Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

I .Bezpečnostná politika IS, organizačná a personálna bezpečnosť
II. Bezpečnostný projekt IS

Ivan Kopáčik

Máj 2013

KPMG
cutting through complexity™

Agenda I.

1. Východiská bezpečnostnej politiky
2. Praktický obsah bezpečnostnej politiky
3. Personálna bezpečnosť vo vzťahu k IS

Politika informačnej bezpečnosti - východiská

- Výnos Ministerstva financií Slovenskej republiky č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy (ďalej len „Výnos“)

- Norma ISO/IEC 27002 Pravidlá dobrej praxe manažérstva informačnej bezpečnosti

Výnos §28 písm. a)

Bezpečnostná politika musí obsahovať:

1. Určenie bezpečnostných cieľov povinnej osoby z hľadiska informačnej bezpečnosti.
2. Určenie spôsobov vyhodnocovania bezpečnostných cieľov, kritérií vyhodnocovania ich dosahovania, spôsobov priebežného hodnotenia ich adekvátnosti a spôsobov kontroly postupov využívaných na ich dosahovanie.
3. Určenie úlohy vedenia povinnej osoby pri zaisťovaní informačnej bezpečnosti a uvedenie vyhlásenia vedenia povinnej osoby o podpore bezpečnostnej politiky povinnej osoby.

Výnos §28 písm. a)

4. Určenie všeobecných a špecifických zodpovedností a povinností v oblasti informačnej bezpečnosti a stanovenie potrebných pozícií pre manažment informačnej bezpečnosti.
5. Určenie povinnosti za zaručenie nenarušenia informačnej bezpečnosti povinnej osoby.
6. Zhodnotenie súladu bezpečnostnej politiky povinnej osoby so všeobecne záväznými právnymi predpismi, vnútornými predpismi povinnej osoby a jej zmluvnými záväzkami.
7. Určenie požiadaviek na informačné systémy verejnej správy, vyplývajúcich zo všeobecne záväzných právnych predpisov, vnútorných predpisov povinnej osoby a jej zmluvných záväzkov, a určenie spôsobu vedenia a aktualizácie dokumentácie o informačných systémoch verejnej správy.

Výnos §28 písm. a)

8. Určenie rozsahu a úrovne ochrany všetkých informačných systémov verejnej správy vrátane hodnotenia slabých miest a ohrození.
9. Určenie rámca pre manažment rizík u povinnej osoby v súvislosti s aktívami, od ktorých závisí činnosť informačných systémov verejnej správy alebo ktoré závisia od činnosti informačných systémov verejnej správy; rámec najmä určí, ktoré aktíva sú pre povinnú osobu kritické, čo ich ohrozuje, a zásady ich ochrany,
10. Určenie rozsahu a periodicity auditu informačnej bezpečnosti u povinnej osoby a zároveň určenie udalosti v informačných systémoch verejnej správy, o ktorých sa vytvára záznam auditu.
11. Určenie operačných smerníc na zálohovanie a určenie, ktoré skupiny údajov, v akom rozsahu, akým spôsobom a s akou periodicitou sa zálohujú v prevádzkovej zálohe a archivačnej zálohe.

Výnos §28 písm. a)

12. Určenie periodicity monitorovania bezpečnosti a aktualizácie softvéru.
13. Určenie dokumentov, ktoré povinná osoba na zaistenie informačnej bezpečnosti vypracuje a uvedie ich zoznam.
14. určenie postupu pri revízii bezpečnostnej politiky povinnej osoby vrátane periodicity pravidelných revízií a dôvodov mimoriadnych revízií bezpečnostnej politiky povinnej osoby.

Súvisiaca bezpečnostná dokumentácia

Bezpečnostná politika je vrcholový, strategický a kompetenčný dokument („zákon“).

Bezpečnostná politika sa rozpracúva a konkretizuje v interných štandardoch a aktoch riadenia („vykonávacie predpisy“).

Výnos §29 písm. f)

Štandardom pre personálnu bezpečnosť je vypracovanie postupu pri ukončení pracovného pomeru vlastného zamestnanca a pri ukončení spolupráce s externým pracovníkom alebo treťou stranou.

Výnos §30 písm. f)

Štandardom pre manažment rizík pre oblasť informačnej bezpečnosti je vypracovanie plánov na obnovu činnosti nefunkčných, poškodených alebo zničených kritických informačných systémov verejnej správy.

Výnos §33 písm. b), c)

Štandardom pre sieťovú bezpečnosť je:

1. vedenie evidencie o všetkých miestach prepojenia sietí v správe povinnej osoby vrátane prepojení s externými sieťami. (písm. b))
2. zabezpečenie, aby pre každé prepojenie podľa písm. b) bol vypracovaný interný akt riadenia prístupu medzi týmito sieťami podľa §40 riadenie prístupu. (písm. c))

Výnos §34 písm. d)

Štandardom pre fyzickú bezpečnosť a bezpečnosť prostredia je vypracovanie a implementácia pravidiel na prácu v zabezpečenom priestore.

Výnos §34 písm. h)

Štandardom pre fyzickú bezpečnosť a bezpečnosť prostredia je vypracovanie, zavedenie a kontrola dodržiavania pravidiel na:

1. údržbu, uchovávanie a evidenciu technických komponentov informačného systému verejnej správy a zariadení informačného systému verejnej správy,
2. používanie zariadení informačného systému verejnej správy na iné účely, na aké boli pôvodne určené,
3. používanie zariadení informačného systému verejnej správy mimo určených priestorov,
4. vymazávanie, vyraďovanie a likvidovanie zariadení informačného systému verejnej správy a všetkých typov relevantných záloh,
5. prenos technických komponentov informačného systému verejnej správy alebo zariadení informačného systému verejnej správy mimo priestorov povinnej osoby,
6. narábanie s elektronickými dokumentmi, dokumentáciou systému, pamäťovými médiami, vstupnými a výstupnými údajmi informačného systému verejnej správy tak, aby sa zabránilo ich neoprávnenému zverejneniu, odstráneniu, poškodeniu alebo modifikácii.

Výnos §36 písm. a)

Štandardom pre monitorovanie a manažment bezpečnostných incidentov je vypracovanie interného aktu obsahujúceho:

1. postup pri ohlasovaní bezpečnostných incidentov a odhalených slabých miest informačných systémov verejnej správy, najmä na účel včasného prijatia preventívnych a nápravných opatrení,
2. postup pri riešení jednotlivých typov bezpečnostných incidentov a spôsob ich vyhodnocovania,
3. spôsob evidencie bezpečnostných incidentov a použitých riešení.

Výnos §40 písm. b), j)

Štandardom pre riadenie prístupu je:

a) vypracovanie interného aktu riadenia prístupu k údajom a funkciám informačného systému verejnej správy založeného na zásade, že používateľ má prístup iba k tým údajom a funkciám, ktoré sú potrebné na vykonávanie jeho úloh. (písm. b))

b) vedenie formalizovanej dokumentácie prístupových práv všetkých používateľov informačného systému verejnej správy. (písm. j))

Výnos §41 písm. e)

Štandardom pre aktualizáciu informačno-komunikačných technológií je uchovávanie a aktualizácia dokumentácie o informačných systémoch verejnej správy alebo ich častiach, ktorá obsahuje:

1. používateľskú dokumentáciu, ktorou je návod na používanie informačného systému verejnej správy,
2. administrátorskú dokumentáciu, ktorou je návod na správu a prevádzku informačného systému verejnej správy,
3. prevádzkovú dokumentáciu, ktorou je dokumentácia o architektúre informačného systému verejnej správy alebo jeho časti, jeho konfigurácii a väzbách na existujúce informačné systémy verejnej správy.

ISO/IEC 27002

Hlavným cieľom je poskytnúť usmernenie pre riadenie a podporu informačnej bezpečnosti v súlade s požiadavkami / potrebami organizácie a relevantnými zákonmi a nariadeniami.

„Manažment by mal prostredníctvom vydania a udržiavania politiky informačnej bezpečnosti v rámci organizácie určiť jasný smer politiky v súlade so svojimi cieľmi a demonštrovať svoju podporu a angažovanosť z hľadiska informačnej bezpečnosti.“

ISO/IEC 27002

Dokument bezpečnostnej politiky by mal byť schválený manažmentom, vydaný a oznámený všetkým zamestnancom, ako aj relevantným externým partnerom.

Dokument politiky by mal obsahovať:

a) definíciu informačnej bezpečnosti, jej celkové ciele, účel a dôležitosť bezpečnosti ako mechanizmu umožňujúceho spoločné používanie informácií,

b) vyhlásenie zámerov manažmentu, podpory cieľov a princípov informačnej bezpečnosti v súlade so stratégiou organizácie a cieľmi,

c) rámec na nastavenie cieľov riadenia a opatrení, vrátane štruktúry preskúmavania rizík a riadenia rizík,

ISO/IEC 27002

d) stručné vysvetlenie bezpečnostných politík, princípov, štandardov a zhody s požiadavkami, dodržiavanie, ktorých má pre organizáciu zvláštnu dôležitosť, napr.:

1. dodržiavanie legislatívnych, regulačných a zmluvných požiadaviek,
2. požiadavky na bezpečnostné vzdelávanie, zácvik a budovanie bezpečnostného povedomia,
3. riadenie kontinuity činnosti organizácie,
4. následky porušení bezpečnostnej politiky.

e) definíciu všeobecných a špecifických zodpovedností z hľadiska manažmentu informačnej bezpečnosti, vrátane ohlasovania bezpečnostných incidentov,

ISO/IEC 27002

f) odkazy na dokumentáciu, podporujúcu danú politiku, napr. detailnejšie bezpečnostné pravidlá a postupy pre špecifické informačné systémy alebo bezpečnostné pravidlá, ktoré by mali používatelia dodržiavať.

S bezpečnostnou politikou by mali byť oboznámení používatelia v rámci celej organizácie, a to formou, ktorá je dostupná a pochopiteľná pre očakávaného čitateľa.

Toľko teória....a teraz prax

Bezpečnostná politika IS v praxi

Úprava zásad, kompetencií, zodpovedností, povinností a opatrení na implementáciu a využívanie bezpečnostnej politiky.

Rozsah: bezpečnostná politika sa vzťahuje na všetky aktíva tvoriace informačný systém organizácie vrátane všetkých aplikácií, dát, elektronických služieb a komunikačnej infraštruktúry.

Typické bezpečnostné ciele organizácie štátnej správy

Dodržiavanie všeobecne záväzných právnych predpisov a požiadaviek relevantných pre oblasť informačnej bezpečnosti.

Minimalizácia finančných a iných strát súvisiacich s narušením prevádzky informačného systému organizácie.

Vytvorenie a prevádzkovanie dôveryhodných a spoľahlivých informačných systémov pre zamestnancov organizácie.

Minimalizácia rizík ohrozenia aktív informačného systému.

Zaistenie poskytovania služieb informačného systému užívateľom informačného systému v stanovenej kvalite a rozsahu aj pri neštandardných (havarijných) stavoch informačného systému.

Ochrana dobrého mena organizácie.

Spôsoby dosahovania bezpečnostných cieľov – typické princípy

Na ochranu informácií sa vytvoria zodpovedajúce technické a organizačné predpoklady, ktoré sa skonkretizujú v záväzných dokumentoch nadväzujúcich na bezpečnostnú politiku, v bezpečnostných projektoch pre jednotlivé IS a ďalších interných predpisoch organizácie.

Informácie uložené a spravované v informačnom systéme je dovolené spracúvať iba prostredníctvom aplikačného programového vybavenia, ktoré zodpovedá platným štandardom používaným v organizácii.

Pre všetky informačné systémy, ktoré zabezpečujú kontinuálnu činnosť organizácie, sa vypracujú a priebežne aktualizujú havarijné plány.

Účinnosť bezpečnostných opatrení slúžiacich k ochrane informačného systému sa pravidelne kontroluje a vyhodnocuje.

Spôsoby dosahovania bezpečnostných cieľov typické princípy II.

Implementácia nových a rozvoj existujúcich bezpečnostných opatrení sú plánované a koordinované aktivity.

Riešenie informačnej bezpečnosti je súčasťou každého nového projektu, súvisiaceho s ľubovoľným IS (existujúcim alebo novým).

Úroveň bezpečnostného povedomia všetkých zamestnancov organizácie sa pravidelne rozvíja v súlade s cieľmi bezpečnostnej politiky.

Zásady bezpečnostnej politiky sa v relevantnej miere aplikujú aj na tretie strany (napr. dodávateľské firmy a ich zamestnanci).

Potreba priradenia kľúčových zodpovedností

Vypracovanie, aktualizácia a koordinácia uplatňovania bezpečnostnej politiky.

Definovanie a aktualizácia bezpečnostných štandardov organizácie resp. ich prevzatie.

Metodické riadenie organizačných útvarov v oblasti informačnej bezpečnosti.

Koordinácia činností pri analýze a riadení rizík IS a schvaľovaní prvkov IS z hľadiska plnenia bezpečnostných požiadaviek.

Vyhodnocovanie bezpečnostných prvkov prevádzkovaných v IS a posudzovanie požiadaviek na nové IS z hľadiska ich bezpečnosti.

Zabezpečenie školení zamestnancov v oblasti informačnej bezpečnosti.

Koordinácia činností pri prešetrovaní a zvládaní bezpečnostných incidentov.

Sledovanie dodržiavania bezpečnostných opatrení.

Monitorovanie a koordinácia vyhodnocovania záznamov o prístupoch k údajom.

Implementácia a správa systémov ochrany IS.

Potreba priradenia kľúčových zodpovedností II.

Realizácia a koordinácia projektov na zvýšenie informačnej bezpečnosti.

Riadenie prístupu užívateľov IS k aplikáciám.

Monitorovanie a vyhodnocovanie neoprávnených prístupov/pokusov o prístup do IS.

Akceptačné testovanie, schvaľovanie prvkov IS z hľadiska plnenia bezpečnostných požiadaviek.

Spracovanie a vedenie prehľadu o realizovaných riešeniach a opatreniach z oblasti bezpečnosti IS.

Kontrola dodržiavania pracovných postupov v IS.

Zabezpečenie odstraňovania havarijných stavov a bezpečnostných incidentov vrátane ich dôsledkov.

Vývoj APV pri dodržaní bezpečnostných opatrení.

...a kto to bude robiť? SATO ? Niekto ?

Systém riadenia informačnej bezpečnosti (samostatná téma).

Bezpečnostný manažér, bezpečnostný správca, vlastníci aktív/gestori IS, komisia pre informačnú bezpečnosť v organizácii, útvar IT / technický prevádzkovateľ, nadriadený/podriadený, externé firmy, ...

Dôležité je stanoviť ZMYSLUPLNÉ, REALISTICKÉ a DOSIAHNUTEĽNÉ bezpečnostné ciele.

Ešte dôležitejšie je zriadiť a personálne pokryť pracovné miesta / roly, ktoré pomôžu bezpečnostné ciele naplniť.

Gestor IS / vlastník

Poverený pracovník alebo útvar organizácie, ktorý koordinuje a metodicky riadi IS, stanovuje a zodpovedá za požadovanú funkcionalitu IS.

V praxi zodpovedá najmä za:

- definovanie požiadaviek na bezpečnosť aplikácie / IS a požiadaviek na ochranu údajov,
- klasifikáciu údajov a IS organizácie z hľadiska ich citlivosti a definovanie požiadaviek na bezpečnosť ako jednej z funkcionalít pri tvorbe aplikácie a pri jej zmenách,
- definovanie požiadaviek na riadenie a kontrolu prístupu k spracovaným údajom a službám IS,
- vymedzenie a odsúhlasovanie prístupových oprávnení do jeho IS a evidenciu udelených oprávnení,
- definovanie kritických kombinácií prístupových práv,
- definovanie požiadaviek na zmeny v aplikáciách / IS a akceptáciu úplnosti a správnosti vykonaných zmien.

Technický prevádzkovateľ

Správa IKT z hľadiska bezpečnosti plní priame aj nepriame úlohy.

Používanie programových prostriedkov v súlade s licenčnými požiadavkami.

Zabezpečenie správnej, bezporuchovej funkčnosti a systémovej podpory IS.

Implementácia a prevádzkovanie antivírusových prostriedkov.

Spracovanie, pravidelné revidovanie a testovanie plánu obnovy činnosti IS.

Vedenie evidencie všetkých problémov a použitých riešení.

Nadriadený / podriadený

Nadriadený v rozsahu pôsobnosti ním riadeného útvaru:

- zabezpečenie oboznámenia svojich podriadených s ich povinnosťami a zodpovednosťou z hľadiska bezpečnosti IS,
- definovanie požiadaviek na prístupové práva do aplikácií IS pre svojich podriadených v rozsahu ich pracovných povinností a vedenie evidencie o požiadavkách,
- oznamovanie podozrení z narušenia bezpečnosti IS, podozrení z nesprávnej funkcionality IS alebo dostupnosti údajov pre okruh zamestnancov, ktorým tieto údaje nie sú určené alebo narušenia dôvernosti, integrity a dostupnosti údajov a služieb IS.

Používateľ

Používateľ IS zodpovedá za:

- ochranu údajov, ktoré vytvára, spracúva, prijíma, ku ktorým pristupuje alebo kontroluje,
- ochranu pridelených autentizačných údajov a prostriedkov,
- dodržiavanie platných bezpečnostných zásad v potrebnom rozsahu na bezpečné využívanie IS a spracovanie údajov na základe preukázateľného dôvodu oprávňujúceho na prístup do IS,
- bezodkladné oznámenie podozrenia z narušenia bezpečnosti IS (svojmu nadriadenému),
- oznámenie podozrenia z nesprávnej funkcionality využívaného IS alebo dostupnosti údajov pre okruh zamestnancov, ktorým tieto údaje nie sú určené, svojmu nadriadenému,
- správne využívanie zabudovaných bezpečnostných mechanizmov IS.

Organizácia bezpečnosti IS

Cieľom organizácie bezpečnosti IS je kontinuálne a efektívne riadiť informačnú bezpečnosť vrátane vzťahov k tretím stranám a servisným alebo dodávateľským partnerom.

Pre všetky významné IS sa zavedie proces riadenia rizík vykonávaný najmä prostredníctvom analýzy rizík a návrhu bezpečnostných opatrení na zmiernenie identifikovaných rizík na prijateľnú úroveň.

Všetky rozhodnutia o prijatí alebo neprijatí bezpečnostných opatrení sú založené na výsledkoch príslušnej analýzy rizík.

Analýza rizík musí byť primerane formalizovaná, ale nič sa nemá preháňať.

Dôležitá je definícia kľúčových prvkov riadenia informačnej bezpečnosti.

Zodpovednosti za informačnú bezpečnosť v zmluvných vzťahoch s tretími stranami, servisnými alebo dodávateľskými partnermi sa explicitne vymedzujú.

Personálna bezpečnosť vo vzťahu k IS

Potrebujeme redukovať riziká súvisiace s ľudskými chybami, zlyhaniami, zneužitím práv, vedomými alebo nevedomými porušovaniami bezpečnostných zásad.

§ 29 Personálna bezpečnosť (Výnos)

Okrem požiadaviek Výnosu...

- Zákon č. 552/2003 Z. z. o výkone práce vo verejnom záujme
- Zákon č. 400/2009 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov
- Zákon č. 311/2001 Z. z. Zákonník práce

Obsahujú podmienky pracovno-právnych vzťahov, upravujú aj niektoré aspekty personálnej bezpečnosti:

- predpoklady a podmienky prijatia do štátnej služby, resp. výkonu práce vo verejnom záujme – previerka,
- práva a povinnosti zamestnanca ako aj zamestnávateľa,
- prehlbovanie a zvyšovanie kvalifikácie zamestnancov,
- základné zásady pri porušení pracovnej disciplíny,
- podmienky a povinnosti pri skončení pracovného pomeru.

Ministerstvo financií Slovenskej republiky

EFQM Recognised for excellence 5 star - 2012

Zlyhanie ľudského faktora

Neúmyselné

- nedostatočne zabezpečené heslo
- strata nosičov s dátami, dôležitých dokumentov
- neúmyselné prezradenie citlivých informácií
- ignorovanie varovných signálov IS...

Úmyselné

- úmyselné prezradenie citlivých dát (prístupové heslá, nastavenia systému...)
- poskytnutie osobných údajov tretej osobe
- ukradnutie dôležitého aktíva
- poškodenie alebo obmedzenie prevádzky...

Dôsledky

- strata citlivých dát
- priama alebo nepriama finačná strata
- strata dobrého mena organizácie..

KPMG cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Bezpečnosť ľudských zdrojov

Pred nástupom do zamestnania

Počas zamestnania

Ukončenie alebo zmena počas zamestnania

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Bezpečnosť ľudských zdrojov pred nástupom do zamestnania

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

Ciele

EFQM
Recognised for excellence
5 star - 2012

Zabezpečiť, že zamestnanci aj tretie strany porozumejú svojim zodpovednostiam a že sú vhodní na výkon rolí, ktoré im budú pridelené.

Bezpečnostné zodpovednosti by mali byť adresované už na úrovni náboru/prijímania pracovníkov a zahrnuté v primeranom opise práce a podmienkach pre pracovnú pozíciu.

Potenciálni zamestnanci, zmluvní partneri alebo používatelia v pozícii tretích strán by mali byť primerane preverení.

Všetci zamestnanci, zmluvní partneri a používatelia v pozícií tretích strán by mali mať podpísané zmluvy stanovujúce ich zodpovednosti počas trvania pracovnoprávneho vzťahu.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Prijímacie konanie - proces preverovania

Požiadavka na vykonanie previerky personálneho pozadia všetkých uchádzačov o zamestnanie v súlade s:

- príslušnými zákonmi a právnymi nariadeniami,
- požiadavkami organizácie,
- etikou,
- klasifikačným stupňom infomácií, ku ktorým sa bude pristupovať,
- vnímanými rizikami súvisiacimi s danou pozíciou.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Bezpečnosť ľudských zdrojov počas zamestnania

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Ciele

Zabezpečiť, že zamestnanci, zmluvní partneri a používatelia v pozícii tretích strán sú si vedomí hrozieb informačnej bezpečnosti, ich zodpovednosti a záväzkov a že sú pripravení dodržiavať a podporovať bezpečnostnú politiku v priebehu ich každodennej činnosti, ako aj znižovať riziká ľudskej chyby.

Personálna bezpečnosť má byť uplatňovaná počas celého obdobia zamestnania jednotlivca v organizácii.

Primeraná úroveň vzdelávania a školenia v oblasti bezpečnostných postupov a správneho používania prostriedkov na spracúvanie informácií by mali byť poskytnuté všetkým zamestnancom ako i tretím stranám, čím sa minimalizujú bezpečnostné riziká.

Mal by byť zavedený formálny disciplinárny proces riešenia narušení bezpečnosti.

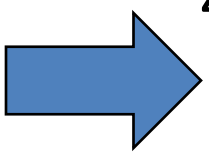
KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

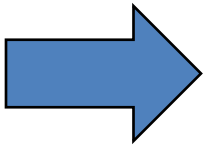
Manažérske zodpovednosti

Neznalosť bezpečnostných zodpovedností zamestnancov



Zvýšené riziko spôsobenia škody, incidentu

Motivovaný, upovedomený personál



Tendencia byť spoľahlivý, nebyť príčinou incidentu

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Manažérske zodpovednosti

Povinnosť manažmentu vyžadovať uplatňovanie informačnej bezpečnosti od:

- zamestnancov,
- zmluvných partnerov,
- používateľov v pozícii tretích strán.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Povedomie o informačnej bezpečnosti, vzdelávanie a školiaca činnosť

Cieľom je umožniť rozpoznať problémy a incidenty v informačnej bezpečnosti a reagovať primerane vzhľadom na svoje pracovné zaradenie.

Všetci zamestnanci organizácie by mali absolvovať periodické školenia za účelom udržiavania bezpečnostného povedomia a mali by im byť poskytované aktuálne verzie politík a smerníc organizácie, ak si to vyžaduje ich pracovné zaradenie.

KPMG
cutting through complexity™

Disciplinárny proces

Musí byť stanovený formálny disciplinárny proces pre zamestnancov, ktorí spôsobili porušenie informačnej bezpečnosti (pracovný poriadok, smernica o personálnej bezpečnosti a pod.).

Disciplinárny proces by sa nemal začať bez predošlého overenia, či naozaj došlo k narušeniu bezpečnosti vedomým konaním zo strany zamestnanca.

Disciplinárny proces slúži predovšetkým ako <u>odstrašujúci prostriedok:</u>

- vystríha zamestnancov pred porušovaním zákonov, riadiacich aktov a vnútorných predpisov organizácie, ako aj akýmkoľvek iným narušeniam bezpečnosti,
- demonštruje vážny záujem organizácie v oblasti dodržiavania zásad (nielen) informačnej bezpečnosti.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Bezpečnosť ľudských zdrojov
ukončenie alebo zmena pracovného pomeru

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Cieľ

Zabezpečiť, aby zamestnanci opustili organizáciu alebo zmenili podmienky svojho pracovného vzťahu primeraným spôsobom, nenarúšajúcim informačnú bezpečnosť.

Definovanie zodpovedností - opustenie organizácie zamestnancom má byť riadené, bude navrátené všetko poskytnuté vybavenie, budú odňaté príslušné prístupové práva.

Zmena zodpovednosti a pracovného vzťahu v rámci organizácie by mala prebehnúť riadeným spôsobom (je potrebné mať definovaný postup a náležitosti takejto zmeny).

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Vrátenie aktív

Pri ukončení pracovného vzťahu je zamestnanec povinný odovzdať všetky aktíva, ktoré sú v jeho správe a spolupracovať pri prevedení činností, ktoré vykonával, na iného zamestnanca.

Navrátanie aktív má byť evidované (výstupný list zamestnanca).

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Vrátenie aktív

V procese výpovede musí byť zahrnuté odovzdanie:

- pracovných pomôcok,
- hardvérového a softvérového vybavenia,
- dokumentov v listinnej aj elektronickej forme, správy elektronickej pošty obsahujúce dôležité pracovné informácie,
- všetkých ostatných poznatkov dôležitých z hľadiska zaistenia kontinuity výkonu činností (nezdokumentované postupy, korešpondencia, špecifické znalosti nadobudnuté počas pracovného vzťahu...).

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Odňatie prístupových oprávnení

Prístupové práva všetkých zamestnancov a zmluvných partnerov k informáciám a prostriedkom na ich spracúvanie musia byť na základe ukončenia pracovného resp. zmluvného vzťahu bezodkladne odobrané (cieľom je zabrániť neoprávnenému prístupu alebo zneužitiu prístupových práv).

KPMG
cutting through complexity™

Odňatie prístupových oprávnení

Prístupové práva, ktoré by mali byť odňaté alebo modifikované zahŕňajú:

- fyzický a logický prístup,
- kľúče, identifikačné karty,
- prostriedky na spracúvanie informácií,
- predplatené služby,
- odstránenie zo všetkej dokumentácie, ktorá ich zaraďuje k aktuálnym zamestnancom organizácie.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

II. Bezpečnostný projekt IS

Ivan Kopáčik
Gordias, s.r.o.

KPMG
cutting through complexity™

II. Agenda

Motivácia

Legislatívne východiská

Obsah a rozsah bezpečnostného projektu

Analýza a riadenie rizík

Bezpečnostné smernice

Záver

Motivácia

Každá zlozitejšia a komplexnejšia aktivita musí byť vopred „naprojektovaná“ (stavba RD, implementácia IS, výrobný postup ...).

Projekt: konkrétne vypracovaný návrh uskutočnenia určitého zámeru.

Projekt musí mať:

- Vopred identifikované definované požiadavky (prečo? ako? kto?)
- Stanovené ciele, rozsah a výstupy
- Harmonogram vypracovania a realizácie
- Pridelené zdroje potrebné na jeho vypracovanie a realizáciu

Bezpečnostný projekt - východiská

Pre podmienky verejnej správy

- Zákon o ochrane osobných údajov
- Výnos Ministerstva financií Slovenskej republiky č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy (ďalej len Výnos)
- Zákon č. 45/2011 o kritickej infraštruktúre
- „Zdravý rozum“
- Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností

Zákon o ochrane osobných údajov I.

- Za bezpečnosť osobných údajov zodpovedá prevádzkovateľ. Prevádzkovateľ je povinný chrániť spracúvané osobné údaje pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania. Na tento účel príjme primerané technické, organizačné a personálne opatrenia (ďalej len „bezpečnostné opatrenia“) zodpovedajúce spôsobu spracúvania osobných údajov, pričom berie do úvahy najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných osobných údajov ako aj rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému.
- Bezpečnostné opatrenia prevádzkovateľ zdokumentuje v bezpečnostnom projekte informačného systému.

Zákon o ochrane osobných údajov II.

- Bezpečnostný projekt vymedzuje rozsah a spôsob bezpečnostných opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.

- Bezpečnostný projekt obsahuje najmä
  - názov informačného systému, na ktorý sa vzťahuje,
  - bezpečnostný zámer,
  - analýzu bezpečnosti informačného systému,
  - bezpečnostnú smernicu.

Zákon o ochrane osobných údajov III.

Bezpečnostný zámer vymedzuje základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu informačného systému pred ohrozením jeho bezpečnosti.

Bezpečnostný zámer obsahuje najmä:

- formuláciu základných bezpečnostných cieľov a minimálne požadovaných bezpečnostných opatrení,
- špecifikáciu technických, organizačných a personálnych opatrení na zabezpečenie ochrany osobných údajov v infomačnom systéme a spôsob ich využitia,
- vymedzenie okolia informačného systému a jeho vzťah k možnému narušeniu bezpečnosti,
- vymedzenie hraníc určujúcich množinu zvyškových rizík.

Zákon o ochrane osobných údajov IV.

Analýza bezpečnosti informačného systému je podrobný rozbor stavu bezpečnosti informačného systému s vymedzením rozsahu jeho odolnosti a zraniteľnosti. Analýza bezpečnosti obsahuje najmä:

- kvalitatívnu analýzu rizík, v rámci ktorej sa identifikujú hrozby pôsobiace na jednotlivé aktíva infomačného systému spôsobilé narušiť jeho bezpečnosť alebo funkčnosť; výsledkom kvalitatívnej analýzy rizík je zoznam hrozieb pre dôvernosť, integritu a dostupnosť spracúvaných osobných údajov, s uvedením rozsahu možného rizika, návrhov opatrení na elimináciu alebo minimalizáciu vplyvu rizík a s vymedzením súpisu nepokrytých rizík,
- použitie bezpečnostných štandardov (Napríklad STN ISO/IEC 27001, STN ISO/IEC 27002, Výnos Ministerstva financií Slovenskej republiky č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov) a určenie iných metód a prostriedkov ochrany osobných údajov; súčasťou analýzy bezpečnosti informačného systému je posúdenie zhody navrhnutých bezpečnostných opatrení s použitými bezpečnostnými štandardami, metódami a prostriedkami.

Zákon o ochrane osobných údajov V.

Bezpečnostná smernica obsahuje najmä:

- popis technických, organizačných a personálnych opatrení a spôsob ich uplatňovania v konkrétnych podmienkach,
- rozsah oprávnení, popis povolených činností a spôsob identifikácie a autentizácie jednotlivých oprávnených osôb,
- rozsah zodpovednosti oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov,
- spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému,
- postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie rizika vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou, poruchou alebo inou mimoriadnou situáciou.

Výnos

Analyzovanie rizík vyplývajúcich z hrozieb pre informačné systémy verejnej správy, od ktorých závisia kritické procesy.

Analýza rizík v súvislosti s informačnými systémami verejnej správy, vyplývajúcich z činnosti tretích strán v týchto informačných systémoch, najmä dodávateľov, externých spolupracovníkov, orgánov verejnej správy, fyzických osôb, a zabezpečenie takých technických, organizačných a právnych podmienokna činnosť tretích strán v informačných systémoch verejnej správy, aby nebola narušená bezpečnosť informačného systému verejnej správy a bezpečnostná politika povinnej osoby.

Zákon č. 45/2011 o kritickej infraštruktúre

Bezpečnostný plán

- obsahuje popis možných spôsobov hrozby narušenia alebo zničenia prvku, zraniteľné miesta prvku a bezpečnostné opatrenia na jeho ochranu.

Bezpečnostné opatrenia sú najmä

- mechanické zábranné prostriedky, technické zabezpečovacie prostriedky, bezpečnostné prvky informačných systémov, fyzická ochrana, organizačné opatrenia, kontrolné opatrenia a ich vzájomná kombinácia.

Rozsah bezpečnostných opatrení na ochranu prvku sa určuje na základe posúdenia hrozby narušenia alebo zničenia prvku.

Zákon č. 45/2011 o kritickej infraštruktúre

Pri vypracúvaní bezpečnostného plánu sa postupuje nasledovne:

- Určujú sa dôležité zariadenia prvku.
- Vyhodnocuje sa riziko hrozby narušenia alebo zničenia jednotlivých zariadení prvku, ich zraniteľné miesta, predpokladané
- dôsledky ich narušenia alebo zničenia na funkčnosť, integritu a kontinuitu činnosti prvku.
- Uskutočňuje sa výber hlavných bezpečnostných opatrení na ochranu prvku, ktoré sa členia na
  - trvalé bezpečnostné opatrenia, ktorými sú investície a postupy na zabezpečenie ochrany prvku, a to
    - mechanické zábranné prostriedky,
    - technické zabezpečovacie prostriedky,
    - bezpečnostné prvky informačných systémov,
    - organizačné opatrenia s dôrazom na postup pri vyrozumení a varovaní, ako aj na krízové riadenie,
    - odborná príprava osôb, ktoré zabezpečujú ochranu prvku,
    - kontrolné opatrenia na dodržiavanie trvalých bezpečnostných opatrení,
  - mimoriadne bezpečnostné opatrenia, ktoré sa uplatňujú v závislosti od intenzity hrozby narušenia alebo zničenia prvku.
- Určujú sa hlavné bezpečnostné opatrenia na ochranu prvku.
- Bezpečnostný plán sa počas jeho tvorby konzultuje s orgánmi, ktorých súčinnosť sa predpokladá pri ochrane prvku.

Zdravý rozum

Pri implementácii nových alebo aktualizácii existujúcich IS sa odporúča v primeranej miere aplikovať nasledovné princípy:

- súčasťou každého projektu IS musí byť analýza rizík súvisiaca s vývojom a prevádzkovým prostredím nových prvkov IS,
- pre každý projekt IS musia byť identifikované a špecifikované bezpečnostné požiadavky,
- súčasťou každého projektu IS musí byť návrh bezpečnostných testov a návrh formy overenia dostatočnosti bezpečnosti nových prvkov IS pred ich zavedením do rutinnej prevádzky,
- súčasťou každého projektu IS musí byť vypracovanie príslušnej projektovej dokumentácie (používateľskej, administrátorskej a prevádzkovej dokumentácia k IS),
- v každom projekte IS musí byť zriadená a obsadená rola, ktorá zodpovedá za integráciu bezpečnostných opatrení do predmetu projektu IS,
- na zaistenie primeranej úrovne bezpečnosti musí byť v každom projekte IS vývojové a testovacie prostredie oddelené od produkčného prostredia,
- v každom projekte IS sa musia určiť role, ktoré budú vykonávať údržbu predmetu projektu IS po jeho zavedení do rutinnej prevádzky.

Obsah a rozsah bezpečnostného projektu I.

- „Prečo, ako a čoho bezpečnosť vlastne ideme riešiť?“
- „Akú metodiku / štandard použijeme?“
- „Aké sú právne požiadavky na riešenie bezpečnosti?“
- „Ako „vysokú„ bezpečnosť potrebujeme dosiahnuť?“
- „Aké okruhy rizík ideme minimalizovať?“
- „Aké riziká sú pre nás akceptovateľné?“
- „Aké opatrenia sme schopní prijať?“

1. časť bezpečnostného projektu: **<u>bezpečnostný zámer</u>**

Obsah a rozsah bezpečnostného projektu II.

- „Čo sú naše hodnoty (aktíva), čo chceme chrániť?“
- „Pred akými hrozbami chceme naše aktíva chrániť?“
- „Aké negatívne dôsledky nám hrozby môžu spôsobiť?“
- „Aká je šanca (pravdepodobnosť), že riziko sa naplní?“
- „Ako veľké sú riziká, ktoré nám hrozia?“
- „Aké opatrenia treba prijať, aby sa riziká minimalizovali na prijateľnú úroveň“?

2. časť bezpečnostného projektu: **<u>analýza bezpečnosti.</u>**

Obsah a rozsah bezpečnostného projektu III.

- „Ako zavedieme do praxe jednotlivé opatrenia?“
- „Ako budeme používať a dodržiavať jednotlivé opatrenia?“
- „Čo budeme robiť, ked niektoré riziko skutočne nastane?“
- „Ako budeme hodnotiť dostatočnosť a účinnosť opatrení?“
- „Ako odhalíme nové riziká?“
- „Kto a za čo je z hľadiska bezpečnosti zodpovedný?“
- „Aké sú práva a povinnosti zúčastnených strán?“

3. časť bezpečnostného projektu: **bezpečnostné smernice.**

Bezpečnostný zámer

Obsah podľa OOÚ

Zohľadnenie požiadaviek ďalších právnych predpisov

Zohľadnenie stavu IS (existujúci vs. plánovaný)

Špecifické bezpečnostné ciele nad rámec OOÚ

Väzby na existujúcu bezpečnostnú dokumentáciu

Analýza bezpečnosti

Popis použitej metodiky

Použité katalógy (hrozieb, aktív, dopadov)
Identifikácia a klasifikácia rizík

Návrh a prioritizácia opatrení na elimináciu alebo minimalizáciu vplyvu rizík a s vymedzením súpisu nepokrytých rizík.

Bezpečnostné smernice

Rozsah podľa OOÚ

Špecifická smernica pre ochranu osobných údajov (ak sú spracúvané)

Bezpečnosť na úrovni zariadení, operačných systémov a databáz

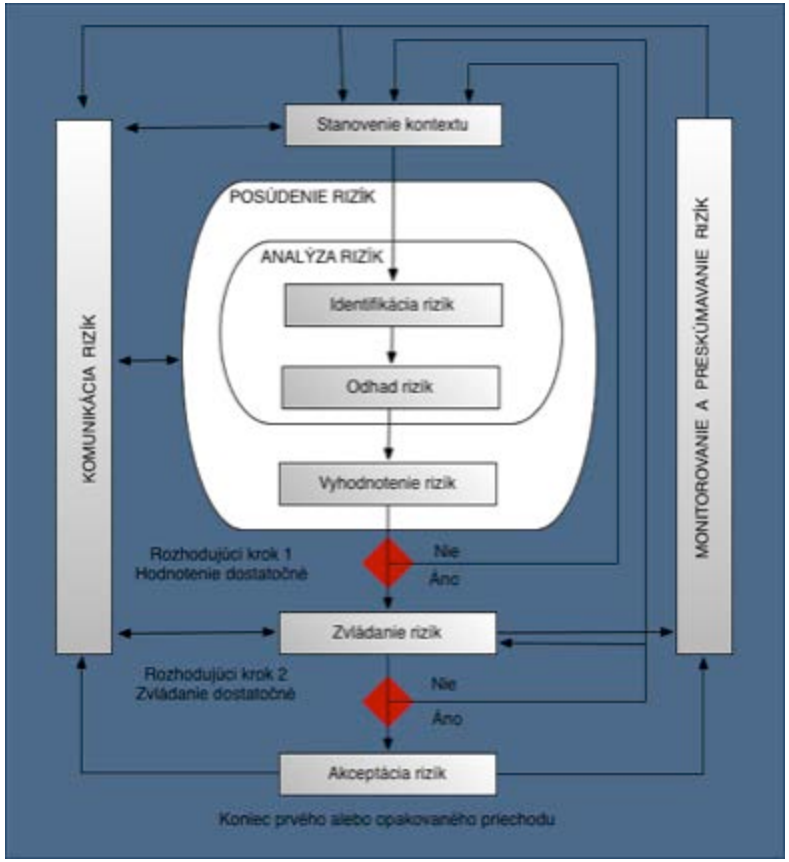
Monitorovanie a dohľad

- Monitorovanie na úrovni infraštruktúry
- Auditovanie údajov a operácií
- Vyhodnocovanie zaznamenaných udalostí

Vývoj, nasadzovanie a riadenie zmien

.....

Riadenie rizík – komplexný pohľad ISO27005



Analýza rizík – pojmy I.

- ***Aktívum*** je dôležitá informácia a dokumentácia, zmluva, programové vybavenie, technické zariadenie, poskytovaná služba, kvalifikovaní ľudia, dobré meno a ďalšie skutočnosti, ktoré považuje organizácia za hodnotné a vyžadujúce si ochranu. ***Informačné aktívum*** chápeme ako dokument, údaj, súbor alebo ich logické zoskupenie s definovaným významom, vlastníkom a určením.
- ***Analýza rizík*** je činnosť, ktorej náplňou je identifikácia a ohodnocovanie bezpečnostných rizík.
- ***Analýza bezpečnosti*** je zisťovanie rizík informačného systému s cieľom navrhnúť spôsob jeho maximálneho zabezpečenia (pojem „ analýza rizík“ je synonymum).

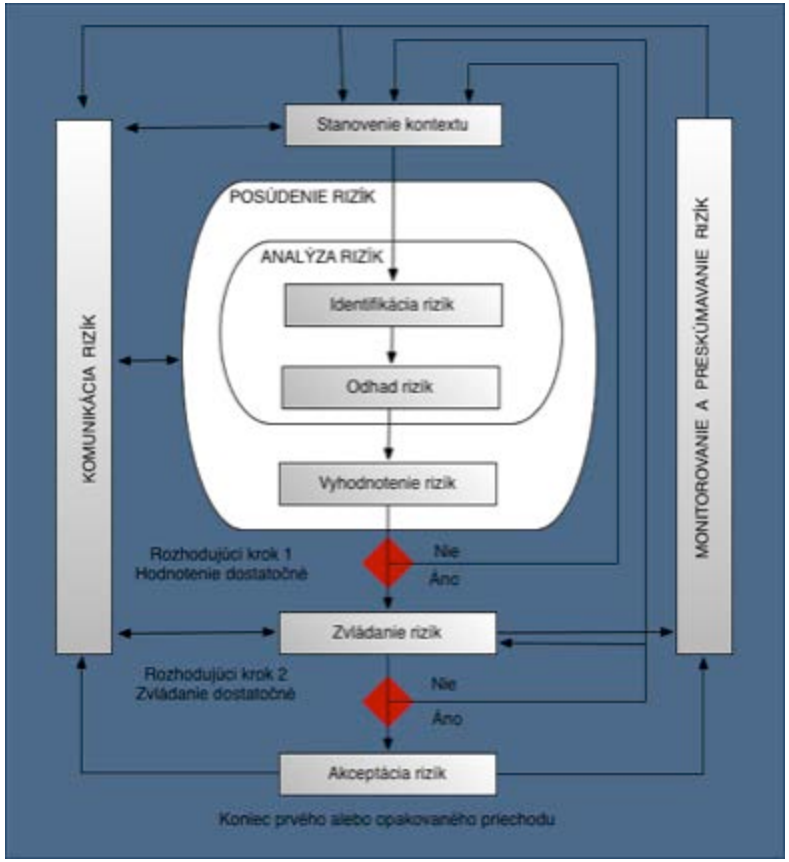
Analýza rizík – pojmy II.

- ***Hrozba*** je objektívna skutočnosť, ktorá môže využitím zraniteľnosti aktíva negatívne ovplyvniť činnosť, stav alebo existenciu daného aktíva
- ***Zraniteľnosť*** je technické riešenie, okolnosť, spôsob použitia, slabé miesto, nedostatok alebo nejaká vlastnosť aktíva, ktorá umožňuje, aby došlo k naplneniu hrozby voči aktívu vyznačujúcemu sa danou zraniteľnosťou
- ***Dopad hrozby*** predstavuje negatívne dôsledky naplnenia hrozby voči aktívu (zníženie až strata funkčnosti, poškodenie, zníženie hodnoty až zničenie) na aktívum a inštitúciu, ktorá je vlastníkom aktíva
- ***Bezpečnostné opatrenie*** je technické, organizačné, právne alebo iné riešenie, ktoré úplne alebo čiastočne odstraňuje zraniteľnosť aktíva, a/alebo znižuje pravdepodobnosť naplnenia hrozby a/alebo v prípade jej naplnenia znižuje jej dopad na aktívum a organizáciu, ktorá ho

Analýza rizík – pojmy III.

- ***Riziko*** predstavuje pravdepodobnosť, že zraniteľnosť v IS ovplyvní overenie alebo dostupnosť, pravosť, integritu alebo dôvernosť spracúvaných alebo prenesených údajov, ako aj vážnosť dopadu úmyselného alebo neúmyselného využitia takejto zraniteľnosti.
- ***Zvyškové riziko*** je riziko, ktoré ostane po prijatí bezpečnostných opatrení zameraných na jeho minimalizáciu.
- ***Riadenie rizika*** je vedomý proces pochopenia rizika, dohodnutia sa na príslušných opatreniach a realizácii týchto opatrení na zníženie rizika na definovanú úroveň, ktorá je akceptovateľnou úrovňou rizika pri akceptovateľných nákladoch; tento prístup je charakterizovaný identifikovaním, meraním a riadením rizík na úroveň odpovedajúcu stanovenej úrovni.

Riadenie rizík – komplexný pohľad ISO27005



Posúdenie rizík

Riziká by sa mali identifikovať, kvantifikovať alebo kvalitatívne opísať a prioritizovať vzhľadom na kritériá vyhodnotenia rizík a cieľov organizácie.

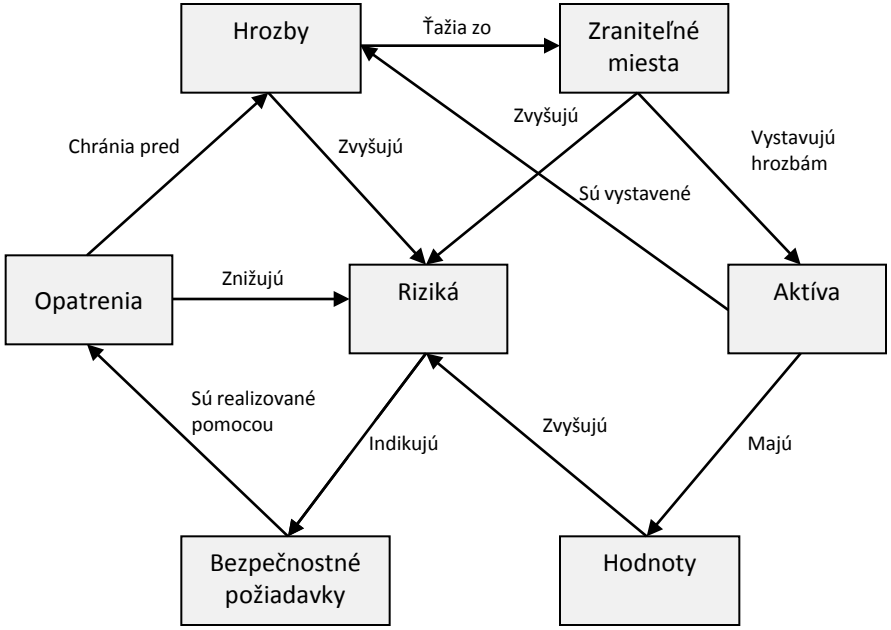
Pre posúdenie rizík je kľúčová analýza rizík zahŕňajúca pre každé riziko jeho identifikáciu a analýzu / ohodnotenie súvisiacich aktív, hrozieb, zraniteľností, dopadov.

Analýza rizík – východiská

- Množstvo metodík, nástrojov a techník (kvalitatívny versus kvantitatívny prístup, kontrolné zoznamy/Checklists, analýzy pomocou scenára, FRAP, brainstorming, BIA, matice hodnoty aktív/zraniteľností/dopadov, ISO/IEC-27005 *Riadenie rizík informačnej bezpečnosti*, ISO 31000 *Manažérstvo rizika. Zásady a návod,* generické katalógy aktív/hrozieb/dopadov, automatizované nástroje CRAMM, ALE /Annual Loss Expectancy ...).

- Neexistuje univerzálna metodika vhodná „pre všetko“- výber a použitie vhodnej metodiky závisí na cieľoch, rozsahu a hĺbke analýzy, veľkosti a charaktere organizácie, zložitosti IKT infraštruktúry, stave IKT – prevádzkový IS versus implementovaný IS, ...).

Anatómia rizika



Analýza rizík

Bez ohľadu na zvolenú metodiku zahŕňa:

- Identifikáciu rizík
- Preskúmanie a ohodnotenie rizík

Posúdenie rizík sa často vykonáva vo viacerých iteráciách:

- vysokoúrovňové (identifikácia potenciálne vysokých rizík, ktoré si vyžadujú ďalšie posúdenie),
- dôkladnejšie (hĺbkové) preskúmanie potenciálne vysokých rizík zistených počas úvodnej iterácie.

Hodnotenie dopadov

- Berieme do úvahy identifikované aktíva a ich hodnoty.
- „Čo by stálo opätovné vytvorenie aktíva?“
- „Aké dôsledky bude mať, keď aktívum nebude možné použiť minútu/hodinu/deň...?“
- Rôzne hrozby a zraniteľnosti majú rôzne vplyvy na aktíva (strata dôvernosti, integrity alebo dostupnosti).
- Dopady môžu byť vyjadrené v peňažných, technických alebo personálnych metrikách alebo v iných jednotkách.

Zvládanie a riadenie rizík

Návrh opatrení na zníženie rizík

- obídenie rizika: rozhodnutie zmeniť prostredie, v ktorom sa riziko vyskytuje tak, aby toto riziko neprichádzalo do úvahy,
- prenesenie rizika: rozhodnutie preniesť následky realizácie rizika mimo organizáciu,
- redukcia rizika: rozhodnutie pomocou vhodných opatrení dosiahnuť zníženie následkov realizácie rizika alebo zníženie pravdepodobnosti jeho realizácie,
- akceptácia rizika.

Počas výberu opatrenia je dôležité zvážiť náklady na obstaranie, implementáciu, správu, prevádzku, monitorovanie a údržbu opatrení oproti hodnote chránených aktív.

Výber opatrení

Opatrenia podľa času ich realizácie

- preventívne opatrenia: vykonávajú sa pred vznikom rizika,
- reakčné opatrenia: vykonávajú sa po vzniku rizika (ich cieľom je redukcia škôd, ktoré riziko spôsobí, zníženie nákladov na zvládnutie dôsledkov rizika alebo zefektívnenie procesu zvládnutia situácie).

Vyberáme najvýhodnejšiu možnosť z hľadiska nasledovných kritérií

- minimalizácia nákladov na realizáciu opatrení (napríklad finančné, časové, organizačné náklady),
- minimalizácia negatívnych dopadov opatrení na používateľov IS, nimi vykonávaných činnosti a iných neželaných efektov,
- dostupnosť zdrojov potrebných na realizáciu a prevádzku opatrení (napríklad technika, ľudské zdroje),
- zohľadnenie štandardne používaných postupov v organizácii pre danú oblasť rizík.

Riadenie a monitorovanie rizík

Cieľom riadenia rizík je zníženie a udržiavanie závažnosti rizík na prijateľnej úrovni.

Riadenie rizík v praxi znamená predovšetkým:

- evidovanie rizík,
- sledovanie rizík,
- priebežné vyhodnocovanie rizík.

Vedenie organizácie prostredníctvom riadenia rizík získava:

- informácie o najdôležitejších rizikách, s ktorými sa organizácia stretáva,
- zabezpečenie primeranej úrovne uvedomovania si rizík v celej organizácii,
- ubezpečenie sa o účinnom zvládaní rizík.

Monitorovanie rizík

Monitorovanie riadenia rizík je kontinuálne vykonávaný proces, ktorý permanentne overuje a ubezpečuje vedenie organizácie o tom, že riadenie rizík je funkčné a plní svoje úlohy.

Monitorovanie má poskytovať informácie o:

- priebehu riadenia rizík pre potreby vedenia organizácie,
- realizácii kontrolných aktivít v oblasti riadenia rizík,
- prijímaní opatrení na skvalitnenie procesu riadenia rizík,
- vyhodnotení účinnosti prijatých opatrení.

Výsledky monitorovania rizík a ich riadenia

Monitorovanie riadenia rizík môže viesť k úprave alebo pridaniu prístupu, metodiky alebo nástrojov používaných v závislosti od

- identifikovaných zmien,
- iterácie posúdenia rizík,
- cieľa procesu riadenia rizík informačnej bezpečnosti,
- predmetu procesu riadenia rizík informačnej bezpečnosti (napr. celá organizácia, organizačná jednotka, informačný proces, jeho technická implementácia, aplikácia, pripojenie k internetu).

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Otázky a diskusia

Ďakujem za pozornosť

KPMG
cutting through complexity™