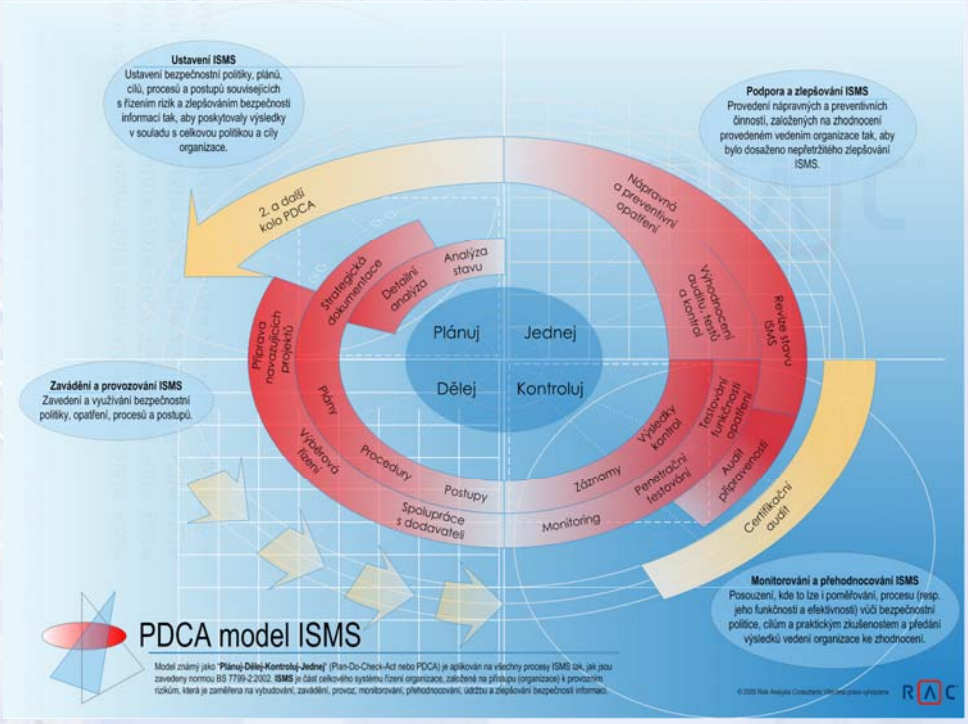
ISMS v malých a středních firmách

1.díl Plan - Plánuj

Zásady budování a využívání systému řízení bezpečnosti informací (ISMS – Information Security Management System) stanovené dnes platnými a v českém jazyce dostupnými normami (tj. ISO/IEC 17799:2005 a ISO/IEC 27001:2005) se dají interpretovat různými způsoby v závislosti na velikosti organizace. Jejich podstata však zůstává stejná – informační bezpečnost musí být řízena. Velikost organizace a rozsáhlost jejího systému jsou jedním ze základních parametrů při určování způsobu zavádění ISMS. Tento čtyřdílný seriál popisuje kroky zavádění a využívání ISMS podle modelu Plánuj – Dělej – Kontroluj – Jednej - (PDCA - procesní diagram používaný ISO 27001). První část srovnává, podle velikosti firmy, činnosti v zřejmě nejtěžším kroku Plánuj (Plan), o dalších krocích pojednávají následující díly.

Zavedení ISMS

Doporučení, zda zavést ISMS, zní pro všechny organizace **jednoznačně *ANO*** a otázka jejich velikosti je irelevantní. ISMS lze zavést a používat v organizaci s deseti pracovníky, a stejně tak i v obřím holdingu, kde se každý den můžete potkat s tisíci zaměstnanci. Zjednodušeně lze říci, že ISMS je jen jeden a to ten, který je popsán v normě ISO 27001. Interpretace a implementace jednotlivých doporučení se však může výrazně lišit podle rozsahu systému, počtu uživatelů, způsobů zpracování dat a jejich hodnoty apod. Například bezpečností politika, jako ten nejvyšší dokument o bezpečnosti informací v organizaci, může být velmi podobná pro živnostníka i pro obrovskou akciovku. Naopak tomu je o organizace bezpečnosti. Pokud se ISMS zavádí ve velké společnosti, je nutné pro tisíce uživatelů zřídit samostatné bezpečností oddělení s 5-10 lidmi, ve střední firmě na to stačí 2 pracovníci a pokud máme systém pro 10 lidí, tak jeden člověk na půl úvazku je až moc.



V tomto seriálu jsou popsány jednotlivé kroky zavádění a používání systému řízení bezpečnosti informací podle modelu PDCA (viz ISO 27001) **pro malé a střední firmy rozdílně**. I když jejich dělení může být občas složité, jsou pro tento účel definovány podle počtu zaměstnanců (do 15/do 150) a úrovní vedení (1-2/3-5). I když je téma zaměřeno na malé a střední firmy, je pro více objektivní srovnání ve vybraných případech popsána také situace ve velkých společnostech.

Strategie bezpečnosti

Strategie bezpečnosti nebývá ve středních firmách popsána nijak detailně, jako je tomu zvykem ve velkých společnostech. Zpravidla stačí, aby ředitel středně velké organizace měl vůli řešit bezpečnostní otázky a pak není nutné sepisovat rozsáhlý dokument o koncepci řízení bezpečnosti. Je dostatečné, pokud se ředitel na své poradě s dalšími vedoucími pracovníky shodne na strategii a ta se začne prosazovat. V malých firmách je toto ještě jednodušší, protože od první úvahy ředitele je k započetí realizace stejně daleko, jako od jeho dveří k zasedací místnosti

Správná volba a způsob prosazení strategie řízení bezpečnosti není jednoduchá záležitost a už v tuto chvíli je vhodné se obrátit na odborníky, pokud tito nejsou ve vlastních řadách. Pro střední a malé firmy je však samotnou strategií už jen to, že se organizace roz-

Seriál vyšel v upravené podobě v časopise Data Security Management 03/2004 až 06/2004.

Jan Mikulecký pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 1999. Hlavní specializací je provádění analýzy rizik informačních systémů a zavádění ISMS v různých organizacích. Dále školí metodiky a standardy v oblasti bezpečnosti informací v Česku i dalších zemích Evropy. Absolvoval ČVUT v Praze, kde nyní pokračuje v doktorandském studiu.
Jan.Mikulecky@rac.cz

ISMS v malých a středních firmách

1.díl Plan - Plánuj

hodla řídit bezpečnost svých informací. Pokud se rozhodnutí rozšíří na řízení bezpečnosti v souladu se standardem ISO 27001 (definující způsob aplikace opatření z ISO 17799), je strategie vcelku rozumně nalajnována a další diskuse o tom, co a jak a kdy provádět je zbytečná, protože zavedení ISMS má své pevné zásady a postupy.

Bezpečnostní politika

Proces vytvoření a schválení *Bezpečnostní politiky* je **společný pro všechny typy organizací** včetně publikování politiky vůči všem zaměstnancům. Také rozsah a obsah dokumentu je velmi podobný. Nedávno jsme v rámci projektu zavádění ISMS tvořili bezpečnostní politiku pro velkou telekomunikační společnost (cca 3000 lidí). Souběžně jsme podobný projekt prováděli ve státní organizaci se stovkou zaměstnanců. Oba dokumenty měly strukturu podle ISO 17799 a na první pohled byly velmi podobné. Bezpečnostní politika **definuje zásady a pravidla na úrovni cílů** a ty jsou zpravidla shodné pro všechny organizace. Musí také obsahovat odkaz na dokument popisující rozsah ISMS, protože systém řízení bezpečnosti v malé ani střední firmě nemusí být zaveden pro celý informační systém (stejně jako systém řízení kvality podle ISO řady 9000).

V dokumentu by měla být popsána mj. **organizační struktura bezpečnosti**, v které se také lišily obě výše zmiňované politiky. Popis bezpečnostních rolí a jejich odpovědností musí odpovídat velikosti systému a počtu uživatelů. Navíc je nutné respektovat zavedenou organizační strukturu a proto je možné pro stejně velké společnosti použít různé modely organizace bezpečnosti.

V malých firmách nemusí být jmenován bezpečnostní ředitel na plný úvazek. Jeho kompetence zpravidla bere na sebe ředitel firmy, který prosazuje bezpečnostní zásady kombinací direktivního a osobního přístupu. Ředitel má na starosti mj. účinnou implementaci bezpečností politiky a vyhodnocování (ne analýzu) rizik a rozhodnutí o způsobu jejich pokrytí. Podobně je tomu i s dalšími bezpečnostními rolemi. Administrátor sítě má odpovědnost za praktické provedení bezpečnostních zásad a metodik, o kterých rozhodl ředitel. Některé činnosti z oblasti bezpečnostní dokumentace mohou být v kompetenci vybraného pracovníka, který může mít na starosti také audit. Kumulace práv a pravomocí souvisejících s bezpečností informací a se správou systému je pro malé organizace rizikem, které je nutné přijmout.

Podle Průzkumu informační bezpečnosti 2003, mají 3 firmy ze 4 bezpečnostní oddělení jako součást útvaru IS/IT a lze předpokládat, že spíše velké společnosti vytváří separátní tým lidí s odpovědností za oblast bezpečnosti. Pokud má systém pouze několik desítek uživatelů, je možné jednotlivé kompetence rozdělit mezi několik stávajících pracovníků nejen z IT. **Nemusí však být vždy efektivní** pro 150 lidí **jmenovat bezpečnostního ředitele na plný úvazek**. Tímto se může stát například zástupce ředitele a ne zřídka spadnou dané kompetence na vedoucího IT oddělení. Kumulace pravomocí zejména ve výkonu bezpečnosti je rizikem i pro firmu střední velikosti.

Příkladem může být projekt analýzy rizik který jsme prováděli ve společnosti s cca 80ti uživateli. Celý systém měli na starosti dva administrátoři, kteří mezi sebou sdíleli přístupová práva ke všemu. Analýza ukázala, že pochybnosti vedení o jejich loajalitě vůči firmě jsou více než oprávněné a obava z poškození systému (vymazání nebo modifikace dat) je zcela na místě. Nicméně bylo nutné jmenovat pracovníka odpovědného za výkon bezpečnosti a situace nedovolovala okamžitou výměnu obou administrátorů ani najmutí nového zaměstnance.

Řešení bylo jednoduché: bezpečnostním manažerem byl jmenován zástupce ředitele, každá hlavní aplikace (celkem měli tři) dostala svého vlastníka a při správě např. při definici uživatelských přístupových práv, bylo zavedeno tzv. „pravidlo čtyř očí“ (také známé jako „pravidlo dvou osob“). Pokud byl zakládán nový uživatel nebo měněna práva stávajícímu, bylo vyžadováno potvrzení administrátora sítě a správce aplikace. Ani jeden toto nemohl provést samostatně. Sám administrátor neměl přístup ke konkrétním datům, protože ho nepotřeboval. Je zřejmé, že původní administrátoři ztratili neomezenou vládu nad systémem a tím také možnost cokoli poškodit.

Organizace bezpečnosti v souvislosti s kumulací práva a povinností v oblasti bezpečnosti není vyřešena ani v mnoha velkých organizacích. Téměř v každé se najde jeden nebo několik „neomezených vládců systémů“, na jejichž oddanost firmě všichni spoléhají. Pro tyto situace nelze nalézt univerzální řešení a proto jsou prosazována a uplatňována různá pravidla a technologická opatření, jejichž popis je na samostatný článek.

Analýza rizik

Znalost bezpečnostních rizik je základním kamenem pro vytvoření a správně řízení ISMS. Proto provedení analýzy rizik je nutná nikoli však postačující podmínka pro všechny organizace. Rozhodnutí, zda provést detailní či jen základní analýzu, je na vedení firmy, nicméně pouze detailní analýza provedená podle vybrané metodiky může poskytnou podklady pro efektivní výběr a implementaci bezpečnostních opatření.

Risk Analysis Consultants, Španělská 2, 120 00 Praha 2, Czech Republic, tel.+420 221 628 400, fax +420 221 628 401, rac@rac.cz, www.rac.cz

ISMS v malých a středních firmách

1.díl Plan - Plánuj

Analýza musí zabrat celý rozsah ISMS a její hloubka závisí na dostupných zdrojích a požadovaných výstupech. V malé firmě lze provést detailní analýzu (například metodikou CRAMM) **za dva až tři týdny**. Je možné spolupracovat s konzultační firmou nebo vše udělat za pomoci vlastních (znalých) pracovníků. Zatížení firmy je minimální a počet respondentů nepřevýší 5 lidí. Pro hodnocení dat se vyberou 2-4 zaměstnanci, kteří nejvíce znají charakter a použití definovaných datových aktiv, a administrátor sítě provede hodnocení hrozeb a zranitelností včetně identifikace existujících protiopatření.

Detailní analýza ve středně velké organizaci trvá zpravidla **3-5 měsíců** a důvodem není ani tak rozsah, který je samozřejmě větší než u malých firem, ale rychlost odezvy od respondentů či recenzentů (schvalovatelů) výstupů z analýzy. Pro malou firmu jsou závěry shrnuty v jedné zprávě o analýze rizik, po které následuje návrh implementačního plánu. Prezentace takových závěrů je velmi rychlá a jednoduchá a odezva na ni téměř okamžitá. Ve středních firmách se projevují první známky nutné byrokracie a pro schválení závěrů je nezbytné (občas však zbytečné), aby výstupní dokumenty prošli minimálně 3 pracovníci.

Pokud je analýza prováděna dodavatelským či partnerským přístupem, jsou v týmu dva až tři **externí pracovníci** a stejný počet interních. Analýza prochází vždy napříč celou organizací a tomu odpovídá i zatížení dotčených pracovníků. Počet respondentů pro hodnocení dat se pohybuje mezi 5 až 15 uživateli a hodnocení hrozeb a zranitelností včetně zavedených protiopatření je úkolem pro 3-5 administrátorů sítě či další respondenty odpovědné za různé oblasti bezpečnosti (např. pracovník s odpovědností za fyzickou bezpečnost).

Obsah dokumentace, která je výstupem z projektu analýzy rizik, je velmi podobný pro všechny typy organizací. Liší se jen rozsahem podpůrných reportů, které jsou zpravidla výstupem z použité metodiky, ale manažerský styl zpráv o aktivech a dopadech či o analýze rizik je shodný. Pro malé firmy je možné vytvořit jen jednu zprávu, ale pro střední organizace je vhodné závěry separovat minimálně do dvou dokumentů.

Plán implementace a Prohlášení o aplikovatelnosti

Krokem logicky navazujícím na analýzu a poslední činností v části plánování podle modelu PDCA je vytvoření **Plánu implementace** a následně Prohlášení **o aplikovatelnosti (opatření)**. Bezpečnostní protiopatření by měla být vybrána na pokrytí zjištěných rizik a způsob jejich výběru je nezávislý na velikosti organizace. Jejich implementace bude rozdílná, ale například pro všechny organizace lze použít BIS-PD 3005 nebo knihovnu protiopatření CRAMM. Velký rozdíl však je ve způsobu a zejména v rychlosti jejich prosazení. Při výběru bezpečnostních opatření je vždy nutné zohlednit jejich **dopad na uživatele a na procesy organizace**. V malé firmě je možné jednouše a rychle změnit téměř jakýkoli proces, aby byl více bezpečný. Stačí vůle ředitele a o změně je rozhodnuto. Čím je organizace větší, tím je složitější měnit procesy a zavedené postupy. Proto je nutné při výběru protiopatření ve střední firmě více respektovat současný stav.

Prohlášení o aplikovatelosti (opatření) je jedním z dokumentů nutných k certifikaci. Obsahuje informace o implementovaných opatřeních normy, případně dalších protiopatřeních navržených na pokrytí rizik. Hlavním cílem je dokumentovat rozhodnutí, proč dané protiopatření bylo či nebylo vybráno k zavedení. Pokud firma neplánuje být v budoucnosti certifikována, není nutné vytvářet samostatný dokument. Pro malou i střední firmu je plně dostačující, pokud se vhodným způsobem zaznamená rozhodnutí o výběru tak, aby i za několik měsíců bylo jasné, proč není nutné určité protiopatření implementovat.

Závěr 1.dílu

Zavedení systému řízení bezpečnosti informací je správným krokem pro každou organizaci, která chce zabezpečit své informace a dostatečně řídit rizika. S ohledem na její velikost je však nutné velmi rozdílně a hlavně „s citem“ interpretovat jednotlivá doporučení normy. Úvodní, výše popsaný krok Plánuj (Plan) je v prvním průchodu modelu PDCA vždy velmi složitý a poměrně zdlouhavý, nicméně velmi důležitý.. V následujících třech dílech budou podobně srovnány činnosti v dalších krocích vedoucích k implementaci a provozu (Dělej/Do), monitorování a kontrole (Kontroluj/Check) a zlepšování ISMS (Jednej/Act) včetně následné certifikace systému řízení a dokumentů k ní nutných.

Seriál vyšel v upravené podobě v časopise Data Security Management 03/2004 až 06/2004.

Jan Mikulecký pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 1999. Hlavní specializací je provádění analýzy rizik informačních systémů a zavádění ISMS v různých organizacích. Dále školí metodiky a standardy v oblasti bezpečnosti informací v Česku i dalších zemích Evropy. Absolvoval ČVUT v Praze, kde nyní pokračuje v doktorandském studiu.
Jan.Mikulecky@rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

1.díl Plan - Plánuj

V celém seriálu jsou detailně popsané činnosti pro zavedení a provoz ISMS. Jejich souhrn pro jednotlivé kroky PDCA je uveden za každým dílem. Pro rychlé srovnání jsou popisy činností, případně výstupů, uvedeny

	Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
PLAN	**Plán / projekt bezpečnosti**	Schválení strategie/plánu pro bezpečnost	Schválení celkové koncepce bezpečnosti Schválení projektu bezpečnosti	Schválení celkové koncepce bezpečnosti Vymezení rozsahu projektu + odhad zdrojů a harmonogramu Schválení projektu bezpečnosti Analýza stavu bezpečnosti (GAP analýza)
	Bezpečnostní politika	Musí být napsána a schválena vedením Popisuje základní zásady bezpečnosti na úrovni cílů Definuje organizaci bezpečnosti, odpovědnosti a strukturu bezpečností dokumentace Obsahuje odkaz na rozsah ISMS	Musí být napsána a schválena vedením Popisuje základní zásady bezpečnosti na úrovni cílů Definuje organizaci bezpečnosti, odpovědnosti a strukturu bezpečností dokumentace Obsahuje odkaz na rozsah ISMS	Musí být napsána a schválena vedením Popisuje základní zásady bezpečnosti na úrovni cílů i strategií pro jejich dosažení včetně závazku podpory a alokace zdrojů Definuje organizaci bezpečnosti, odpovědnosti a strukturu bezpečností dokumentace Obsahuje odkaz na rozsah ISMS
	Organizace bezpečnosti	Oddělení/Odbor bezpečnosti: NE Bezp. ředitel: ředitel firmy Bezp. administrátor: administrátor IS Bezp. auditor: odpovědnost delegována na pracovníka (mimo administrátora IS)	Oddělení/Odbor bezpečnosti: ANO (pod IT) Bezp. ředitel: jmenován člen vedení Bezp. manažer: jmenováni 1-3 Bezp. auditor: pracovník interního auditu, nebo delegováno na pracovníka mimo IS Bezp. administrátoři: administrátoři částí systémů	Oddělení/Odbor bezpečnosti: ANO (v IT i mimo) Bezp. ředitel: jmenován člen vrcholového managementu Existuje oddělení bezp. s odpovědnostmi za řízení i správu všech oblastí bezpečnosti Bezp. auditor: zajišťuje oddělení interního auditu
	Analýza rizik	Nutné provést: ANO Čas: max. 1 měsíc Členové projektového týmu: jeden interní pracovník a/nebo konzultant Respondenti: max. 5 Výstupy: Zpráva o analýze rizik + Implementační plán	Nutné provést: ANO Čas: 3 - 5 měsíců Členové projektového týmu: 2-3 interní pracovníci a/nebo 2-3 konzultanti Respondenti: 5-20 Výstupy: Zpráva o aktivech a dopadech + Zpráva o analýze rizik + Implementační plán	Nutné provést: ANO Čas: 4 - 12 měsíců Členové projektového týmu: 2-n interních pracovníků a/nebo 2-3 konzultanti Respondenti: desítky Výstupy: Zpráva o aktivech a dopadech + Zpráva o analýze rizik + Implementační plán
	Výběr opatření a plán implementace	Protiopatření vyplývají z AR Prosazuje: ředitel firmy	Protiopatření vyplývají z AR Prosazuje: ředitel a vedoucí oddělení společně	Protiopatření vyplývají z AR Prosazuje: podle významu protiopatření od vedení společnosti po vedoucí oddělení
	Prohlášení o aplikovatelnosti	Dokumentované rozhodnutí, samostatný dokument pouze v případ certifikace	Dokumentované rozhodnutí, samostatný dokument pouze v případ certifikace	Dokument Prohlášení o aplikovatelnosti
ISMS	**Doporučení zavést ISMS**	Ano	Ano	Ano
	Doporučení certifikace ISMS	Ne (ANO pokud je nějaký systém řízení již certifikován)	Ano (jako další systém řízení)	Ano (jako součást IMS)

Risk Analysis Consultants, Španělská 2, 120 00 Praha 2, Czech Republic, tel.+420 221 628 400, fax +420 221 628 401, rac@rac.cz, www.rac.cz

ISMS v malých a středních firmách

2.díl Do - Dělej

Seriál článků s názvem „ISMS v malých a středních firmách“ popisuje proces zavádění, využívání a zlepšování systému řízení bezpečnosti informací (dále ISMS) tak, aby splnil požadavky pro zajištění bezpečnosti informací dle normy ISO/IEC 17799:2005 a požadavky pro zavedení a provoz ISMS dle normy ISO/IEC 27001. Způsob naplnění těchto požadavků lze vždy přizpůsobit specifickým podmínkám každé organizace a ne jinak je tomu i v prostředí malých a středních firem. Tento 2.díl popisuje činnosti kroku Dělej (Do), ve kterém jsou potřebná opatření ISMS zaváděna do praxe a využívána

Provoz ISMS

Úvodní díl tohoto seriálu pojednával o hlavních krocích první fáze Plánuj (Plan) procesu zavádění a využívání ISMS v organizacích, dle procesního modelu PDCA (Plan-Do-Check-Act), obecně používaného pro implementaci a provoz systémů řízení. Jeho obsahem bylo mj. stanovení rozsahu ISMS, vytvoření bezpečnostní politiky, definování organizace bezpečnosti a provedení analýzy rizik. Výstupem z analýzy jsou doporučení na zajištění bezpečnosti, která by měla být implementována, zdokumentována a správně používána právě v kroku Dělej (Do).

Způsob implementace opatření a metody prosazení

Výběr okruhů opatření ISMS je podobný pro malou i středně velkou firmu. Velký rozdíl však je ve způsobu a zejména v rychlosti jejich prosazení. V malé firmě rozhoduje zpravidla ředitel o tom, kdo bude mít přístup k jakým datům. Ve středně velké firmě je nutné vytvořit proces přidělování uživatelských oprávnění, aby nemohla nastat situace, se kterou jsme se setkali v jedné softwarové firmě (cca 70 uživatelů): Administrátor sítě byl odpovědný za přidělování přístupu na základě požadavků vedoucích oddělení. Ti však zásadně odmítali vyplnění jakéhokoli formuláře (zdržovalo je to) a administrátor odmítal přidělovat práva na základě telefonické žádosti. Situaci vyřešilo zavedení administrativního procesu přidělování přístupu pro všechny uživatele systému.

V malých firmách je běžné, že **bezpečnostní ředitel** (zpravidla ředitel firmy) **rozhodne ráno** o změně délky hesla z 6 na 9 znaků. Bezpečnostní administrátor (zpravidla správce sítě) protiopatření zavede ještě před obědem a v rámci příjemně strávené siesty si všichni uživatelé rádi změní heslo. Následující den je protiopatření v systému již zcela zavedeno a automaticky používáno a akceptováno. Taková rychlost implementace je typická pouze pro malé firmy. Ve středně velkých organizacích je nutné vzít v úvahu akceptovatelnost protiopatření ze strany uživatelů a další souvislosti jejich realizace. Prosadit například změnu délky hesla vyžaduje revizi příslušné směrnice, **zapojení několika administrátorů** do práce a seznámení desítek uživatelů se změnou, například formou školení. Poté by měla následovat kontrola funkčnosti opatření.

Bezpečnostní dokumentace

Značné rozdíly mezi malou a středně velkou firmou jsou ve formě a míře detailu dokumentace bezpečnosti. Není příliš známo, že uvedené normy **striktně nevyžadují** papírovou formu dokumentace ani její pevnou strukturu, ale ponechávají na preferencích jednotlivých firem, jakou formu a obsah zvolí. Přitom právě obava z přílišné formální administrativy nejčastěji odpuzuje malé a středně velké organizace od zavádění doporučení těchto norem. Dokumentace ISMS požadovaná k certifikaci podle ISO 27001 pochopitelně musí obsahovat určité, taxativně uvedené typy dokumentů, dané jednotlivými kroky procesu ISMS, ale jejich rozsah, obsah a forma může být překvapivě jednoduchá a flexibilní, jak si popíšeme dále.

Pracovníci malých firem se osobně znají a velká část bezpečnosti je založena na jejich vzájemné důvěře. Není nutné vytvářet složitý systém politik, směrnic a postupů. Postačí stručné pravidlo, že bezpečnostní dokumentace je vedena ve sdílené složce elektronické pošty, definovat role a přístupy zodpovědných osob a nezbytné typy bezpečnostních dokumentů realizovat formou elektronických záznamů, obsahující stručný popis realizace daného pravidla, postupu nebo odpovědnosti.

Středně velká firma se v této oblasti opatření blíží firmě velké. Zde je již **nutné zavádět podrobnější administrativní procedury**, neboť existuje více oddělených rolí a odpovědností a také více definovaných pravidel. Tato administrativa je nutná, aby byly eliminovány činnosti, které se dějí při práci s daty jen tak, na „dobré slovo“. Pracovníci středně velkých firem se většinou také znají, ale jistá úroveň anonymity může být impulsem k tomu, že se někteří budou snažit bezpečnostní procedury obejít zejména, když nebudou přesněji definovány a kontrolovány.

Rozsah a aktuálnost bezpečnostní dokumentace bývá často jedním z klíčových kritérií při posuzování kvality ISMS a míry dosažené shody s požadavky no-

Seriál vyšel v upravené podobě v časopise Data Security Management 03/2004 až 06/2004.

Marek Skalický pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 2003. Dříve pracoval ve společnosti Aero Vodochody a.s., kde v letech 2001-2003 vykonával funkci Bezpečnostního správce IS. Nyní se věnuje projektům zavádění ISMS v organizacích, přípravě organizací na zpracování utajovaných skutečností, službám správy zranitelností ICT (VM) a jako člen Znaleckého ústavu RAC také forenzním analýzám IS.
Marek.Skalicky@rac.cz

ISMS v malých a středních firmách

2.díl Do - Dělej

rem. Příklady rozsahu bezpečnostní dokumentace pro typické kvalitativní úrovně řízení bezpečnosti v organizacích, jak se s nimi nejčastěji setkáváme v praxi, jsou uvedeny v tabulce na konci celého seriálu.

Program zvyšování bezpečnostního povědomí

Mezi další metody prosazení bezpečnosti v organizacích patří program zvyšování bezpečnostního povědomí v organizacích. Tento krok, jakkoliv komplikovaně znějící, je ve skutečnosti poměrně **jednoduchá, levná a velice účinná metoda**, která bývá bohužel mnohdy v malých a středně velkých organizacích opomíjena. Má za cíl zvýšit u všech zaměstnanců informovanost jednak o obecných principech a souvislostech informační bezpečnosti a o konkrétních rizicích, opatřeních, odpovědnostech a pravidlech, vyplývajících ze zaváděného nebo již provozovaného ISMS.

V čem vlastně spočívá „síla jednoduchosti" tohoto opatření? Program je zaměřen na zaměstnance (a na externí spolupracující osoby apod.), kteří jsou často zdrojem bezpečnostních incidentů a kteří mohou, pokud jsou správně informováni, svým včasným jednáním šíření a škodám incidentů zabránit. Stále se ještě při každém bezpečnostním školení firem různých velikostí setkáváme s mnoha užaslými tvářemi, když vysvětlujeme, že nejvyšší hodnotu pro organizaci mají v informačním systému data a nikoliv hardware a software. Existuje stále také mnoho uživatelů, kteří pokládají svou disketu nebo lokální harddisk „svého PC" v kanceláři za mnohem bezpečnější místo, než síťový disk s transparentně nastavenými přístupovými právy a pravidelným zálohováním.

U malých firem postačí, pokud zvyšování bezpečnostního povědomí opřeme o stručné **vstupní školení všech zaměstnanců** a občasné prodiskutování aktuálních bezpečnostních otázek dle potřeb organizace a vývoje nových potencionálních hrozeb (může být využito outsourcingu).

U středně velkých organizací se zvyšují nároky na informovanost zaměstnanců a rozsah jejich znalostí o bezpečnostní problematice, realizovaných opatřeních, povinnostech a odpovědnostech z nich vyplývajících. **Základní bezpečnostní školení** se doporučuje realizovat pro všechny nové zaměstnance bez rozdílu. Zde se však vyplatí potrápit zaměstnance trochu déle a více se zaměřit na popis a rozbor typických hrozeb a bezpečnostních incidentů. Bohužel právě **odstrašující příklady**, včetně **zmínky o sankcích** při nedodržování pravidel, zaberou i tam, kde dobrá rada nepřesvědčí. Samozřejmě i u středně velkých organizací by nemělo být opomenuto informovat všechny zaměstnance dle potřeby o aktuálních hrozbách a opatřeních, např. formou zřízení centrálního informačního místa o bezpečnostních otázkách na firemním intranetu.

Způsob zvládání rizik za provozu

Jedním z hlavních důvodů proč zavádět ISMS, je potřeba zajistit kontinuální proces zvládání a řízení informačních rizik. Základem pro jejich úspěšné řízení je identifikace a analýza všech potencionálních rizik a následné rozhodnutí o způsobu jejich zvládání a sledování v čase. Účelem řízení rizik není veškerá identifikovaná rizika bezezbytku pokrýt (mnohdy s vynaložením neadekvátních zdrojů), ale pokrýt zvolenými opatřeními pouze taková, u kterých je to efektivní. Ostatní **rizika** může organizace **akceptovat a sledovat**, některá může přenést na jinou organizaci, případně je pojistit. Pouze pokud organizace zná a sleduje všechna rizika související se zabezpečením informací a adekvátně rozhoduje o způsobu jejich zvládání, potom může prohlásit, že tyto rizika řídí (má je pod kontrolou).

Tyto zásady jsou opět společné pro všechny velikosti a typy organizací. Otázkou je, jak se s nimi malé a středně velké organizace efektivně vypořádají. U těchto firem bude většinou velikost negativního dopadu bezpečnostního incidentu i pravděpodobnost jeho výskytu průměrně nižší než u velkých společností. Je tedy zřejmé, že vedení těchto firem bude mít **tendence více rizika akceptovat** a přesune svůj zájem spíše do oblasti jejich sledování a efektivního zvládání případných bezpečnostních incidentů.

Pro sledování nových typů rizik a rozpoznání bezpečnostních incidentů je nutné **aktivovat generování záznamů** o nejdůležitějších bezpečnostních událostech (v papírové i elektronické formě) a tyto záznamy vyhodnocovat. Mezi takové záznamy patří minimálně záznamy o přístupech do budov a zabezpečených místností, přihlašování a odhlašování do počítačových systémů a citlivých aplikací, přístupy a manipulace se zvlášť citlivými informacemi apod. Řada těchto záznamů je generována automaticky po instalaci jednotlivých systémů (EZS, doménový řadič, účetní aplikace apod.).

Na co se však často zapomíná, je jejich systematické ukládání, zabezpečení a vyhodnocování. Jeden příklad za všechny: Při forenzním zkoumání zneužití systému el. bankovnictví v jedné malé firmě se ukázalo, že oprávnění zaměstnanci této firmy se všichni přihlašovali do systému elektronického bankovnictví pod stejným uživatelským účtem, i když tato aplikace samozřejmě nabízela individuální přihlašovací účty. Protože byl tento sytém provozován na samostatném PC, se zastaralou verzí Windows, navíc nepřipojeném k firemní

Risk Analysis Consultants, Španělská 2, 120 00 Praha 2, Czech Republic, tel.+420 221 628 400, fax +420 221 628 401, rac@rac.cz, www.rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

2.díl Do - Dělej

LAN, neexistovaly žádné jiné typy záznamů o jeho využívání. Z bankovního účtu této firmy byly převedeny částky na cizí účty transakcemi ověřenými platnými privátními elektronickými klíči této firmy. Naštěstí byly tyto transakce zrealizovány ve dnech, kdy nikdo ze zaměstnanců elektronického bankovnictví nepoužil. Vyšetřování nakonec prokázalo, že částky byly převedeny pracovníkem uživatelské podpory banky z jiného PC, na které privátní elektronické klíče poškozené firmy zkopíroval (poté, co je zcizil při jejich instalaci). Pracovník banky však smazal část nezabezpečených logů na straně serverů banky a tím ztížil prokázání činu. Tento příklad demonstruje nutnost vedení, zabezpečení a občasného vyhodnocování důležitých bezpečnostních záznamů u všech typů společností bez rozdílu.

U malých organizací bude **proces řízení a zvládání rizik realizován neformálním způsobem**, bez stanovení speciálních pravomocí a oddělení rolí. Je zde totiž účelné dosáhnout shodné úrovně informovanosti a pravomocí u všech zaměstnanců. Pro středně velké firmy je již doporučeno **rámcově definovat postupy, oddělit pravomoci** a provádět namátkové revize tohoto procesu. Pro získání přehledu o způsobu a důslednosti plnění povinností při zvládání rizik a incidentů je namístě zřídit evidenci závažných hrozeb a zranitelností a způsobů jejich pokrytí.

Nároky na provoz opatření a zajištění bezpečnosti

Součástí plánu zvládání rizik je i sledování nároků na provoz jednotlivých opatření a celkového zajištění bezpečnosti. Zatímco u malých firem není potřeba plánovat ani **vyhrazovat samostatný rozpočet**, neboť případný nákup a provoz nezbytných opatření je operativně schválen ředitelem a hrazen dle aktuálních potřeb organizace, u středních a velkých firem je nezbytné provádět alespoň rámcové plánování potřebných finančních i lidských zdrojů.

Z hlediska preferencí při výběru opatření hrají celkové nároky na jejich zavedení a provoz hlavní roli. Zatímco pro malé organizace není překážkou pružně zavádět administrativní a personální opatření i za cenu vyšších požadavků lidské zdrojů, úskalím však bývají finanční náklady na pořízení složitých technologických opatření. U velkých společností lze tyto preference vysledovat obráceně, neboť pro ně bývá snazší pružně zavést nové technologické opatření, než jej nahradit administrativními či organizačními změnami. V případě preferencí středně velkých firem je stav logicky někde uprostřed. Záleží na pružnosti řízení, technologické úrovni a znalostech pracovníků firmy, k jakým typům opatření se budou přiklánět více.

Zavedení opatření DRP a IRH

Poslední důležitou oblastí opatření při zavádění a provozu ISMS je tvorba a údržba *Havarijních plánů* (DRP – Disaster Recovery Planning) a *Postupů řešení bezpečnostních incidentů* (IRH – Incident Response Handling). Stejně jako v případě ostatních formálních postupů i zde platí, že pro malé organizace je neefektivní vypracovávat a udržovat podrobné formální havarijní plány. Pro obnovu systémů jim plně postačí vytvoření **stručného univerzálního havarijního "checklistu"** pro všechny možné případy havárie, který bude obsahovat postup bezpečného vypnutí a restartu technického vybavení a serverů, jednoduchý záznam výsledné konfigurace technologií a aplikací, postup obnovení dat ze záložních médií a seznam kontaktů na interní a externí osoby, které mohou pomoci při výskytu havárie nebo závažného bezpečnostního incidentu. Tyto havarijní postupy by měly být alespoň jednorázově otestovány a poté postačí testy opakovat až při zásadní změně používaných technologií a služeb.

U středně velkých organizací je doporučeno rozšířit zmíněný havarijní „checklist" i o popis kroků instalace jednotlivých částí informačního systému a obnovy dat a aplikací ze záložních médií. U komplikovanějších informačních systémů je třeba rozlišit obnovu klíčových aktiv od ostatních a tomu přizpůsobit priority v havarijním plánování. Pro výběr strategie způsobu obnovy a nastavení priorit je nejlépe realizovat **analýzu dopadů na činnosti organizace** (BIA – Business Impact Analysis). Pokud byla správně realizována analýza rizik, lze informace o negativních dopadech nedostupnosti jednotlivých aktiv nalézt tam. Na základě těchto výsledků je vypracován strukturovaný havarijní plán obnovy, obsahující varianty postupu dle specifikovaných typů havarijních stavů. Takovýto plán je nezbytné pravidelně testovat a aktualizovat a na základě výsledků testů (v porovnání s cíly obnovy) vylepšovat.

Závěr 2.dílu

Nebylo možné v rámci vymezeného prostoru prodiskutovat veškeré činnosti, realizované v rámci etapy „Dělej ISMS". Důležité je v závěru upozornit na fakt, že při implementaci a provozu opatření, zvolených v předchozí fázi Plánuj (Plan) se nezavádí a neprovozují pouze primárně účinná technická a organizační opatření typu: „nastav autentizační mechanizmus" nebo „eviduj pohyb osob v serverovně" ale spolu s nimi je třeba myslet na stejně důležitá sekundární řídící opatření, která mají za cíl potřebnou úroveň bezpečnosti dlouhodobě udržovat a komplexně rozvíjet.

Seriál vyšel v upravené podobě v časopise Data Security Management 03/2004 až 06/2004.

Marek Skalický pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 2003. Dříve pracoval ve společnosti Aero Vodochody a.s., kde v letech 2001-2003 vykonával funkci Bezpečnostního správce IS. Nyní se věnuje projektům zavádění ISMS v organizacích, přípravě organizací na zpracování utajovaných skutečností, službám správy zranitelností ICT (VM) a jako člen Znaleckého ústavu RAC také forenzním analýzám IS.
Marek.Skalicky@rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

2.díl Do - Dělej

	Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
PLAN	**Plán / projekt bezpečnosti**			
	Bezpečnostní politika			
	Organizace bezpečnosti			
	Analýza rizik			
	Výběr opatření a plán implementace			
	Prohlášení o aplikovatelnosti			
DO	**Způsob implementace opatření**	Okamžitě, rychle, efektivně, bez zbytečné administrativy	Podle významu protiopatření formou projektů nebo direktivním nařízením	Formou projektů
	Metody prosazení bezpečnosti	Direktivní – Osobní - Neformální Stručné pokyny (email, Intranet) a verbální působení na všechny zaměstnance	Direktivní – Neosobní - Formální Kombinace verbálních pokynů vedoucích a písemných organizačních. Závazné a formální seznámení s nařízeními	Direktivní – Neosobní – Důsledně formální Písemné organizační pokyny Závazné a formální seznámení s nařízeními
	Bezpečnostní dokumentace	Bezpečnostní politika, některé směrnice, občas konkrétní postupy	Bezpečnostní politika a další dokumentace včetně směrnic, postupů, návodů apod.	Kompletní řízená bezpečnostní dokumentace a její průběžná (plánovaná) revize
	Program zvyšování bezpečnostního povědomí	Jednorázové informace dle potřeby. Bezpečnostní minimum součástí úvodního zaškolení.	Nepravidelné pokyny a nařízení Bezpečnostní minimum součástí úvodního zaškolení. Specializovaná školení pro vybrané zaměstnance.	Strukturovaný kontinuální vzdělávací program. Pravidelná specializovaná školení všech zaměstnanců.
	Způsob zvládání rizik za provozu	Neformální proces, bez speciálních postupů a pravomocí. Pokrytí a kontrola bezprostředně po identifikaci.	Formální proces s rámcově stanoveným postupem a odpovědnostmi. Revize zvládání rizik nepravidelná, dle potřeby.	Formálně řízený proces s předem stanovenými postupy a pravomocemi. Pravidelné analýzy a kontroly zvládání rizik.
	Nároky na provoz opatření a zajištění bezpečnosti	Krátkodobé plánování. Není separátní rozpočet. Externí spolupráce není obvyklá.	Krátkodobé a střednědobé plánování Rozpočet v rámci IT/IS Prosazuje se outsourcing	Dlouhodobé plánování Individuální rozpočet Běžné využití outsourcingu
	Zavedení opatření DRP a IRH (Havarijní plány)	Zpravidla řada neformálních havarijních postupů pro jednotlivá aktiva.	Formální univerzální havarijní plán Postupy zvládání bezpečnostních incidentů	Provedena analýza dopadů (BIA) Strukturované havarijní plány Formální postupy zvládání bezpečnostních incidentů
CHECK	**Monitoring IS a testování funkčnosti opatření**			
	Kontrola a audit bezpečnostních opatření			
	Revize adekvátnosti a efektivnosti ISMS			
ACT	**Vyhodnocení fáze CHECK, identifikace a analýza neshod**			
	Nápravná a preventivní opatření			

Risk Analysis Consultants, s.r.o. je nezávislá poradenská společnost poskytující řešení, služby a konzultace ve všech oblastech bezpečnosti informací v souladu s mezinárodními normami, související národní legislativou a s přihlédnutím k individuálním podmínkám klientů. Od roku 1995 pomáhá zajišťovat bezpečnost informací v informačních systémech organizací státní správy, finančních institucí, telekomunikačních společností a průmyslových podniků v České republice i v zahraničí. V roce 2003 se z rozhodnutí Ministra spravedlnosti České republiky stala prvním soukromým znaleckým ústavem, kvalifikovaným pro výkon znalecké činnosti v oblasti kybernetiky a výpočetní techniky.

Risk Analysis Consultants, Španělská 2, 120 00 Praha 2, Czech Republic, tel.+420 221 628 400, fax +420 221 628 401, rac@rac.cz, www.rac.cz

ISMS v malých a středních firmách

Příklady typických úrovní implementace řízení bezpečnosti informací (ISM) v organizacích

Rozsah a aktuálnost bezpečnostní dokumentace bývá často jedním z klíčových kritérií při posuzování kvality ISMS a míry dosažené shody s požadavky norem. Příklady rozsahu bezpečnostní dokumentace pro typické kvalitativní úrovně řízení bezpečnosti v organizacích, tak jak se s nimi nejčastěji setkáváme v praxi, jsou uvedeny v následující tabulce.

Poznámka: Rozsah bezpečnostní dokumentace, uvedený u příslušné úrovně zavedeného ISM, obsahuje zároveň i veškerou dokumentaci, popsanou u nižších úrovní řízení ISM.

Kvalitativní úrovně implementace a provozu řízení bezpečnosti informací (ISM) v organizacích

Typická úroveň řízení ISM	Stav implementace a provozu ISM (dle dosažené úrovně řízení)	Rozsah bezpečnostní dokumentace (dle dosažené úrovně řízení ISM)*
Re-certifikovaný ISMS (bezpečnost informací je prokazatelně dlouhodobě řízena dle BS 7799-2:2002)	Organizace opakovaně provádí re-certifikaci provozovaného ISMS dle standardu BS 7799-2:2002. Aktualizuje stav opatření a dokumentace ISMS dle změn v podnikatelských cílech, prostředí a procesech organizace a dle aktualizovaných výsledků analýzy rizik .	Aktualizace rozsahu ISMS a výsledků analýzy rizik. Pravidelná revize Bezpečnostní politiky informací. Aktualizace návrhu opatření, prohlášení o aplikovatelnosti a implementačního plánu opatření a procesů ISMS. Pravidelná revize a aktualizace bezpečnostní dokumentace opatření a procesů ISMS.
Certifikovaný ISMS (bezpečnost informací je prokazatelně zavedena a řízena dle BS 7799-2:2002)	Organizace se rozhodla certifikovat ISMS a realizovala kontrolní pre-certifikační audit, na základě jehož výsledků zavedla chybějící opatření a dopracovala procesy a dokumentaci dle požadavků BS 7799-2. Poté přistoupila k certifikaci ISMS.	Zpráva o výsledcích pre-certifikačního auditu ISMS. Plán řízení zdrojů ISMS. Kompletní provozní dokumentace opatření ISMS. Kompletní řídící a kontrolní dokumentace ISMS. Zpráva o certifikaci ISMS. Certifikát ISMS dle BS 7799-2:2002.
Implementovaný ISMS v souladu s normou (bezpečnost informací je systematicky řízena a zlepšována, rizika jsou řízena a zvládána)	V organizaci je implementován a provozován ISMS v souladu s normou ISO/IEC 17799:2000. Rozsah ISMS, jeho řízení, procesy a odpovědnosti jsou definovány. Jsou identifikována a zvládána všechna rizika a zavedena opatření schválená k implementaci. Bezpečnostní dokumentace pokrývá všechny oblasti ISMS, nicméně nemusí být zcela dle požadavků certifikace (revize, aktualizace)	Působnost (rozsah) ISMS. Plán zvládání rizik . Prohlášeni o aplikovatelnosti opatření. Strategie BCP + DRP a IRH dokumenty a postupy. Základní provozní a řídící dokumentace opatření ISMS. Záznamy o provozu, využívání a zlepšování ISMS. Evidence bezpečnostních incidentů a následných reakcí a opatření. Výsledky auditu a evidence nalezených neshod, nápravných a preventivních opatření.
Částečně implementovaný ISMS (koncepce bezpečnosti a plán zavedení ISMS je neúplná, nebo teprve postupně realizována)	Je přijata koncepce bezpečnosti managementem. Byla provedena analýza rizik a návrh opatření. Zavedena pouze vybraná opatření (priorita, zdroje). ISMS není řádně zdokumentován, nejsou realizovány veškeré řídící procesy (zejména kontrolní a nápravné) a řízeny zdroje ISMS. Není prováděn audit ISMS.	Zpráva o aktivech a dopadech. Zpráva o analýze rizik. Návrh opatření a implementační plán, případně Prohlášení o aplikovatelnosti opatření. Částečná provozní a řídící dokumentace procesů ISMS. Nekompletní záznamy o provozu , fungování řídících procesů ISMS a evidence bezpečnostních incidentů. Dílčí projekty/plány implementace prioritních opatření.
Plánovaný ISMS (zavedení systému řízení bezpečnosti a zvládání rizik ve fázi přípravy a plánování)	Je přijata koncepce řízení bezpečnosti managementem na základě cíle zvládání rizik . Je vytvořen rámcový plán/projekt ISMS a případně delegován rozpočet na bezpečnost. Je vytvářeno bezpečnostní povědomí v organizaci.	Strategie bezpečnosti. Bezpečnostní politika informací. Program zvyšování bezpečnostního povědomí. Výsledky přehledové (případně detailní) analýzy rizik. Rámcový projekt bezpečnosti informací. Plán implementace ISMS a zvládání rizik.
Ad-hoc ISM (řízení bezpečnosti informací bez znalosti a systematického zvládání bezpečnostních rizik)	Neexistuje systematická koncepce bezpečnosti, ISM „je řízena přes neznalost rizik“. Částečné bezpečnostní povědomí některých pracovníků. Zavedeny vybrané dílčí opatření a procesy ISM spolu s technickými opatřeními.	Neexistuje řízená systematická bezpečnostní dokumentace. Pouze dílčí interní dokumentace pokrývající určité oblasti nebo systémy. Možný výskyt neprovázané dodavatelské dokumentace některých systémů.
Nezavedený ISM (neprobíhá řízení bezpečnosti informací)	Neexistuje žádné bezpečnostní povědomí, řízení ani koncepce. Realizovány jsou pouze dílčí technické opatření, bez potřebných ISM procesů a dokumentace.	Interní bezpečnostní dokumentace v oblasti bezpečnosti informací neexistuje. Možný výskyt neprovázané dodavatelské dokumentace některých systémů.

Seriál vyšel v upravené podobě v časopise Data Security Management 03/2004 až 06/2004.

Marek Skalický pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 2003. Dříve pracoval ve společnosti Aero Vodochody a.s., kde v letech 2001-2003 vykonával funkci Bezpečnostního správce IS. Nyní se věnuje projektům zavádění ISMS v organizacích, přípravě organizací na zpracování utajovaných skutečností, službám správy zranitelností ICT (VM) a jako člen Znaleckého ústavu RAC také forenzním analýzám IS.
Marek.Skalicky@rac.cz

ISMS v malých a středních firmách

3.díl Check - Kontroluj

Žádný proces, opatření nebo činnost sledující cíl a plnící určitou funkci v systému není možné udržet, řídit a zlepšovat v čase, pokud se neprovádí periodická kontrola jejich funkčnosti, efektivity a souladu s požadovaným stavem. Nejinak je tomu i v procesu zavádění a provozování systému řízení bezpečnosti informací (ISMS) dle normy ISO/IEC 27001:2005. Jak efektivně provádět kontrolu ISMS v prostředí malých a středních organizací popisuje tento 3.díl seriálu.

Kontrola ISMS

Jak již bylo uvedeno v předchozích dílech tohoto seriálu, ISMS (Information Security Management System) slouží k vybudování, provozování, sledování, řízení a zlepšování bezpečnosti informací v organizacích. Jedná se o systematický a konzistentní proces v čase, který je realizován dle periodického procesního modelu PDCA (Plan-Do-Check-Act). Hlavní kroky a opatření v etapách Plánuj (Plan) a Dělej (Do) byly předmětem 1. a 2. dílu seriálu. Tento 3. díl se zabývá náplní etapy Kontroluj (Check), která slouží jako **zpětná vazba**, podávající vedení organizace i dalším odpovědným osobám informace o tom do jaké míry byly naplněny zásady a cíle bezpečnostní politiky informací, zda byla zavedena všechna bezpečnostní opatření uvedená v Prohlášení o aplikovatelnosti opatření a zda fungují dostatečně spolehlivě a efektivně.

Ono nechvalně známé rčení „důvěřuj ale prověřuj" je v oblasti bezpečnosti informací nanejvýš namístě a s trochou nadsázky lze dodat, že pokud „Opakování je matkou moudrosti", pak „Prověřování je otcem bezpečnosti" a jejich společným potomkem je právě tato etapa „Kontroluj".

Protože během budování ISMS jsou v organizaci zaváděna jednak funkční bezpečnostní opatření, zvolená z ISO 17799dle výsledků analýzy rizik a dále opatření (proces) pro jejich řízení a zlepšování v čase dle ISO 27001, je třeba se při kontrole ISMS zaměřit na obě tyto skupiny opatření. K tomu slouží řada technik a postupů, jejichž popis s přihlédnutím k prostředí malých a středních firem je obsahem tohoto článku. Na konci tohoto dílu je uveden seznam procesů, obsahující hlavní kroky ISMS s detailem na etapu Kontroluj (Check) procesu PDCA.

Monitoring provozu

Monitoring provozu klíčových prvků IS a ochranných opatření je základním zdrojem informací pro kontrolu jejich funkčnosti a spolehlivosti. Pokud organizace zavádějící ISMS plánuje v budoucnu i jeho certifikaci, musí **vytvářet a shromažďovat záznamy** o fungování alespoň těch opatření, která jsou uvedena v Prohlášení o aplikovatelnosti (ty budou předmětem auditu). Bohužel ne všechny typy opatření samy automaticky generují záznamy o činnosti a tak je nezbytné přistoupit i v prostředí malých a středních firem k nepopulárnímu **ručnímu generování záznamů** u takových opatření, která tuto vlastnost nemají (především organizační a administrativní). Nemusí se přitom zdaleka jednat o únavnou administrativu, protože rozsah a složitost opatření, zvláště u malých a středních firem, nebývá nijak velký. Příkladem toho, co postačí pro audit funkčnosti opatření „bezpečnostní školení uživatelů IS" (viz. předcházející díl seriálu), jsou seznamy účastníků školení a datum a předmět školení. Zodpovědná a systematická asistentka si je stejně pořídí a pokud tak učiní do připravené tabulky, kterou bude dle potřeby aktualizovat a iniciativně nesmaže, je povinnost vůči auditu ISMS splněna. Pochopitelně pouze za jedno opatření - školení pracovníků, nicméně časová náročnost se pohybuje v rámci jednotek minut.

Pro monitoring ICT postačí u malých organizacích výchozí nastavení logování dle standardní instalace většiny produktů a jejich ruční **namátková kontrola** pracovníkem, pověřeným na půl úvazku základními bezpečnostními povinnostmi. U středních organizací, je již vzhledem ke komplikovanosti IS infrastruktury nedostatečné spolehnout se pouze na namátkové ruční kontroly log souborů a je třeba využít **automatických nástrojů** pro jejich filtrování a vyhodnocování nestandardních událostí např. pomocí skriptů nebo dodatečných produktů. Podrobnější bezpečnostní monitoring se vyplatí aktivovat pouze krátkodobě, při podezření na výskyt bezpečnostního incidentu (což při pozdní reakci může skončit příslovím „s křížkem po funuse").

Testování funkčnosti opatření

Abychom při provozu IS pomyslnému funusu předešli, je třeba uvedené pasivní metody kontroly doplnit i o aktivní a preventivní způsoby, jakými jsou např. aplikační kontroly chyb výpočtů a zpracování dat nebo testování zranitelností, případně penetrační testování systémů. Zatímco komplikovanější a časově i finančně náročnější penetračního testování má za cíl simulaci reálných útoků ze zvoleného prostředí a identifikaci možných negativních dopadů na IS, bezesporu jednodušším, rychlejším a levnějším způsobem testování odolnosti vůči útokům je vyhledání a testování zranitelností provozovaných ICT produktů.

Risk Analysis Consultants, Španělská 2, 120 00 Praha 2, Czech Republic, tel.+420 221 628 400, fax +420 221 628 401, rac@rac.cz, www.rac.cz

ISMS v malých a středních firmách

3.díl Check - Kontroluj

Oba způsoby mohou být prováděny z interní sítě, nebo častěji z externího prostředí – zpravidla Internetu nebo bezdrátových sítí, což by měly být v případě malých a středních firem hlavní oblasti prevence proti útokům na IS. Protože se v případě penetračního testování jedná o vysoce specializovanou činnost, vyžadující detailní znalosti o technikách a nástrojích hackingu, stejně jako o bezpečnostních slabinách jednotlivých ICT produktů a komunikačních protokolů, bývá tento úkol svěřován specializovaným externím firmám, které mají dostatečné profesní zázemí pro jejich kvalifikovanou realizaci. Naproti tomu testování zranitelností je proces, který si mnohdy mohou počítačově gramotní uživatelé udělat sami, pomocí dostupných programů nebo využít **specializovaných webových služeb** (např. QualysGuard®).

Pro malé organizace lze testování zranitelností doporučit, pokud využívají permanentní připojení k externím sítím nebo provozují bezdrátovou LAN v husté zástavbě. V případě vybalení a zapojení „chytrého“ VLAN přístupového bodu se Vám totiž může stát, že až se po několika minutách budete chtít k tomuto zařízení připojit na administrátorskou konzolí, bude Vám hlásit že administrátorské připojení již využívá jiný počítač a Váš to rozhodně nebude! Pro střední organizace by **testování zranitelností klíčových serverů a služeb IS mělo být samozřejmostí**, alespoň po implementaci bezpečnostních opatření a před rutinním provozem komunikačních spojů. Pokud střední organizace provozují citlivá data a aplikace na Internetu, mohou zvážit realizaci penetračního testování nebo podrobný technický bezpečnostní audit konfigurace klíčových prvků IS a bezpečnostních opatření jako např. Firewallu, DNS nebo Internetového aplikačního nebo databázového serveru či routeru na rozhraní LAN/WAN.

Audit a kontrola bezpečnostních opatření

Spolu s monitorováním provozu, testováním zranitelností a technicky zaměřeným auditem konfigurace ICT, je další metodou kontroly implementace a provozu IS / ISMS realizace Auditu a kontrol bezpečnosti IS. Obecně lze říci, že audit opatření musí být prováděn v každém typu a velikosti organizace, která provozuje systém řízení nad opatřeními, jinak by neexistovala zpětná vazba o stavu reality vůči plánu a návrhu požadovaného cílového stavu. Každý typ auditu by se měl řídit pravidly ISO 19011:2002 a měl by probíhat dle schváleného ročního i operativního plánu.Je zřejmé, že takovéto formální „harakiri“ malé a střední organizace dobrovolně nepodstoupí a že přichází v úvahu pouze v případě potřeby certifikace systému řízení.

V případě ISMS by měl audit zahrnovat kontrolu funkčních bezpečnostních i řídících opatření ISMS, která jsou deklarována v Prohlášení o aplikovatelnosti a popsána v bezpečnostní dokumentaci. Audit by měl ověřit jak jsou realizována v praxi.

U malých organizací není třeba vytvářet samostatná oddělení nebo pracovní funkce **interního auditora**, ale je nutné i v malé organizaci funkci interního auditora dedikovat, alespoň jako přidruženou pracovní náplň nějakému zaměstnanci. Jednou ročně je nezbytné projednání zjištěných výsledků plánovaných auditů i namátkových kontrol s majitelem / ředitelem organizace a následně se všemi zaměstnanci.

V případě středně velké organizace se již doporučuje zvážit existenci samostatné funkce interního auditora, kterému připadne i funkce **bezpečnostního auditora**. I v tomto případě má za úkol provádění plánovaných i namátkových kontrol dle ročního i operativního plánu auditu, který je sestavován s přihlédnutím k největším rizikům a nálezům předchozích auditů. Pro dosažení vyšší odborné úrovně a komplexnosti výsledků kontroly je doporučeno realizovat alespoň jednou ročně přehledový srovnávací audit stavu ISMS, vzhledem k požadavkům ISO 27001, s účastí jednoho externího odborného konzultanta.

Revize adekvátnosti a efektivnosti ISMS

Kromě ověření funkčnosti, spolehlivosti a úplnosti funkčních i řídících opatření je třeba přibližně jednou ročně zrevidovat rozsah, adekvátnost a efektivnost celého ISMS ve vztahu k potřebám, cílům a prostředí organizace. Výsledek této celkové revize ISMS by měl být stejně jako souhrnné výsledky auditů opatření **projednán s vedením organizace** a pořízeny záznamy o přijatých závěrech.

Jelikož se jedná o činnost vyžadující široký přehled a značné zkušenosti z oblasti bezpečnosti informací a implementace ISMS v organizacích, musejí se malé i střední organizace spolehnout na pomoc externích specialistů, stejně jako v případě analýzy informačních rizik v etapě Plánuj.

Závěr 3.dílu

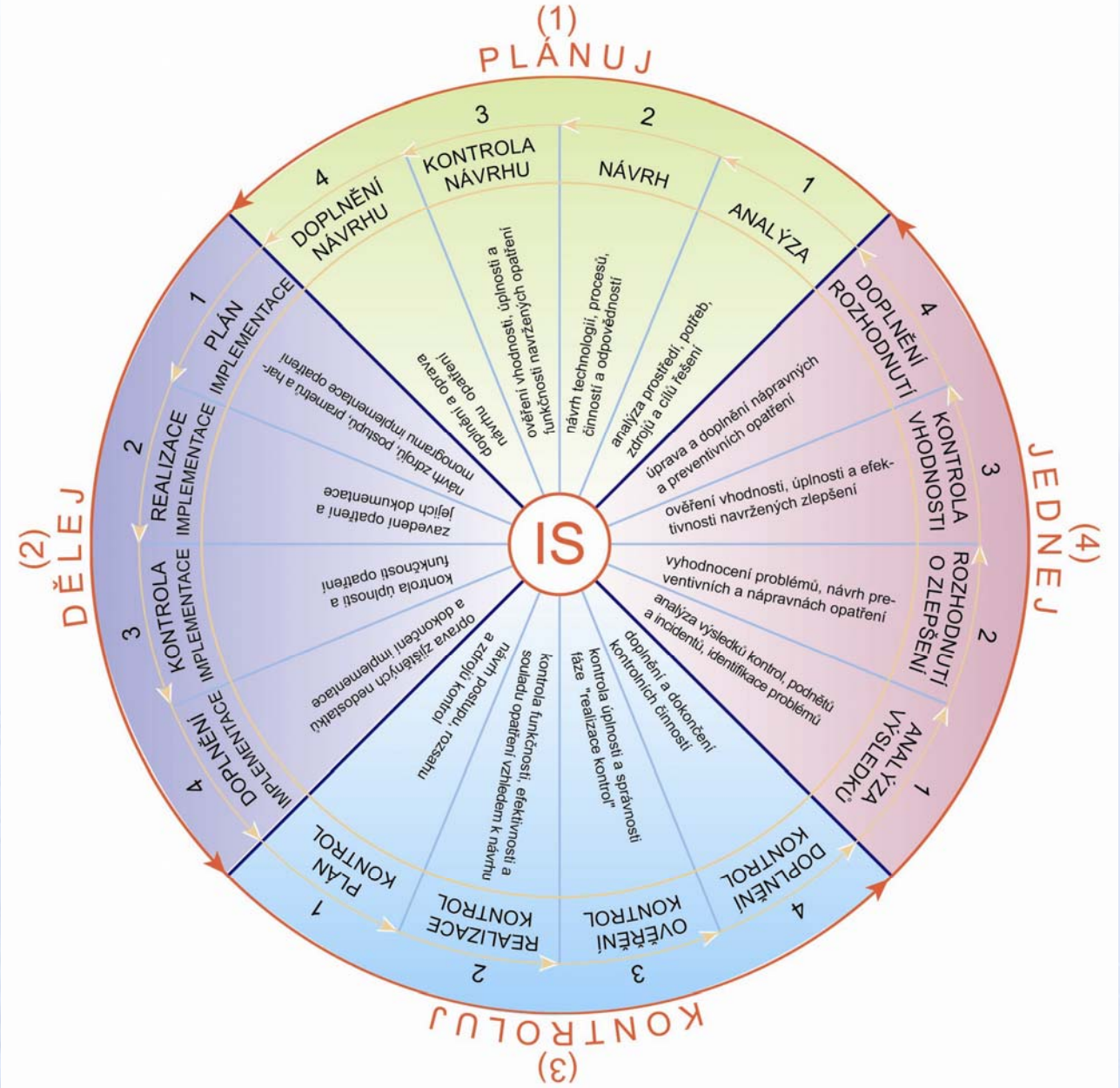
Dlouhodobé zajištění bezpečnosti informací, stejně jako udržení a zlepšování kvality produktů a služeb či stavu životního prostředí, je kontinuální a konzistentní proces v čase, pro jehož systematické řízení byl zaveden normami řízení (ISO 27001, ISO 9001, ISO 14001) shodný periodický procesní model PDCA. Ten je možné aplikovat na celkový proces řízení stejně jako na každé opatření a činnosti, které jsou v rámci systému řízení zavedeny a prováděny.

Seriál vyšel v upravené podobě v časopise Data Security Management 03/2004 až 06/2004.

Marek Skalický pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 2003. Dříve pracoval ve společnosti Aero Vodochody a.s., kde v letech 2001-2003 vykonával funkci Bezpečnostního správce IS. Nyní se věnuje projektům zavádění ISMS v organizacích, přípravě organizací na zpracování utajovaných skutečností, službám správy zranitelností ICT (VM) a jako člen Znaleckého ústavu RAC také forenzním analýzám IS.
Marek.Skalicky@rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

3.díl Check - Kontroluj



PDCA není přísně lineární proces, ale nekonečný proud navzájem vnořených PDCA smyček na různých úrovních detailu pohledu, které jsou realizovány v rámci jednotlivých činností a opatření každé etapy PDCA.

Nejlépe je to vidět na příkladu etapy Kontroluj (Check) celého procesu řízení bezpečnosti informací, která je realizována i v průběhu etap plánování (testování vhodnosti opatření při jejich výběru), zavádění opatření do provozu a jejich využívání (kontrola funkčnosti a nastavení), v průběhu kontroly ISMS (audit souladu s interní/externí dokumentací) a v průběhu zlepšování (výběr a testování nápravných a preventivních opatření).

Právě poslední etapa Jednej (Act) představuje ve své podstatě pouze rozhodovací krok, který spouští další paralelní obrátky PDCA procesů využívání a zlepšování ISMS. O této etapě a o významu certifikace ISMS pro malé a střední firmy pojednává následující díl tohoto seriálu.

Risk Analysis Consultants, Španělská 2, 120 00 Praha 2, Czech Republic, tel.+420 221 628 400, fax +420 221 628 401, rac@rac.cz, www.rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

3.díl Check - Kontroluj

	Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
PLAN	**Plán / projekt bezpečnosti**			
	Bezpečnostní politika			
	Organizace bezpečnosti			
	Analýza rizik			
	Výběr opatření a plán implementace			
	Prohlášení o aplikovatelnosti			
DO	**Způsob implementace opatření**			
	Metody prosazení bezpečnosti			
	Bezpečnostní dokumentace			
	Program zvyšování bezpečnostního povědomí			
	Způsob zvládání rizik za provozu			
	Nároky na provoz opatření a zajištění bezpečnosti			
	Zavedení opatření DRP a IRH Havarijní plány)			
CHECK	**Monitoring IS a testování funkčnosti opatření**	Namátkový monitoring provozu IS a vyhodnocování logů a záznamů událostí (v papírové i el. podobě). Otestování zranitelností u systémů připojených k Internetu.	Pravidelný monitoring a vyhodnocování logů a záznamů událostí (v papírové i elektronické podobě). Otestování zranitelností u systémů připojeným k externím subjektům (třetím stranám).	Centralizovaný a automatizovaný monitoring provozu ICT a vyhodnocování logů a záznamů událostí. Pravidelné testování zranitelností doplněné o penetrační testování (simulaci „hacker" útoků). Bezpečnostní analýza klíčových prvků systému.
	Audit a kontrola bezpečnostních opatření	Audit opatření včetně ISMS dle dokumentace a plánu auditu (v případě certifikace ISMS). Iniciuje ředitel, provádí vybraný pracovník jako rozšíření standardní pracovní náplně. Namátková interní kontrola stavu opatření.	Audit opatření včetně ISMS dle dokumentace a plánu auditu (v případě certifikace ISMS). Bezpečnostní technický audit nastavení klíčových ICT systémů. Namátková interní kontrola stavu opatření.	Pravidelná interní kontrola a audit bezpečnostních a ISMS opatření, dle interních směrnic a politik (vyhrazený interní auditor). Průběžný bezpečnostní technický audit konfigurace ICT a bezpečnostních záplat.
	Revize adekvátnosti a efektivnosti ISMS	Rámcová revize procesu ISMS a vyhodnocení aktuálnosti, efektivnosti a adekvátnosti opatření. 1 denní workshop s využitím externího konzultanta.	Roční podrobná revize procesu ISMS a stavu opatření s využitím externího konzultanta. Porovnávání stávajících opatření s novými trendy a vývojem hrozeb a zranitelností.	Srovnávací audit stavu ISMS s normou. Průběžné přehodnocování míry zbytkových a akceptovaných rizik vůči cílům organizace. Revize podnětů na zlepšení efektivnosti.
ACT	**Vyhodnocení fáze CHECK, identifikace a analýza neshod**			
	Nápravná a preventivní opatření			
ISMS	**Doporučení zavést ISMS**	Ano	Ano	Ano
	Doporučení certifikace ISMS	Ne (ANO pokud je nějaký systém řízení již certifikován)	Ano (jako další systém řízení)	Ano (jako součást IMS)

Seriál vyšel v upravené podobě v časopise Data Security Management 03/2004 až 06/2004.

Marek Skalický pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 2003. Dříve pracoval ve společnosti Aero Vodochody a.s., kde v letech 2001-2003 vykonával funkci Bezpečnostního správce IS. Nyní se věnuje projektům zavádění ISMS v organizacích, přípravě organizací na zpracování utajovaných skutečností, službám správy zranitelností ICT (VM) a jako člen Znaleckého ústavu RAC také forenzním analýzám IS.
Marek.Skalicky@rac.cz

ISMS v malých a středních firmách

4.díl Act - Jednej

Je bezpečnost informací problematikou spíše technologickou nebo manažerskou? Jak zajistit její dlouhodobou stabilitu a konzistentnost v čase, navzdory měnícím se vnitřním i vnějším podmínkám a prostředí organizace? Co je hlavním motorem procesu zavádění, údržby a zlepšování bezpečnosti informací, kde začíná a kde vlastně končí? Lze bezpečnost informací měřit a má smysl její certifikace? O těchto otázkách pojednává závěrečný 4.díl seriálu ISMS v malých a středních firmách.

Zlepšování ISMS

V předchozích částech byly popsány nejobsáhlejší a zdánlivě i nejdůležitější kroky procesu zavádění a využívání systému řízení bezpečnosti informací (ISMS) podle procesního diagramu PDCA normy ISO/IEC 27001:2005. V každém z dílů byly postupně nastíněny hlavní činnosti jednotlivých fází: Plánuj (PLAN), Dělej (DO) a Kontroluj (CHECK), s přihlédnutím na specifické prostředí malých a středních firem. Logickou náplní tohoto závěrečného dílu je tedy popis poslední (nikoliv však významem) čtvrté fáze Jednej (ACT), představující nejdůležitější rozhodovací krok celého procesu. Součástí tohoto dílu je i celkové zhodnocení významu ISMS a jeho certifikace pro prostředí malých a středních firem. Přehled všech hlavních kroků ISMS procesu s detailem na fázi Jednej (ACT) je uveden, jako v každém díle, na konci v tabulce.

V úvodu jsem pro první tři fáze PDCA procesu záměrně použil spojení „zdánlivě nejdůležitější“ což nyní uvedu na pravou míru: Aby bylo možné ve fázi Dělej (DO) implementovat a provozovat IS, aplikaci, bezpečnostní opatření nebo systém řízení, je vhodné realizovat nejdříve analýzu prostředí a potřeb a následně vybrat řešení a naplánovat jeho implementaci, neboli zrealizovat fázi Plánuj (PLAN). Pokud záleží na funkčnosti a spolehlivosti objektu, který byl ve fázi Dělej (DO) implementován a je provozován a všichni pořád dokola „otravují s tou bezpečností“, je nanejvýš vhodné realizovat kontrolu úplnosti a správnosti implementace zvoleného řešení (naplánovaného ve fázi Plánuj) a ověřit také splnění požadovaných parametrů. Jinými slovy realizovat fázi Kontroluj (CHECK). Tím jsou nastíněny hlavní principy závislostí prvních třech fází, ale bez přidání klíčové čtvrté fáze by se stal cyklus PDCA pouze jednorázovým procesem, díky němuž by se zabezpečení informací stalo statickou a velmi rychle zastaralou událostí v historii.

Klíčovým významem 4. fáze Jednej (ACT) je tedy **vyhodnotit výsledky auditu a kontrol funkčnosti** bezpečnostních opatření i ISMS procesu samotného a nastartovat další cyklus PDCA, ve kterém budou naplánovány, zavedeny, zkontrolovány a opět vyhodnoceny nápravná a preventivní opatření k zajištění požadovaného a konzistentního stavu bezpečnosti v čase.

Provedení každé fáze PDCA cyklu je vhodné také naplánovat, zrealizovat, poté zkontrolovat a doplnit. Proto v sobě obsahují další vnořené PDCA cykly, které se samostatně roztáčejí pro realizaci každého kroku, které byly pro danou fázi popsány v tomto seriálu. Princip vnořených PDCA fází uvnitř základního PDCA procesu ISMS znázorňuje obrázek na předchozí straně.

Popisem hlavních činností nejdůležitější rozhodovací fáze Jednej (ACT) procesu ISMS v prostředí malých a středních firem se zabývají následující kapitoly.

Vyhodnocení fáze Kontroluj

Základním předpokladem pro správné rozhodnutí „co a jak dál“ by vždy měly být co nejpřesnější a nejúplnější informace o aktuálním stavu a cílech organizace. Informace o aktuálním stavu týkající se monitoringu provozu, evidence chyb a bezpečnostních incidentů, výsledků testování funkčnosti a spolehlivosti implementovaných opatření, výsledků testování zranitelností a výsledky interních i externích auditů poskytuje předcházející fáze Kontroluj (CHECK). **Vyhodnocení** těchto informací **provádí v malých firmách pracovník pověřený činností bezpečnostního managera** na částečný úvazek, jako přidruženou činnost ke své pracovní náplni. Výsledky svého šetření by měl minimálně jednou ročně předložit majiteli, případně řediteli organizace a společně provést jejich analýzu a vyhodnocení.

U středních a velkých organizací se již vyplatí přidat do tohoto kroku také revizi návrhů a možných zlepšení bezpečnosti informací i procesu ISMS, jejichž evidenci zajišťuje **fórum pro bezpečnost** informací, složené ze zástupců uživatelů, dodavatelů a odborných rolí delegovaných pro oblast bezpečnosti informací v organizaci. V rámci procesu řízení rizik je prováděno také pravidelné přehodnocování úrovně zbytkových a přenesených rizik, s ohledem na změny v organizaci, technologiích, podnikatelských cílech a vnějších událostech a hrozbách.

Identifikace a analýza neshod

I když byla revize výsledků auditu zahrnuta již do předcházejícího kroku, je vhodné tuto činnost popsat podrobněji. Identifikace a analýza neshod má za úkol rozebrat výsledky interního i případného externího

Risk Analysis Consultants, Španělská 2, 120 00 Praha 2, Czech Republic, tel.+420 221 628 400, fax +420 221 628 401, rac@rac.cz, www.rac.cz

ISMS v malých a středních firmách

4.díl Act - Jednej

auditu a posoudit, které z nalezených neshod jsou skutečné, které pouze potenciální a vyřadit nesprávně identifikované neshody. Toto rozhodnutí je opět vhodné zaevidovat formou tabulky. Nakonec je pro odstranění skutečně identifikovaných neshod třeba navrhnout nápravná opatření a pro zabránění opakovaného výskytu skutečných i potencionálních neshod v budoucnu je třeba navrhnout preventivní opatření. Jejich výběr, implementace a ověření funkčnosti je již náplní dalších paralelních PDCA procesů (koleček), které jsou spuštěny pro každé nově navržené opatření.

U malých organizací provede tuto **analýzu neshod** majitel, případně ředitel organizace, ve spolupráci s pracovníkem pověřeným funkcí bezpečnostního managera. S výsledným rozhodnutím je vhodné seznámit všechny zaměstnance. Implementace těchto rozhodnutí bývá velmi rychlá a flexibilní. Pokud malá firma usiluje o certifikaci ISMS, je vhodné obrátit se pro pomoc na externího konzultanta, případně zrealizovat **srovnávací audit procesu ISMS vzhledem k ISO 27001** externí specializovanou firmou a s její pomocí navrhnout potřebná nápravná opatření pro dosažení souladu.

U středních firem bude interpretace výsledků auditů i návrh nápravných a preventivních opatření komplikovanější a formální proces, řízený pracovníky interního auditu ve spolupráci s dalšími zainteresovanými odbornými pracovníky organizace. Při přípravě na certifikaci ISMS se i zde doporučuje sáhnou pro pomoc externích odborníků, pokud takoví nejsou ve vlastních řadách.

Nápravná a preventivní opatření

Nápravná opatření slouží k odstranění skutečně nalezených nedostatků a chyb, spojených s implementací a provozem ISMS a k zabránění jejich dalšímu trvání (opakování). Jedná se například o neúplnou implementaci opatření zvolených v Prohlášení o aplikovatelnosti opatření, o chybějící dokumentaci těchto opatření, o nedostatečné proškolení pracovníků zainteresovaných v procesu ISMS apod.

Preventivní opatření jsou vybírána s cílem **zabránit výskytu potencionálních neshod** v budoucnu, tedy za účelem eliminace příčin, které by mohly vést ke vzniku reálné nežádoucí situace a reálné neshody. Příkladem takové potencionální neshody může být například nedodržení oddělení rolí u některých činností a opatření ISMS nebo nedůsledné provádění potřebných monitorovacích a kontrolních činností.

Pro malé organizace je typická rychlá praktická změna bez byrokratických průtahů a příklon především k organizačním a personálním opatřením, jejichž „pořízení a zavedení“ bývá pro majitele malých firem nejpřijatelnější.

Pro střední organizace, stejně jako ve fázi Dělej (popis nároků na provoz opatření), není již hledisko nákladů na pořízení a zavedení opatření tak palčivé jako pro malé organizace a bude při jejich výběru více rozhodovat jeho účinnost a pokrytí nalezených nedostatků.

Zavést ISMS?

Uvedeným přehledem byly popsány všechny hlavní kroky tvořící pilíře procesu ISMS, tak jak jsou definovány normou ISO 27001, která se v roce 2006 stane také součástí soustavy norem ČSN.

Existuje jednoznačná odpověď na otázku zda zavádět ISMS proces v prostředí malých a středních firem? Pokud existence, poslání nebo strategické cíle těchto firem závisejí na zajištění některého z „parametrů“ bezpečnosti informací – tj. na dostupnosti, důvěrnosti nebo integritě informací a dat, je odpověď **jednoznačně ANO**. Zavedení systému řízení samo o sobě nezaručuje kvalitativní nárůst některého z parametrů bezpečnosti informací, ale představuje odzkoušený a celosvětově uznávaný postup, jak dosáhnout bezpečnosti informací adekvátní požadavkům a cílům organizace a jak jí udržovat a efektivně zlepšovat v čase, za pomocí ochranných opatření, odpovědností, činností a řídících a kontrolních procesů. Vzhledem ke své formalizaci tak poskytuje zdokumentovanou inventuru činností a odpovědností, které se ve velké míře stejně v organizacích provádějí, většinou ale nesystematicky a nedůsledně, což v praxi způsobuje vážná rizika a bezpečnostní incidenty.

Certifikovat ISMS?

Odpověď zda certifikovat ISMS prozatím tak jednoznačná není. Zavedení ISMS má prokazatelně pozitivní efekt. Vzhledem k narůstající závislosti firem na informačních systémech, jejich propojování a sdílení informací v rámci B2B a B2C aplikací a vzhledem k požadavkům platné národní a nadnárodní legislativy na zabezpečení informací a dat je správně zavedený a provozovaný ISMS chápán jako vysoký stupeň záruky adekvátní ochrany dat. Zvyšující se počty projektů implementace ISMS i v České republice jsou toho důkazem.

Lze ale míru (stupeň) zabezpečení informací v IS organizace objektivně měřit? Celková bezpečnost informací v organizacích je zajišťována kombinací technologických opatření, fyzických, personálních a administrativních, které by měly být implementovány

Seriál vyšel v upravené podobě v časopise Data Security Management 03/2004 až 06/2004.

Marek Skalický pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 2003. Dříve pracoval ve společnosti Aero Vodochody a.s., kde v letech 2001-2003 vykonával funkci Bezpečnostního správce IS. Nyní se věnuje projektům zavádění ISMS v organizacích, přípravě organizací na zpracování utajovaných skutečností, službám správy zranitelností ICT (VM) a jako člen Znaleckého ústavu RAC také forenzním analýzám IS.
Marek.Skalicky@rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

4.díl Act - Jednej

v rozsahu a kvalitě odpovídající prostředí a potřebám každé jednotlivé organizace. Jednou z možností jak hodnotit míru bezpečnosti informací je posouzení kvality procesu řízení bezpečnosti informací ISMS, vyhodnocením míry souladu s požadavky na tento proces dle normy ISO 27001.

Pro malé a střední firmy představuje proces přípravy a samotné certifikace akreditovanou certifikační autoritou nemalou investici, kterou je třeba manažersky a ekonomicky zvážit. Pokud firma podniká v sektoru, kde je důvěryhodnost vysoce ceněným faktorem a podmínkou úspěšných obchodních vztahů, může být pro takovou firmu užitečné realizovat certifikaci bezpečnosti informací **jako další důkaz kvality řízení** k certifikátu QMS nebo EMS (dle ISO 9001:2000 a ISO 14001:1996). Certifikace ISMS do prostředí firem, kde je již certifikován jiný systém řízení, je méně náročnou variantou. Vzhledem k harmonizovanému PDCA modelu ISMS, QMS a EMS je řada procesů a odpovědností již nastavena.

Ve světě existují již téměř dva tisíce (stav k 11/2005) certifikátů ISMS dle normy BS 7799:2000, která je předchůdcem ISO/IEC 27001:2005. Podle ISMS International User Group – Certificate Register (*http://www.xisec.com*) bylo nejvíce certifikátů bylo dosud uděleno ve Velké Británii a Japonsku. V České Republice má v rámci integrovaného systému řízení certifikovaný ISMS zatím pouze společnost Eurotel (více informací viz. Aktuality DSM 5/2004). Stojí za zmínku, že zkušenosti získané v rámci implementace ISMS a přípravy této organizace na certifikaci přispěly ke vzniku tohoto seriálu. Vlna certifikací ISMS je teprve před námi a jeví se velice pravděpodobné, že se prosadí ve stejné míře jako dnes certifikace QMS a EMS.

Závěr

Touto prognózou končí seriál ISMS v malých a středních firmách, který si kladl za cíl prakticky popsat hlavní kroky procesu implementace a využívání ISMS, s přihlédnutím k podmínkám malých a středních firem. Při jeho tvorbě jsme se setkali s kritickými i pozitivními ohlasy na ISMS. Ty kritické zpochybňovaly aplikovatelnost a efektivnost principů ISMS pro prostředí těchto firem a zatracovaly ISMS jako zbytečnou byrokracii. Naopak pozitivní, kterých bylo mnohem více, zdůrazňovaly **univerzálnost PDCA modelu řízení a jeho využitelnost pro bezpečnost informací nejen malých a středních firem**.

Je třeba přiznat, že zavedení a provoz ISMS přináší zaměstnancům i vedení firem nárůst režijních kapacit. To ale zejména proto, že donutí odpovědné osoby vykonávat činnosti, které bývají v běžné praxi opomíjeny a nebo v horších případech nejsou vůbec delegovány.

Zbývá odpovědět na první otázku z perexu tohoto dílu: Bezpečnost informací v organizacích JE problematikou technologickou stejně jako manažerskou. Jedna část nemůže účinně a efektivně fungovat bez druhé. Správná konfigurace ICT produktů a bezpečnostních opatření poskytuje většinou dobrou úroveň ochrany informací. Bez zajištění ISMS řídícího procesu jsou však časem znehodnoceny na úroveň zapomenuté zrezlé závory s utrženou cedulí „Zákaz vstupu“, kolem které vede vyšlapaná stezka do zakázaného prostoru. Známe to přeci z praxe všichni.

Využité zdroje a další informace:

- www.ISO27000.cz
- ISO/IEC 17799:2005 IT - Security techniques - Code of practice for information security management
- ISO/IEC 27001:2005 IT - Security techniques - Information security management systems - Requirements
- BS 7799-2:2002 ISMS - Specification with guidance for use
- ISO 9001:2000 QMS – Requirements
- ISO 14001:1996 EMS - Specification with guidance for use
- ISO 19011:2002 - Guidance for management systems auditing
- PD 3002:2002 Guide to BS 7799 Risk Assessment
- PD 3004:2002 Guide to the implementation and auditing of BS 7799 controls
- PD 3005:2002 Guide on the selection of BS 7799 controls
- ISMS International User Group – Certificate Register (*http://www.xisec.com*)

Risk Analysis Consultants, Španělská 2, 120 00 Praha 2, Czech Republic, tel.+420 221 628 400, fax +420 221 628 401, rac@rac.cz, www.rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

4.díl Act - Jednej

	Proces	Malá organizace do 15 zaměstnanců 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců 3-5 úrovní vedení	Velká organizace nad 150 zaměstnanců 4 a více úrovní vedení
PLAN	Plán / projekt bezpečnosti			
	Bezpečnostní politika			
	Organizace bezpečnosti			
	Analýza rizik			
	Výběr opatření a plán implementace			
	Prohlášení o aplikovatelnosti			
DO	Způsob implementace opatření			
	Metody prosazení bezpečnosti			
	Bezpečnostní dokumentace			
	Program zvyšování bezpečnostního povědomí			
	Způsob zvládání rizik za provozu			
	Nároky na provoz opatření a zajištění bezpečnosti			
	Zavedení opatření DRP a IRH Havarijní plány)			
CHECK	Monitoring IS a testování funkčnosti opatření			
	Kontrola a audit bezpečnostních opatření			
	Revize adekvátnosti a efektivnosti ISMS			
ACT	Vyhodnocení fáze Kontroluj	Revize zejména bezpečnostních incidentů, chyb a průběhu jejich řešení (dle potřeby). Revize penetračního a zkušebního testování, pokud bylo realizováno. Revize výsledků ročního auditu.	Pravidelná revize incidentů, chyb a průběhu jejich řešení. Revize penetračních a dalších typů testů. Revize výsledků auditu. Revize nápadů a podnětů ke zlepšení. Revize adekvátnosti a efektivnosti ISMS.	Proces průběžné revize výsledků monitoringu provozu, IDS systémů, incidentů, chyb a průběhu jejich řešení. Revize penetračních testů a technických auditů konfigurace systémů. Revize nápadů a podnětů ke zlepšení. Revize adekvátnosti a efektivnosti ISMS.
	Identifikace a analýza neshod	Identifikace a evidence možností zlepšování, reálných neshod a potenciálních problémů. Interpretace a okamžitý návrh opatření ředitelem / majitelem.	Identifikace a evidence možností zlepšování, reálných neshod a potenciálních problémů. Interpretace výsledků kontrol interním auditem s využitím externích odborníků. Jednoduchý projekt pro návrh opatření.	Identifikace a řízená evidence možností zlepšování, neshod a potenciálních problémů. Vícestupňový proces analýzy neshod bezp. auditem a jejich interpretace bezp ředitelem. Kompletní projekt pro návrh a testování opatření
	Nápravná a preventivní opatření	Přednostní výběr jednoduchých organizačních a personálních opatření, bez nutnosti investic. Rychlé zavedení dostupných opatření do praxe.	Výběr organizačních opatření podpořených technologiemi a nástroji. Testování opatření před uvedením do praxe. Aktualizace bezpečnostní dokumentace.	Výběr a implementace opatření formou projektu Primárně výběr robustních a automatizovaných opatření s podrobným testování a sledováním účinnosti a přizpůsobení organizaci. Řízená aktualizace bezpečnostní dokumentace.
ISMS	Doporučení zavést ISMS	Ano	Ano	Ano
	Doporučení certifikace ISMS	Ne (ANO pokud je nějaký systém řízení již certifikován)	Ano (jako další systém řízení)	Ano (jako součást IMS)

Seriál vyšel v upravené podobě v časopise Data Security Management 03/2004 až 06/2004.

Marek Skalický pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 2003. Dříve pracoval ve společnosti Aero Vodochody a.s., kde v letech 2001-2003 vykonával funkci Bezpečnostního správce IS. Nyní se věnuje projektům zavádění ISMS v organizacích, přípravě organizací na zpracování utajovaných skutečností, službám správy zranitelností ICT (VM) a jako člen Znaleckého ústavu RAC také forenzním analýzám IS.
Marek.Skalicky@rac.cz

ISMS v MALÝCH A STŘEDNÍCH FIRMÁCH

Management Summary

Plánuj

Způsob zavádění ISMS ve smyslu ISO/IEC 17799:2005 a ISO/IEC 27001:2005 je rozdílný pro organizace s ohledem na jejich velikost. První se čtyř dílů článku popisuje rozdíly v procesu plánování ISMS v malých a středních firmách. Zaměřuje se na strategii bezpečnosti, bezpečnostní politiku, organizační strukturu bezpečnosti, způsoby provádění analýzy rizik a výběr vhodných protiopatření. Další díly popisují zbývající činnosti zavádění a využívání ISMS podle modelu PDCA.

Dělej

Základní opatření ISMS a činnosti při jeho zavádění a využívání v malých a středních organizacích jsou rámcově shodné jako v prostředí velkých organizací. Liší se však ve způsobu, rozsahu a hloubce jejich aplikování, přizpůsobeným na míru konkrétním organizacím. Tento článek popisuje příklady náplní hlavních činností kroku Dělej (Do) a jejich specifika v prostředí malých a středních firem.

Kontroluj

Pro kvalifikované řízení každé činnosti nebo procesu v čase je třeba periodicky získávat informace o její funkčnosti, spolehlivosti a efektivnosti. Pokud jsou stanoveny cíle a deklarovány opatření k jejich naplnění, je možné kontrolovat i míru dosažení shody s požadovaným stavem. Etapa Kontroluj (Check) využívá všech těchto kontrolních kroků a opatření k dosažení konzistentní bezpečnosti informací, deklarované v bezpečnostní dokumentaci.

Jednej

Závěrečný díl seriálu ISMS popisuje hlavní kroky fáze „Jednej" (ACT), která představuje rozhodovací krok ke zlepšování úrovně bezpečnosti informací na základě vyhodnocení výsledků kontrolních činností a návrhu nápravných a preventivních opatření. V závěru článku jsou zhodnoceny přínosy zavedení a certifikace ISMS pro sektor M&S firem.

Plan

The method of ISMS implementation as described in IEC 17799:2005 and ISO/IEC 27001:2005 is different for organizations of various sizes. This is the first part of a series of four articles and describes differences in the ISMS planning process in small and medium enterprises. It focuses on security strategy, policy, security infrastructure, risk analysis methods and selection of appropriate countermeasures. The next articles in the series will deal with the remaining activities related to implementation and use of ISMS according to the PDCA model.

Do

The main controls and processes for ISMS implementation and operation are basically the same for small and medium enterprises as for large enterprises. The main difference is in the method, range and depth of their application, which are adapted to the requirements of the individual organization. This article describes examples of the "Do" stage controls and processes, adapted for small and medium enterprise areas.

Check

Periodic information about functionality, reliability and efficiency is necessary for the proper management of any activity or process. Compliance with a desired status can be checked only if the objectives are declared and the measures to achieve the objectives are defined. The "Check" stage uses all these controls to attain consistent information security described in the security documentation.

Act

Last in the series of articles describing the main activities is the "Act" stage that represents a decision-making step towards improving the information security level based on the evaluation of control activity results and suggested corrective and preventive measures. The article concludes with an evaluation of the benefits of implementation and certification of ISMS for small and medium enterprises.

Jan Mikulecký pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 1999. Hlavní specializací je provádění analýzy rizik informačních systémů a zavádění ISMS v různých organizacích. Dále školí metodiky a standardy v oblasti bezpečnosti informací v Česku i dalších zemích Evropy. Absolvoval ČVUT v Praze, kde nyní pokračuje v doktorandském studiu.
Jan.Mikulecky@rac.cz

Marek Skalický pracuje jako konzultant ve společnosti Risk Analysis Consultants od roku 2003. Dříve pracoval ve společnosti Aero Vodochody a.s., kde v letech 2001-2003 vykonával funkci Bezpečnostního správce IS. Nyní se věnuje projektům zavádění ISMS v organizacích, přípravě organizací na zpracování utajovaných skutečností, službám správy zranitelností ICT (VM) a jako člen Znaleckého ústavu RAC také forenzním analýzám IS.
Marek.Skalicky@rac.cz