013. ISBN 978-0-13-266855-6.

MITNICK, Kevin a William SIMON. *Umění klamu*. Gliwice: Helion, 2003. ISBN 83-736-1210-6.

NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing. Právo pro praxi, 2017. ISBN 978-80-271-0668-4.

SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-80-247-4644-9

Online zdroje:

ESET.COM: Firewall. *ESET.COM* [online]. 2019 [cit. 2020-01-28]. Dostupné z: https://www.eset.com/cz/firewall/

EVROPSKÁ KOMISE. *První rok nařízení o ochraně údajů.* [online]. 2019 [cit. 2020-03-02]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/cs/IP_19_2956

EY. *20th Global Information Security Survey 2017–18*. [online]. 2017 [cit. 2020-01-28]. Dostupné z: https://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/01/GISS-2017-%E2%80%93-High-Resolution.pdf

GDPR. *Nařízení (EU) 2016/679* [online]. 2016 [cit. 2020-01-28]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=32394

GDPR.CZ: *Obecné nařízení o ochraně osobních údajů* [online]. 2016 [cit. 2020-01-28]. Dostupné z: https://www.gdpr.cz/gdpr/

IT SLOVNÍK. *Informace* [online]. 2020 [cit. 2020-01-14]. Dostupné z: https://it-slovnik.cz/pojem/informace

LUPA.CZ: *Cambridge Analytica je jen špičkou ledovce. Je tu začátek konce Facebooku?* [online]. 2018 [cit. 2020-01-28]. Dostupné z: https://www.lupa.cz/clanky/cambridge-analytica-je-jen-spickou-ledovce-je-tu-zacatek-konce-facebooku/

ManagementMania. *ISO 27001: Systém managementu bezpečnosti informací.* [online]. 2015 [cit. 2020-01-28]. Dostupné z: https://managementmania.com/cs/iso-27001

MBI. *Organizační a řídící dokumenty* [online], 2014 [cit. 2020-04-07]. Dostupné z: https://mbi.vse.cz/public/cs/obj/DOCUMENT-5

NÚKIB. *Varování NÚKIB před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation.* [online]. 2018 [cit. 2020-03-02]. Dostupné z: https://nukib.cz/download/uredni-deska/Varov%C3%A1n%C3%AD%20N%C3%9AKIB%202018-122-17.pdf

NÚKIB. *Ministerstva, úřady i firmy vzaly varování NÚKIB vážně*. [online]. 2019, [cit. 2020-03-02]. Dostupné z: https://www.nukib.cz/cs/informacni-servis/aktuality/1349-ministerstva-urady-i-firmy-provedly-predepsane-analyzy-prijimaji-opatreni-ke-snizeni-rizika/

NÚKIB. *NÚKIB* [online]. 2020 [cit. 2020-01-28]. Dostupné z: www.nukib.cz

NÚKIB. *Publikace.* [online]. 2020 [cit. 2020-03-02]. Dostupné z: https://www.nukib.cz/cs/informacni-servis/publikace/

PRACOVNÍ SKUPINA 29. *Pokyny pro souhlas podle nařízení 2016/679*. [online]. 2018 [cit. 2020-03-02]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31896.

PWC. *Obecné nařízení o ochraně osobních údajů.* [online]. 2017 [cit. 2020-03-02]. Dostupné z: https://www.pwc.com/cz/cs/temata/gdpr.html

PWC. *Kyberbezpečnost a my.* [online]. 2018 [cit. 2020-03-02]. Dostupné z: https://www.pwc.com/cz/cs/rizeni-rizik/assets/kyber-bezpecnost-a-my.pdf

ROOT.CZ. *CERT/CSIRT týmy a jejich role.* [online]. 2013 [cit. 2020-01-28]. Dostupné z: https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/

ČESKO. *Vyhláška č. 317/2014 Sb.: Vyhláška o významných informačních systémech a jejich určujících kritériích.* In: Sbírka zákonů České republiky. 2014, částka 127, s. 4007-4013. Dostupná také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=27583. ISSN 1211-1244.

ČESKO. *Vyhláška č. 205/2016 Sb.: Vyhláška, kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.* In: Sbírka zákonů České republiky. 2016, částka 77, s. 3175-3180. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=55916. ISSN 1211-1244.

ČESKO. *Zákon č. 181/2014 Sb.: Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů.* In: Sbírka zákonů České republiky. 2014, částka 75, s. 1926-1936. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=27231. ISSN 1211-1244.

ČESKO. *Vyhláška č. 82/2018 Sb.: Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.* In: Sbírka zákonů České republiky. 2018, částka 43, s. 1122-1163. Dostupná také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=38431. ISSN 1211-1244.

ČESKO. *Zákon č. 110/2019 Sb.: Zákon o zpracování osobních údajů.* In: Sbírka zákonů České republiky. 2019, částka 47, s. 890-911. Dostupný také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=38632. ISSN 1211-1244.

Seznam zkratek, grafů, obrázků a tabulek

Zkratky:

CERT	Computer Emergency Response Team – Skupina poskytující bezpečnostní rady a informace
CRM	Customer Relationship Management – Systém pro řízení vztahů se zákazníky
CSIRT	Computer Security Incident Response Team - Skupina zajišťující koordinaci řešení a prevenci počítačové bezpečnosti
DLP	Data Loss Prevention – Systém ochrany dat
DoS/ DDos	Distributed Denial of Service – Typ internetového útoku, zahlcuje cíl požadavky
DPO	Data Protection Officer – Pověřenec pro ochranu osobních údajů
EU	Evropská unie
GDPR	General Data Protection Regulation – Nařízení (EU) 2016/679 o ochraně osobních údajů
ICT	Information and Communication Technologies - Informační a telekomunikační technologie
ISMS	Information Security Management System- Systém řízení bezpečnosti informací
NBÚ	Národní bezpečnostní úřad
NCKB	Národní centrum kybernetické bezpečnosti
NDA	Non-disclosure agreement – Smlouva o sdílení důvěrných materiálů a informací.
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
ÚNMZ	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví
ZoKB	Zákon o kybernetické bezpečnosti

Grafy:

Obrázky:

Tabulky:

Přílohy

Příloha č. 1: Příručka pro administrátory – Bezpečnostní doporučení NÚKIB pro administrátory 4.0

Příloha č. 2: GDPR implementace – Dopadová karta

Příloha č. 3: Souhlas se zpracováním osobních údajů a poučení

Příloha č. 4: Vzor směrnice „Organizace a řízení bezpečnosti informací“

Příloha č. 5: Vzor školení v oblasti informační bezpečnosti pro koncové uživatele

Příloha č. 6: Vzor závěrečného testu po absolvování školení

Příloha č. 7: Vzor formuláře „Prezenční listina účastníků školení“

Příloha č. 1

Příručka pro administrátory

BEZPEČNOSTNÍ DOPORUČENÍ NÚKIB PRO ADMINISTRÁTORY 4.0

INFRASTRUKTURA

ČLEŇTE SÍŤ NA MENŠÍ CELKY (SEGMENTACE) A STRIKTNĚ ODDĚLUJTE UŽIVATELSKÁ PRÁVA NAPŘÍČ UŽIVATELI (SEGREGACE)
s cílem oddělit citlivé informace a kritické služby typu autentizace uživatelů (např. Microsoft Active Directory) a vytvořit zóny s různou úrovní bezpečnostních omezení.

BLOKUJTE ŠKODLIVÉ IP ADRESY A DOMÉNY NA ÚROVNI GATEWAY (BLACKLISTY).

NASAĎTE SÍŤOVÉ SYSTÉMY DETEKCE / PREVENCE PRŮNIKU (IDS/IPS)
používající signatury a heuristiky k identifikaci anomálního provozu v rámci sítě i překračujícího perimetr.

SLEDUJTE SÍŤOVÝ PROVOZ
pomocí vybraných síťových prvků nebo rozmístěním dedikovaných síťových sond. Sledujte komunikaci mezi klienty a servery, komunikaci klientů do internetu, komunikaci mezi servery i provoz na perimetru sítě a identifikujte provozní a bezpečnostní problémy.

UCHOVÁVEJTE SÍŤOVÝ PROVOZ
z/do kritických pracovních stanic a serverů a provoz překračující perimetr sítě pro případné forenzní zkoumání po průniku do sítě a systémů. Záznamy síťového provozu doporučujeme uchovávat po dobu minimálně 12 měsíců, více podle místních okolností a významu sítě – v případě kritické informační infrastruktury (KII) a u informačních systémů základní služby (PZS) podle zákona o kybernetické bezpečnosti a návazných vyhlášek je minimální lhůta 18 měsíců. V případě sítí strategického významu zvažte i možnost automaticky aktivovaného plného záznamu datového provozu (PCAP), a to jak na primárních, tak záložních systémech (např. webových nebo systémových serverech).

KONTROLUJTE PŘÍCHOZÍ E-MAILY
pomocí mechanismů Sender ID, SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) a DMARC (Domain-based Message Authentication, Reporting and Conformance) a blokujte podvržené zprávy. Tyto mechanismy nastavte i pro možnou kontrolu odchozích zpráv druhou stranou.

POUŽÍVEJTE ŠIFROVANÉ SPOJENÍ MEZI POŠTOVNÍMI SERVERY (TLS)
pro zajištění důvěrnosti e-mailové komunikace, v ideálních případě použijte DANE (DNS-based Authentication of Named Entities). Kontrolu obsahu provádějte až poté, co je e-mailový provoz dešifrován.

PROVÁDĚJTE AUTOMATIZOVANOU DYNAMICKOU ANALÝZU OBSAHU E-MAILŮ A WEBŮ
prováděnou v sandboxu – hledejte podezřelé chování podle síťového provozu, tvorby nových souborů, úpravy stávajících souborů nebo změn konfigurace.

POVOLTE NA FIREWALLU POUZE ŽÁDOUCÍ SLUŽBY A STANDARDNÍ PROVOZ.
V případě koncových stanic nezapomeňte také blokovat spojení z Vámi nekontrolované sítě.

KONTROLUJTE POUŽÍVANÉ KLÍČE/CERTIFIKÁTY
především pro SSH autentizaci, webové servery, vzdálenou plochu apod. Kde je to možné, použijte šifrovanou komunikaci.

ZAJISTĚTE CENTRALIZOVANÉ A ČASOVĚ SYNCHRONIZOVANÉ LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ
(povolených a blokovaných) s okamžitým automatickým vyhodnocováním a uložením po dobu minimálně 18 měsíců, více podle místních okolností a významu sítě.

APLIKUJTE WHITELISTING WEBOVÝCH DOMÉN
pro všechny domény – pokud to dovoluje charakter práce uživatelů. Tento přístup je účinnější než blacklistovat malé procento škodlivých domén.

VOLTE JEDNODUCHÉ DOMÉNOVÉ NÁZVY,
aby byly jasně viditelné případné záměny písmen ve phishingových e-mailech.

NASAĎTE ANTI-DDoS TECHNOLOGIE,
které můžete po důkladné úvodní analýze řešit buď vlastními silami, nebo ve spolupráci s poskytovatelem internetového připojení. Anti DDoS ochranu nasaďte na kompletní IP rozsahy vaší organizace.

VYPRACUJTE DISASTER RECOVERY PLAN (DRP)
a mějte připravené správné a funkční emailové adresy a telefonní čísla na ostatní administrátory, nadřízené pracovníky a CERT/CSIRT týmy.

STANICE A SERVERY

UDRŽUJTE AKTUÁLNÍ OPERAČNÍ SYSTÉM
pravidelnými aktualizacemi a v co nejkratší době aplikujte všechny vydané bezpečnostní záplaty.

UDRŽUJTE AKTUÁLNÍ SOFTWARE,
pravidelně kontrolujte verze instalovaného softwaru. U neaktuálního softwaru proveďte v rámci možností update. Zastaralé mohou být i verze použitých doplňků či modulů nebo firmware zařízení.

NEPOUŽÍVEJTE NEPODPOROVANÉ PRODUKTY,
používejte pouze produkty (software i operační systémy), pro které jsou dostupné bezpečnostní záplaty.

OVĚŘUJTE IDENTITU APLIKACÍA SOUBORŮ
a povolte jen ty důvěryhodné včetně skriptů a DLL knihoven. V prostředí Windows použijte Device Guard, AppLocker, popřípadě Zásady omezení softwaru (SRP).

PROVÁDĚJTE HARDENING KONFIGURACE UŽIVATELSKÝCH APLIKACÍ
– povolte jen funkcionalitu, která je vyžadována pro práci uživatelů. Dodatečné funkce (např. Java a Flash ve webovém prohlížeči, makra v MS Office) povolte pouze, je-li to nutné.
POUŽÍVEJTE OBECNÉ PREVENTIVNÍ MECHANISMY, které mohou pomoci ochránit systém před zero-day zranitelnostmi, jako např. DEP (Data Execution Prevention) nebo SELinux v linuxových systémech.

POUŽÍVEJTE OBECNÉ PREVENTIVNÍ MECHANISMY,
které mohou pomoci ochránit systém před zero-day zranitelnostmi, jako např. DEP (Data Execution Prevention) nebo SELinux v linuxových systémech.

AKTIVUJTE IDS/IPS SYSTÉMY NA KONCOVÝCH STANICÍCH
detekující anomální chování jako např. injekci kódu do jiných procesů, změnu chráněných registrových klíčů, zachytávání stisků kláves, načítání neznámých ovladačů, snahu o zajištění perzistence a další.

ZAJISTĚTE CENTRALIZOVANÉ A ČASOVĚ SYNCHRONIZOVANÉ LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ
(povolených a blokovaných) s okamžitým automatickým vyhodnocováním a uložením pro kritickou informační infrastrukturu (KII) a provozovatele základní služby (PZS) po dobu minimálně 18 měsíců, pro významné informační systémy (VIS) po dobu minimálně 12 měsíců a pro ostatní systémy podle místních okolností a významu sítě.

FILTRUJTE OBSAH E-MAILŮ A PROPOUŠTĚJTE POUZE RELEVANTNÍ DRUHY PŘÍLOH
– po důkladné analýze chování uživatelů určete typy souborů, které potřebují posílat e-mailem. Ostatní formáty příloh blokujte – především spustitelný kód. Dále ověřujte soulad přípony souboru a jeho skutečného formátu.

PRAVIDELNĚ ZÁLOHUJTE DŮLEŽITÁ A CITLIVÁ DATA
jako např. obsah webového serveru, databází nebo konfigurací služeb. Zálohu umístěte do odděleného prostředí mimo produkční síť. Pravidelně testujte, jestli dokážete data obnovit a jestli jsou data po obnově funkční.

ZAVEĎTE STANDARD OPERATING ENVIRONMENT (SOE)
se standardizovanou konfigurací pro pracovní stanice i servery, kde budou vypnuty všechny nevyžádané funkcionality.

ZAMEZTE PŘÍMÉMU PŘÍSTUPU PRACOVNÍCH STANIC NA INTERNET
a směrujte provoz přes split DNS server, e-mailový server nebo autentizovaný web proxy server. Nezapomeňte vynutit pro IPv4 i Ipv6.

POUŽÍVEJTE ANTIVIROVÝ A BEZPEČNOSTNÍ SOFTWARE
a nástroje, které zakazují spouštění nebezpečných aplikací (mimo přesně definovaný seznam privilegovaných aplikací), či nástroje, které pomáhají chránit systém v době, kdy nejsou dostupné klasické bezpečnostní aktualizace.

ŠIFRUJTE DISKY
– zejména u přenosných počítačů – včetně centrální evidence klíčů.

VYUŽÍVEJTE TRUSTED PLATFORM MODULE (TPM),
tedy zabezpečený kryptografický modul pro generování a uložení hesel a kryptografických klíčů, je-li jím počítač vybaven.

NASTAVTE HESLO UEFI/BIOS
unikátní pro každou stanici s centrální správou hesel.

VYNUCUJTE SECURE BOOT
a nastavte pořadí zařízení určených pro boot systému. Boot manager musí být zabezpečen heslem.

CHRAŇTE SE PŘED ÚTOKY NA HESLA
u všech služeb, kam se přihlašují uživatelé. Například pomocí fail2ban, využití funkcí určených pro ukládání hesel (Argon2, bcrypt, scrypt, PBKDF2) nebo CAPTCHA.

PRO SPRÁVU SERVERŮ POMOCÍ SSH V VYUŽÍVEJTE PRO PŘIHLÁŠENÍ KLÍČE, ZAKAŽTE HESLA.
Pro svázání otisku klíče se serverem, kde je použitý, využívejte SSHFP záznamy v DNS ideálně v kombinaci s DNSSEC, který zajistí autenticitu odpovědi obsahující SSHFP záznam.

PROVÁDĚJTE HARDENING KONFIGURACE SERVEROVÝCH APLIKACÍ
tj. databází, webových aplikací, CRM systémů, účetních systémů, HR systémů a dalších systémů ukládání dat.

KONTROLUJTE PŘENOSNÁ MÉDIA
jako součást širší strategie prevence ztráty dat, včetně vedení seznamu povolených USB zařízení, jejich skladování, šifrování, mazání a likvidace.

OMEZTE PŘÍSTUP K SERVER MESSAGE BLOCKU (SMB) A NETBIOSU
na pracovních stanicích a serverech, kde kolivje to možné.

POUŽÍVEJTE REŽIM CHRÁNĚNÉHO PŘÍSTUPU PŘI PRÁCI SE SOUBORY NA ÚROVNI PRACOVNÍCH STANIC
může se např. jednat o Protected View nebo Protected mode.

VYNUŤTE VYTÁČENÍ VPN,
pokud se zařízení připojuje mimo síť organizace. Omezte síťovou aktivitu, dokud není navázáno VPN spojení.

ZAJISTĚTE FYZICKOU BEZPEČNOST IT TECHNIKY

SPRÁVA ÚČTŮ

ZAVEĎTE CENTRÁLNÍ SPRÁVU UŽIVATELSKÝCH ÚČTŮ A OPRÁVNĚNÍ
a nastavte jednotnou bezpečnostní politiku. Účtům, u kterých to není vyžadováno, odeberte rozšířená oprávnění a zakažte spouštění skriptů, instalaci softwaru, úpravy registru atd.

VYNUCUJTE VÍCEFAKTOROVOU AUTENTIZACI
zejména pro akce vyžadující vyšší úroveň oprávnění a kritické operace jako vzdálený přístup nebo přístup k citlivým informacím.

ODDĚLTE ADMINISTRÁTORSKÉ ÚČTY
Pro správu používejte speciální účty pro administraci systémů. Pro své ostatní pracovní aktivity (e-mail, web atd.) používejte běžný neprivilegovaný účet. Účet s oprávněním doménového administrátora je použít pouze ke správě Domain Controlleru (tzn. nepřistupujeme na klientské stanice a servery).

PŘIDĚLTE KAŽDÉMU ADMINISTRÁTOROVI VLASTNÍ ÚČET
pro správu systémů. Nepoužívejte sdílené účty.

ZABEZPEČTE LOKÁLNÍ ADMINISTRÁTORSKÉ ÚČTY.
Nastavte unikátní heslo na každé stanici, v prostředí Windows můžete využít například LAPS (Local Administrator Password Solution).

VYNUŤTE POUŽÍVÁNÍ SILNÝCH HESEL
s ohledem na vyžadovanou složitost, délku a dobu platnosti. Zamezte opakovanému použití stejných hesel a používání slovníkových výrazů. Vynuťte změnu hesla, existuje-li podezření, že bylo kompromitováno.

PRAVIDELNĚ KONTROLUJTE UŽIVATELSKÉ ÚČTY A JEJICH OPRÁVNĚNÍ
a to jak lokální, tak centrálně spravované.

www.nukib.cz

Národní úřad pro kybernetickou a informační bezpečnost

Příloha č. 2

GDPR implementace – Dopadová karta

GDPR implementace- Dopadová karta:	
Zadavatel:	Datum zahájení:
Projektový manažer:	Datum ukončení:
Dotčené oblasti:	

Rozsah projektu
Zadání projektu:
Mimo rozsah projektu:
Rizika, omezení, limity:

Výstupy projektu	
Výstup	Popis

Projektové fáze			
Název	Popis	Zahájení	Dodání

Potřebné zdroje	
Interní	Externí

Potřebné vstupy		
Popis	Formát vstupu	Dodavatel

Příloha č. 3

Souhlas se zpracováním osobních údajů a poučení

Já, níže podepsaný/á

Jméno a příjmení

……..……..

Narozen/á

……..……..

Bytem

……..……..

(dále jen „**Subjekt údajů**“)

uděluji tímto společnosti **První výpočetní, a.s.**, se sídlem Uliční 10, Praha 1, PSČ 100 00, IČO: 12345678, zapsané v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 12458, emailový kontakt: info@prvnivypocetni.cz (dále jen „**Správce**“), souhlas se zpracováním mých osobních údajů, a to za níže uvedených podmínek:

1. **Osobní údaje, které budou zpracovány:**
   - jméno a příjmení,
   - poštovní adresa,
   - emailová adresa,
   - telefonický kontakt.

2. **Účelem zpracování osobních údajů je:**

Zápis do evidence uchazečů o zaměstnání u Správce.

3. **Doba zpracování osobních údajů je:**

Tři měsíce od doby uzavření konkrétního výběrového řízení, nejdéle však jeden rok od udělení souhlasu.

4. **Osobní údaje nebudou poskytovány třetím osobám.**

Subjekt údajů prohlašuje, že byl Správcem řádně poučen o zpracování a ochraně osobních údajů*, že výše uvedené osobní údaje jsou přesné a pravdivé a jsou Správci poskytovány dobrovolně.

V …… dne ……

Podpis Subjektu údajů ……

***Poučení Subjektu údajů**

Správce tímto v souladu s ustanovením čl. 13 Nařízení Evropského parlamentu a Rady (EU) č.2016/679 ze dne 27. dubna 2016, obecného nařízení o ochraně osobních údajů (dále jen „Nařízení"), informuje, že:

a) osobní údaje Subjektu údajů budou zpracovány na základě jeho svobodného souhlasu, a to za výše uvedených podmínek,

b) důvodem poskytnutí osobních údajů Subjektu údajů je zájem Subjektu údajů o získání zaměstnání u Správce, což by bez poskytnutí těchto údajů nebylo možné,

c) při zpracování osobních údajů Subjektu údajů nebude docházet k automatizovanému rozhodování ani k profilování,

d) Správce nepověřil zpracováním osobních údajů žádného zpracovatele ani neurčil zástupce pro plnění povinností ve smyslu Nařízení,

e) Správce nemá v úmyslu předat osobní údaje Subjektu údajů do třetí země, mezinárodní organizaci nebo jiným než výše uvedeným třetím osobám,

f) Subjekt údajů má právo kdykoliv odvolat svůj souhlas se zpracováním osobních údajů, právo požadovat od Správce přístup ke svým osobním údajům, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, má právo na přenositelnost těchto údajů k jinému správci, jakož i právo podat stížnost u Úřadu pro ochranu osobních údajů, má-li za to, že Správce při zpracování osobních údajů postupuje v rozporu s Nařízením.

g) Správce má jmenovaného pověřence pro ochranu osobních údajů, jeho kontaktní e-mail je: poverenec@prvnivypocetni.cz

Příloha č. 4

Vzor směrnice „Organizace a řízení bezpečnosti informací“

ORGANIZACE A ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

Rozdělovník písemných výtisků

Č. výtisku	Majitel výtisku - funkce
1	10001 Asistentka
2	—
3	—

Schválení

Zpracoval:		Schválil:	
Datum:		Datum:	
Podpis:		Podpis:	
Účinnost:		Výtisk č.:	
Ruší se:			

Změnový list

Číslo:	Změna:	Schvaluje:	Datum:

Obsah

Pojmy a definice rolí

Pro účely tohoto dokumentu jsou použity následující pojmy a definice:

Pojem	Definice
PV	První výpočetní, a.s.
IS	Informační systém
ISMS	Systém řízení bezpečnosti informací
ICT	Informační a komunikační technologie
SLA	Smlouva o úrovni služby
KPR	Komise pro rozvoj
VT	Výpočetní technika
Role	Definice
Uživatel	Uživatel je zaměstnanec PV nebo třetí strany, který se zúčastňuje procesu komunikace a zpracování informací v rámci PV. Před první komunikací je povinen se seznámit s touto směrnicí.
Správce ICT	Správce ICT je zaměstnanec PV, který obdržel oprávnění k administraci ICT. Tato správcovská oprávnění musí být oddělena od jeho práv uživatelských.
Auditor bezpečnosti informací	Auditor je odpovědný za systematický, nezávislý a dokumentovaný proces získávání důkazů o kontrolovaném předmětu a jeho objektivního hodnocení s cílem stanovit rozsah splnění stanovených kritérií. Auditorem může být externí pracovník.
ServisDesk	Systém pro řízení nahlášených událostí (požadavků, incidentů, problémů) s cílem udržet, popřípadě obnovit, funkce informačních systémů v dohodnutém rozsahu a čase.
Bezpečnostní manažer	Bezpečnostní manažer informačního systému PV je role odborného vedoucího pracovníka pro informační bezpečnost, jehož hlavním úkolem je organizovat, řídit a zajišťovat odborné úkoly informační bezpečnosti.
Vlastník aktiva	Role, která odpovídá za identifikaci, evidenci a ohodnocení aktiva, stanovuje způsob využití aktiva a úrovně přístupu k aktivu, a odpovídá za realizaci přijatých opatření ke zvládání rizik spojených s aktivem.
Vedoucí zaměstnanci	Vedoucí organizačních složek PV.
Třetí strany	Subjekt, který není organizačním útvarem nebo zaměstnancem PV.

Definice organizace bezpečnosti informací

Vzhledem k tomu, že informační bezpečnost zahrnuje oblast informačních technologií a systémů, oblasti organizační administrativní, personální, právní, ochrany majetku, krizového řízení a dalších, se v rámci společnosti První výpočetní zavádí proces organizace a řízení bezpečnosti informací.

Organizace bezpečnosti informací

Na organizaci a řízení bezpečnosti informací se podílejí všichni vedoucí zaměstnanci v rozsahu uvedeném v této směrnici a v ostatní bezpečnostní dokumentaci, včetně konkrétních práv a povinností. Tato směrnice byla vydána na podkladě Směrnice č. 03/2020 Řídící dokumentace k informační bezpečnosti ISMS.

1. Interní organizace

V souvislosti s cílem organizovat a řídit bezpečnost informací se vytváří řídící rámec pro zahájení a řízení implementace bezpečnosti informací v PV.

1.1 Závazek vedení směrem k bezpečnosti informací

Vedení PV stanovuje jasný směr a aktivně podporuje bezpečnost ICT v rámci celé organizace. Zároveň demonstruje svůj závazek a jednoznačně přiřazuje a vymezuje role v oblasti bezpečnosti informací. Závazek vedení je obsažen v dokumentech organizace – Politika ISMS a v Bezpečnostní politice IS, ve které je dále rozveden a konkretizován.

Závazek jasně stanovuje dlouhodobé cíle, vize a oblasti, kterých se bezpečnost informací v organizaci týká. V rámci procesu Plan-Do-Check-Act (Plánuj-Dělej-Kontroluj-Jednej) je závazek vedení pravidelně přezkoumáván, a to min. 1x ročně. Na základě tohoto přezkoumání dochází k jeho případné aktualizaci.

1.2 Koordinace bezpečnosti informací

Koordinace bezpečnosti informací je v PV zajištěna prostřednictvím zástupců různých útvarů s odpovídajícími rolemi a pracovním zařazením.

Hlavní důvody pro koordinaci bezpečnosti informací:

- zajištění všech aktivit týkajících se oblasti bezpečnosti informací tak, aby byly v souladu s Bezpečnostní politikou IS;
- bezpečnosti IS ve správě PV;
- určení toho, jakým způsobem bude naloženo se zjištěnými nesoulady;
- zajištění schválení specifických metodik a postupů v oblasti bezpečnosti informací (hodnocení rizik, systém bezpečnostní klasifikace, aj.);
- identifikace významných změn hrozeb a vystavení informací a prostředků pro zpracování informací vůči těmto hrozbám;
- vyhodnocení aplikovatelnosti bezpečnostních opatření a zajištění koordinace při jejich zavádění;
- zajištění podpory vzdělávání v oblasti bezpečnosti informací v rámci PV (školení, program zvyšování bezpečnostního povědomí, aj.);
- vyhodnocení informací získaných z procesů monitorování a přezkoumávání bezpečnostních incidentů, a doporučení vhodného způsobu reakce na identifikované bezpečnostní incidenty.

Koordinaci ISMS v rámci PV zajišťuje Bezpečnostní manažer.

1.3 Přidělení odpovědností v oblasti bezpečnosti informací

V rámci organizace a řízení bezpečnosti informací v PV jsou jednoznačně určeny práva a odpovědnosti v oblasti bezpečnosti informací. Práva a povinnosti pro jednotlivé odborné orgány a role v systému organizace a řízení bezpečnosti informací jsou uvedeny v této kapitole. Jsou plně v souladu s platnou Bezpečnostní politikou IS.

Komise pro rozvoj

Komise pro rozvoj PV je poradním orgánem představenstva PV.

Hlavní úkoly KPR jsou:

- zajišťovat rozvoj informačního systému;
- zajišťovat výstavbu, obnovu a provoz infrastruktury informačních a komunikačních technologií;

- řídit a koordinovat řízení bezpečnosti informací v rámci organizace;
- připravovat a řídit společnou strategii IS/ICT v PV;
- předkládat ke schválení představenstvu PV návrhy informační strategie a rozpočtu PV na IS/ICT.

Bezpečnostní manažer

Bezpečnostní manažer informačního systému PV (dále jen Bezpečnostní manažer) je role odborného vedoucího pracovníka pro informační bezpečnost, jehož hlavním úkolem je organizovat, řídit a zajišťovat odborné úkoly informační bezpečnosti. Bezpečnostního manažera jmenuje představenstvo PV. Bezpečnostní manažer plní v souvislosti s organizací a řízením bezpečnosti informací tyto hlavní úkoly:

- zajišťuje organizaci a výkon centrální správy informační bezpečnosti;
- zajišťuje jednotnou správu Bezpečnostní politiky IS PV a je jejím vlastníkem (garantem);
- řídí bezpečnost informací plánováním, organizováním, přidělováním pracovních úkolů a kontroluje informační zdroje PV;
- vede registr právních a jiných normativních požadavků, předpisů EU a standardů souvisejících s řízením bezpečnosti informací;
- zodpovídá za vytvoření metodických návodů a poskytování odborné pomoci vlastníkům informací;
- na základě podkladů vlastníků informací (určení informace – dle klasifikace) a ve spolupráci odborem právním, vypracovává návrhy dohod o ochraně důvěrných informací, včetně povinností zachovávat mlčenlivost;
- připravuje pro představenstvo PV Zprávu o stavu informační bezpečnosti PV a plnění Bezpečnostní politiky IS a návrhy na opatření;
- provádí výklad Bezpečnostní politiky IS a přijímá stanoviska, v nezbytných případech řeší výjimky z této politiky – o přijatých opatřeních bez zbytečného odkladu informuje představenstvo PV;
- seznamuje s Bezpečnostní politikou IS uživatele informačního systému, a to před přidělením přístupu k IS;
- navrhuje postupy, které přesně určují, za jakých podmínek a kým by měly být kontaktovány orgány veřejné správy (např. dozorčí orgány, hasiči, policie, aj.) a postupy včasného hlášení bezpečnostních incidentů v případech, kdy existuje podezření na porušení zákonů.
- posuzuje návrhy bezpečnostních politik a jejich změn, dalších vnitřních norem PV týkajících se informační bezpečnosti,
- koordinuje zavádění bezpečnostních opatření v rámci působnosti PV,

- vyhodnocuje plnění Bezpečnostní politiky IS PV a implementaci principů informační bezpečnosti v projektech informačních systémů a vnitřních normách,
- doporučuje určení vlastníků informací, informačních aktiv a stanovení jejich působnosti,
- předkládá a projednává Zprávu o stavu informační bezpečnosti PV a plnění Bezpečnostní politiky IS PV s návrhy na opatření v představenstvu PV.

Garanti informačních systémů

Garanti informačních systémů jsou vedoucí týmů, v jejichž působnosti je provozování jednotlivých informačních systémů.

Garanti plní v rámci PV úlohu správců informačních systémů a odpovídají za výměnu informací s jinými informačními systémy.

Garanti informačních systémů:

- odpovídají za správnost, využitelnost a ochranu informací v rámci své působnosti,
- odpovídají za stanovení požadavků na zajištění dostupnosti, důvěrnosti a integrity informací a za implementaci požadavků vyplývajících z právních, interních a jiných relevantních předpisů v oblasti jejich působnosti,
- odpovídají za realizaci postupů a splnění náležitostí procesů životního cyklu informačního systému,
- odpovídají za plnění všech platných standardů informačních systémů týkající se provozovaného nebo vyvíjeného informačního systému,
- stanovují procesy zpracování informací (informační činnosti), stanovují a formulují požadavky na vývoj informačního systému a jeho změny, na dokumentaci informačního systému a uživatelskou dokumentaci.

Výkonem svých práv a povinností mohou garanti pověřit vlastníky informací a další pracovníky.

Vlastníci informací

Vlastníci informací (informačních aktiv) jsou určení pracovníci organizačních útvarů PV.

Vlastníci informací:

- spravují konkrétní informační aktiva, vymezují pravidla manipulace s nimi, zejména pravidla pořizování informací, seznamování se s informacemi a jejich zveřejňování, provádění změn a likvidace informací; tato pravidla se promítají do definice rolí a z nich

vyplývajících přístupových práv uživatelů, do klasifikace informací a procesů zveřejňování informací,

- vedou přehled o výměně informací poskytovaných mimo informační systém jiným subjektům a informací přijatých ke zpracování v rámci příslušného informačního aktiva (včetně sdílení dat); součástí této evidence je spis obsahující seznam smluvních ujednání a jejich písemné vyhotovení, na jejichž základě PV poskytuje či přijímá tyto informace,
- podílejí se na specifikaci požadavků na vývoj informačního systému a jeho změny, vyjadřují se k uživatelské dokumentaci aplikačních systémů,
- uplatňují požadavky na dodatečná opatření k zajištění důvěrnosti informací dle klasifikace.

Za vytvoření metodických návodů a poskytování odborné pomoci vlastníkům informací odpovídá bezpečnostní manažer IS.

Auditoři informačních systémů

Auditor informačního systému (dále jen auditor) je role odborného pracovníka pro provádění kontroly bezpečnosti provozu systémů informačních a komunikačních technologií. Auditora určuje představenstvo PV.

Vedoucí zaměstnanci

Na výkonu činností k zajištění bezpečnosti informací, včetně bezpečnosti informačních systémů PV a na jejich kontrole se podílejí všechny organizační útvary PV. Vedoucí zaměstnanci všech stupňů v souvislosti s organizací a řízením bezpečnosti informací jsou povinni:

- zodpovídat za realizaci Bezpečnostní politiky IS v rámci své působnosti;
- prosazovat Bezpečnostní politiku IS;
- vést své podřízené k dodržování povinností vyplývajících z Bezpečnostní politiky IS PV a dalších interních přepisů majících vztah k řízení bezpečnosti informací, a kontrolovat plnění stanovených zásad v denní praxi.

Uživatelé informačního systému

Uživateli informačního systému PV se rozumí fyzické osoby, které mají právo v předem definovaném rozsahu používat informační systém PV, zejména pak využívat a pořizovat informace. Uživatelé informačního systému plní v souvislosti s organizací a řízením bezpečnosti informací tyto hlavní úkoly:

- seznamují se s Bezpečnostní politikou IS a jinou bezpečnostní dokumentací organizace;
- plní všechny požadavky specifikované v bezpečnostní dokumentaci a jiných předpisech (např. v pracovních náplních), včetně smluv.

Osoby s přidělenou odpovědností mohou jednotlivé činnosti v oblasti bezpečnosti delegovat. Nicméně v konečném důsledku zůstávají odpovědné a měly by být schopny zaručit, že jakékoliv delegované činnosti byly vykonány správně.

V registru informačních aktiv a registru IS/ICT, který vede Bezpečnostní manažer, jsou jasně specifikovány jednotlivé systémy, včetně jednotlivých jeho součástí - aktiv. Zároveň jsou zde vymezeny odpovědnosti uživatelů informačního systému za ochranu jednotlivých aktiv.

1.4 Schvalovací proces prostředků pro zpracování informací

V rámci organizace a řízení bezpečnosti informací se ustavuje a zavádí postup schvalování nových prostředků pro zpracování informací.

O koncepcích a plánech rozhoduje a zodpovídá za ně představenstvo PV.

Zodpovědnou rolí pro pořízení, aktualizaci provozních prostředků pro zpracování a jiné činnosti týkající se nižších úrovní tohoto procesu je představenstvo PV. To na základě vyjádření Komise pro rozvoj o účelnosti a použití nových zařízení pro zpracování informací tyto prostředky schvaluje, a to s přihlédnutím k zjištění, zda zavedením nového prostředku nebudou porušeny žádné relevantní bezpečnostní politiky a požadavky.

Zvláštní pozornost se věnuje použití soukromých prostředků pro zpracování informací (notebooků, domácích PC nebo jiných mobilních zařízení). Schválení těchto prostředků spadá do gesce představenstva PV, které na základě vyjádření Bezpečnostního manažera rozhodne o možnosti použití těchto prostředků.

1.5 Dohody o ochraně důvěrných informací

Dohody o ochraně důvěrných informací nebo o povinnosti zachovávat mlčenlivost slouží k ochraně informací organizace. Zavazují účastníky k odpovědnosti informace chránit, používat a zveřejňovat je pouze odpovědným a oprávněným způsobem.

Za tuto oblast nese odpovědnost Bezpečnostní manažer. Ve spolupráci s právní kanceláří vytváří a v pravidelných intervalech přezkoumává dohody obsahující požadavky na ochranu důvěrnosti nebo povinnost zachovávat mlčenlivost, reflektující potřeby organizace na ochranu informací.

Dohody o ochraně důvěrnosti nebo o povinnosti zachovávat mlčenlivost by měly zajistit požadavek na ochranu důvěrné informace s využitím zákonem vymahatelných prostředků a pokut v případě jejich nedodržení. Veškeré tyto dohody musí být v souladu s platnými zákony a předpisy. Při určení požadavků na dohody o ochraně důvěrnosti nebo povinnost zachovávat mlčenlivost je nutné vzít zejména v úvahu:

- identifikace/určení důvěrných informací, tedy informací, které mají být chráněny;
- očekávanou dobu trvání dohody a specifikace případů, ve kterých je požadavek na ochranu důvěrnosti uplatňován i po ukončení doby platnosti takové dohody;
- určení kroků následují po ukončení dohody;
- určení odpovědností a popis kroků, které účastníci dohody podniknou k zamezení neoprávněného vyzrazení informací;
- vlastnictví informací, obchodní tajemství a ochrana duševního vlastnictví a jejich souvislost s ochranou důvěrných informací;
- práva účastníků dohody na použití důvěrných informací;
- popis práv a auditu a přezkumu činnosti, které zahrnují důvěrné informace;
- způsob oznámení a podání zprávy o neoprávněném vyzrazení nebo porušení důvěrnosti informace;
- podmínky a způsoby vrácení či zničení informací po ukončení dohody o ochraně informací;
- kroky a případně sankce, které budou podniknuty v případě porušení dohody.

V závislosti na bezpečnostních potřebách účastníků mohou být dohody o ochraně důvěrných informací nebo povinnost zachovávat mlčenlivost doplněny o další potřebná ustanovení.

Veškeré požadavky obsažené v dohodách o ochraně důvěrných informací nebo o povinnosti zachovávat mlčenlivost budou v pravidelných intervalech, min. 1x ročně, a v případě jakýchkoliv dalších změn ovlivňujících tyto požadavky, přezkoumávány.

Dohody o ochraně důvěrných informací nebo o povinnosti zachovávat mlčenlivost mají vždy písemnou podobu. Bezpečnostní manažer vede evidenci těchto dohod.

1.6 Kontakt s orgány veřejné správy

V rámci organizace a řízení bezpečnosti informací se zavádí postupy, které přesně určují, za jakých podmínek, jakým způsobem a kým jsou kontaktovány orgány veřejné správy (policie, hasiči, dozorčí orgány, NÚKIB), a postupy včasného hlášení bezpečnostních incidentů v případech, kdy existuje podezření na porušení zákonů.

Bezpečnostní manažer či jím pověřený zaměstnanec (např. Vlastník informací) na základě interního oznámení či jím zjištěných skutečností souvisejících s ohrožením bezpečností informací, informuje dle typu incidentu patřičné orgány veřejné správy. O provedeném ohlášení bezodkladně informuje představenstvo PV.

Bezpečnostní manažer vypracovává a vede registr relevantních kontaktů na orgány veřejné správy, vede evidenci hlášení a spolupracuje s třetími stranami zajišťující internetové připojení nebo telekomunikačními operátory, a to pro případ podniknutí opatření nápravy v případě útoku z internetu. Není-li v ostatní bezpečnostní dokumentaci stanoveno jinak, zajišťuje kontakt s orgány veřejné správy.

2. Externí subjekty

V souvislosti s cílem zachovat bezpečnost informací a prostředků pro zpracování informací, které jsou přístupné, zpracovávané, sdělované nebo spravované externími subjekty, je nutné kontrolovat přístup těchto externích subjektů k prostředkům pro zpracování informací a informacím, a to z důvodu zamezení snížení bezpečnosti při zavedení produktů a služeb třetích stran.

Pro účely této směrnice se externími subjekty rozumí:

- subjekty, se kterými si PV vyměňuje informace (orgány veřejné správy, zákazníci, soukromé a další organizace);
- dodavatelé technologií a služeb pro informační systém;
- další subjekty, které zabezpečují služby pro organizaci.

Za správu a řízení rizik spojených s přístupem třetích stran k informačnímu systému a informacím zodpovídá PV a Vlastníci informací.

Proces výběru, kontrahování a řízení dodavatelů je upraven procesem Řízení vztahů s dodavateli v řídící dokumentací IT Řízení služeb (dle normy ISO 20000).

2.1 Identifikace rizik vyplývajících z přístupu externích subjektů

Vzhledem k tomu, že informace mohou být ohroženy přístupem třetích stran s neodpovídajícím řízením bezpečnosti, je nutné předtím, než je externím subjektům povolen přístup k informacím organizace a prostředkům pro zpracování informací, zajistit ze strany PV a Vlastníků informací

provedení hodnocení rizik tak, aby byly identifikovány požadavky na opatření. Na základě zjištění vyplývajících z hodnocení rizik se vyberou a následně implementují vhodná opatření na jejich pokrytí.

Při identifikaci rizik spojených s přístupem externích subjektů se zohledňuje následující:

- identifikace prostředků pro zpracování informací, ke kterým je potřebný přístup externích subjektů;
- typ přístupu, který bude mít externí subjekt k prostředkům pro zpracování informací, např. fyzický přístup, např. přístup do kanceláří, do místností s počítači, do kartoték, logický přístup, např. přístup k databázím organizace, do informačních systémů, typ síťového spojení mezi organizací a externím subjektem, např. trvalé spojení, vzdálený přístup, zda je přístup z prostor organizace anebo mimo ně;
- hodnota, citlivost a kritičnost příslušných informací pro organizaci;
- opatření nutná k ochraně informací, ke kterým nemají mít externí subjekty přístup;
- identifikace osob na straně externích subjektů, které budou mít přístup k informacím;
- způsob, jakým je identifikována organizace nebo osoby mající oprávnění k přístupu, jakým způsobem je toto oprávnění ověřeno a jak často znovu potvrzováno;
- postupy a opatření používané externími subjekty při ukládání, komunikaci, sdílení a výměně informací;
- jaký může mít dopad nedostupnost informací a prostředků pro zpracování informací externím subjektem. Dopad, jaký může mít zadání nebo obdržení nepřesných nebo klamných informací externím subjektem;
- směrnice a postupy pro řešení bezpečnostních incidentů a potenciálních poškození, podmínky a okolnosti, za jakých bude umožněn přístup externím subjektům v případě bezpečnostního incidentu;
- zákonné požadavky, požadavky předpisů a jiné smluvní požadavky ve vztahu k externím subjektům;
- vliv identifikovaných rizik na zájmy akcionářů, podílníků a ostatních zájmových skupin.

Do doby, než jsou implementována přiměřená bezpečnostní opatření a podepsána dohoda, ve které se vymezí podmínky síťového propojení nebo přístupu externích subjektů do prostor organizace a pracovní podmínky, se externím subjektům neumožní přístup k informacím a prostředkům pro zpracování informací. V dohodě s externími subjekty se zaváží k akceptaci odpovědnosti a povinnostem souvisejícím s přístupem k informacím PV, k jejich zpracování, sdílení a správě.

2.2 Bezpečnostní požadavky pro přístup klientů

Předtím, než je klientům umožněn přístup k informacím nebo aktivům organizace, by měly být identifikovány všechny požadavky pro zajištění bezpečnosti:

- ochrana aktiv, která zahrnuje postupy k ochraně aktiv PV včetně informací a programového vybavení a řízení známých zranitelností, postupy sloužící ke zjištění, zda nedošlo ke kompromitaci aktiv (ztrátě či modifikaci dat), integrity aktiv a k omezení kopírování a šíření informací;
- popis každé služby nebo produktu, které jsou třetí straně zpřístupněny;
- důvody, požadavky a výhody vyplývající z přístupu umožněného zákazníkům;
- politika řízení přístupu, která zahrnuje povolené metody přístupu, řízení a použití jedinečných identifikátorů, jako jsou uživatelské identifikátory a hesla, autorizační proces pro přístup uživatele a jeho oprávnění, prohlášení, že každý přístup, který není explicitně povolen, je zakázán, včetně procesu zrušení přístupových práv nebo přerušení spojení mezi systémy;
- systém hlášení, upozorňování a vyšetřování nepřesností informací (např. osobních údajů), bezpečnostních incidentů a případů prolomení bezpečnosti;
- popis každé služby, která je třetí straně zpřístupněna;
- cílová úroveň služby a neakceptovatelné úrovně služby;
- právo monitorovat a zakázat aktivity uživatele;
- konkrétní závazky a odpovědnosti na straně organizace a zákazníka;
- odpovědnosti vyplývající z právních norem, například z legislativy na ochranu osobních údajů, zvláště v případech uzavírání smluv mezi stranami z různých států je nutné vzít v úvahu národní požadavky zákonů a předpisů;
- ochrana duševního vlastnictví a autorské právo a ochrana jakékoliv týmové práce.

V závislosti na typu a rozsahu přístupu nemusí být všechny uvedené požadavky aplikované. Mohou být však rozšířeny o další, a to dle stávajícího stavu. Požadavky týkající se přístupu klientů jsou obsaženy v uzavřených dohodách se zákazníkem.

Tuto činnost týkající identifikace požadavků zajišťuje PV ve spolupráci s Vlastníky informací.

2.3 Bezpečnostní požadavky v dohodách se třetí stranou

Dohody uzavřené s třetími stranami, zahrnující přístup, zpracování, šíření nebo správu informací organizace nebo správu prostředků pro zpracování informací (případně dodávku produktů nebo služeb k zařízení pro zpracování informací), pokrývají veškeré relevantní

bezpečnostní požadavky. Z uzavřených dohod musí vyplývat, že mezi PV, jejími jednotlivými složkami a třetí stranou neexistuje nesoulad ve výkladu předmětu jejich plnění. Aby se předešlo zpoždění v dodávce služeb, musí být v dohodách uzavíraných se třetí stranou ošetřeny případy, kdy třetí strana není schopna dostát smluvním závazkům. Dohody uzavřené s třetími stranami mohou zahrnovat také další subjekty. Dohody, které umožňují přístup třetích stran, by měly zahrnovat formu, rozsah a podmínky, za jakých může být těmto subjektům povolen přístup. Dohody o poskytování služeb formou outsourcingu zpravidla připravuje PV. V ojedinělých případech, kdy jsou tyto dohody připraveny třetí stranou, je nezbytné zajistit, aby jí navrhované požadavky neměly dopad na bezpečnost PV.

Pro pokrytí všech identifikovaných požadavků na bezpečnost se do dohod zařazují zpravidla následující oblasti:

- politiky bezpečnosti informací;
- opatření pro zajištění ochrany aktiv, které zahrnují postupy sloužící k ochraně aktiv organizace včetně informací a programového a technického vybavení, jakákoliv opatření fyzické ochrany a mechanizmy, které zajišťují jejich plnění, opatření k zajištění ochrany před škodlivým programovým vybavením, postup sloužící ke zjištění, zda nedošlo ke kompromitaci aktiv, například ztrátě nebo modifikaci informací, programového a technického vybavení, opatření zajišťující vrácení či zničení informací/aktiv po ukončení smluvního vztahu nebo v jeho průběhu, důvěrnost, integritu, dostupnost a další důležité vlastnosti aktiv, omezení kopírování a šíření informací a dodržování dohod o ochraně důvěrných informací;
- školení uživatelů a správců v metodách, postupech a v bezpečnosti;
- zajištění dostatečného povědomí uživatelů o bezpečnosti informací a jejich odpovědnostech;
- tam, kde je to vhodné, podmínek přechodu zaměstnanců mezi smluvními stranami;
- politiky řízení přístupu, které zahrnují důvody, požadavky a výhody, které činí přístup třetích stran nezbytným, povolené metody přístupu, kontrola a použití jedinečných identifikátorů, jako jsou uživatelské identifikátory (ID) a hesla, povolené metody přístupu, autorizační proces pro přístup uživatele a jeho oprávnění, požadavky na vedení a dostupnost seznamu jednotlivců, kteří jsou vzhledem ke svým přednastaveným právům a privilegiím oprávněni využívat nabízené služby, prohlášení, že každý přístup, který není explicitně povolen je zakázán, proces zrušení přístupových práv nebo přerušení spojení mezi systémy;
- systému hlášení, upozorňování a vyšetřování bezpečnostních incidentů a případů narušení bezpečnosti, stejně tak jako porušení jakýchkoliv podmínek stanovených v dohodách;

- popisu každé služby, která je třetí straně zpřístupněna a popis každé zpřístupněné informace včetně bezpečnostní klasifikace;
- cílové úrovně služby a neakceptovatelné úrovně služby;
- popisu ověřitelných kritérií výkonnosti, způsob jejich sledování a hlášení;
- práva monitorovat a zakázat jakékoliv aktivity uživatele mající vztah k aktivům organizace;
- práva auditovat povinnosti stanovené v dohodách nebo mít právo nechat provést tyto audity třetí stranou a jmenovitě uvést legitimní práva auditorů;
- ustavení procesu eskalace při řešení problému;
- požadavků na kontinuitu služeb, včetně opatření pro zajištění dostupnosti a spolehlivosti, v souladu se stanovenými prioritami organizace;
- konkrétních závazků a odpovědnosti na straně organizace a zákazníka;
- odpovědnosti vyplývající z právních norem, například z legislativy na ochranu osobních údajů, zvláště v případech uzavírání smluv mezi stranami z různých států je nutné vzít v úvahu národní požadavky zákonů a předpisů;
- ochrany duševního vlastnictví a autorské právo, a ochrana jakékoliv společné práce;
- spolupráce třetích stran se subdodavateli a bezpečnostní opatření, která musí subdodavatelé přijmout;
- podmínek obnovení/ukončení dohod.

Tam, kde je to potřebné, mohou být požadavky na opatření a postupy podrobněji rozvedeny v plánu řízení bezpečnosti.

V rámci organizace a řízení bezpečnosti informací zajišťuje v souvislosti s požadavky v dohodách s třetími stranami veškeré činnosti PV ve spolupráci s Vlastníky informací.

Závěrečná ustanovení

Bezpečnostní manažer provádí výklad této směrnice a přijímá stanoviska v případě nejasností jednotlivých ustanovení – o přijatých závěrech informuje člena představenstva PV pověřeného řízením společnosti.

Změny těchto pravidel musí být řízeny ve shodě se směrnicí „Bezpečnostní dokumentace ISMS“ zejména v návaznosti na:

- pravidelnou (roční) prověrkou aktuálnosti,
- změnu české národní legislativy, předpisů a doporučení EU,
- změnu bezpečnostních politik PV,
- změnu v hodnocení rizik,
- nedostatky zjištěnými při kontrolní činnosti,
- bezpečnostní incident,

zdůvodněný návrh kterékoliv role v systému řízení bezpečnostní dokumentace.

Záznamy požadované směrnicí ISMS

Přehled požadovaných záznamů:

Název záznamu	Formulář číslo	Místo uložení záznamu	Doba archivace
Jmenovací dekrety		bezpečnostní manager	
Zápisy z jednání		bezpečnostní manager	

Související dokumentace

Realizace cíle kategorie bezpečnosti prostřednictvím jednotlivých opatření je pro zajištění přehlednosti upřesněno v těchto dokumentech:

1. **Příručky**

Název příručky	Místo uložení	Vlastník
Příručka pro uživatele IS	kancelář bezpečnostního manažera	bezpečnostní manažer
Příručka pro garanta IS		
Příručka pro bezp. manažera		

2. **Pracovní směrnice a postupy**

Název pracovního postupu	Místo uložení	Vlastník

3. **Formuláře**

Název formuláře	Místo uložení	Vlastník

4. **Podpůrné dokumenty**

Název dokumentu	Místo uložení	Vlastník
Politika ISMS	kancelář bezpečnostního manažera	bezpečnostní manažer
Bezpečnostní politika IS	kancelář bezpečnostního manažera	bezpečnostní manažer

Příloha č. 5

Vzor školení v oblasti informační bezpečnosti pro koncové uživatele

Školení v oblasti informační bezpečnosti pro koncové uživatele informačních systémů společnosti První výpočetní, a.s.

Verze 202003.1

1. Současná platná legislativa pro provoz IS/IT a informační bezpečnost v PV

- Směrnice PV S 01 - Základní bezpečnostní řád pro uživatele informačních systémů
- Směrnice PV S 02 – Bezpečnostní politika informačního systému PV
- Směrnice PV S 03 – Řídící dokumentace k informační bezpečnosti ISMS
- Směrnice PV S 04 – Zabezpečení kontinuity informačních systémů
- Směrnice PV S 05 – Pravidla pro bezpečnostní zóny v systému řízení bezpečnosti informací

2

2. Pravidla pro přístup k informačním systémům

- Počítače a data, která jsou na nich uložena (včetně dat na obrazovce), je třeba chránit před odcizením a před neoprávněným přístupem. K tomu je třeba zajistit následující nutná technická a organizační opatření.

2.1 Uživatelská jména a hesla

- Přístupová práva každého zaměstnance PV (uživatele informačních systémů) k informačním systémům musí být realizována uživatelským jménem a autentizačními prostředky, jako je heslo (příp. identifikační karta, klíče, tokeny apod.)
- S uživatelským jménem jsou spojena oprávnění aktivně nebo pasivně pracovat s určitými zdroji informačního systému – pořizovat, měnit nebo zjišťovat informace, využívat služby počítačové sítě, pracovat s pevným diskem (hard disk) a programovým vybavením počítače (software).
- **Anonymní přístup k informačnímu systému není povolen.**

3

2.2 Pravidla pro používání hesel

- Uživatel musí neprodleně nahradit přednastavené heslo osobním heslem.
- Uživatel je odpovědný za veškerou činnost, která se provádí pod jeho heslem, proto je v jeho vlastním zájmu, aby heslo nebylo vyzrazeno.
- Uživatel musí heslo chránit tak, aby se nedostalo do cizích rukou.
- Heslo musí být minimálně osmimístné a musí obsahovat písmena a číslice, případně i zvláštní znaky.
- Heslo nesmí být jednoduše odhadnutelné (nesmí být např. použito jméno uživatele)
- Heslo musí být obměňováno alespoň jednou za 90 dní.
- Heslo smí být změněno pouze jednou za pracovní den.
- Heslo nesmí být identické s posledními pěti používanými hesly.
- Heslo nesmí být uloženo na disku počítače ani zapsáno v papírové formě a uloženo na volně dostupném místě.
- Po pěti neúspěšných pokusech o přihlášení se přístup do počítače zablokuje.

4

2.3 Opuštění pracoviště

- Pokud uživatel opouští pracoviště, musí se ujistit, že žádná neoprávněná osoba nemůže používat jeho počítač. Toto lze realizovat např. vypnutím počítače, ukončením autorizace (ukončení aplikace, odhlášení se od zdrojů dat, odhlášení se ze systému), zablokováním obrazovky či klávesnice nebo uzamknutím místnosti.
- Uživatel může použít spořič obrazovky, který na základě ručního požadavku nebo po uplynutí nastavené doby neaktivity automaticky uzamkne obrazovku a klávesnici.

2.4 Obcházení přístupové ochrany

- Uživatel se nesmí pokoušet se o přístup k datům, k nimž nemá přístupová oprávnění. Uživatel rovněž nesmí používat jakékoli nástroje (např. programy pro zjišťování hesel), s nimiž by bylo možné obejít přístupovou ochranu.

5

2.5 Zaměstnanci opouštějící společnost PV, a zaměstnanci, u kterých dochází ke změně pracovního zařazení

- V případě odchodu zaměstnance z PV, musí být vymazána všechna jeho přístupová oprávnění.
- Nadřízený pracovník je povinen prostřednictvím aplikace ServisDesk neprodleně požádat o zrušení všech přístupových oprávnění . ServisDesk jej bude zpětně informovat o zrušení přístupových oprávnění s uvedením data a přesného času.
- Nadřízený odcházejícího zaměstnance je povinen zajistit, aby byl před vymazáním přístupových oprávnění zajištěn převod přístupových oprávnění na nového zaměstnance.

6

3. Personální a organizační bezpečnostní opatření - zabezpečení dat

- K zajištění ochrany firemních dat musí uživatelé svá data zálohovat, tj. ukládat je mimo produktivní verzi (data jsou zpravidla uložena na pevném disku počítače) i na centrální datové úložiště, na kterém se zajišťuje jejich pravidelné zálohování.
- Ve výjimečných a odůvodněných případech může uživatel zálohovat data lokálně na přenosných nosičích dat (např. na DVD, Flashdisk atd.). Takto zálohovaná data musí být chráněna před neoprávněným přístupem. Data uložena na mobilních nosičích dat se musí ukládat na uzamčeném místě (např. uzamčený psací stůl nebo trezor).

7

4. Bezpečnostní opatření – notebook

- Ztráta či odcizení přenosného počítače znamená jak ztrátu investičního majetku, tak i ztrátu informací.
- K zamezení odcizení přenosných počítačů v prostorech, které jsou obecně přístupné,
  je uživatel povinen přenosné počítače zabezpečit před odchodem z pracoviště jejich umístěním do uzamykatelných prostorů (psací stůl, skříň, trezor apod.).
- Pokud je uživatel s přenosným počítačem na cestách, musí mít svůj přenosný počítač neustále pod kontrolou. Uživatel nesmí nechat přenosný počítač volně ležet v automobilu či na hotelovém pokoji. Rovněž uživatel nesmí přenechávat přenosný počítač hotelovému personálu a odevzdávat jej jako zavazadlo v letadle. V případě,
  že přenosný počítač musí zůstat v hotelu, je uživatel povinen umístit přenosný počítač do hotelového trezoru/sejfu.

8

5. Ochrana před škodícími programy (viry)

- Počítačové viry jsou díky své škodící funkci neustále vážným ohrožením pro všechny informace uložené v počítači. Viry mohou mimo jiné pozměnit, zlikvidovat data nebo je zaslat neoprávněným osobám. K přenosu virů dochází jak prostřednictvím datových nosičů, tak prostřednictvím elektronické pošty (e-mailů) nebo přenosem souborů přes datové sítě.
- K nákaze viry může například dojít při načítání programů nebo dokumentů uložených v přílohách e-mailů, z Internetu či z jiných míst mimo společnost PV. Viry se mohou nacházet nejen v kopírovaných programech a dalších spustitelných souborech, ale také v textových souborech, kalkulačních tabulkách (tzv. makroviry) a dalších souborech. Spuštění nakaženého programu nebo otevření nakaženého souboru má obvykle za následek reprodukci viru a zahájení jeho škodící funkce.
- Permanentní prevence proti škodícím programům je nezbytná. Z tohoto důvodu jsou na počítačích nainstalovány antivirové programy, které všechny data při přístupu automaticky kontrolují na přítomnost virů. Z tohoto důvodu **je přísně zakázáno měnit konfiguraci antivirového programu**.

9

5. Ochrana před škodícími programy (viry) - pokračování

- Antivirový program na počítači může uživatel kdykoli manuálně spustit a prověřit tak pevné disky a paměť svého počítače. Při manuálním spuštění se nesmí průběh antivirového programu předčasně přerušit.
- Za žádných okolností nesmí uživatel spouštět soubory, které který byly zaslány e-mailem a mají příponu .exe, .com, .bat, .cmd, .scr, .vbx.
- Používaný software MS Office je nakonfigurován tak, aby makroviry, které by mohly být obsaženy v dokumentech Office, nemohly být při otevření dokumentu automaticky spuštěny. Tato přednastavení nesmí uživatel, z důvodu ochrany dat před makroviry, měnit.
- Každý výskyt škodícího programu či podezření na jeho výskyt musí uživatel okamžitě nahlásit na ServisDesk. Pokud má uživatel dojem, že došlo k virové nákaze jeho počítače, nesmí počítač dále provozovat, dokud nedojde k prověření počítače odbornými pracovníky ServisDesku.

10

6. Užívání počítačového vybavení

- V počítačové síti PV je povoleno používat pouze schválené a řádně licencované standardní a aplikační počítačové programy.
- **Uživatel nesmí:**
  - samostatně instalovat jakékoliv počítačové programy,
  - používat jakékoliv neoprávněné kopie licencovaných programů,
  - stahovat jakékoliv počítačové programy (update, patche a nové verze programů), výjimku z tohoto nařízení mají prohlížeče na prohlížení dat, které se dodávají jako součást počítačových programů.
- Veškeré požadavky na změnu programového vybavení počítače, schválené vedoucím musí uživatel zadat na ServisDesk.

11

7. Vzdálené připojení počítačů do počítačové sítě společnosti PV, a.s.

- Vzdálené připojení do počítačové sítě PV, (zpravidla přes veřejnou síť) představuje značné riziko pro případný průnik do systému. Proto musí být zabezpečeno dalšími prostředky.
- V současnosti je přístup do počítačové sítě realizován systémy SSL VPN a je chráněn certifikátem a heslem.
- Uživatel nesmí za žádných okolností nedovoleným jednáním přispět k tomu, aby se otevřela vnitrofiremní síť pro nežádané přístupy zvenčí.

12

8. Přístup k Internetu a jiným externím datovým sítím

- Internetové stránky mohou obsahovat programové prvky (ActiveX, moduly Java atd.), které mohou být aktivovány již při zobrazení této stránky na počítači. Tyto programové prvky jsou schopny informace číst, posílat, vymazávat a měnit. Stejně tak mohou zanechat v systému počítače i škodící programy.
- Pro přístup na Internet smí uživatel využívat pouze přístupové cesty, které poskytuje PV a které jsou zajištěny odpovídajícími ochrannými prvky (Firewall apod.).
- Za žádných okolností nesmí uživatel nedovoleným jednáním přispět k tomu, aby se otevřela vnitrofiremní síť pro nežádané přístupy zvenčí.

13

9. Bezpečnostní opatření při používání e-mailu

- Uživatel nesmí zřizovat žádné automatické přeposílání příchozí elektronické pošty do veřejné sítě.
- Uživatel je povinen dodržovat všechny směrnice PV, které se týkají firemních informací a jejich rozesílání přes Internet nebo ostatní veřejné sítě.
- Při práci s přílohami e-mailů je uživatel povinen postupovat dle pokynů uvedených v kapitole Ochrana před škodícími programy.

14

10. Ostatní pravidla

Data vztahující se k osobám

- Ochranu osobních údajů o fyzických osobách, práva a povinnosti při zpracování těchto údajů a podmínky, za nichž se uskutečňuje jejich předávání do jiných států upravuje Zákon o ochraně osobních údajů číslo 110/2019 Sb. v platném znění. Dle tohoto zákona se evidují tzv. registrované databáze, obsahující osobní údaje. V ostatních zemích platí odpovídající národní zákony.
- Uživatelé jsou povinni dbát na dodržování tohoto zákona a dalších směrnic PV o ochraně dat.

15

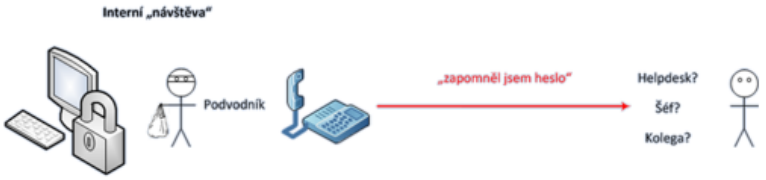
11. Šifrování

- Data, na která jsou vysoké nároky na poskytování důvěrnosti a integrity, musí být chráněna na základě zvláštních opatření (fyzická přístupová ochrana nebo kryptografické způsoby). Cílem je, aby žádná neoprávněná osoba nemohla tato data číst či s nimi manipulovat.
- Použitím kryptografie (šifrování) na jasně čitelném textu (čistý text, čitelná data) se tento text změní na posloupnost znaků, která zanechává dojem nesmyslnosti. Takto zašifrovaná data jsou pro neoprávněné osoby nečitelná a tedy bezcenná. Na zašifrovaných datech nelze provést cílené manipulace, neboť tyto manipulace vedou ke zničení dat a k odhalení pokusu o zneužití.
- Působnost ochrany zašifrováním je závislá na utajení používaného klíče.
- Uživatel musí zajistit bezpečné uložení přidělených tajných klíčů pro zašifrování dat a zpráv, aby se nedostaly do nesprávných rukou.

16

12. Typy počítačových útoků

12.1 Sociální inženýrství



- Tento typ útoku spočívá v tom, že útočník se vydává za někoho jiného a snaží se oklamáním oběti (ServisDesk, HeplDesk, kolega atd.) získat přístupy (uživatelské jméno a heslo) například do zamknutého počítače, ze kterého by následně mohl odcizit důvěrné firemní informace nebo někoho/něco poškodit.
- Útok může být proveden jak fyzicky na místě, tak i vzdáleně pomocí telefonu, e-mailu nebo pošty.

17

12.2 Instalace škodlivého kódu (malware) kvůli ukradení dat

- Každá aplikace může obsahovat ať už úmyslně nebo jen chybou autora část schopnou vykonávat nežádoucí činnosti. Například může pomocí ní útočník získat přístup k datům, ke kterým by jinak měl přístup pouze oprávněný uživatel.
- Malware je jakýkoliv škodlivý kód – vir, trojský kůň, spyware atd., který je určen pro vniknutí nebo poškození počítačového systému.
- Takto nakažený počítač potom může bez vědomí oprávněného uživatele „krást“ pod jeho uživatelskými oprávněními data z počítače a odesílat je podvodnému autorovi – útočníkovi. Útočník na základě takto získaných informacím může způsobit škody velmi velkého rozsahu.

18

12.3 SPAM - snaha o podvod nebo nabízení výrobku

SPAM je velmi jednoduše proveditelný způsob útoku na uživatele. Útok spočívá v poslání e-mailové zprávy se lživou informací. Na příkladu se spamová zpráva vydává za regulérní informativní e-mail z banky, ve kterém je uvedeno, že vám byl vytvořen nový přístup na stránky internetového bankovnictví s možností přístupu rovnou přes odkaz v e-mailu. V tomto případě se otevře stránka, která bude vypadat úplně stejně jako stránka internetového bankovnictví vaší banky, jen s tím rozdílem, že bude falešná. Pokud na takovéto stránce vyplníte vaše přihlašovací údaje a potvrdíte je, budou vaše údaje odeslány útočníkovi. Ten je pak může použít pro přístup do vašeho pravého internetového bankovnictví a tam provádět činnosti od poslání vašich peněz na jiný účet až po sjednání úvěru na vaši osobu atd.

19

12.4 Cloudové služby

- Cloudové služby lze charakterizovat jako poskytování služeb či programů uložených na serverech na Internetu s tím, že uživatelé k nim mohou přistupovat pomocí webového prohlížeče a používat je prakticky odkudkoliv.
- Největším rizikem cloudových služeb je, že uživatel nahraná data do cloudu nemá nikdy pod kontrolou, nemá jistotu, že se k datům nedostane nikdo jiný, ať už za účelem odcizení nebo pozměnění atd. Z těchto důvodu je třeba vždy zvážit, jestli důležitost ukládaných dat odpovídá možným rizikům použité služby, případně smluvním ujednáním.

20

12.5 Cloudové služby (pokračování)

Před použitím cloudových služeb je třeba si položit několik otázek:

- co se stane, když o uložená data v cloudové službě přijdu?
- co se stane, když se k uloženým datům dostane někdo neoprávněný a obsažené informace zveřejní nebo předá konkurenci?
- co se stane, když mi někdo uložená data pozmění (například změna částky ve smlouvě atd.)?
- Pokud je vaše reakce na kteroukoliv z otázek negativní nebo vede k obavám, potom data do cloudové služby za žádnou cenu nenahrávejte.
- Cloudové služby jsou například DropBox, MegaUpload, Ulozto atd., které jsou nabízeny zdarma nebo za úplatu.

21

12.6 Sociální sítě - ztráta majetku nebo sexuální zneužití

- Nejvíce útoků tohoto typu v současné době zaznamenávají uživatelé sociálních sítí (Facebook, Twitter, Linkedin atd.), kteří práci útočníkům maximálně usnadňují tím, že o sobě do světa „vykřičí“ téměř všechno.
- Pokud má potenciální zloděj možnost přečíst si, že rodina bude příští týden na dovolené a že dům po tuto dobu bude zcela prázdný, zvlášť když jsou komukoliv dostupné vaše kontakty, jako je adresa, pevná linka domů atd., je to pro zloděje dost silný motiv jít se k vám ve vaší nepřítomnosti podívat a odnést si vše, co se dá zpeněžit.

- Na základě vámi umístěných informací může dojít i k sexuálnímu zneužití, což se týká zejména dětí.

22

12.7 Sociální sítě ztráta majetku nebo sexuální zneužití (pokračování)

- Ochrana je v podstatě velmi jednoduchá. Nikdy o sobě na sociálních sítích neuvádějte informace, které může někdo jiný použít ve váš neprospěch.
- Pochlubte se s vaší dovolenou teprve, až když se z ní vrátíte.
- V žádném případě neuvádějte svoje kontakty (adresu, telefon) nebo jejich zobrazení omezte pouze na nejbližší známé. Jen tak budete mít jistotu, že vaše příspěvky nebudou použity proti vám.

23

12.8 Získání osobních dat – phishing

- Když přistupujete na zabezpečenou stránku (označení https), typicky například na internetové bankovnictví, vždy si raději zkontrolujte, že jste na té správné, nikoliv na falešné, útočníkem podstrčené stránce. Útočník se pokouší získat vaše přihlašovací údaje, aby je mohl zneužít ve svůj prospěch – viz. kapitola 12.3 SPAM.
- Jako první proveďte kontrolu **url adresy**. V adrese nesmí být zaměněno žádné písmenko, přidáno žádné znaménko atd. Útočník využívá maličkostí a doufá ve vaší nepozornost, takže se můžete setkat například s url adresou vypadající například takto:

  https://www.service24.cz

  https://www.servis2A.cz

  https://www.servis24.com

24

12.9 Získání osobních dat - phishing (pokračování)

- Jako druhou věc proveďte kontrolu certifikátu, kterým je šifrovaná stránka internetového bankovnictví podepsána. To provedete rozkliknutím zámečku v adresním řádku. Zde je vidět, že certifikát byl vydán certifikační autoritou VeriSign a byla vydána např. pro Českou spořitelnu a.s.
- Pro kontrolu, že je vše v naprostém pořádku, ještě rozklikněte volbu „Zobrazit Certifikáty“. Zobrazí se vám informační okno, kde jsou důležité tři údaje: **Vystaveno pro**, **Vystavitel** a **Platnost od do**.
- Pokud **Vystaveno pro** odpovídá přesně **www.servis24.cz**, pak je to v pořádku.
- Pokud je **Vystavitel** důvěryhodná certifikační autorita (seznam všech důvěryhodných certifikačních autorit je možné nalézt na Internetu) pak je to také v pořádku.

25

12.10 Získání osobních dat - phishing (pokračování)

- Pokud je aktuální datum v intervalu uvedeném v **Platnost od do** pak je to také v pořádku.
- Pokud je ale jakákoliv hodnota uvedena chybně, za žádnou cenu nepokračujte v přihlašování, riskujete tím, že vaše přihlašovací údaje budou zneužity.
- V případě takovéhoto zjištění doporučujeme kontaktovat banku se žádostí o prověření.

26

13. Klasifikace informací

13.1 Klasifikace informací

- Bezpečnostní politikou IS PV je zavedena klasifikace informací z hlediska důvěrnosti, která vyjadřuje míru zájmu a povinnosti na zachování důvěrnosti informací.
- PV respektuje právo zachování důvěrnosti a klasifikaci svěřených informací, které patří jiným subjektům.
- Klasifikace, označování, postupy zpracování a životní cyklus informací jsou popsány ve Směrnici pro klasifikaci a způsob zpracování informací.
- Vázané informace a Zvláštní skutečnosti odpovídají klasifikaci EU – LIMITED.
- Informační systém, respektive subsystém musí podléhat takové ochraně informací, která odpovídá nejvyššímu stupni klasifikace informací v něm zpracovávaných.

27

13.1.1 Neklasifikované informace

- Jako neklasifikované informace jsou označeny takové informace, u nichž není potřebné zajistit dostupnost, důvěrnost ani integritu.

13.1.2 Klasifikované informace

- Jako klasifikované informace jsou souhrnně označeny ostatní skupiny informací, u nichž je nutné zabezpečit alespoň jeden z atributů: dostupnost, důvěrnost a integritu.
- Informace klasifikované představují omezený okruh informací důvěrných z hlediska ochrany osobnosti a soukromí (osobní údaje), obchodního tajemství, důvěrnosti majetkových poměrů, krizového plánování (zvláštní skutečnosti), státní statistické služby, duševního vlastnictví, některých vnitřních pokynů a předpisů a informací vznikajících při přípravě rozhodnutí organizačních útvarů nebo v rámci správních činností.“

28

- Na klasifikované informace s výjimkou Veřejně přístupných informací se vztahuje omezení práva na informace a jsou důvěrné v rozsahu a po dobu stanovenou příslušnými právními předpisy. Přístup k těmto informacím je řízen podle zásady „potřeba vědět“. V souhrnu se těmto informacím obecně říká citlivé.

13.1.2.1 Veřejně přístupné informace

- Jedná se o veřejně přístupné informace ve smyslu ustanovení zákona č. 106/1999 Sb. v současném znění o svobodném přístupu k informacím.
- Informace klasifikované jako „veřejné informace“ představují široký okruh informací k zajištění činností PV, u kterých není požadováno dodržení důvěrnosti.
- Zveřejňování informací je řízený proces, který v souladu s právními předpisy a vnitřními normami představuje závazné postupy poskytování informací.

29

13.1.2.2 Provozní informace

- Provozní informace jsou informace vyskytující se v informačním systému, spojené s provozem informačního systému, předmětem činnosti nebo s provozovatelem / správcem informačního systému. Přístup k informacím je vázán na splnění specifických podmínek, aby nebyla ohrožena nebo omezena činnost informačního systému, nebo zájmy provozovatele / správce.

30

13.1.2.3 Vázané informace

- Vázané informace jsou takové informace, ke kterým je v souladu s ustanoveními právních předpisů a kategorizačních atributů regulovaný (vázaný) přístup.
- Např.: Informace o osobních údajích; Individuální údaje pro statistické účely; Informace označené jako obchodní tajemství; Informace podléhající mlčenlivosti při daňovém řízení; Informace které se neposkytují, atd.

13.1.2.4 Zvláštní skutečnosti

- Zvláštními skutečnostmi jsou informace z oblasti krizového řízení, které by v případě ztráty, poškození nebo zneužití mohly vést k ohrožení základních funkcí státu.
- Tato skupina vychází ze zákona č. 240/2000 Sb. a vyhlášky č. 462/2000 Sb.

31

Dotazy a diskuze

32

Příloha č. 6

Vzor závěrečného testu po absolvování školení

Závěrečný test školení v oblasti informační bezpečnosti pro zaměstnance společnosti První výpočetní, a.s.

Jméno: _____

Osobní číslo: _____

Datum: _____

Číslo testu: _____

Správnou odpověď označte křížkem

Otázka:				Otázka:			
1	A	B	C	6	A	B	C
2	A	B	C	7	A	B	C
3	A	B	C	8	A	B	C
4	A	B	C	9	A	B	C
5	A	B	C	10	A	B	C

Správných odpovědí: ☐

Potvrzuji, že zaměstnanec byl proškolen v oblasti informační bezpečnosti a úspěšně absolvoval závěrečný test.

Jméno a podpis školitele: _____

Datum: _____

Příloha č. 7

Vzor formuláře „Prezenční listina účastníků školení“

Prezenční listina účastníků školení

Název školení: _____

Datum: _____

Jméno školitele: _____

	Příjmení	Jméno	Osobní číslo	Podpis
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				