Dnešní téma se vztahuje k problematice **Řízení rizik bezpečnosti informací - zvládání rizik bezpečnosti informací.**

Jakmile jsou identifikovány bezpečnostní požadavky a rizika, a bylo rozhodnuto, jakým způsobem bude se zjištěnými riziky naloženo, měla by být vybrána a implementována opatření zajišťující snížení rizik na přijatelnou úroveň. Taková opatření mohou být vybrána z tohoto dokumentu nebo i z jiných souborů opatření. Pro pokrytí specifických potřeb mohou být vytvořena zcela nová opatření. Výběr konkrétních opatření je na rozhodnutí každé organizace. Rozhodnutí je založeno na kritériích určujících akceptaci nebo zvládání rizika a celkovém přístupu organizace k řízení rizik. Při výběru opatření by měla být zohledněna příslušná národní a mezinárodní legislativa a regulace.

Některá opatření mohou být chápána jako základní doporučení pro řízení bezpečnosti informací a mohou být využita ve většině organizací.

Východiska bezpečnosti informací

Řada opatření může být považována za základní principy představující dobrá východiska pro implementaci bezpečnosti informací. Mohou vycházet ze základních legislativních požadavků nebo jsou obecně považována za nejlepších způsob řešení bezpečnosti informací.

Opatření, která by měla být pro organizaci podstatná z pohledu legislativy, jsou:

a) ochrana osobních údajů;

b) ochrana důležité dokumentace organizace, jako například účetních záznamů ;

c) ochrana duševního vlastnictví.

Opatření, považovaná za základ nejlepších praktik (best practices) pro zajištění bezpečnosti informací, jsou:

a) dokument bezpečnostní politiky informací;

b) přidělení odpovědností v oblasti bezpečnosti informací;

c) vzdělávání, školení a zvyšování povědomí v oblasti bezpečnosti informací;

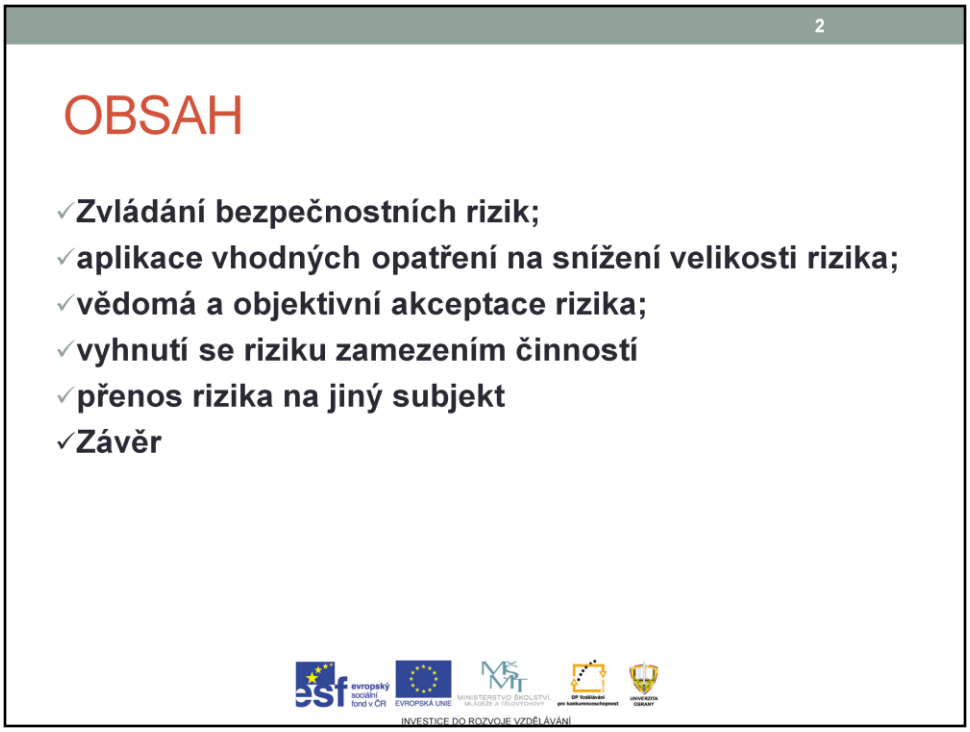
d) bezchybné zpracování v aplikačních systémech;

e) řízení technických zranitelností;

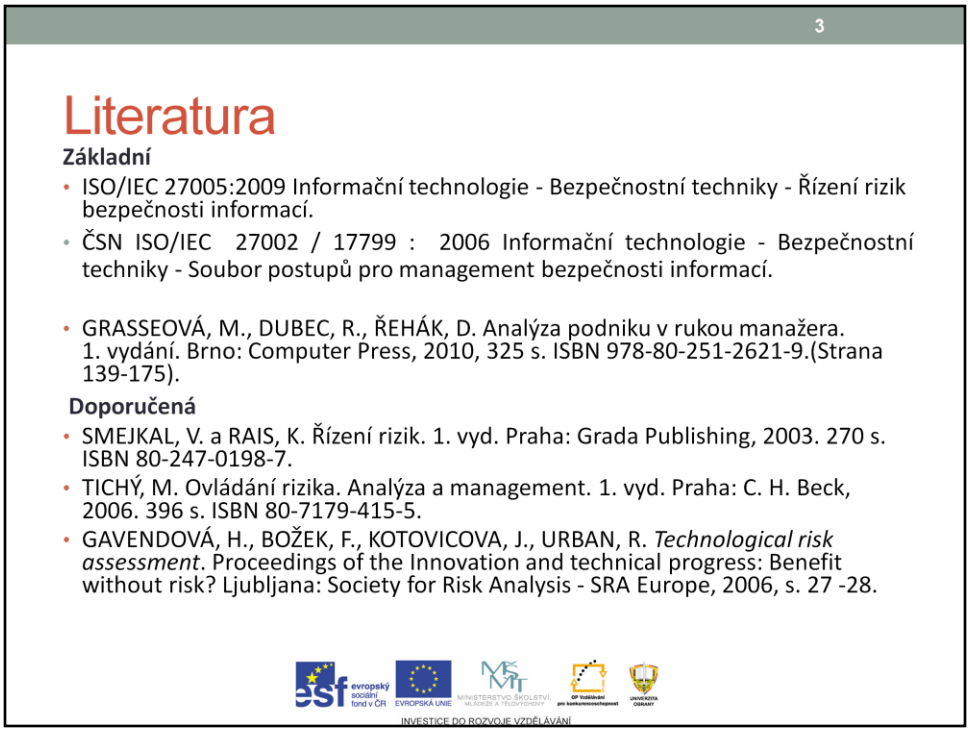
f) řízení kontinuity činností;

g) zvládání bezpečnostních incidentů a kroky k nápravě.

Tato opatření fungují ve většině organizací a prostředí. Je nutné si uvědomit, že o výběru a aplikaci konkrétních opatření by mělo být rozhodnuto až ve světle specifických rizik, kterým organizace čelí. I když výše uvedené doporučení může být považováno za dobré východisko, nenahrazuje výběr opatření vycházející z hodnocení rizik.



V rámci tohoto tématu se budeme zabývat následujícími oblastmi– viz snímek.



Pro studium této problematiky mezi základní literaturu patří norma ISO/IEC 27005:2009 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací a norma ČSN ISO/IEC 27002 / 17799 : 2006 Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací.

Další neméně významnou publikací je monografie GRASSEOVÁ, M., DUBEC, R., ŘEHÁK, D. Analýza podniku v rukou manažera. 1. vydání. Brno: Computer Press, 2010, 325 s. ISBN 978-80-251-2621-9.(Strana 139-175), popisující obecné přístupy k řízení rizik a základní postupy pro zavedení tohoto nástroje do organizace.

Pro zájemce mohu doporučit publikaci SMEJKAL, V. a RAIS, K. Řízení rizik. 1. vyd. Praha: Grada Publishing, 2003. 270 s. ISBN 80-247-0198-7. a TICHÝ, M. Ovládání rizika. Analýza a management. 1. vyd. Praha: C. H. Beck, 2006. 396 s. ISBN 80-7179-415-5.

Další normou vztahující se k přednášené problematice jako například **ISO/IEC 27001**

Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací -Požadavky .

Tato mezinárodní norma specifikuje požadavky na ustavení, implementaci, provozování, monitorování, přezkoumávání a zlepšování formálně schválených systémů řízení bezpečnosti informací (ISMS) v **kontextu celkových obchodních rizik organizace**. Specifikuje požadavky na implementaci bezpečnostních kontrolních opatření upravených podle potřeb jednotlivých organizací nebo jejich částí. **Tato mezinárodní norma je univerzální pro všechny druhy organizací (tj. komerční podniky, vládní úřady, neziskové organizace).**

Účelem této normy je poskytnout normativní požadavky na vývoj a provoz ISMS, **včetně sady kontrolních opatření pro řízení a zmírnění rizik spojených s informačními aktivy**, které organizace vyhledává, aby je chránila provozováním ISMS.

Zvládání bezpečnostních rizik

Předtím, než je rozhodnuto o způsobu zvládání rizika, měla by být stanovena kritéria, na jejichž základě bude určováno, je-li riziko pro organizaci akceptovatelné. Riziko může být akceptováno například z důvodu, že je nízké anebo, že náklady spojené s jeho zvládáním jsou pro organizaci cenově neúnosné. O takovýchto rozhodnutích by měly být vytvořeny záznamy.

Následně po provedeném hodnocení rizik musí být učiněno rozhodnutí, jakým způsobem bude s identifikovanými riziky naloženo. Možné varianty zahrnují:

a) aplikace vhodných opatření na snížení velikosti rizika;

b) vědomá a objektivní akceptace rizika, za předpokladu, že je tak učiněno v souladu s politikou organizace a kritérii pro akceptaci rizika;

c) vyhnutí se riziku zamezením činností, které jsou příčinou jeho vzniku;

d) přenos rizika na jiný subjekt (např. pojišťovny, dodavatele).

Jestliže bylo učiněno rozhodnutí o zvládání rizika formou aplikace vhodných opatření, měl by být výběr těchto opatření proveden na základě požadavků identifikovaných v rámci hodnocení rizik.

Opatření by měla zaručit snížení rizika na přijatelnou úroveň, přičemž v úvahu by mělo být vzato následující:

a) požadavky a omezení národní a mezinárodní legislativy a předpisů;

b) cíle organizace;

c) provozní požadavky a omezení;

d) cena za implementaci a provozní náklady spojené s přijetím opatření na snížení rizika, podle požadavků a omezení organizace;

e) potřeba udržovat rovnováhu mezi investicemi spojenými s implementací a provozem opatření a případnými škodami způsobenými selháním bezpečnosti.

Opatření k implementaci mohou být vybírána z normy nebo z jiných obdobných souborů opatření, případně mohou být navržena zcela nová opatření tak, aby co nejlépe odpovídala požadavkům organizace. Je důležité si uvědomit, že ne všechna opatření uvedená v normách budou aplikovatelná pro každý informační systém, prostředí nebo organizaci. Jako příklad lze uvést opatření, které popisuje oddělení jednotlivých rolí jako způsob prevence proti podvodům a chybám. Zejména u malých organizací nemusí být toto opatření realizovatelné a pro dosažení stejného cíle bude nutné hledat jiná opatření. Jiným příkladem může být opatření, popisující monitorování přístupu k systému a sběr důkazů. Popsaná opatření, např. zaznamenávání událostí, mohou být v rozporu s platnou legislativou, jako je ochrana soukromí zákazníků nebo ochrana soukromí na pracovišti.

Opatření by měla být vybírána již ve fázi návrhu a specifikace požadavků projektu

nového systému. Opačný případ může mít za následek dodatečné zvýšení nákladů, méně účinná řešení a v nejhorším případě neschopnost dosáhnout požadované úrovně bezpečnosti.

Žádná sada opatření nemůže sama o sobě zajistit kompletní bezpečnost. Na podporu cílů organizace by měly proto být zavedeny řídící činnosti pro monitorování, vyhodnocování, zlepšování výkonnosti a účinnosti bezpečnostních opatření.

Zvládání rizik

Vstupem pro zahájení činnosti zvládání rizik jsou výstupy z předešlých činností uskutečněných v rámci hodnocení rizik. Tímto vstupem je seznam rizik, kterým byla udělena priorita podle kritérií vyhodnocení rizik v souvislosti se scénáři incidentů, jež k těmto rizikům vedou.

V rámci činnosti zvládání rizik by měla být vybrána opatření k redukci, podstoupení, vyvarování se nebo přenosu rizik a měl by být definován plán zvládání rizik.

K dispozici jsou čtyři volby pro zvládání rizik: redukce rizika, podstoupení rizika, vyvarování se rizika a přenos rizika.

Způsoby zvládání rizik by se měly vybírat na základě výstupu z hodnocení rizik, očekávaných nákladů na implementaci a očekávaných přínosech plynoucích z těchto způsobů. Když lze zajistit velké snížení rizik při poměrně nízkých výdajích, měla by být uplatněna tato možnost. Další možnosti pro zlepšení mohou být neekonomické a je třeba posoudit, zda jsou obhajitelné.

Obecně řečeno, nepříznivé následky rizik by měly být redukovány na nejnižší přiměřeně dosažitelnou míru a bez ohledu na jakákoliv absolutní kritéria. Vedoucí pracovníci by měli zvažovat i ojedinělá, ale velmi závažná rizika. V takových případech může být nutné přijmout opatření, která nejsou z přísně ekonomického hlediska odůvodnitelná (například opatření pro zajištění kontinuity činností organizace na pokrytí konkrétních vysokých rizik).

Tyto čtyři způsoby zvládání rizik se vzájemně nevylučují. Někdy může organizace získat podstatnou výhodu kombinací způsobů jako je snížení pravděpodobnosti rizik, snížení jejich následků a přenos nebo podstoupení jakéhokoliv zbytkového rizika.

Některé způsoby zvládání rizik mohou účinně řešit více než jedno riziko (například školení a povědomí o bezpečnosti informací). Měl by být definován plán zvládání rizik, který jasně identifikuje pořadí priorit, v kterém budou aplikovány jednotlivé způsoby zvládání rizik, včetně jejich časových rámců. Priority lze stanovit za použití různých technik, včetně klasifikace rizik a analýzy nákladů a výnosů. Je na odpovědnosti vedoucích pracovníků organizace rozhodnout, kde je rovnováha mezi náklady na přijetí opatření a přidělováním rozpočtu.

Identifikace existujících opatření může na základě porovnání nákladů včetně údržby určit, že existující opatření přesahují současné potřeby. Pokud se uvažuje o odstranění nadbytečných nebo zbytečných opatření (zejména; když tato opatření vyžadují vysoké náklady na údržbu), musí být brány v úvahu faktory bezpečnosti informací nákladů. Protože se opatření mohou ovlivňovat navzájem, mohlo by odstranění nadbytečných opatření vést ke snížení celkové bezpečnosti. Kromě toho může být i levnější ponechat nadbytečná nebo zbytečná opatření r místě, než je odstranit.

Při zvažování způsobů zvládání rizik by se mělo přihlížet:

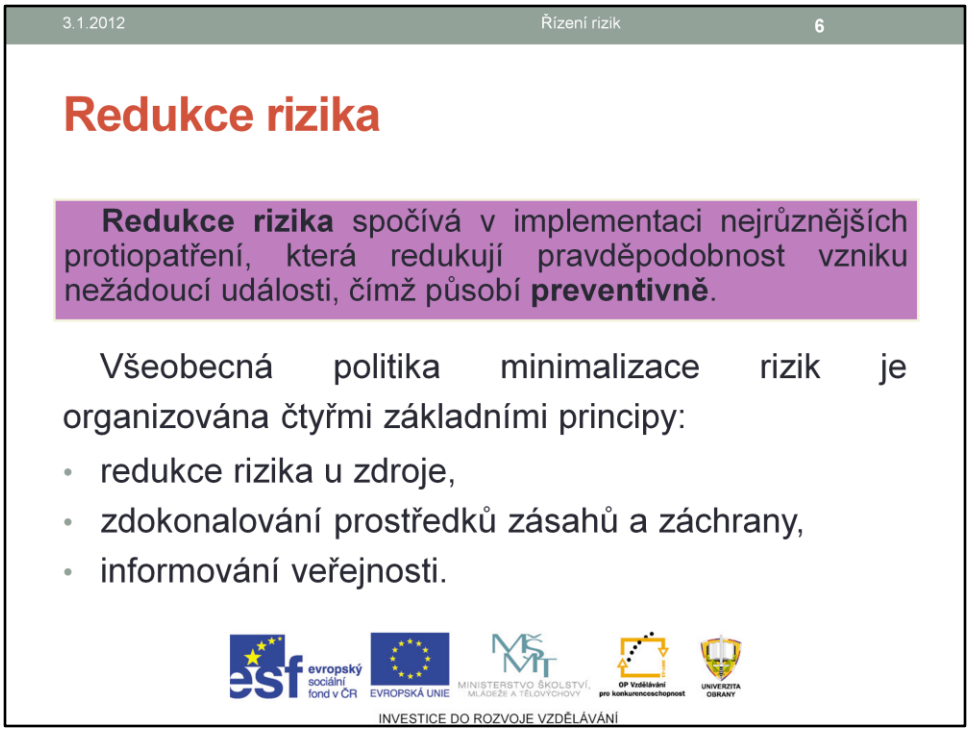
- k tomu, jak riziko vnímají dotyčné strany
- k nejvhodnějším způsobům, jak s těmito stranami komunikovat.

Stanovení kontextu (viz Kritéria vyhodnocení rizik) poskytuje informace o právních a regulačních požadavcích, které musí organizace splnit. Rizikem pro organizace je nedodržet tyto požadavky, a proto by měly být uplatněny možnosti, jak tuto možnost omezit. Při zvládání rizik by měla být zvažována všechna omezení - organizační technická, strukturální atd. - která jsou identifikována během činnosti stanovení kontextu.

Jakmile je definován plán zvládání rizik, musí být určena zbytková rizika. To vyžaduje aktualizaci nebo opakování hodnocení rizik, přičemž je nutno brát v úvahu očekávané

účinky navrhovaných způsobů zvládání rizik. Pokud zbytkové riziko stále ještě nesplňuje kritéria organizace na akceptaci rizik, může být nutné další opakování zvládání rizik, než se přejde k akceptaci rizik. Více informací je uvedeno v ISO/IEC 27002, 0.3.

Výstup: Plán zvládání rizik a zbytková rizika vyžadující rozhodnutí vedoucích pracovníků organizace o jejich akceptaci.



Redukce rizika

Redukce rizika může být v zásadě realizována dvěma přístupy. Prvním přístupem je snížení pravděpodobnosti výskytu nežádoucí události. Jedná se o ofenzivní přístup založený na implementaci preventivních opatření. Druhým přístupem je snížení závažnosti dopadu (následků) již proběhlé nežádoucí události a urychlení rekonstrukce zasaženého aktiva.

V tomto případě se jedná o defenzivní přístup založený na opatřeních ex post. U obou přístupů pak mohou být rizika minimalizována buď na straně zdroje hrozby, anebo na straně aktiva. Obecně nejlepší kombinací výše uvedených možností redukce rizika je snížení pravděpodobnosti výskytu nežádoucí události na straně zdroje hrozby. Za optimální

(současně však také nejnáročnější a téměř nerealizovatelnou) variantu lze považovat eliminaci zdroje hrozby (např. naprosté vymýcení teroristických skupin a organizací).

Činnost: Úroveň rizik by měla být snížena výběrem opatření tak, aby mohlo být zbytkové riziko přehodnoceno jako přijatelné.

Doporučení k realizaci:

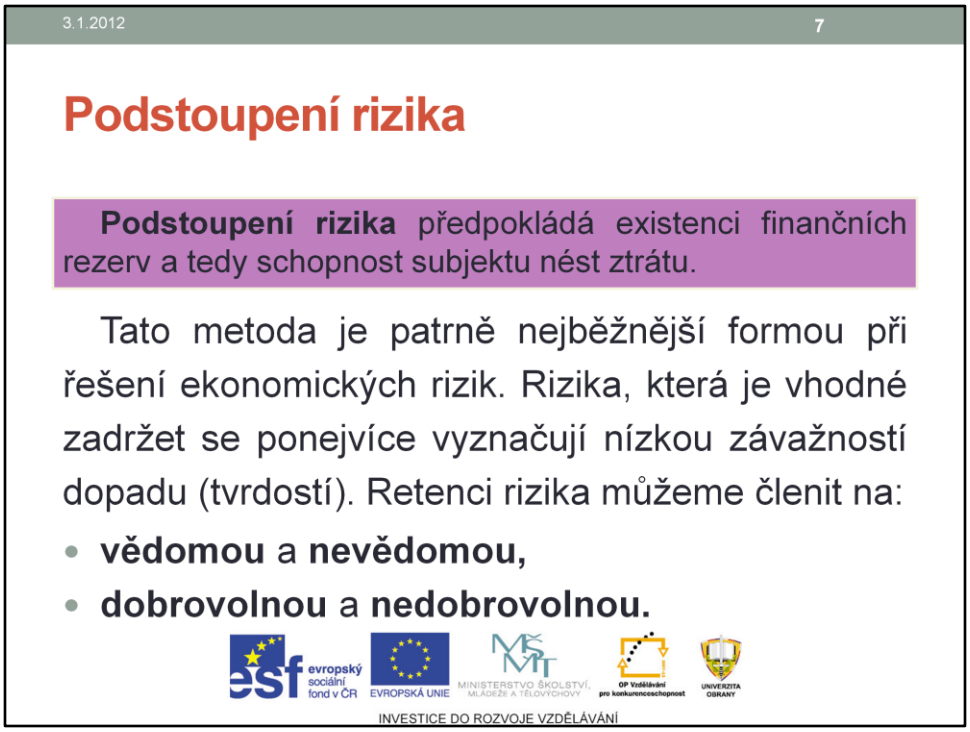
Měla by být vybrána vhodná a odůvodněná opatření ke splnění požadavků identifikovaných v rámci hodnocení rizik a zvládání rizik. Tento výběr by měl brát v úvahu kritéria akceptace rizik, jakož i právní, regulační a smluvní požadavky. Tento výběr by měl také brát v úvahu náklady a časový rámec pro přijetí opatření, nebo technické, ekologické a kulturní aspekty. Často je možné snížit celkové náklady na vlastnictví systému se správně vybranými opatřeními pro bezpečnost informací.

Obecně řečeno, opatření může zajistit jeden nebo více z následujících typů ochrany: nápravu, vyloučení, prevenci minimalizaci dopadu, odstrašování, odhalení, obnovení, monitorování a povědomí. Během výběru opatření je důležité zvážit náklady na získání, zavedení, spravování, provozování, monitorování a údržbu opatření ve vztahu k hodnotě chráněných aktiv. Kromě toho by měla být brána v úvahu návratnost investic, pokud jde o redukci rizik a potenciál využívat nové obchodní příležitosti, které určitá opatření nabízejí. Kromě toho je vhodné přihlížet i k tomu, že k definování a přijetí nových opatření nebo ke změně existujících opatření mohou být zapotřebí specializované způsobilosti. ISO/IEC 27002 poskytuje podrobné informace o opatřeních. Existuje mnoho omezení, jež mohou ovlivnit výběr opatření. Technická omezení, jako jsou požadavky na výkon ovladatelnost (požadavky na provozní podporu) a otázky kompatibility, mohou bránit používání určitých opatření, nebo by mohly vyvolat lidskou chybu bud' anulováním kontrolních mechanismů, poskytováním nepravdivého pocitu bezpečnosti nebo dokonce zvýšením rizika za hranice možností kontrolovat (například požadováním kompletních hesel bez řádného školení vedoucím k tomu, že si uživatelé hesla napíší). Navíc by se mohlo jednat o případ, že by opatření ovlivňovalo výkon. Vedoucí pracovníci by se měli pokusit identifikovat řešeni, která

splní požadavky na výkon a budou přitom garantovat dostatečnou bezpečnost informací. Výsledkem tohoto kroku je seznam možných opatření s jejich náklady, zisky a prioritou uplatnění.

Při výběru opatření a během jejich zavádění by měla být brána v úvahu různá omezení. Obvykle se jedná o tato omezení:

- Časová omezení
- Finanční omezení
- Technická omezení
- Provozní omezení
- Kulturní omezení
- Etická omezení
- Ekologická omezení
- Právní omezení
- Snadnost použití
- Osobní omezení
- Omezení při integraci nových a existujících opatření



Podstoupení rizika

Retence rizika je legitimní a pravděpodobně nejběžnější metoda zvládání rizik. Spočívá v tom, že organizace čelí téměř neomezenému počtu rizik, ovšem ve většině případů proti nim nic nedělá. Retence rizik může být vědomá či nevědomá. K vědomé retenci rizika dochází tehdy, je-li riziko rozpoznáno a nedojde k aplikaci některé z jiných možností zvládání

rizika (např. formou jeho transferu nebo redukce). Pokud není riziko rozpoznáno, je nevědomě zadrženo. V těchto případech organizace nikterak neřeší důsledky možných ztrát, jelikož si jejich vznik ani neuvědomuje. Retence rizika může být rovněž dobrovolná nebo nedobrovolná. Dobrovolná retence rizika je charakterizována rozpoznáním existence

rizika a tichým souhlasem s převzetím v něm obsažené ztráty. Rozhodnutí o dobrovolné retenci rizika je přijímáno proto, že neexistují žádné lepší varianty. Nedobrovolná retence rizik existuje tehdy, jsou-li rizika nevědomě zadržena, anebo

pokud riziko nemůže být transferováno či redukováno, případně pokud se mu nelze vyhnout.

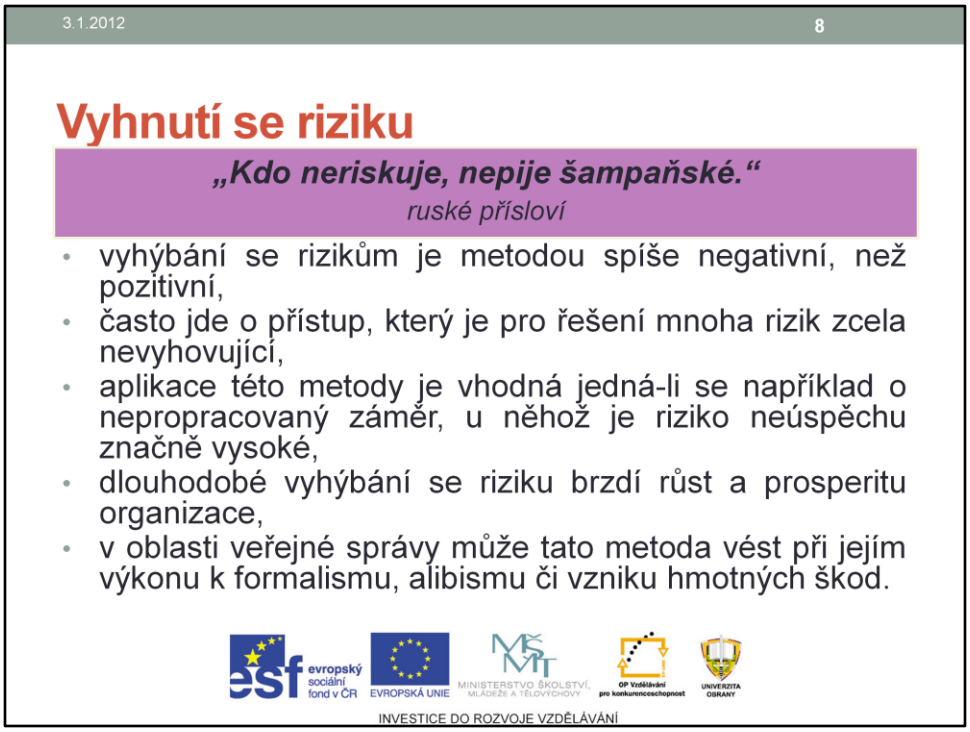
Podstoupení rizika

Činnost: Rozhodnutí o podstoupení rizika bez další akce by mělo být učiněno v závislosti na vyhodnocení rizik.

POZNÁMKA ISO/IEC 27001 4.2.1 f 2) "vědomá a věcná akceptace rizik pod podmínkou, že jasně vyhovují politikám a kritériím pro akceptaci rizik organizace" popisuje stejnou činnost.

Doporučení k realizaci:

Jestliže úroveň rizik splňuje kritéria akceptace rizik, není zapotřebí přijímat další opatření a riziko lze podstoupit.

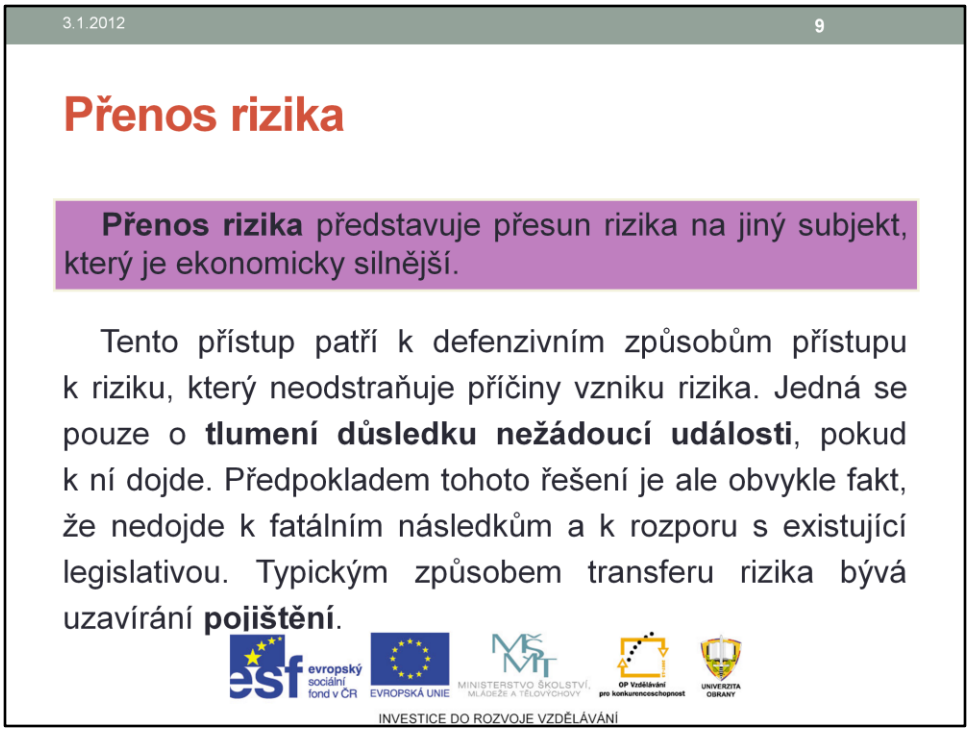


Vyhnutí se riziku

Je další možností zvládání rizik, tzn. danou aktivitu nerealizovat. Jedná se však o přístup spíše negativní než pozitivní, který je pro řešení mnoharizik zcela nevyhovující. Tento přístup je doporučován pouze v krajních případech, to znamená, pokud jsou pravděpodobnost výskytu a závažnost dopadu hrozby natolik vysoké, že není možno danou úroveň rizika akceptovat (např. nepropracovaný podnikatelský záměr, u něhož je riziko neúspěchu neúměrně velké). Činnost: Organizace by se měla vyhnout činnosti nebo podmínce, která dává riziku vzniknout.

Doporučení k realizaci:

Když jsou identifikovaná rizika považována za příliš vysoká, nebo když náklady na uplatnění jiných způsobů zvládání rizik převyšují přínosy, organizace může přijmout rozhodnutí o celkovém vyhnutí se riziku tím, že upustí od plánované nebo existující činnosti nebo souboru činností, nebo změní podmínky, za nichž tuto činnost provozuje. Například u rizik způsobených přírodou může být z hlediska nákladů nejúčinnější alternativou fyzicky odstěhovat zařízení zpracovávající informace na místo, kde toto riziko neexistuje nebo je pod kontrolou.



Přenos rizika patří mezi možnosti, pro něž je charakteristický defenzivní přístup k riziku. Jedná se o přesun rizika na jiný subjekt, který je ekonomicky silnější. Transfer rizika tak neodstraňuje příčiny vzniku nežádoucí události (např. odstranění konkurence z trhu ekonomickou či politickou silou), nýbrž se soustřeďuje pouze na tlumení jejích případných

dopadů. Za nejtypičtější příklad transferu rizika lze považovat uzavírání nejrůznějších druhů pojistek. Mezi další způsoby přesunu rizika patří např. uzavírání dlouhodobých kupních smluv za předem stanovené ceny (eliminace možného inflačního rizika jeho přesunem na prodejce), uzavírání obchodních smluv podmiňujících odběr minimálního množství zboží (snížení odbytového rizika jeho přesunem na odběratele), leasing (přesun finančního rizika, které je spojeno s vlastnictvím daného předmětu, z prodávajícího subjektu na leasingovou společnost) či odkup krátkodobých pohledávek, tzv. faktoring

(přesun rizika nezaplacení pohledávky z dodavatele na faktoringovou společnost).

Činnost: Riziko by mělo být přeneseno na jinou stranu, která může toto konkrétní riziko podle hodnocení rizik nejúčinněji zvládnout.

Doporučení k realizaci:

Přenos rizika zahrnuje rozhodnutí sdílet určitá rizika s externími stranami. Přenos rizika může vytvářet nová rizika nebo měnit existující, identifikovaná rizika. Proto může být nutné další zvládání rizik.

Přenos lze provést pojištěním, které bude pokrývat následky, nebo uzavřením smlouvy s obchodním partnerem, jehož úkolem bude monitorovat informační systém a přijmout okamžitá opatření k zastavení útoku, než bude způsobena škoda určité úrovně.

Je však nutné upozornit na to, že je možné přenést odpovědnost za zvládnutí rizika, ale obvykle není možné přenést odpovědnost za dopad. Zákazníci obvykle posuzují nepříznivý dopad jako chybu organizace.

Akceptace rizik bezpečnosti informací

Plán zvládání rizik a hodnocení zbytkových rizik v závislosti na rozhodnutí o akceptaci vedoucích pracovníků organizace.

Činnost: Měla by být učiněna a formálně zaznamenána rozhodnutí akceptovat rizika a odpovědnosti za tato rozhodnutí (toto souvisí s ISO/IEC 27001 odstavec 4.2.1 h)).

Doporučení k realizaci: Plány zvládání rizik by měly popisovat, jak se mají hodnocená rizika zvládat, aby vyhovovala kritériím akceptace rizik (viz Kritéria akceptace rizik). Pro odpovědné vedoucí pracovníky je důležité přezkoumávat a schvalovat navrhované plány zvládání rizik a výsledná zbytková rizika a zaznamenávat všechny podmínky spojené s tímto schvalováním. Kritéria akceptace rizik mohou být komplexnější, než aby jen určovala, zda zbytkové riziko spadá nebo nespadá nad nebo pod určitou prahovou úroveň. V některých případech nemusí úroveň zbytkového rizika vyhovovat kritériím akceptace rizik, protože uplatňovaná kritéria neberou v úvahu převažující okolnosti. Například lze argumentovat tím, že je nutné akceptovat rizika, protože

přínosy doprovázející rizika jsou velmi atraktivní, anebo protože náklady na redukci rizik jsou příliš vysoké. Tyto okolnosti naznačují, že jsou kritéria akceptace rizik nepřiměřená a měla by byt revidována, je-li to možné. Avšak pokaždé není možné revidovat kritéria akceptace rizik včas. V takových případech ti, co rozhodují, mohou být nuceni akceptovat rizika, která nesplňují běžná kritéria akceptace. Je-li toto nutné, ti, co rozhodují, by měli j explicitně uvést komentář k těmto rizikům s odůvodněním pro svoje rozhodnutí o tom, že na běžná kritéria akceptace' rizik nedbali.

Výstup: Seznam akceptovaných rizik s odůvodněním pro ta, která nesplňují běžná kritéria akceptace rizik organizace.

Závěr

Dodržování základních zásad řízení rizik bezpečnosti informací přispívá ke:

- zkvalitnění ISMS v organizaci a to na všech stupních řízení
- vytváření prostředí pro zajištění ochrany informací, informovanosti řídících výkonných struktur a jejich uvědomění o nutnosti předcházet nežádoucímu dopadu rizik souvisejících s plněním stanovených úkolů při zajišťování schválených záměrů a cílů organizace.
- podpoře kultury tohoto prostředí

Dotazy?

pplk. Ing. Radek Dubec, Ph.D.
Univerzita obrany, Fakulta ekonomiky a managementu
Katedra celoživotního vzdělávání
E-mail.: radek.dubec@unob.cz

Dotazy?