Informační aktiva a rizika

Způsoby řešení definovaných problémů

část II.

Z minula víme, jaké problémy provázejí organizace se zavedeným řízením informačních aktiv a rizik. Dosud jsme však nedostali uspokojivou odpověď na otázku, zda a jak je možné tyto problémy řešit. V této části seriálu se proto podíváme na možná řešení dříve jmenovaných problémů.

IT rizika informační aktiva kontrolní opatření GRC

V minulém dílu jsme si představili běžné problémy spojené s řízením informačních aktiv a rizik, s nimiž jsme se v naší praxi setkali. Mezi ty nejčastější patří:

- chybějící nebo nevhodně navržená metodika pro řízení rizik,
- nezohlednění hodnoty aktiv a efektivity kontrolních opatření,
- generalizace soupisu informačních aktiv,
- chybějící agregační bod a nesdílení informací v organizaci,
- práce s neaktuálními informacemi,
- chybějící křížové odkazy mezi primárními a podpůrnými aktivy,
- automatizovaný reporting a zohledňování trendů při vyhodnocování rizik.

Všechny zde uvedené problémy se vyznačují několika málo společnými znaky: vysoké personální nároky, závislost na aktuálních datech a nejednoznačné definice. Pro čtenáře je nutné podotknout, že jak jsou některé nedostatky propojené mezi sebou, jsou často i jejich řešení úzce svázána, přičemž my jsme ta vhodná identifikovali při řešení reálných zákaznických projektů.

Vypořádání se s problémy

Organizace, které již řízení informačních aktiv a rizik mají zavedeno a potýkají se s alespoň některým z výše definovaných problémů, obvykle nemají dostatek lidských zdrojů nebo nejsou ve svých procesech dostatečně efektivní. Pro zlepšení tohoto stavu nemají příliš na výběr. Mohou buď zvýšit počet zaměstnanců, které alokují na činnosti s tímto spojené (obvykle se jedná aktualizaci tabulek, které obsahují stěžejní informace), nebo zavést IS, který umožní zaměstnancům vykonávat jejich práci efektivněji. Který z těchto přístupů však bude fungovat lépe při řešení jednotlivých problémů?

Konzistentní metodika procesu řízení informačních aktiv a rizik

Základem dobře fungujícího procesu je jeho dokumentace, která zahrnuje mimo jiné i metodiku výpočtu hodnoty rizik, tvorbu plánu zvládání rizik a další dílčí prvky. Tyto metodiky, dokumenty a procesy lze následně integrovat do tzv. GRC systémů (viz Box 1).

Přestože současné GRC IS již mají vestavěný proces řízení informačních aktiv a rizik, není ho téměř nikdy možné přejmout a přímo zavést v organizaci. Příčinou může být např. atypická organizační struktura. Do procesu je nutné

zapojit zaměstnance, který je v této oblasti zběhlý. Výhodou bývá, když zaměstnanec zná interní prostředí a procesy organizace, díky čemuž dokáže metodiku vhodně uzpůsobit. Pro organizaci je také přínosné, pokud vytvářená metodika reflektuje i vyhovující části integrovaných procesů vyskytujících se v GRC IS. V několika implementacích se jako žádoucí ukázalo integrovat do metodiky i vlastní inovativní myšlenky.

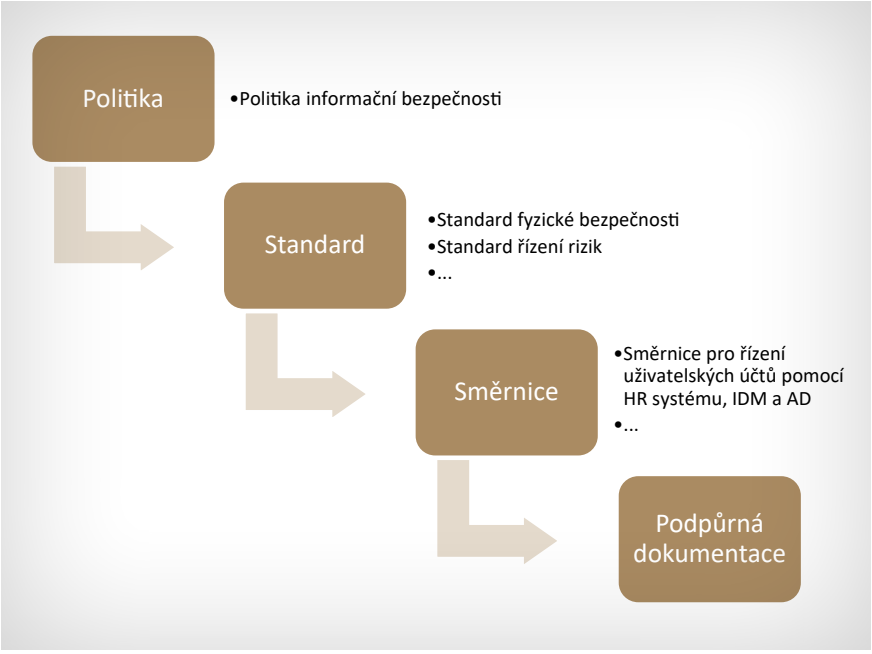
Při našich implementacích se nejvíce osvědčila bezpečnostní dokumentace, a to včetně částí týkajících se řízení informačních aktiv a rizik. Má čtyři úrovně: Politika bezpečnosti, Standardy bezpečnosti pro jednotlivé zájmové oblasti, Implementační směrnice, Doplňující materiály (viz Obr. 1). Účelem rozdělení je na první úrovni definovat celkový rozsah rámce bezpečnosti, na druhé úrovni ustanovit požadavky bezpečnosti v každé oblasti zájmu a na třetí úrovni popsat jejich naplnění. Čtvrtá, doplňující úroveň má obsahovat např. vzorové formuláře a další nutné materiály pro podporu bezpečnostních procesů. Takto vytvořená, komplexní a úplná bezpečnostní dokumentace poskytne kvalitní základ pro jakýkoli GRC systém.

Dosaženým výsledkem je konzistentní metodika definující všechny důležité pojmy, např. inherentní a reziduální riziko, primární a podpůrná aktiva, vzorce a stupnice pro výpočet rizik, způsoby zvládání rizik a tvorby plánu zvládání rizik, zodpovědné osoby za jednotlivé části procesu řízení informačních aktiv a rizik. Klíčové položky pro tuto část: zkušený zaměstnanec, schopnost nechat se inspirovat zavedenými procesy v IS a otevřenost k inovaci. GRC systémy zde tvoří pouze podpůrnou složku.

[1] S tématem GRC jsme vás poprvé seznámili v článku nazvaném „Informační bezpečnost a problematika GRC“, který napsal Pavel Krátký pro DSM 4/2016.

Definice pojmů informace a dokument BOX 1

Už v roce 2007 byl jako součást vědecké studie definován pojem GRC, tedy Governance, Risk & Compliance[1] (česky správa, riziko a soulad), který byl následně publikován v časopise International Journal of Disclosure and Governance [1]. Tuto definici lze parafrázovat slovy: „Jedná se o soubor schopností, díky kterým je organizace schopná efektivně dosáhnout stanovených cílů, uceleně čelit rizikům a nejistotě.“ Nástroj, který toto podporuje, můžeme označit za GRC IS.



Obr. 1: Rozdělení bezpečnostní dokumentace dle jednotlivých úrovní

Hodnocení aktiv a efektivity kontrolních opatření

Hodnocení primárních a podpůrných aktiv a efektivity zavedených či plánovaných kontrolních opatření je prvním krokem k úspěšnému zavedení GRC řešení. Díky inovativnímu přístupu by model řízení rizik měl mimo jiné začlenit hodnotu aktiva do výpočtu rizik. Výpočet musí rozlišit uplatnění hrozby (např. odposlech), pokud se týká informačních aktiv s nízkou důvěrností (např. interní údaje) potažmo hodnotou anebo vysokou důvěrností (např. osobní údaje). Hodnota rizika v takových případech musí jasně demonstrovat, že prioritní ochranu si zaslouží údaje s vyšším stupněm důvěrnosti. Obdobně musí metodika popisovat zohlednění míry implementace jednotlivých kontrolních opatření a jejich příspěvek ke zmírnění rizik, což slouží k výpočtu reziduálních rizik. Best practise při výpočtech klade důraz i na bezpečnostní incidenty, které se v prostředí organizace vyskytly a mohly ovlivnit rizika dodatečně. GRC IS a modely v nich navržené reflektují tyto principy, ale v konečném důsledku to bude zaměstnanec, kdo ucelenou metodiku vytvoří.

Ukázku našeho způsobu hodnocení efektivity implementace kontrolního opatření „Public Key Infrastructure“ lze vidět v Tab. 1. Při tomto vzorovém vyplnění je vidět, že celé opatření je děleno do tří dále rozpracovaných částí: Dokumentace, Implementace a Monitorování/Vyhodnocování. Organizace musí u každého z dílčích bodů určit, zda je interně zaveden. Stejným způsobem jsou ohodnocena všechna opatření a jejich hodnoty jsou reflektovány v analýze rizik, kde alikvotně mitigují rizika k nim navázaných hrozeb.

Název kontrolního opatření	Zavedeno?	Míra implementace (%)
Public Key Infrastructure		55,00
Dokumentace		
■ součást bezpečnostní dokumentace (politika, standard, směrnice)	ANO	10,00
■ postupy zahrnují práci s interními i externími certifikáty	NE	0,00
Implementace		
■ serverové certifikáty pro zabezpečení komunikace	ANO	10,00
■ uživatelské certifikáty pro šifrování dat a emailové komunikace	NE	0,00
■ je používán software pro správu certifikátů	NE	0,00
■ kořenový certifikát je schvalovaný bezpečnostním výborem	ANO	10,00
■ je zavedena evidence „veřejně podepsaných certifikátů“	ANO	10,00
■ zabezpečení přístupů do prostřední organizace skrze VPN	ANO	10,00
Monitorování/vyhodnocování		
■ generování certifikátů je logováno (SIEM)	ANO	5,00
■ použití kořenového certifikátu pro potřeby podepisování je monitorováno	NE	0,00
■ expirace certifikátu je sledována	NE	0,00
■ únik privátního klíče kořenového a intermediate certifikátů je evidován jako incident	NE	0,00

Tab. 1: Ukázka hodnocení efektivity kontrolního opatření nazvaného PKI

Seznam konkrétních podpůrných informačních aktiv

Jak již bylo zmíněno v minulém dílu seriálu, generalizace vede k nepřesnostem při výpočtu rizik, tudíž je smysluplné udržovat soupis konkrétních podpůrných aktiv. Jedná se zejména o konkrétní lokality, hardware, software a informační aktiva, jejichž možným ohrožením se řízení rizik zaobírá. Optikou řízení rizik se tedy jedná spíše o prerekvizitu, která musí být splněna, než je možné analýzy provádět.

Důležitým aspektem při identifikaci konkrétních informačních aktiv je kvalita zdrojových dat. V malých organizacích nebo start-upech lze počítat konkrétní aktiva v řádech desítek až stovek, oproti tomu velké organizace si nevystačí ani s desítkami tisíc záznamů. Největší rozdíl odvíjející se od velikosti organizace lze nalézt v používání systémů na ukládání záznamů o konkrétních aktivech. Menší organizace buď evidenci postrádají, nebo ji udržují v jednoduché formě. Velké společnosti používají nástroje pro správu aktiv, např. pro potřeby řízení provozu či audit. Ať už se jedná

o kteroukoli situaci, je nutné zajistit vznik takové evidence spolu s možností její integrace do procesu řízení rizik (ať už manuální nebo automatizované), protože neaktualizovaná nebo zavádějící data ve zdrojových systémech následnou analýzu rizik zkreslí obdobně jako generalizovaná aktiva.

V dříve zmíněné metodice jsou popsány informace, které musejí zdrojová data obsahovat z pohledu řízení informačních aktiv a rizik, stejně tak způsoby integrace do tohoto procesu. Klíčová jsou tedy kvalitní data ve zdrojových systémech, která ovlivňují primárně zaměstnanci, a možnosti integrace těchto systémů s nástrojem GRC.

Agregace a sdílení informací

V návaznosti na předchozí odstavec je nutné zmínit, že zdrojová data nutná pro provádění uceleného procesu řízení informačních aktiv a rizik jsou obvykle roztroušena ve více organizačních jednotkách. Je proto výhodnější exportovat data z jejich systémů manuálně do tabulek a následně je spojovat? Nebo zdrojové IS (např. CMDB[2]) integrovat s GRC nástrojem napřímo? Již samotná první varianta se zdá být pro potřeby agregace dat dostačující. Pokud však mají mít k takto vytvořeným tabulkám (nebo z nich vypočítaným hodnotám) přístup zaměstnanci z různých oddělení, je nutné zvážit problém se sdíleným přístupem k dokumentům, který lépe řeší IS než pouhé kopírování tabulek. Velké organizace tím jednoduše vyřeší dva problémy současně.

Naše doporučení pro řízení přístupů k záznamům obsaženým v GRC IS je skrze RBAC[3], které vychází z definovaných rolí pro jednotlivé činnosti prováděné v nástroji a jejich následné přiřazení jednotlivcům nebo týmům s danou kompetencí. Zde se může jednat o klasická CRUD[4] oprávnění – vytvořit, číst, upravit, smazat. Při návrhu této struktury dále doporučujeme zohlednit stávající procesy a jejich případnou úpravu. Mezi prvními dokumenty, které vznikají ještě před samotnou implementací systému, musí být vytvořen soupis rolí, jejich oprávnění a procesů, do nichž budou vstupovat. Podcenění této fáze mívá fatální následky v závěru implementačních projektů. Toto základní řízení přístupů je vhodné obohatit o dílčí řízení na úrovni jednotlivých záznamů (viz dále).

[2] CMDB – Configuration Management Database
[3] RBAC – Role Based Access Control
[4] CRUD – Create, Read, Update, Delete

Obr. 2: Pilíře úspěšného řízení informačních aktiv a rizik

Udržování aktuálních dat

Dílčím problémem, který je úzce spjatý s agregováním a sdílením informací, je udržování aktuálních informací. Jak často bude docházet k aktualizaci dat v tabulkách nebo v IS, je zde stěžejní. Pravidelnou aktualizaci na měsíční (nebo delší) bázi je možné provádět v obou přístupech bez znatelných dopadů na zdroje. Zohledníme-li i fakt, že některé informace, např. seznamy zaměstnanců a jejich přístupová oprávnění k datům, je vhodné či přímo nutné aktualizovat častěji (optimálně na denní bázi), zjistíme, že manuální aktualizace není dostatečně efektivní a přináší vysoké nároky na školené zaměstnance. Při řešení tohoto problému vyhrávají pravidelné automatické aktualizace dat prováděné GRC IS při integraci se zdrojovými systémy nebo jejich databázemi nad přístupem vyžadujícím lidské zdroje.

Spojením zde předložených faktů s informacemi z předchozího odstavce docházíme k závěru, že spoléhat se na manuální agregaci a sdílení dat nemůže být z dlouhodobého hlediska efektivní. Na základě tohoto závěru se zavedení GRC nástroje jeví jako nejvhodnější alternativa. Při vytváření importů pro jednotlivé typy dat se můžete setkat s problémem, kdy kvůli povaze dat je nebude možné nahrát všechna najednou, ale bude nutné je nahrávat po částech. Typickým příkladem je organizační struktura, kde může být nutné nahrávat jednotlivé úrovně postupně. V těchto případech musíme dbát na přípravu vstupních dat, která je potřeba do těchto úrovní rozčlenit. Úvodní dělení navrhujeme provést manuálně pro snazší odstranění chyb. Poté, co jste si jisti výslednou strukturou importovaných dat, doporučujeme jednotlivé kroky transformace nascriptovat tak, aby nemusely být prováděny manuálně.

Křížové odkazy mezi informačními aktivy

Významným přínosem při řízení informačních aktiv a rizik jsou křížové odkazy, které určují provázanost různých typů aktiv mezi sebou. Využití nacházejí nejen při mapování primárních aktiv (např. business procesů) na aktiva podpůrná, ale i v jiných situacích, jako je např. identifikace podpůrných aktiv (softwaru a informací), které využívají hardware těch výrobců, kteří již nejsou pro organizaci důvěryhodní. Bez křížových odkazů je taková identifikace téměř nemožná.

Na tvorbě křížových odkazů se vždy musejí podílet zaměstnanci, kteří chápou vazby mezi informačními aktivy a dokážou je jasně definovat. Pokud se organizace rozhodne využívat tabulkového procesoru s jednoznačnými (obvykle číselnými) identifikátory záznamů, nebude pro běžného uživatele vůbec snadné takové vazby číst a chápat. GRC IS disponují širokou paletou možností zobrazení jednotlivých vazeb. Díky křížovým odkazům je navíc možné obohatit způsob řízení přístupů k jednotlivým záznamům o speciální případy, kdy např. auditor je i správcem některých aktiv. Zatímco roli „Auditor“ má obvykle přiřazenou díky své pracovní náplni a vyplývá z RBAC, role „správce aktiva“ je v pojetí GRC chápána jako vazba mezi ním (zaměstnancem) a určitým aktivem. GRC systémy však umožňují spravovat i přístupy na úrovni těchto vazeb, a tak je možné zaměstnancům bez ohledu na jejich role udělit oprávnění pro správu jim přiřazených aktiv. Kombinací obou těchto přístupů je možné zaměstnancům poskytnout plnohodnotné přístupy, díky nimž budou schopni vykonávat činnosti spadající pod obě tyto role.

Reporting, workflow a sledování trendů

Mezi nejdůležitější výstupy, které řízení informačních aktiv a rizik poskytují, patří plán zvládání rizik a reporting, jež lze v obou případech generovat stejně efektivně za pomoci vestavěných funkcí. Tabulky však zaostávají za GRC nástroji co do možností sledování trendů nebo integrace workflow.

GRC nástroje využívají schvalovacích workflow nebo notifikací pro podporu vnitrofiremní spolupráce při řízení informačních aktiv a rizik. Sledování dlouhodobých trendů pro vyhodnocování efektivity celého řízení je pro GRC IS rovněž snadné. Informační systém může obsahovat i více hodnot (např. historických) u jednoho záznamu aktiva, které mohou být použity ke generování trendů. Ukládání historických hodnot v tabulkách obvykle vede k tvorbě duplicit. Ve všech aspektech zde vítězí GRC IS nad tabulkovou konkurencí.

Klíčové pilíře

Které body jsou pro efektivní řízení informačních aktiv a rizik stěžejní? Z článku vyplývá, že zaměření pouze na implementaci GRC nástroje kýžené výsledky nepřinese, jelikož je problematika poněkud komplexnější. Moderní řízení informačních aktiv a rizik se musí opírat o tři základní pilíře (viz Obr. 2):

- dokumentaci a procesy,
- kvalitní vstupní data,
- správně implementovaný GRC IS.

První a druhý bod stojí a padá s kvalitou a počtem zaměstnanců, kteří dokumentaci, procesy a data připravují, jak je nastíněno v popisu prvních tří problémů výše. Třetí pilíř spojený s implementací GRC IS lépe pokryje zbývající problémy. GRC IS, který zohlední dokumentaci a integruje data ze zdrojových systémů, proces řízení informačních aktiv a rizik jednak zrychlí, ale i zefektivní a managementu organizace přinese výstupy nutné pro strategické rozhodování v krátkém čase. Tyto tři body by proto měly sloužit každé organizaci k posouzení aktuálního stavu a k vyhodnocení, se kterými problémy se potýká, a tudíž které pilíře potřebuje vyztužit.

Závěrem

V návaznosti na první díl, kde jsme definovali problémy spjaté s řízením informačních aktiv a rizik, jsme určili způsob, jakým se s nimi vypořádat. Zkvalitnění výstupů z procesu řízení informačních aktiv a rizik je možné, a to i bez obrovských investic do dedikovaného softwaru. Bylo by však naivní si myslet, že investicí pouze do dvou pilířů odstraníme všechny problémy.

Finální doporučení tedy zní provést menší investici do revize dokumentace, procesů a vstupních dat, která umožní identifikovat a opravit slabá místa. Až následně zvažovat implementaci GRC IS, jež bude mít díky tomu hladší průběh a organizaci přinese zejména sdílení informací pro strategické i operativní rozhodování nad aktuálními daty, částečnou nebo úplnou automatizaci řídících procesů, ověřování klíčových procesů a dat díky integrovaným workflows. Nyní si již každá organizace dokáže zodpovědět otázku, zda je pro ni GRC IS vhodnou investicí a který z pilířů potřebuje renovaci.

Miroslav Buda
Miroslav.Buda@aec.cz

Mgr. Miroslav Buda

Specialista bezpečnosti se zaměřením na procesy informační bezpečnosti a zavádění nástrojů pro podporu GRC ve společnosti AEC a. s. V současné době se účastní i projektů implementace procesů souvisejících s bezpečností vývoje.

POUŽITÉ ZDROJE

[1] MITCHELL, SCOTT, L. GRC360: A framework to help organisations drive principled performance. International Journal of Disclosure and Governance. 2007. ISSN 1741-3591.