

CRAMM 5 CASE STUDY

ANALÝZA RIZIK JE NUTNÁ PRO CERTIFIKACI ISMS PODLE ISO 27001

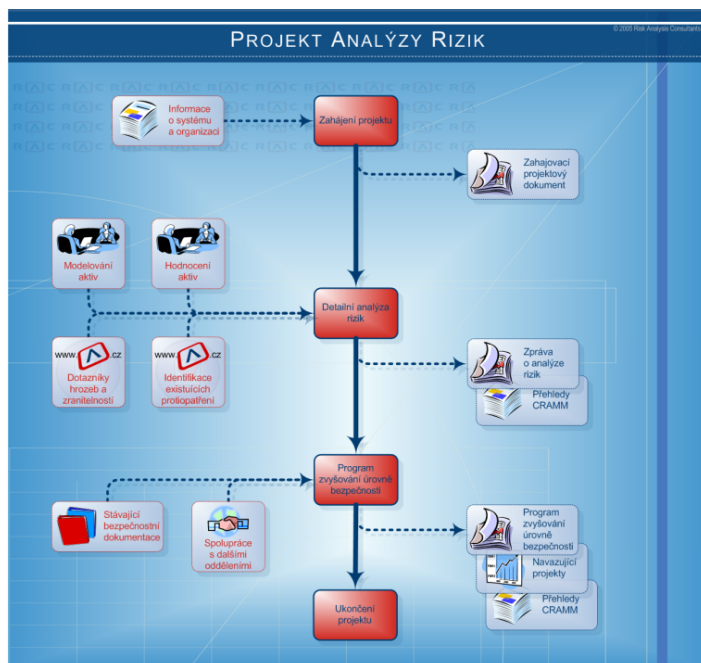
Management významného českého holdingu se rozhodl zavést a provozovat Systém řízení bezpečnosti informací (ISMS). Analýza rizik provedená metodikou CRAMM byla nedílnou součástí projektu, který později vedl k úspěšné certifikaci systému podle ISO/IEC 27001 (BS7799-2). Metodika CRAMM je v Evropě nejužívanější metodikou pro analýzu a řízení rizik a její kvality byly potvrzeny již při mnoha certifikacích ISMS. Zejména rozsáhlá knihovna opatření a šablony bezpečnostní dokumentace jsou velmi užitečné při zavádění i provozu ISMS.

Pracovníci bezpečnostního oddělení chtěli přípravu na certifikaci ISMS zvládnout velmi efektivně a proto požádali přední konzultační společnost o spolupráci. Pro projekt byl zvolen **partnerský přístup**, v rámci kterého pracovníci holdingu a konzultanti prováděli veškeré činnosti v úzké spolupráci. Tento způsob práce efektivně využil všechny zdroje a zajistil přenos know-how na pracovníky holdingu.

Zahájení projektu

Projektový tým byl sestaven ze dvou pracovníků bezpečnostního oddělení a dvou konzultantů, z nich jeden celý projekt vedl. Pro řízení projektu byla využita metodika PRINCE2, podle které proběhly všechny činnosti nutné pro úspěšné zahájení. Cíl projektu, přístup, plán kvality, časový harmonogram, tým a zejména popis všech činností včetně zdrojů a odpovědností projektu byly shrnuty v Zahajovacím projektovém dokumentu, který se stal prvním výstupem.

V rámci přípravy byly shromážděny informace o používaných systémech a provedena revize stávající bezpečnostní dokumentace.



Zahajovací projektový dokument

- 📄 **Cíl projektu**
- 📄 **Přístup k provedení projektu, použité metodiky**
- 📄 **Projektový tým, role v projektu**
- 📄 **Fáze projektu, včetně zdrojů, výstupů a odpovědností**
- 📄 **Časový harmonogram projektu**
- 📄 **Plán kvality, rizika projektu**

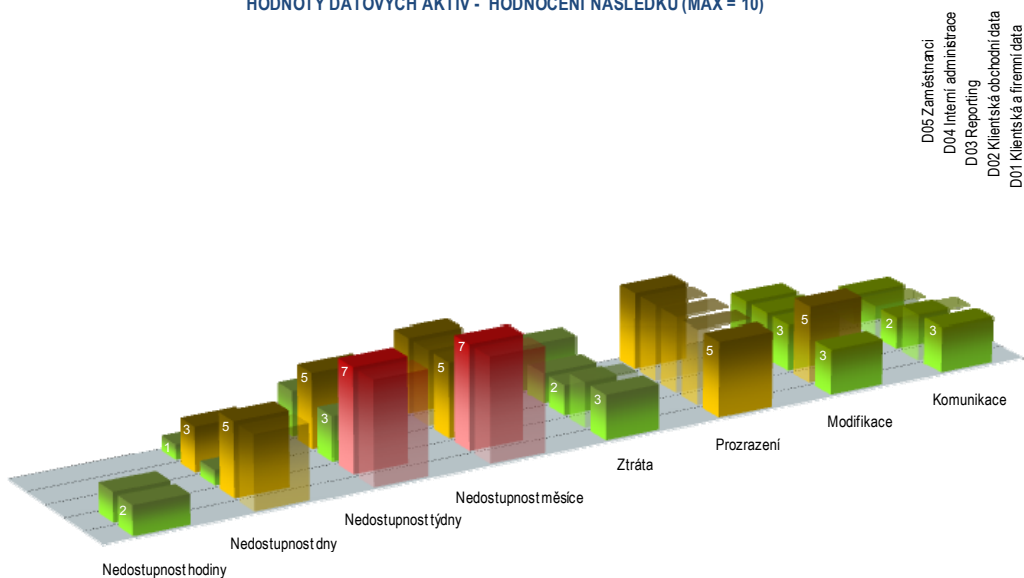
„Měli jsme omezené zdroje, ale díky partnerskému přístupu a metodice CRAMM jsme je využili velmi efektivně.“
Jan Novák, Bezpečnostní manager

EFEKTIVNÍ NÁSTROJE PRO HODNOCENÍ RIZIK

Identifikace aktiv

Aktivem v organizaci je prakticky vše, co má souvislost se zpracováním informací. Nejdůležitější jsou aktiva datová, jejichž identifikace není pokaždé jednoduchá. Holding zpracovával obrovské množství informací o výrobě, zákaznících, dodavatelích, osobní údaje zaměstnanců, strategické informace managementu včetně účetnictví a další.

HODNOTY DATOVÝCH AKTIV - HODNOCENÍ NÁSLEDKŮ (MAX = 10)



Nejdříve byly specifikovány skupiny dat, v rámci kterých byly v průběhu analýzy definovány podskupiny, například podle druhu a obsahu dat, oddělení anebo citlivosti. Celkem bylo identifikováno 54 podskupin seříděných do 10 základních skupin dat.

Již v průběhu identifikace byly sumarizovány podklady pro modely aktiv. Každý server, pracovní stanice, síťový prvek, aplikace, linky apod. byly podrobeny jednoduché analýze a vznikly tak typové modely vyjadřující vztahy a závislosti mezi daty, procesy, aplikacemi, hardwarem a prostory.

Analýza dopadů

Hodnocení datových aktiv proběhlo v rámci několika interview s předem vybranými respondenty (uživatelé jednotlivých skupin nebo podskupin dat). Tito pracovníci popisovali potencionální následky, které by mohli finančně i jinak poškodit holding při nedostupnosti dat, při jejich prozrazení nebo modifikaci.

Při stanovení hodnot dat byly zkoumány mj. finanční dopady, narušení výroby, ztráta dobrého jména nebo újma na zdraví. Reálné popisy těchto následků byly porovnávány s vodítky hodnocení, která jsou pevnou součástí metodiky CRAMM. Ta poskytla velmi kvalitní podporu při určení konečné hodnoty datových aktiv.

V rámci škály hodnot 1-10 byly nejdříve ohodnoceny podskupiny dat, a poté byly odvozeny maximální hodnoty pro každou skupinu reprezentující jedno datové aktivum v CRAMM.

U fyzických aktiv (hardware) byla určena jejich hodnota na obnovu, tedy výše aktuálních nákladů na jejich nové pořízení a instalaci v případě celkového zničení.

Hodnocení hrozeb a zranitelností

Cílem druhé části detailní analýzy bylo určit míru rizik ohrožující systém. Pro každé aktivum byly specifikovány hrozby a zranitelnosti a poté pomocí dotazníků ohodnoceny. Respondenti, převážně administrátoři a pracovníci z odd. fyzické bezpečnosti, odpovídali na jednotlivé otázky prostřednictvím webového rozhraní CRAMM, které bylo přístupné na intranetu holdingu.

Po vyplnění všech dotazníků byla nástrojem CRAMM vypočtena míra rizika a mohla být vygenerována bezpečnostní protiopatření pokrývající rizika.

CRAMM definoval doporučenou sadu protiopatření pro všechny oblasti bezpečnosti. Dalším úkolem bylo zaznamenat již zavedená opatření a vybrat ta, která budou učená k implementaci. Proto přišla na řadu opět webová aplikace, kde respondenti volili stavy jednotlivých opatření, případně rozhodovali o jejich aplikovatelnosti.

EFEKTIVNÍ NÁSTROJE PRO HODNOCENÍ RIZIK

Pro Zprávu o analýze rizik byla využita šablona dokumentu z CRAMM. Zpráva shrnovala, kromě hodnocení a modelování aktiv, také úroveň hrozeb a zranitelností, míru rizika a popis aktuálního stavu bezpečnosti.

Popis byl založen na statistice stavů protiopatření prezentující, kolik procent doporučených bezpečnostních opatření je zavedeno a jakou část je nutné ještě implementovat.

Všechny závěry byly prezentovány v manažerské (shrnující) formě. Nicméně na jejich podporu byla vytvořena sada reportů CRAMM, které poskytly detailní hodnoty pro každé aktivum, jeho míru rizika, relevantní hrozby nebo konkrétní protiopatření. Reporty byly, kvůli jejich velkému rozsahu, vygenerovány pouze v elektronické podobě v mnoha variacích.

Program zvyšování úrovně bezpečnosti

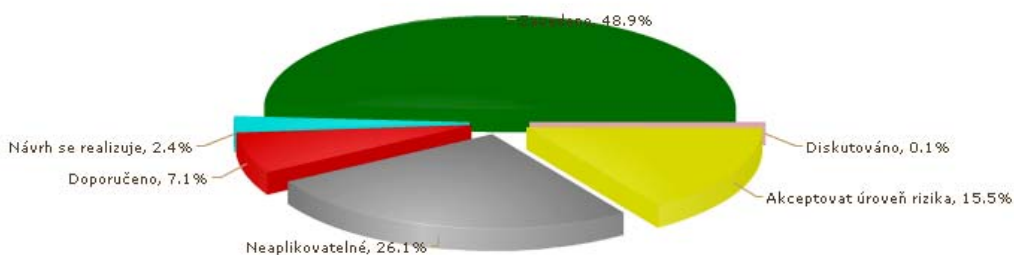
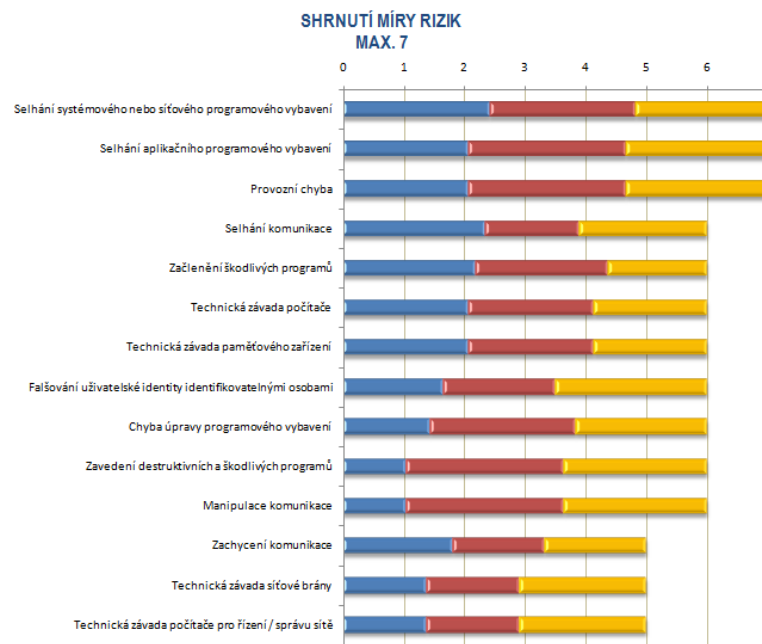
Detailní analýza rizik ukázala slabá místa v zabezpečení systému. Proto byly pro proces implementace protiopatření definovány rámce navazujících projektů.

Cílem každého z nich bylo zvýšit úroveň bezpečnosti pro určitý systém anebo oblast výroby či podpory.








projekty pro vytvoření bezpečnostní dokumentace, zavedení nových technologií nebo zlepšení fyzické bezpečnosti.

Všechny implementační projekty zastřešoval Program na zvyšování úrovně bezpečnosti, který popisoval činnosti, zdroje, odpovědnosti a

výstupy jednotlivých projektů. Součástí Programu bylo také prohlášení managementu o maximální podpoře při jeho realizaci.



Program zvyšování úrovně bezpečnosti (rámeček navazujících projektů)

-  Tvorba bezpečnostní dokumentace
-  Změna organizace bezpečnosti
-  Zvýšení fyzické bezpečnosti
-  Kontinuální program pro zvýšení bezpečnostního povědomí
-  Zavedení incident managementu
-  Business Continuity Management
-  eSecurity Infrastructure

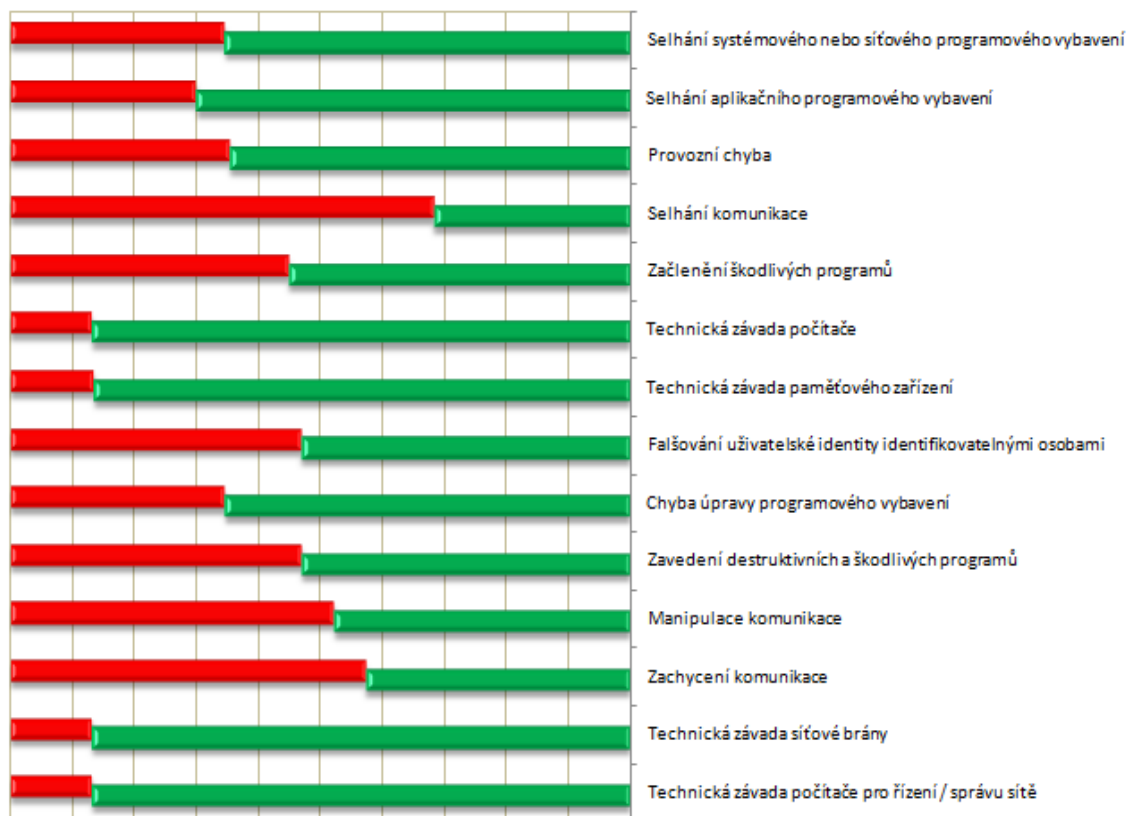
Analýza rizik byla základním krokem k úspěšnému zavedení ISMS. V holdingu jsou nyní všechna rizika

řádně řízena, což potvrdil i certifikační audit provedený akreditovanou organizací.

Získání certifikátu podle ISO/IEC 27001 je dostatečným důkazem pro zákazníky, dodavatele i pracovníky holdingu, že informace o nich jsou dostatečně a efektivně zabezpečeny.

Nástroj je stále využíván pro řízení informačních rizik a podporu ISMS. Holding aktuálně uvažuje o zavedení systému řízení kontinuity (BCMS), kde CRAMM zcela jistě najde své uplatnění v analytické části přípravy.

AKTUÁLNÍ STAV PROTIPATŘENÍ



Risk Analysis Consultants, s. r. o.
Španělská 2
120 00 Praha 2
Česká republika
+420 221 628 400
rac@rac.cz
www.rac.cz

Risk Analysis Consultants je nezávislá poradenská společnost poskytující služby a řešení ve všech oblastech bezpečnosti informací v souladu s mezinárodními normami, související národní legislativou a respektováním individuálních podmínek klientů. Od roku 1995 pomáhá zajišťovat bezpečnost informací v informačních systémech organizací státní správy, bank, finančních institucí, telekomunikačních společností a průmyslových podniků v České republice i v zahraničí.



QR kód RAC