Slovenská technická univerzita v Bratislave
Fakulta informatiky a informačných technológií
Ilkovičova 3, 842 16 Bratislava 4

Nástroje na analýzu rizík

Dávid Oros, Roman Panenka

Študijný program: Počítačové a komunikačné systémy a siete
Predmet: Bezpečnosť a manažment informačných systémov
Ročník: Ing. 1.
Akademický rok: 2010/2011

OBSAH

1. ÚVOD

1.1. ÚČEL A OBSAH DOKUMENTU

Nasledovný dokument venujeme softvérovým podporným nástrojom na analýzu rizík informačných systémov (IS). Analýza rizík IS je dôležitá časť implementácie a prevádzky informačných systémov, ktorá môže ušetriť nemalé prostriedky na eliminovanie neskorších škôd , a preto by jej mali spoločnosti venovať primeranú pozornosť.

V prvej časti dokumentu sa uvedieme do problematiky analýzy rizík ako takej a spomenieme ako pomáha táto analýza pri bezpečnosti IS. Priblížime si rôzne prístupy k analýze rizík a výhody použitia práve softvérových nástrojov.

Druhá časť dokumentu sa venuje európskej agentúre pre sieťovú a informačnú bezpečnosť (ENISA) a jej vzťahu k analýze rizík IS. Ďalej si priblížime sedem vybraných nástrojov na analýzu rizík IS, pričom sa budeme venovať vlastnostiam, výhodám a nevýhodám týchto nástrojov.

V poslednej, tretej, časti si zhrnieme výsledky našej analýzy nástrojov, porovnáme ich výhody podľa rozličných, nami zvolených, aspektov, zhodnotíme použitie nástrojov v rozličných sférach, uvedieme pre ktoré cieľové skupiny sú nástroje vhodné a naše zistenia zhrnieme v závere.

1.2. ZÁKLADNÉ POJMY

Pre zlepšenie prehľadnosti dokumentu uvádzame v tejto kapitole význam základných pojmov z oblasti tento problematiky a význam používaných skratiek.

Aktíva – sú všetok majetok z hľadiska jeho formy, teda konkrétnych druhov. Jeden konkrétny druh majetku sa nazýva aktívum.

Informačný systém (IS) - je systém na zber, udržiavanie, spracovanie a poskytovanie informácií. Systém nemusí byť nutne automatizovaný pomocou počítačov a môže byť aj v papierovej forme.

Hrozba - možná príčina neželaného incidentu, ktorý môže vyústiť do poškodenia systému alebo organizácie.

Riziko - vyjadruje potenciálnu možnosť, že daná hrozba využije zraniteľnosť systému alebo spoločnosti, aby spôsobila stratu alebo poškodenie aktív.

Analýza rizík - Analýza rizík identifikuje hrozby a ich riziká, ktoré je potrebné akceptovať alebo korigovať. Cieľom analýzy rizík je identifikovať a ohodnotiť hrozby, ktorým je informačný systém vystavený, aby mohli byť vybrané relevantné ochranné opatrenia.

Manažment rizík - je riešenie rizík, ktoré môžu nastať v organizácii alebo časti činnosti organizácie. Väčšinou sú tieto riziká určené v procese analýzy rizík.

ISO 27001 - Systém riadenia informačnej bezpečnosti podľa ISO 27001 je určený k ochrane informácií a teda k zvládaniu rizík, ktoré tieto informácie môžu potenciálne ohrozovať.

ISMS (Information Security Management System) - Systém riadenia bezpečnosti informácií je dokumentovaný systém, v ktorom sú chránené definované informačné aktíva, sú riadené riziká bezpečnosti informácií a zavedené opatrenia sú kontrolované.

Európska únia (EÚ) je medzinárodné spoločenstvo, ktoré od posledného rozšírenia v roku 2007 tvorí 27 členských štátov s celkovým počtom 496 miliónov obyvateľov

2. ANALÝZA RIZÍK

2.1. ÚVOD DO PROBLEMATIKY

V súčasnom svete informačných technológií sa nedá s úplnom istotou spoliehať na žiadnu technológiu. To spôsobuje, že každý informačný systém sa môže začať správať neštandardne a môže spôsobiť radu problémov tak na strane zákazníka alebo dodávateľa. Inak povedané, pred nasadením informačného systému do produkcie je potrebné nájsť potenciálne riziká. Riziko vyjadruje potenciálnu možnosť, že daná hrozba využije zraniteľnosť systému alebo spoločnosti, aby spôsobila stratu alebo poškodenie aktív, a teda priamo alebo nepriamo spoločnosti.

Zneužitie takýchto rizík v informačných systémoch môžu do veľkej miery obmedziť a ochromiť podnikové napredovanie, biznis ako taký a v neposlednej rade aj reputáciu podniku medzi konkurenciou a stálymi zákazníkmi.

Analýza rizík je proces, prostredníctvom ktorého sa identifikujú bezpečnostné riziká, ktoré je potrebné kontrolovať alebo akceptovať. Preto by mala každá osoba nasadzujúca informačný systém do produkcie za účelom zisku alebo poskytovanie služieb minimálne zvážiť analýzu potenciálnych rizík. Túto analýzu by mal pravidelne opakovať a prispôsobovať aktuálnym a novým bezpečnostným hrozbám.

2.2. AKO POMÁHA ANALÝZA RIZÍK PRI BEZPEČNOSTI IS

V kontexte bezpečnosti informačných systémov je analýza rizík chápaná nielen ako nástroj na analýzu hodnôt aktív, hrozieb a zraniteľností, ale aj ako nástroj na určenie potenciálnych rizík, vyplývajúcich zo zneužitia týchto zraniteľnosti.

Analýza rizík IS poskytuje viacero výhod pre zvýšenie bezpečnosti IS:

- určenie pravdepodobných rizík týkajúcich sa aktív spoločnosti
- je výstupnou bránou pre manažment rizík
- počiatočná krátka analýza všetkých informačných systémov môže byť vykonaná rýchlo a bez nutnosti ďalších investícií
- určenie systémov, ktoré môže byť chránené na základe všeobecných postupov a kontrol
- určenie systémov, ktoré budú podstúpené podrobnejšej analýze rizík

2.3. PRÍSTUPY K ANALÝZE RIZÍK

Základný prístup

Základný prístup poskytuje výhodu minimálneho množstva zdrojov pre analýzu a manažment rizík. Pri tomto prístupe sa totiž aplikuje rovnaká základná bezpečnosť pre všetky informačné systémy. Na dosiahnutie bezpečnosti sa používajú štandardné bezpečnostné opatrenia. Tento prístup môže spôsobovať nedostatočnú alebo nadmernú mieru bezpečnosti pre niektoré IS.

Klasický prístup

Klasický prístup vyžaduje taktiež malé množstvo vstupných zdrojov a je vykonávaný omnoho rýchlejšie, no prináša zo sebou aj viacero rizík. Nehovorí sa tu totiž o žiadnych štruktúrovaných metódach, ale využíva vedomosti jednotlivcov. To do procesu analýzy zavádza určitý stupeň subjektivity, neodbornosti a nekompletnosti procesov. Prevádzané zmeny nie sú dokumentované.

Detailný prístup

Detailný prístup vyžaduje viac úsilia a vedomostí. Informačné systémy sú podstupované hĺbkovej analýze a identifikácií možných rizík a zraniteľností. Následne sú navrhnuté a implementované bezpečnostné opatrenia pre dosiahnutie požadovanej úrovne bezpečnosti IS. Tento zdĺhavý ale precízny prístup môže spôsobiť neskoré ošetrenie niektorých zraniteľností.

Kombinovaný prístup

Kombinovaný prístup je najrozumnejší prístup s má veľa výhod. V prvom kroku sa informačné systémy ohodnotia podľa priority z hľadiska spoločnosti a vážnosti ohrozenia na základe základnej analýzy. Následne sú najprioritnejšie IS podrobené detailnej analýze rizík, čiže čas a zdroje sú investované do systémov, ktoré to potrebujú. Jediné nevýhody môžu plynúť z chybnej počiatočnej analýzy.

2.4. VÝHODA POUŽITIA SOFTVÉROVÝCH RIEŠENÍ

Analýza rizík IS je veľmi náročný proces na čas a vedomosti a veľmi náchylný na chyby analýzy. Počas analýzy treba zohľadňovať množstvo aspektov ovplyvňujúcich bezpečnosť IS.

Vzhľadom k vyššie uvedeným vlastnostiam procesu analýzy rizík je pochopiteľná snaha tento proces zrýchliť, sprehľadniť a skvalitniť pomocou špeciálnych softvérových nástrojov. Výber vhodného nástroja je rozhodujúcim faktorom pre budúcu kvalitu analýzy rizík.

3. ENISA

(**European Network and Information Security Agency**)

ENISA je európska agentúra pre sieťovú a informačnú bezpečnosť. Agentúra vznikla v roku 2004 nariadením Európskej Únie 460/2004 a svoju úlohu plní od 1. septembra 2005. Svoje sídlo má na Gréckom ostrove Kréta, v mestečku Heraklion.

Hlavnou náplňou agentúry je pomáhať členským štátom únie v otázkach sieťovej a informačnej bezpečnosti. Predovšetkým veľkým nadnárodným firmám, ktoré sú poskytovateľmi internetového pripojenia alebo telekomunikačných a operátorských služieb. V neposlednom rade pomáha agentúra finančným inštitúciám, predovšetkým bankám. Výsledkom práce agentúry má byť zlepšenie úrovne bezpečnosti komunikačných služieb v únií. Spoluprácou členských štátov, komerčných organizácií a Európskej komisie dochádza k predchádzaniu problémov súvisiacich s informačnou bezpečnosťou.

Agentúra pomáha Európskej únií v príprave novej technickej legislatívy týkajúcej sa informačnej bezpečnosti. Pomáha taktiež pri novelách technických legislatív z danej oblasti.

Ďalším z cieľov je spolupráca na vývoji kultúry sieťovej a informačnej bezpečnosti, aby sa čo najviac dostala do podvedomia bežných ľudí a obyvateľov členských štátov únie. Vytvorením takejto kultúry sa zlepšuje úroveň bezpečnosti od obyčajných používateľov internetu cez spoločnosti so zameraním na informačné technológie až po bankové inštitúcie. Výsledok tejto činnosti má dopad aj na produkčný trh v členských štátoch. Webové sídlo agentúry by malo byť hlavným bodom pri výmene informácií, užitočných rád a poznatkov medzi členskými štátmi.

Vedenie agentúry sa skladá z výkonného riaditeľa a podporných orgánov. Vedenie podporujú experti v daných oblastiach informačnej bezpečnosti, zástupcovia komerčných spoločností a taktiež aj odborníkmi z akademickej sféry. Manažment zložený z reprezentantov členských štátov únie, Európska komisia a akcionári. Taktiež bola vytvorená skupina, ktorá podporuje a dáva rady výkonnému riaditeľovi agentúry. Výkonným riaditeľom ENISA agentúry sa stal 16. októbra 2009 Dr. Udo Helmbrecht. Bol zvolený manažmentom. V agentúre momentálne pracuje približne 55 expertov na oblasť informačnej a sieťovej bezpečnosti.

ENISA pomáha vo viacerých smeroch členským štátom rozvíjať ich informačnú a sieťovú bezpečnosť. Ďalším z týchto smerov je pomoc priamo jednotlivým organizáciám a spoločnostiam zvyšovať úroveň bezpečnosti, čím sa zároveň zvýši bezpečnosť v danom členskom state. Pomoc pre jednotlivé spoločnosti poskytuje aj v oblasti Analýzy a Manažmentu rizík. Tato oblasť je dnes ešte veľmi malo rozšírená. V každom členskom state sú organizácie, ktoré musia spĺňať štandardy. Pravé k získaniu certifikácie štandardov im pomáhajú nástroje na analýzu rizík. ENISA ako agentúra pre informačnú bezpečnosť poskytuje zoznam overených a spoľahlivých nástrojov pre tuto oblasť. Ponuka taktiež rady v oblasti analýzy a manažmentu rizík.

4. VYBRANÉ NÁSTROJE PRE ANALÝZU RIZÍK

Pre analýzu rizík sme vybrali na porovnanie nasledujúcich 7 nástrojov. Tieto nástroje boli vybrané z väčšieho množstva nástrojov odporúčaných agentúrou ENISA. Nástroje sme vyberali predovšetkým tak, aby boli zastúpené rozdielne vlastnosti nástrojov rizík. Vybrané nástroje sú z rôznych krajín a taktiež ich použitie je rozdielne v závislosti od krajiny.

Tieto nástroje si popíšeme z viacerých hľadísk. V ďalšej kapitole si popíšeme jeden z najlepších nástrojov na analýzu rizík CRAMM a porovnáme ho aj k týmto nástrojom.

4.1. CALLIO

Nástroj Callio Secura 17799 vytvorený spoločnosťou Callio Technologies je webovo založený nástroj. Pracuje s databázami a umožňuje používateľovi implementovať a prevádzkovať systém manažmentu informačnej bezpečnosti (ISMS). Podporuje štandardy 17799 a ISO 27001. Dokáže produkovať dokumenty, ktoré sú potrebné pre získanie certifikácie z týchto štandardov. Poskytuje taktiež manažment dokumentov a úpravu ním používanej databázy. Tento nástroj je dostupný aj v demo verzii, ktorá je dostupná na webovej lokalite spoločnosti Callio Technologies pre vyskúšanie.

Pri analýze a manažmente rizík poskytuje tieto metódy:

- Identifikácia rizík, zraniteľnosti a potenciálnych hrozieb
- Poskytuje zoznam známych a rozšírených hrozieb
- Naviazanie týchto rizík a hrozieb na aktíva spoločnosti
- Vyhodnocovanie nájdených rizík a hrozieb
- Kalkulácia potenciálnych rizík a dopad na aktíva
- Poskytuje zoznam odporúčaných kontrol zo štandardu ISO 17799
- Vytvára a vyhodnocuje rôzne bezpečnostné scenáre na základe získaných údajov
- Diagnostika spoločnosti pomocou otázok pre získanie bezpečnostného stavu spoločnosti z pohľadu normy ISO 17799
- Vytvorenie bezpečnostnej politiky
- Overenie stavu spoločnosti pre získanie certifikácie ISO 27001

Iné funkcionality:

- Dokumentačný manažment, príklady dokumentov, overenie dokumentov ISMS
- Automatický generátor reportov
- Slovník pojmov informačnej bezpečnosti
- Centrum hrozieb pre publikácie ohľadom informačnej bezpečnosti pre členov
- Umožňuje vložiť vlastné otázky do databázy pre odhalenie rizík

Nástroj je dostupný v 3 jazykoch a to angličtina, francúzština a španielčina. Je určený pre národné a nadnárodné komerčné organizácie, vládne organizácie a zložky a taktiež aj pre neziskové

organizácie. Mimo Európskej Únie sa používa ešte napríklad v štátoch Kanada, Mexiko a Taiwan. Z požívateľského hľadiska je tento nástroj ľahko ovládateľný, keďže ide o webové riešenie intuitívne rozdelené do sekcií. Obsahuje systém, ktorý je počas práce používateľovi nápomocný vysvetlivkami a pokynmi.

Nevýhodou je podpora iba po telefóne alebo e-mailom a taktiež to, že spoločnosť neposkytuje žiadny technický kurz k tomuto nástroju. Taktiež nie sú k dispozícií žiadne aktualizácie systému.

4.2. COBRA

Nástroj z dielne spoločnosti C&A Systems Security je britský softvérový systém na analýzu rizík. Umožňuje organizácií zamerať sa na bezpečnosť rizikových aktív. Vyhodnocuje možný dopad hrozieb a zraniteľností a následne generuje patričné riešenia a odporúčania. Automaticky spája možné hrozby s dopadom na aktíva spoločnosti. Poskytuje tak možnosť zabezpečiť čo najmenší alebo žiadny dopad na aktíva.

Pri analýze rizík poskytuje metódy:

- Identifikácia rizík, hrozieb a zraniteľností
- Vyhodnocuje mieru jednotlivých rizík
- Priamo spája riziká a hrozby s potenciálnym dopadom na aktíva
- Ponúka detailné riešenia a odporúčania pre zníženie miery jednotlivých rizík
- Vytvára technické a podnikateľské reporty
- Ponúka kontrolu systému na podmienky štandardu ISO 17799

Nástroj COBRA je ponúkaný iba v jazyku angličtina. Je určený predovšetkým pre komerčné organizácie a organizácie, ktoré sú zamerané na ISO 17799. Pre vyskúšanie je dostupná demo verzia na webovej lokalite výrobcu. Ovládanie nástroja by malo byť jednoduché aj pre používateľov, ktorí nemajú skúsenosti s nástrojmi na analýzu a manažment rizík. K dispozícií je aj používateľská pomocná príručka. Nástroj je založený na moduloch, ktoré je možné modifikovať a získať tak presnejšie riešenia a odporúčania. Kompletný systém nie je možné získať so žiadnou zľavou bez ohľadu na zameranie organizácie.

Nevýhodou tohto nástroja je, že neponúkajú žiaden kurz. Nástroj sám o sebe neponúka odporúčania, ktoré oblasti je potrebné zlepšiť pre získanie certifikácie ISO 17799. Výrobca nevydáva žiadne aktualizácie pre nástroj. Výrobca neponúka žiadnu podporu.

4.3. COUNTERMEASURES

CounterMeasures pochádza z USA z dielne spoločnosti Alion. Tento nástroj uskutočňuje analýzu a manažment rizík na základe série amerických štandardov US-NIST 800 a OMB Circular A-130. Nástroj necháva používateľa zadefinovať vyhodnocovacie kritéria a pomocou „tailor-made" zoznamu aktív ponúka objektívne zhodnotenia a určuje bezpečnostné aspekty. Nástroj je dostupný ako v sieťovej tak aj v pracovnej konfigurácií.

Pri analýze a manažmente rizík ponúka tieto metódy:

- Identifikácia rizík pomocou modelu „Survey"
- Zbieranie potrebných dát
- Analýza platformy
- Zhodnotenie rizík
- Zhodnotenie nákladov a odporúčanie pre ozdravenie systému
- Vydávanie reportov o stave systému
- Vydávanie reportov s popisom rizík a ich asociácia na operácie
- Vydanie plánu pre ozdravenie systému spolu s odporučeniami

Nástroj je dostupný iba v jazyku angličtina. Je to jeden z najdrahších nástrojov na analýzu rizík (Enterprise verzia - $14500). Možnosť získania zľavy pre akademický sektor a vládne organizácie. Nástroj môže byť ako nezávislá aplikácia alebo ako webový server. Je určený predovšetkým veľkým nadnárodným organizáciám ako sú napríklad banky, ropné spoločnosti, poisťovne, univerzity a štátne spoločnosti. Cena za produkt v sebe zahŕňa aj 2 dňový tréning pre prácu s aplikáciou. Systém ponúka automatickú inštaláciu a jednoduché rozhranie s pomocnou používateľskou príručkou. Výhodou je podpora produktu zahrnutá v cene. Nástroj ponúka možnosť exportovať dokumenty do MS Excel formátu alebo uloženie do databázy.

Nevýhodou tohto nástroja v rámci Európskej Únie je využívanie amerických štandardov. Avšak amerických spoločností je v Európe čoraz viac. Ďalšou nevýhodou je príliš vysoká cena.

4.4. EAR/ PILAR

Tento nástroj na analýzu rizík pochádza zo Španielska a tvoria ho 2 časti a to sú EAR – komerčný produkt a PILAR – obmedzený iba na verejnú správu. Tento nástroj je podporovaný španielskou agentúrou s názvom CCN (Španielska Národná Agentúra pre bezpečnosť). Pre analýzu a manažment rizík tento nástroj využíva predovšetkým metodológiu „Magerit". Podporuje manažment rizík na dlhé obdobia a poskytuje stupňujúce sa analýzy pre neustále zlepšovanie systému. Zameriava sa predovšetkým na kvalitatívnu a kvantitatívnu analýzu a manažment rizík. Zhodnocuje operácie a ich dopad na podnikateľskú oblasť spoločnosti.

Nástroj podporuje tieto funkcionality:

- Identifikácia rizík a aktív
- Vytvorenie vzťahov medzi rizikami a aktívami spoločnosti
- Zhodnotenie dopadu rizík na spoločnosť
- Identifikácia a ohodnotenie hrozieb
- Analýza jednotlivých rizík a ich dopad
- Určenie potenciálnych a zvyškových hodnôt rizík
- Analýza rizík z kvalitatívneho a kvantitatívneho pohľadu
- Rozdelenie rizík podľa priority
- Kvalitatívny a kvantitatívny inventár dôležitých aktív
- Zbieranie dát pre vypracovanie záchranného plánu v prípade katastrofy
- Zhodnotenie dopadu na aktíva v prípade úplného odstavenia služby
- Vypracovanie politiky a procedúr na zabezpečenie rizík
- Zhodnotenie zvyškových rizík po aplikovaní bezpečnostných procedúr
- Zhodnotenie akceptácie rizík
- Možnosť vypracovania viacerých bezpečnostných politík (lokálna, národná, oblastná a iné)
- Možnosť zadefinovania vlastných špecifických aktív spoločnosti

Nástroj je dostupný v 4 jazykoch a to angličtina, francúzština, taliančina a španielčina. Oblasti, ktoré môžu získať tento nástroj zdarma alebo so zľavou sú akademické organizácie a španielska verejná správa. Iné oblasti, pre ktoré je EAR/PILAR určený sú komerčné nadnárodné spoločnosti, vládne organizácie a lokálne veľké spoločnosti. Nástroj je vytvorený ako klient/server aplikácia. Výrobca poskytuje podporu.

Nástroj sa používa v rámci EU v štátoch Španielsko, Taliansko, Maďarsko a Francúzsko. Mimo EU sa využíva v štátoch Južnej Ameriky: Argentína, Chile, Peru, Columbia. Pri analýze a manažmente rizík využíva nasledovné štandardy:

- **ISO/IEC 13335:2004**
- **ISO/IEC 17799:2005**
- **ISO/IEC 27001:2005**
- ostatné štandardy je možné doplniť

Nástroj pomáha k získaniu certifikácie podľa štandardu ISO/IEC 27001:2005. Výrobca ponúka technický tréning. Inštalácia nástroja je automatická. Používanie je intuitívne, avšak používateľ musí byť oboznámený s metodológiou „Magerit“. Používateľovi sú k dispozícii príklady práce s nástrojom a taktiež pomocná používateľská príručka. Výsledky

Nevýhodou je potrebná znalosť „Magerit“ metodológie, prípadne nutnosť podstúpiť tréning. Pri tomto tréningu sú však potrebné skúsenosti z oblasti manažmentu informačných technológií.

4.5. EBIOS

Ebios vytvorila spoločnosť Central Information Systems Security Division z Francúzska. Nástroj je podporovaný organizáciou s názvom Club Ebios. Tento nástroj sa líši najme tým, že patrí medzi softvér s otvoreným zdrojovým kódom a predovšetkým je zadarmo. Pracuje na princípe metódy 5tich EBIOS fáz. Všetku prácu a výsledky umožňuje používateľovi zachytiť do výsledných dokumentov.

Metóda piatich EBIOS fáz:

1. Identifikovať cieľový systém, základné informácie, oblasť použitia, definovanie entít
2. Odhad rizík a definovanie kritérií rizík
3. Identifikácia jednotlivých rizík
    3.1 Štúdium rizík
    3.2 Štúdium zraniteľnosti
    3.3 Sformovanie rizík, zraniteľnosti a hrozieb
4. Akceptácia a identifikácia bezpečnostných a zvyškových rizík
5. Určenie bezpečnostných odporúčaní a opatrení

Iná funkcionalita:

- Zoznam pojmov z oblasti informačnej bezpečnosti
- Zoznam referenčných dokumentov
- Zoznam hlavných entít spoločnosti
- Zoznam bezpečnostných pravidiel
- Zoznam hrozieb
- Zoznam zvyškových rizík

Nástroj je dostupný v 4 jazykoch a to angličtina, francúzština, španielčina a nemčina. Využívajú ho štáty EU ako Francúzsko, Belgicko, Luxembursko a iné. Mimo EU sa používa napríklad v štátoch Quebec alebo Tunisko. Dnes tento nástroj využíva približne 1000 známych subjektov z verejného ale aj súkromného sektora. Ebios je určený pre vládne a nadnárodné organizácie, komerčné aj nekomerčné spoločnosti.

Ebios je nezávislá aplikácia vytvorená programovacím jazykom Java, ktorá spolupracuje s typom dokumentov XML. Preto nezáleží na akej platforme používateľ využíva služby Ebiosu.

Tento nástroj podporuje nasledovné štandardy:

- ISO 13335
- ISO 15408 + odporúčania
- ISO 17799 + odporúčania

Nástroj podporuje taktiež úpravu rizík, hrozieb a zraniteľnosti. Tak isto ponúka úpravu otázok pri identifikácií rizík.

Nevýhodou je žiadna podpora nástroja, keďže je zadarmo. Nie sú dostupné žiadne aktualizácie systému. Je síce dostupný tréning, ale najprv je potrebné zoznámiť sa s metódou EBIOSu. To isté sa týka aj používania systému, nie je nutná inštalácia, ale je potrebné byť oboznámený so všetkými fázami EBIOSu.

4.6. PROTEUS

Nástroj na analýzu rizík Proteus pochádza z dielne vládnej spoločnosti Infogov Spojeného Kráľovstva. Je orientovaný najme na vládne organizácie po celom svete. Podporujú ho organizácie BSI (Britský Štandardizačný úrad), ISF (Fórum Informačnej Bezpečnosti) a Inštitút HISP.

Proteus je komplexný nástroj pracujúci na úrovni webového servera. Ponúka analýzu a manažment bezpečnostných rizík predovšetkým pre vládne organizácie, ale aj veľké nadnárodné spoločnosti. Proteus pomáha organizáciám pri implementovaní jednotlivých štandardov a bezpečnostných smerníc ako napríklad ISO 17799, BS ISO 27001, BS 25999, SOX, CobiT, PCI DSS a iné.

Podporované funkcionality:

- Identifikácia rizík pomocou kvalitatívnych a kvantitatívnych metód hodnotenia rizík
- Podpora manažmentu rizík, hrozieb a incidentov
- Podpora vytvorenia plánu pre zníženie bezpečnostných rizík
- Reálne a absolútne zhodnotenie váhy každého rizika a akceptácia zvyškových rizík
- Ohodnotenie fyzických rizík, rizikových informácií, služieb a aplikácií
- Previazanie hrozieb s aktívami
- Možnosť importovania vlastných dát
- Integrácia aplikácií tretích strán a možnosť penetračných testov
- Zhodnotenie dopadu na podnikateľskú činnosť
- Akceptácia rizík pomocou auditu systému a všetkých vykonaných zmien
- Automatizovaný systém pre alarm (SMS, e-mail) – rozposielania notifikácií povereným osobám na základe ohrozeného aktíva

Nástroj Proteus je komplexný nástroj na analýzu a manažment rizík. Ponúka od základných prvkov v tejto oblasti aj ďalšie funkcionality uvedené vyššie čím pokrýva oblasť analýzy a manažmentu rizík na veľmi vysokej úrovni. Je dostupný v jazykoch angličtina, španielčina, francúzština, japončina a čínština. Po dohode je možné získať ho na vyskúšanie. Je určený pre vládne organizácie a agentúry a veľké nadnárodné spoločnosti. Využívajú ho organizácie ako finančné organizácie, farmaceutické spoločnosti a iné. Nástroj pomáha pri dosiahnutí certifikácie štandardu ISO 27001.

Pri analýze a manažmente podporuje tieto štandardy:

- BS ISO 17799 a 27001
- BS 25999
- SoGP vydané ISF
- PCI DSS
- SOX
- a iné

Pre beh celého systému je potrebný webový server IIS alebo Apache, databáza MS SQL a podpora skriptovacieho jazyka PHP. Pre správne používanie systému je potrebný tréning, avšak aj tieto možné tréningy vyžadujú skúsenosti v oblasti informačnej bezpečnosti. Ďalšou nevýhodou je slabé podpora – iba telefón a e-mail.

5. CRAMM

Pod skratkou CRAMM(CCTA Risk Analysis and Management Method) môžeme chápať dve odlišné veci:

- Metodiku vlády Veľkej Británie pre ohodnocovanie rizík a analýzu bezpečnosti.
- Podporný softvérový nástroj, ktorý pomáha pri uplatnení tejto metodiky v praxi.

5.1. NÁSTROJ CRAMM

Prvú verziu nástroja CRAMM vyvinula vládna inštitúcia Veľkej Británie CCTA (Central Computer and Telecommunication Agency) v roku 1985, ako odpoveď na stále rastúcú potrebu bezpečnosti IS. Na základe metodológie vlády Veľkej Británie bol Cramm prepracovaný spoločnosťou Insight Consulting. Momentálne je nástroj predávaný vo verzii 5.2 pre operačný systém Microsoft Windows.

V deväťdesiatych rokoch bol CRAMM používaný prednostne vládou UK a prevzali ho taktiež mnohé obchodné organizácie a úrady verejnej správy po celom svete. V súčasnosti je CRAMM najpoužívanejšou metodikou svojho druhu v Európe.

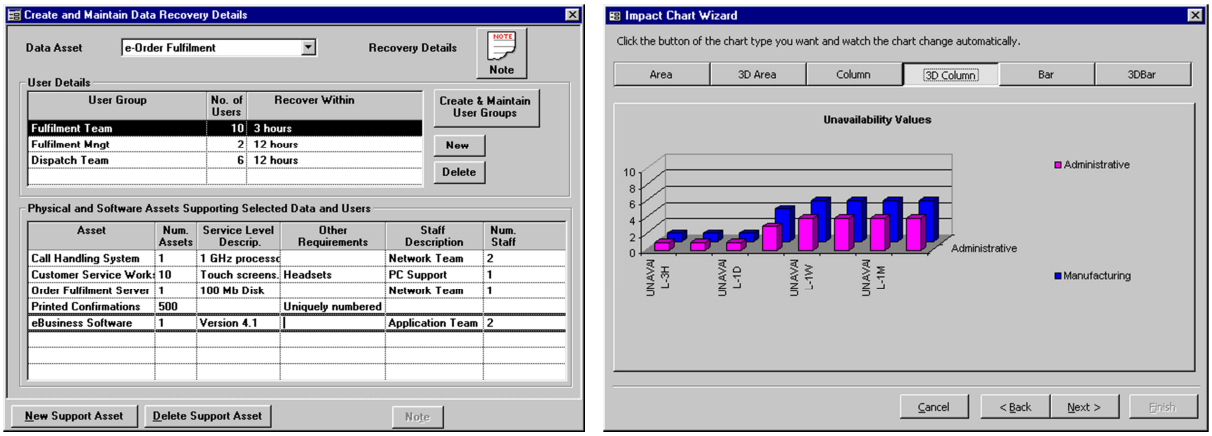
Momentálne sa distribuuje v troch verziách – CRAMM expert, CRAMM express a BS 7799 (ISO 27001) Review. Taktiež sa dá objednať tzv. trial verzia, ktorá slúži na krátkodobé vyskúšanie produktu.

K hlavným výhodám nástroja patrí:

- Komplexný súbor nástrojov pre vyhodnocovanie a analýzu rizík podporujúce normu ISO27001
- Množstvo podporných a pomocných nástrojov a sprievodcov pre vytváranie bezpečnostných politík
- Prevádzanie viacerých spôsobov hodnotenie rizík (okrem detailného a expresného aj viacero iných)
- Preddefinované analýzy rizík na rôzne typy IS
- Rozsiahla knižnica protiopatrení
- Databáza s vyše 3500 bezpečnostnými kontrolami na rôzne aspekty informačnej bezpečnosti v skupinách podľa efektivity a ceny
- Nástroje pre analýzu stavu voči ISO/IEC 27001:2005
- Prípravu na certifikáciu podľa ISO/IEC 27001:2005
- Nástroje pre vytvorenie bezpečnostnej dokumentácie
- Grafický výstup analýz a štatistík
- Množstvo spokojných používateľov po celom svete (napr. NATO)
- Lokalizácia do českého jazyka môže byť výhoda pre nasadenie lokálnych spoločností
- Používateľská podpora telefonicky alebo e-mailom

Keďže sa jedná o robustné riešenie, ovplyvnilo to aj výslednú cenu produktu, ktorá je v súčasnosti v jednotkách sto tisícov. Ako ďalšiu nevýhodu produktu možno spomenúť potrebné zaškolenie personálu na používanie nástroja a porozumenie metódy CRAMM. Na základné využitie funkcionality sa hodí verzia Express, kde nie sú nutné špeciálne znalosti. Medzi ďalšie nevýhody možno zaradiť neschopnosť používania jednej licencie na viacerých počítačoch a zastaralé grafické používateľské rozhranie.

Kvôli zložitosti problému bezpečnosti IS, dát a počítačových sietí nemôže byt jedna osoba odborník na všetky oblasti. Rýchli vývoj IT, neustále zmeny v IS a nové trendy v oblasti bezpečnosti kladú stále vyššie požiadavky na obmedzené zdroje. Takisto existuje široké spektrum rizík, ktoré môžu ohroziť bezpečnosť informačného systému alebo siete. Pri toľkých rizikách je zložité zmerať ich úroveň a lokalizovať zraniteľnosti a slabiny IS. Ak sa to aj podarí, tak zavedením protiopatrení pre jeden okruh, môžu vzniknúť nové riziká na inom mieste. Preto existuje objektívna potreba pre overenú metódu ako CRAMM, ktorá môže slúžiť ako podpora procesov riadenia informačnej bezpečnosti.



OBRÁZOK 1 - UKÁŽKA NÁSTROJA CRAMM

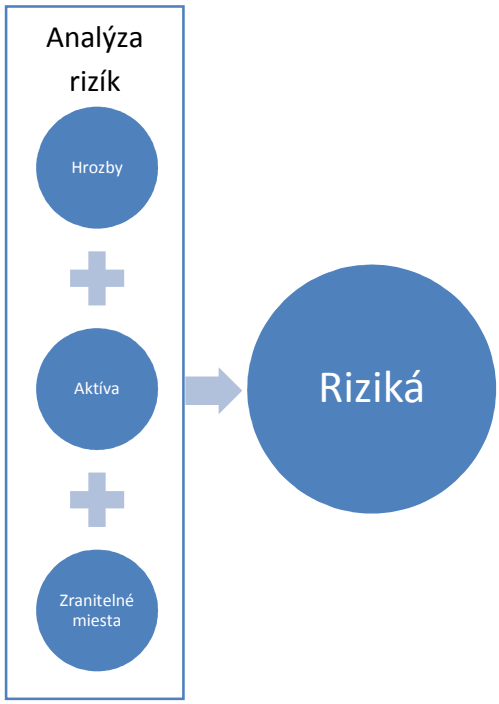
5.2. METODIKA CRAMM

Analýza rizík podľa metodiky CRAMM neskúma bezpečnosť jednotlivých aktív IS, ale ich združuje do logických celkov – modelov aktív, ktoré sú potom predmetom analýzy rizík. Analýza rizík nástrojom CRAMM sa v zmysle metodiky skladá z troch fáz, z ktorých každá je podporovaná dotazníkmi a pokynmi:

- identifikácia a ohodnotenie aktív
- stanovenie rizík - analýza hrozieb a zraniteľností
- riadenie rizík - návrh bezpečnostných opatrení

Manažment rizík vychádza z analýzy a zahŕňa výber a schválenie vhodných bezpečnostných opatrení na zrušenie alebo zníženie rizík,

Všeobecne sa dajú tieto koncepty reprezentovať diagramom na obrázku 2, kde si treba všimnúť, že analýza a manažment rizík sú dve súvisiace ale oddelené aktivity.



OBRÁZOK 2 - PROCES ANALÝZY A MANAŽMENTU RIZÍK

5.2.1. *FÁZA 1 – IDENTIFIKÁCIA A OHODNOTENIE AKTÍV, VYTVORENIE MODELOV*

V prvej fáze sa prevádza identifikácia aktív (dát, služieb nad údajmi, programového vybavenia, fyzických aktív a priestorov) a vytvárajú sa modely aktív, ktoré definujú závislosť medzi rôznymi typmi aktív. Ohodnocujú sa aktíva dátové (dopad pri prezradení, modifikácii, zničení, neprístupnosti), fyzické a programové (náklady na obnovu, rekonštrukciu), čím sa vlastne určujú možné dopady na prevádzku a ciele organizácie.

5.2.2. *FÁZA 2 – STANOVENIE RIZÍK*

V druhej fáze sa robí výpočet rizík, vyplývajúcich z hrozieb pôsobiacich na IS založených na ohodnotení aktív a hodnotení úrovne hrozieb a zraniteľnosti.

5.2.3. *FÁZA 3 – RIADENIE RIZÍK*

Riadenie rizík zahŕňa identifikáciu, výber a zavedenie vhodných bezpečnostných opatrení pre zníženie rizika na prijateľnú úroveň. Nástroj CRAMM vyberá opatrenia zo svojej knižnice opatrení tak, aby pokryli všetky možné hrozby identifikované v druhej fáze s ohľadom na vypočítanú mieru rizika. Takýmto spôsobom vznikne bezpečnostný profil IS.

6. ZÁVER

6.1. POROVNANIE VYBRANÝCH NÁSTROJOV

Pre porovnanie jednotlivých nástrojov sme vytvorili tabuľku s vybranými ôsmymi hlavnými kritériami. Výsledky nášho pozorovania možno sledovať v tabuľke 1.

V tabuľke 1 je popísané, či nástroj pomáha organizácii k získaniu *štandardov* a ak áno tak, ktoré to sú. Ďalej je možné z tabuľky vyčítať *jazykovú a cenovú dostupnosť*, ktoré sú taktiež rozhodujúcimi faktormi pri výbere nástroja spoločnosťou. Stĺpec *Cieľová skupina* poskytuje obraz o tom, pre ktorú sféru je ktorý nástroj vhodnejší, keďže sú nástroje, ktoré sa vyslovene orientujú napríklad na vládne organizácie.

S posledným menovaným kritériom úzko súvisí aj možnosť *modifikácie nastroja*. Táto časť vyjadruje do akej miery je možné prispôsobiť si nástroj podľa svojich predstáv a podľa štruktúry spoločnosti. V neposlednom rade sú dôležité aj kritéria *miera podpory nástroja* od vydavateľa a taktiež či je potrebné k nástroju š*kolenie*.

Vysvetlenie skratiek v tabuľke:

CERT - Podpora získania certifikácie
MOD – Možnosť vlastnej modifikácie nástroja (1 – slabá, 2 – dobrá, 3 - vynikajúca)
ŠKOL – Potreba školenia personálu

EN – Anglický jazyk
FR – Francúzky jazyk
IT – Taliansky jazyk
ES – Španielsky jazyk
CZ – Český jazyk

G – vláda a vládne organizácie
L – veľké spoločnosti
S – malé a stredné spoločnosti
N – nekomerčné CIE
K – komerčné CIE

	CERT	Podporované štandardy	MOD	Jazyková dostupnosť					Cieľová skupina					ŠKOL	Podpora		Cena USD
				EN	FR	IT	ES	CZ	G	L	S	N	K		Tel	Txt	
Calio	● ○	ISO 17799 ISO 27001	2	●	●		●		●	●	●	●	●		●	●	$5950 na 2 pc
Cobra	○	ISO 17799	1	●							●		●				$1995 celý balík
Countermeasures	○		2	●					●	●					●	●	$3990 štandard verzia
Ear/ Pillar	○ ○ ○ ●	ISO 13335 ISO 17799 ISO 15408 ISO 27001	3	●	●	●	●							●		●	$1990 EAR
Ebios	○ ○ ○ ○	ISO 13335 ISO 15408 ISO 17799 Ebios	2	●	●	●	●		●	●	●	●	●	●			freeware
Proteus	● ○ ○ ○ ○	ISO 27001 BS 25999 SoGP PCI DSS SOX	3	●	●		●		●	●	●				●	●	$9400 profesionál verzia Na rok
Cramm	● ○	ISO 27001 Cramm	2	●				●	●	●	●			●	●	●	$4600 expert + 1300/rok

TABUĽKA 1 - POROVNANIE VYBRANÝCH NÁSTROJOV NA ANALÝZU RIZÍK

6.2. ZHODNOTENIE

Cieľom nasej práce bolo poskytnúť prehľad o nástrojoch na analýzu rizík. V úvode prace sme popísali pre úplnosť práce, čo to analýza a manažment rizík je. Pri vypracovaní sme postupovali pomocou rad a odporúčaní Európskej Agentúry pre sieťovú a informačnú bezpečnosť ENISA. Základné informácie o tejto agentúre sme poskytli v kapitole č. 3. Jadrom práce sú kapitoly č. 4 a 5. V kapitole č. 4 sme vybrali šesť nástrojov na analýzu rizík podľa odporúčaní ENISA.

Nástroje boli vyberané na základe viacerých kritérií a to, pôvod nástroja, aby boli zastúpené viaceré Európske štáty, ale aj nástroj z Ameriky. Nástroje majú rôznu pridanú podporu. Všetky tieto nástroje sú popredne nástroje v oblasti analýzy rizík a tak poskytujú všetku základnú funkcionalitu v tejto oblasti. Z tohto dôvodu sme nerozoberali ako presne jednotlivé nástroje vykonávajú analýzu a manažment rizík. Sústredili sme sa v práci na dodatočné informácie o týchto nástrojoch, aby bolo možné komplexnejšie vybrať vhodnejší nastroj. Vybrali sme jeden nastroj - CRAMM, ktorý je dnes považovaný za elitu v tejto oblasti a venovali sme mu kapitolu č. 5. Poprednosť tohto nástroja vyjadruje vysoký počet používateľov z radov veľkých spoločnosti.

7. POUŽITÁ LITERATÚRA

[1] Inventory of Risk Management / Risk Assessment Tools , november 2010
http://rm-inv.enisa.europa.eu/rm_ra_tools.html

[2] Comparison of Risk Management Methods and Tools, december 2010
http://rm-inv.enisa.europa.eu/comparison.html

[3] Callio Secura product fact sheet, november 2010
http://www.callio.com/PDF/Calio_Secura17799.pdf

[4] Cobra Benefits, november 2010
http://www.riskworld.net/benefits.htm

[5] About CounterMeasures, december 2010
http://www.countermeasures.com/about.htm

[6] Introduction to EBIOS methodology, november 2010
http://www.itworks.lu/risk-analysis-ebios.php

[7] Ear database, december 2010
http://www.access.gpo.gov/bis/ear/ear_data.html

[8] About Proteus, november 2010
http://www.infogov.co.uk/proteus_enterprise/index.php

[9] CRAMM V Information Security Toolkit, november 2010
http://www.cramm.com/files/datasheets/CRAMM%20(Datasheet).pdf

[10] Risk Assessment Tools: A Primer , september 2010
http://www.isaca.org/Journal/Past-Issues/2003/Volume-2/Pages/Risk-Assessment-Tools-A-Primer.aspx