Problémy spjaté s řízením informačních aktiv a rizik

část I.

Považujete ve své organizaci řízení informačních aktiv a rizik spíše za přítěž a nutné zlo než za reálný přínos? A zamýšleli jste se nad tím proč? První díl tohoto seriálu poukáže na možné důvody, proč vaše organizace stejně jako spousta dalších nedokáže z procesu řízení rizik vytěžit více.

Zrod

Zjednodušenou optikou je možné na zvýšení informační bezpečnosti nahlížet prostřednictvím zvládání rizik. Z tohoto důvodu je řízení rizik nedílnou součástí rozvoje bezpečnosti v organizaci. Požadavek na implementaci rámce pro řízení informačních aktiv nebo rizik může vyplývat ze samotného zájmu o budování informační bezpečnosti nebo ze závazných požadavků platné legislativy. Mezi tuto legislativu v kontextu České republiky řadíme Nařízení (EU) 2016/679 [1] a Směrnici (EU) 2015/2366, která se vztahuje na všechny druhy služeb elektronických plateb [2]. Dále pak Zákon o kybernetické bezpečnosti [3] spolu s navazující Vyhláškou o kybernetické bezpečnosti [4] vyznačující se menším rozsahem působnosti v počtu subjektů jim podléhajících.

Zmíněnou legislativu však mohou využívat i subjekty, pro které není závazná. V takovém případě je pravděpodobně největším motivem zlepšení úrovně informační bezpečnosti v organizaci. Pro získání širšího rozhledu se pak oba dva typy organizací (přímo podléhající i dobrovolně implementující požadavky legislativy) snaží využívat i další zdroje, např. normu ISO/IEC 27001 [5] nebo Obecné pokyny k bezpečnostním opatřením vydané Evropským orgánem pro bankovnictví [6] aj., díky kterým se snaží v problematice bezpečnosti informací lépe zorientovat.

Organizační nedostatky

Řízení rizik je pro organizace jednou z hlavních oblastí stanovených zmíněnou legislativou. Jako takové musí být podpořeno vhodným procesem správy informačních aktiv tak, aby byla zajištěna jeho úplnost. Kde však organizace často tápou, je zavádění interní metodiky pro tyto procesy, kdy je buď nedostatečně, nebo zcela nevhodně navržena. Při práci na projektech se v zákaznické dokumentaci často setkáváme s nepřesnou interpretací pojmů hrozba vs. riziko nebo nevhodným modelem ohodnocení rizik, který jen zřídka zohledňuje identifikované bezpečnostní incidenty či vlastníky informačních aktiv a rizik [7].

Dalším námi identifikovaným nedostatkem bývá nedostatečná práce s přesahy procesů, které spojují řadu různorodých oblastí a agend v rámci organizace s řízením informačních rizik, viz Obr. 1. Samotné zdroje dat pro analýzu aktiv jsou často roztroušené ve více organizačních jednotkách, protože

každá potřebuje pro svou práci specifickou část zpracovávaných informací. V organizacích tak většinou neexistuje jednotná evidence, kam by zaměstnanci jednotlivých oddělení přistupovali, ale spíše si každé oddělení drží svůj vlastní seznam aktiv (nebo jeho část), se kterým více či méně pravidelně pracuje. Mezi agendami však existují přesahy. Příkladem mohou být např. normy a regulace identifikované na právním oddělení ovlivňující interní směrnice spolu s oddělením interního auditu aj. Vždy je důležité tyto průniky zvažovat, aby opomenutí některého z nich nezapříčinilo vznik dalšího rizika, ale také proto, abychom harmonizací jednotlivých činností zvýšili přidanou hodnotu získanou z analýzy rizik.

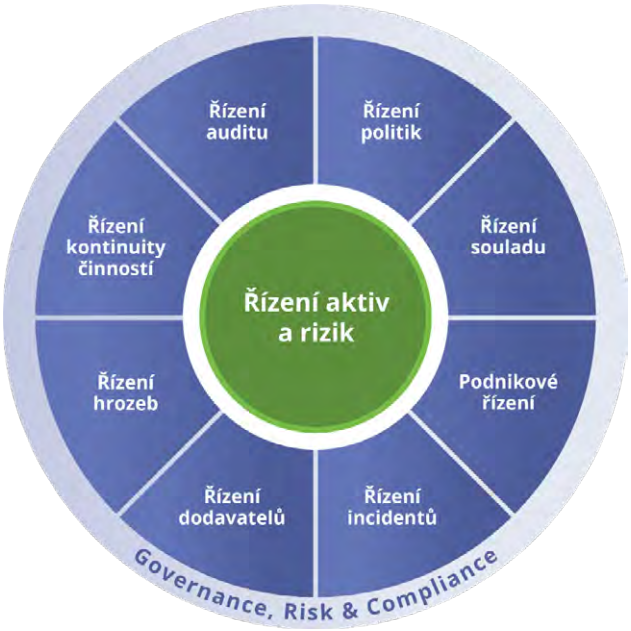
Konkrétní příklad, kdy zákazník při propojení řízení rizik s jinou agendou pochybil, jsme identifikovali minulý rok. Klient měl velmi propracovaný proces interního auditu, který mu pomáhal v dodržování souladu s interními a externími předpisy. Zjištěné auditní nálezy však nebyly agregovány s kontrolními opatřeními, čímž nebylo dosaženo kýženého zmírnění rizik. Důsledkem bylo špatné určení priorit při řešení auditních nálezů a prodloužení doby zvládání nejzávažnějších rizik. V některých případech až na dvojnásobek.

Práci s neaktuálními daty je potřeba zmínit jako další vážný a častý prohřešek. Jedná se zejména o identifikaci nových zranitelností a úpravu rizik při zavádění nových řídicích a kontrolních opatření. Problém může být i v nepravidelné aktualizaci seznamu aktiv vůči seznamu aktivních prvků infrastruktury často označovaném jako konfigurační databáze. Tyto neaktuální informace následně mohou vést k nepřesnostem při hodnocení rizik. Na neaktuální stav hodnocení informačních aktiv a rizik obvykle narážejí klienti ve chvíli, kdy pro jejich výpočet používají zřídka aktualizované tabulky. V momentě, kdy data nejsou pravidelně aktualizována, dochází v lepším případě k nepřesnému určení hodnoty aktiva nebo dopadu a pravděpodobnosti hrozby, v tom horším pak k úplnému opomenutí, nerelevantnímu vypuštění nebo nadbytečnému zařazení některých aktiv nebo rizik. Důsledkem pro organizaci může být zaměření se na nepodstatná rizika a naopak neřešení významných hrozeb.

U jednoho zákazníka jsme díky aktualizaci analýzy rizik byli schopni upravit plán rozvoje bezpečnosti. Bez této úpravy by došlo k milionovým investicím do oblasti fyzické bezpečnosti při zavádění dvoufaktorové autentizace. Uvedená cena odpovídala konkrétní implementaci systému pro ověřování otisků prstů při fyzickém přístupu do budov a serveroven a také faktu, že daný klient zaměstnával tisíce zaměstnanců a spravoval stovky objektů po celé republice. Aktualizací dat v analýze rizik však bylo zjištěno, že business procesy nemají adekvátně stanoveny parametry dostupnosti, což se projevilo nárůstem rizika v oblasti zálohování. Plán rozvoje bezpečnosti byl následně upraven tak, aby tuto aktualizaci reflektoval a organizace se mohla v upraveném plánu soustředit na zlepšení procesu zálohování business procesů namísto fyzické bezpečnosti a smysluplně vynaložit peníze pro rozvoj bezpečnosti.

Prohřešky v procesech řízení aktiv a rizik

Pro informační aktiva a proces jejich řízení jsou typická zjednodušení ve formě generalizace. Nedbá se příliš na konkrétní soupis všech aktiv (instancí) v organizaci, ale pouze na výčet obecných typů se stejnými vlastnostmi, např. servery, pracovní stanice, soubory aj. Toto zjednodušení má pak výrazné dopady na analýzu rizik, kde se v jeho detailnější variantě hodnoty rizika mohou měnit dle umístění serverů nebo uložení informací. Oproti tomu v generalizovaném soupisu aktiv se pracuje s obecnými typy aktiv, kde je však tyto drobné



Obr. 1: Přesahy řízení informačních aktiv a rizik do ostatních procesů informační bezpečnosti

nuance mnohem těžší až nemožné zohlednit. Na zpracované analýze rizik se tento nedostatek v praxi projevuje tak, že generalizovaná podpůrná informační aktiva jsou hodnocena na vysokým stupněm hodnoty aktiva, protože se v databázích i na serverech zpracovávají ty nejcitlivější informace. Důsledkem toho, že při generalizaci není možné oddělit ta nejdůležitější podpůrná aktiva od těch méně důležitých, bývají výsledné hodnoty rizik podpůrných aktiv vyšší, než by tomu bylo při detailnějším rozdělení. Organizaci tudíž může na první pohled připadat, že se rizikům nevěnuje dostatečně.

Vazby mezi primárními a podpůrnými aktivy jsou v organizacích jen zřídka evidovány. Tím se však organizace ochuzují o značnou část přidané hodnoty, kterou jim analýza rizik

může poskytnout. Ohodnocení rizika nedostupnosti procesů se vždy skládá z pravděpodobnosti nedostupnosti jednotlivých prvků, které proces využívá. Bez těchto identifikovaných vazeb jsme nemohli poradit jednomu ze zákazníků se zálohováním jeho systémů. Zmíněný zákazník měl popsané business procesy spolu s jejich důležitostí a maximální dobou výpadku. Také jeho konfigurační databáze obsahovala záznamy o prvcích infrastruktury. Bohužel však neexistovaly křížové odkazy, které by obě dvě složky propojily, důsledkem čehož nebylo možné přenést maximální dobu výpadku z procesů na podpůrná aktiva a určit tak vhodná opatření pro zmírnění rizika výpadku procesu. Zákazníka stálo udržování záloh a rozsáhlé záložní cloudové infrastruktury stovky tisíc korun měsíčně, které mohl ušetřit, pokud by identifikoval vazby mezi business procesy a podpůrnými aktivy.

Stejně jako u posuzování informačních aktiv dochází také u vyhodnocování rizik u organizací k jistým prohřeškům. Příkladem takového prohřešku může být situace, kdy nejsou rozlišována inherentní, residuální a operační rizika a je sledována pouze jedna obecná hodnota rizika [8]. Tím, že tato rizika nejsou oddělena a není k nim přistupováno individuálně, dochází následně při identifikaci těch největších rizik a jejich zvládání k značným nepřesnostem. Stejný efekt pak může mít i ignorování hodnoty aktiva při výpočtu rizik, jehož důsledkem bývá situace, kdy se organizace snaží o snižování i těch nejméně významných rizik místo toho, aby se soustředila na hrozby ohrožující nejcennější aktiva. Obojí vede k nepřesným hodnotám rizik a organizace pak nesnižuje rizika, která jí mohou způsobit největší škody, a plýtvá zdroji na zavádění řídicích a kontrolních opatření v nepodstatných oblastech.

Se zaznamenáváním změn rizik v čase nemívají organizace velký problém. Ten přichází až ve chvíli, kdy je nutné porovnat vývoj rizik v čase a měřit efektivitu zaváděných řídicích a kontrolních opatření na snižování rizik. Prezentační možnosti tabulkových procesorů nebývají pro potřeby managementu dostatečné a vyžadují další manuální zásahy. Čím dál častěji se setkáváme s požadavky zákazníků na detailní sledování trendů a automatické reportování informačních rizik, které však nejsme schopni zajistit bez sofistikovanějšího nástroje, než je tabulkový procesor.

Shrnutí

Řízení informačních aktiv a rizik jsou nedílnou součástí fungování organizace. Jejich správné uchopení je z hlediska efektivity a přesnosti celého procesu zcela nezbytné. Představené problémy v oblasti řízení informačních rizik, které vyplývají z našich zkušeností na zákaznických projektech, je možné shrnout jako:

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

Pokud jsou alespoň některé z předešlých popsaných problémů relevantní i pro vaši organizaci, ale nevíte, jakým způsobem je možné se s nimi vypořádat, věnujte pozornost druhému dílu tohoto seriálu, ve kterém se budeme možnými způsoby jejich řešení zabývat.

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] Evropský parlament. 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)*.
[2] Evropský parlament. Směrnice evropského parlamentu a rady (EU) 2015/2366 ze dne 25. listopadu 2015 *o platebních službách na vnitřním trhu*.
[3] Česko. Zákon č. 181/2014 Sb., ze dne 23. července 2014, *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*.
[4] Česko. Vyhláška č. 82/2018 Sb., ze dne 21. května 2018, *Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)*.
[5] ČSN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.
[6] European Banking Authority. *Obecné pokyny k bezpečnostním opatřením v souvislosti s operačními a bezpečnostními riziky platebních služeb podle směrnice (EU) 2015/2366 (PSD2)*. [online], 2018, [cit. 24. 10. 2018]. Dostupné z: https://www.eba.europa.eu/ documents/10180/2081899/Guidelines%20on%20the%20security%20measures%20under%20PSD2%20(EBA-GL-2017-17)_CS.pdf
[7] PODUŠKA, Jan. *Logické kroky k analýze rizik ve výrobních podnicích*. Digital Economy World. 2016, 2, 11-13. ISSN 2464-5303.
[8] MICHÁLEK, Richard. *Jak na rizika – Řízení rizik neunikneme – část I.* Data Security Management. 2018, 1, 14-17. ISSN 2336-6745.