Monitoring a forenzná analýza

Mať prehľad o aktuálnom stave bezpečnosti informačného systému a vedieť dôkladne vyšetriť bezpečnostné incidenty. To sú aktuálne výzvy pre manažérov bezpečnosti. Ako tieto výzvy riešili v jednej finančnej inštitúcii sa dozviete z nasledujúcich riadkov.

Finančné inštitúcie svoje informačné systémy musia chrániť, aby boli ich služby bezpečné, dôveryhodné, spĺňali požiadavky legislatívy a regulačných orgánov. Cieľom monitorovania bezpečnosti je mať prehľad o aktuálnom stave bezpečnosti a odvrátiť alebo zastaviť útok na informačný systém. Zároveň monitorovací systém poskytuje podklady na dôkladné vyšetrenie identifikovaných bezpečnostných incidentov. Prípadová štúdia voľne nadväzuje na sériu predchádzajúcich článkov venovaných problematike bezpečnostných dohľadových nástrojov[1].

Popis prostredia IT

Projekt bol realizovaný vo finančnej inštitúcii s celoštátnou sieťou pobočiek a zahraničným vlastníkom, ktorá prevádzkuje rozsiahly heterogénny informačný systém. Hlavnými komponentmi IS sú centrálny bankový systém na báze mainframe, podporné centrálne systémy na platformách Windows, UNIX, Linux, sieťová infraštruktúra na komponentoch spoločnosti Cisco, verejný web server, systém elektronického bankovníctva, intranetové aplikácie a špeciálne bankové aplikácie.

Ciele projektu

Pred popisom hlavných cieľov projektu je dôležité podotknúť, že zákazník chápe budovanie bezpečnosti ako dlhodobý proces. O tom svedčí aj skutočnosť, že pristúpil ku komplexnému riešeniu bezpečnosti postavenému primárne na báze štandardu BS 7799 a normách ISO/IEC 17799 a ISO/IEC 13335. K jeho prvým krokom patrilo spracovanie analýzy rizík, vytvorenie riadiacich dokumentov bezpečnosti (Bezpečnostná doktrína, Bezpečnostná architektúra IS a Manuál bezpečnosti), zavedenie vlastníctva aktív a vypracovanie stratégie efektívnej implementácie bezpečnostných technológií na obdobie troch rokov.

Uvedené skutočnosti mali významný vplyv na hlavné ciele projektu, ktorými boli:

- splniť požiadavky kladené na bezpečnosť, ktoré vyplývali z riadiacich dokumentov bezpečnosti, platnej legislatívy a požiadaviek regulačných orgánov;
- naplniť opatrenia vedúce k zníženiu hrozieb a zvýšeniu úrovne bezpečnosti;
- rozšíriť prevádzkovaný bezpečnostný systém o služby centrálneho monitorovania aktuálneho stavu bezpečnosti IS a spätnej analýzy bezpečnostných incidentov;
- vytvoriť potenciálny zdroj dôkazov pre potreby trestného konania;
- podporiť procesy na identifikáciu neštandardných obchodných operácií.

Okrem uvedených cieľov zákazník požadoval, aby použitá technológia tvorila samostatnú vrstvu a z hľadiska bezpečnosti zastrešovala všetky prevádzkované technológie. Ďalej musela spĺňať nasledujúce parametre:

- centralizovaná, ale modulárna architektúra s centrálnou správou;
- nezávislá implementácia jednotlivých modulov;
- minimálne zásahy do prevádzkového prostredia;
- využitie existujúcich rozhraní;
- integrovateľnosť s prevádzkovanými bezpečnostnými technológiami a IT prostredím;
- potenciálne prepojenie so systémami fyzickej bezpečnosti;
- kompatibilita s materskou spoločnosťou.

Koncepcia a výber riešenia

Koncepcia riešenia bola navrhnutá tak, aby riešenie podporovalo dlhodobé uchovávanie zvolených udalostí, umožňovalo ich spätnú analýzu a poskytovalo podporu pri návrhu opatrení na eliminovanie bezpečnostných nedostatkov.

Logická koncepcia riešenia (viď obr. 1) bola navrhnutá v štyroch horizontálnych vrstvách:

- vrstva zberu;
- vrstva evidencie a ukladania;
- vrstva spracovania a analýzy;
- vrstva poskytovania.

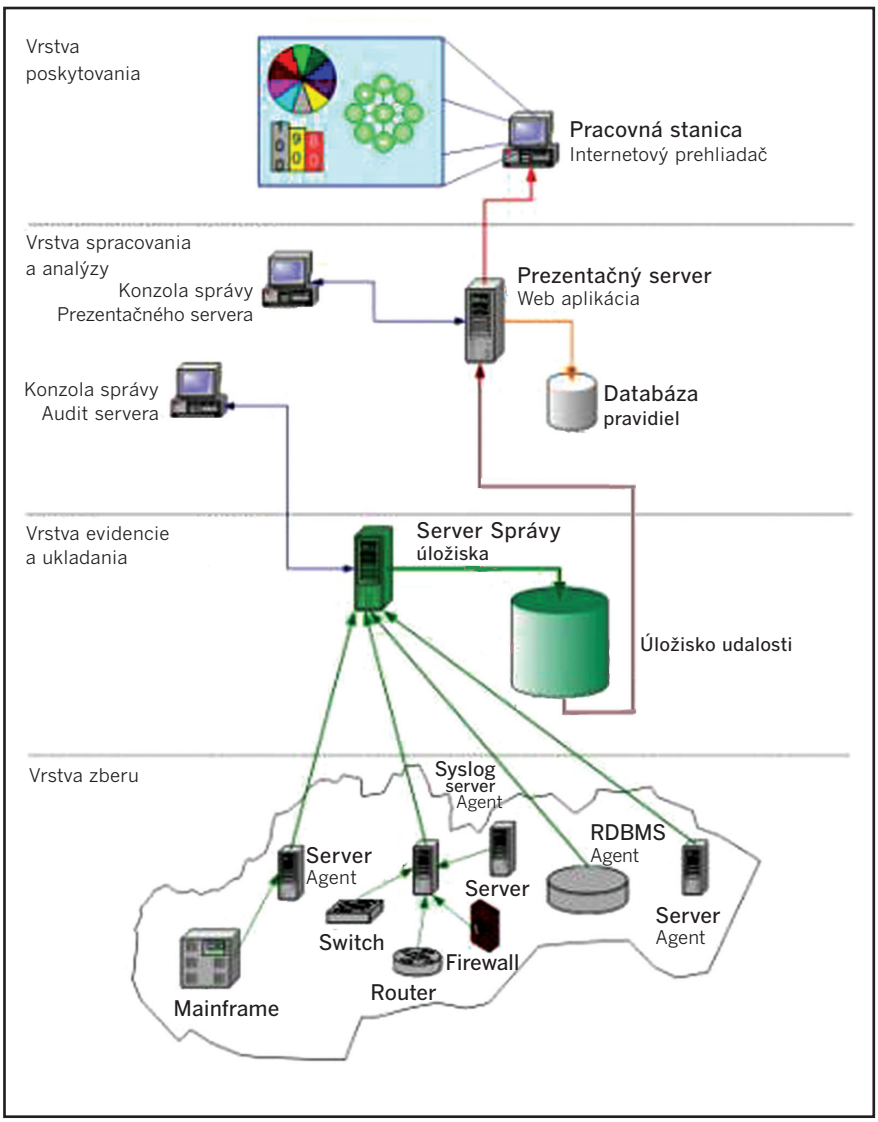
Vrstva zberu

Úlohou tejto vrstvy bolo zabezpečiť zo zdrojových systémov zber relevantných údajov. K dispozícii boli dva typy zberu údajov. Prvým bolo presmerovanie udalostí zo zdrojových systémov na systém, ktorý zabezpečil ich zber, ďalšie spracovanie a postúpenie do vyššej vrstvy (napr. logy sieťových komponentov presmerované na syslog server). Druhý typ realizoval zber, spracovanie a postúpenie udalostí pomocou agenta priamo na zdrojovom systéme (napr. zber udalostí z operačného systému MS Windows).

Vrstva evidencie a ukladania

V tejto vrstve bolo navrhnuté spracovanie udalostí postúpených z vrstvy zberu podľa definovaných pravidiel, ich korelácia a normalizácia s následným uložením v jednotnej štruktúre do úložiska v podobe relačného databázového systému.

[1] Bezpečnostní dohledové nástroje – část I, DSM 2/2005, Bezpečnostní dohledové nástroje – část II, DSM 3/2005, Centrální správa bezpečnostních incidentů, DSM 4/2005.



OBR. 1:
HORIZONTÁLNE ČLENENIE RIEŠENIA.

Vrstva spracovania a analýzy
Spracovanie monitorovacích, analytických a štatistických výstupov bolo v návrhu priradené analytickej časti riešenia. Analytická časť mala zabezpečiť na základe zadefinovaných kritérií výber a spracovanie údajov z úložiska a pripraviť ich podľa definovaných rolí na prezentovanie oprávneným používateľom.

Vrstva poskytovania
Bola navrhnutá pre oprávnených koncových používateľov. Jej úlohou bolo prezentovať údaje požadované používateľmi riešenia, ktoré boli spracované v analytickej časti riešenia.

Na základe uvedenej koncepcie bol realizovaný výber konkrétneho riešenia. Problematike výberu riešení pre bezpečnostný dohľad sa podrobne venoval článok v DSM 3/2005[1]. Okrem metrík uvedených v spomínanom článku bolo potrebné prihliadať na tri špecifické požiadavky zákazníka:

- podpora mainframe systému;
- podpora procesov na identifikáciu neštandardných obchodných operácií;
- potenciálne prepojenie so systémami fyzickej bezpečnosti.

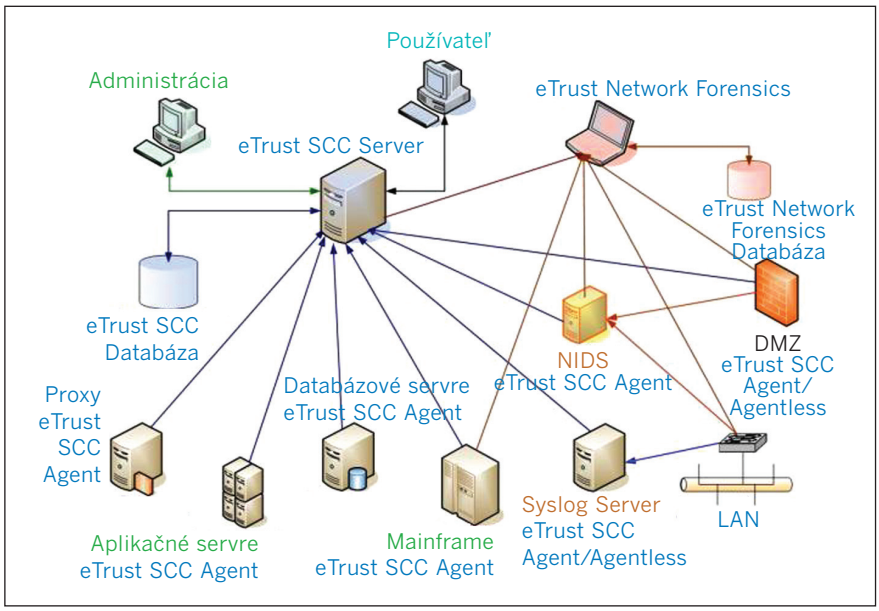
Tieto požiadavky významným spôsobom ovplyvnili konečný výber riešenia, ktorým sa stali produkty eTrust Security Command Center a eTrust Network Forensics spoločnosti Computer Associates. Ďalšími faktormi, ktoré mali vplyv na výber týchto riešení, okrem technických parametrov, boli aj lokálne implementácie v inštitúciách podobného charakteru, lokálni certifikovaní partneri a technická podpora spoločnosti Computer Associates v mieste pôsobenia zákazníka.

K výberu produktu eTrust Network Forensics je ešte potrebné poznamenať, že jeho výber ovplyvnila možnosť využiť ho nielen na analýzu aktivít zaznamenaných v informačnom systéme, ale aj pre podporu procesov na identifikáciu neštandardných obchodných operácií. Zjednodušená technická architektúra riešenia je na obr. 2.

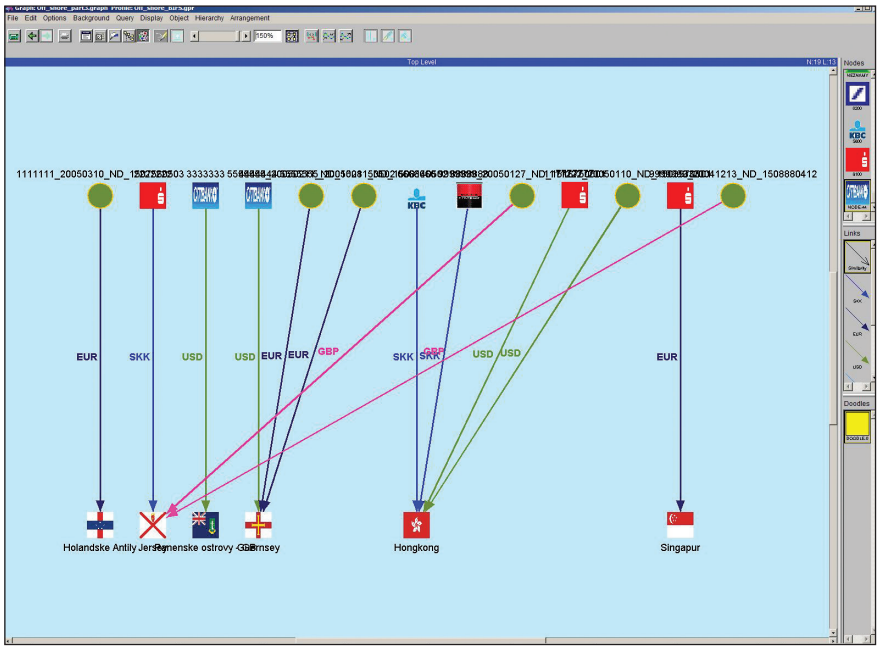
Jadrom riešenia bol centrálny server s operačným systémom MS Windows 2003, databázovým systémom MS SQL 2000 a produktom eTrust Security Command Center. Tento server reprezentoval vrstvu evidencie a ukladania a vrstvu spracovania a analýzy. Vrstvu zberu tvorili mainframový systém, centrálne servery na platforme MS Windows, UNIX/Linux a hlavná banková aplikácia. Zaradenie sieťových komponentov a systému na detekciu narušenia bolo na požiadavku zákazníka z prvej časti projektu vypustené a bude predmetom jeho rozširovania v budúcnosti. Prezentačná vrstva bola postavená na pracovných staniciach s webovým prehliadačom MS Internet Explorer a Sun Java Runtime Environment.

Ďalším významným komponentom dodávaného riešenia bola mobilná pra-

[1] Bezpečnostní dohledové nástroje – část II, DSM 3/2005.



Obr. 2: Technická architektúra riešenia.



Obr. 3: Vizualizácia finančných transferov.

covná stanica na prevádzku produktu eTrust Network Forensics určeného pre potreby forenznej analýzy. Dôvodom výberu mobilnej verzie bola v prípade potreby možnosť analyzovať problémové časti siete kdekoľvek v rámci zákazníkom prevádzkovanej infraštruktúry.

Etapy projektu

Úspešnosť projektu by nebola možná bez internej podpory zo strany zákazníka. Na jeho realizáciu vznikla spoločná pracovná skupina zložená zo zástupcov IT útvaru a útvaru bezpečnosti zákazníka a špecialistov dodávateľa riešenia.

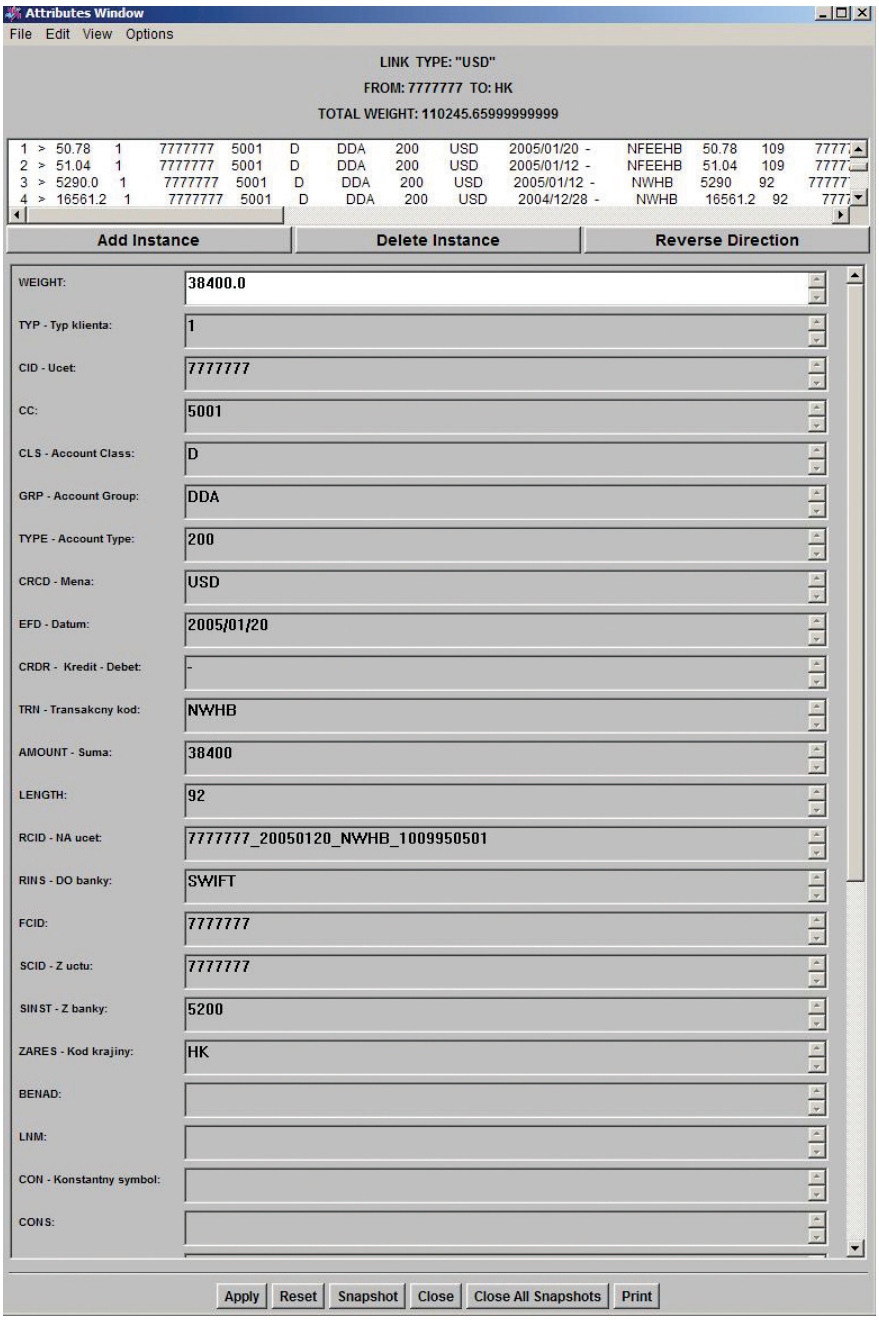
- Projekt bol rozdelený do týchto hlavných etáp:
  - detailná analýza IT prostredia;
  - vypracovanie technickej architektúry riešenia;
  - inštalácia pilotného prostredia a pilotná prevádzka;
  - spracovanie dokumentácie a vypracovanie interných predpisov pre prevádzku riešenia;
  - implementácia a akceptačné testovanie;
  - ostrá prevádzka;
  - implementácia produktu forenznej analýzy.

Prvá, analytická etapa, predstavovala jednu z najdôležitejších etáp. V nej boli veľmi dôkladne analyzované všetky dotknuté systémy s cieľom rozdeliť ich na štandardne podporované a tie, pre ktoré bolo nutné pomocou integračných kitov vyvinúť špeciálnych agentov. Okrem systémov a aplikácií analýza zahŕňala aj sieťovú infraštruktúru, dátové toky a ich objemy. Súčasťou bolo aj analyzovanie aktuálnych nastavení pre záznam auditných udalostí. Všetky výstupy z analytickej etapy poslúžili pri návrhu vhodnej architektúry riešenia, jeho umiestnení do IT prostredia a pri vývoji špeciálneho agenta určeného pre finančnú aplikáciu prevádzkovanú na mainframovom systéme.

Pri návrhu technickej architektúry bolo nutné vysporiadať sa s požiadavkou, aby riešenie tvorilo potenciálny zdroj dôkazov pre potreby trestného konania. K naplneniu uvedenej požiadavky bolo potrebné splniť tieto podmienky:

- zaviesť zdroj a synchronizáciu presného času v rámci celého IS;
- zabezpečiť jednoznačnú identifikáciu monitorovaných komponentov IS;
- zabezpečiť jednoznačnú a nespochybniteľnú identifikáciu používateľov v IS s vylúčením viacerých identifikácií pre jedného používateľa;
- zabezpečiť bezpečný záznam a ukladanie udalostí do centrálneho, chráneného úložiska udalostí bez možnosti modifikovať pôvodné udalosti;
- zabezpečiť archiváciu originálnych logov priamo zo zdrojových systémov na neprepisovateľné médiá s prístupom možným len na čítanie.

Tu je potrebné upozorniť, že náklady na splnenie uvedených podmienok sú vo väčšine prípadov priamo úmerné veľkosti IS, a preto ich realizácia v konečnom dôsledku závisí od pomeru efektívnosti investícií k dôležitosti a cene chránených údajov spracovávaných v IS. Základné overenie navrhnutej architektúry riešenia a jeho parametrov bolo cieľom inštalácie pilotného prostredia a pilotnej prevádzky. V tejto etape bolo dôležité overiť navrhnuté konfigurácie pre každý typ zdroja udalostí. Personál určený na prevádzku riešenia bol vyškolený pred spustením pilotnej prevádzky. Takto sa zabezpečilo kvalitnej-



Obr. 4: Zobrazenie detailov finančného transferu.

šie otestovanie splnenia požiadaviek zákazníka a zjednodušila sa etapa akceptačných testov.

Okrem technických návrhov a implementácie bolo nutné ešte pred začatím ostrej prevádzky spracovať interné predpisy prevádzky riešenia, vrátane návrhov na oddelenie prevádzkových rolí a procedúr na riešenie bezpečnostných incidentov.

Etapa implementácie bola v prípade štandardných platforiem a podporovaných bezpečnostných produktov pomerne jednoduchá a už za krátky čas boli viditeľné jej výsledky. V prípade integrácie riešenia s neštandardnými alebo nepodporovanými systémami bolo potrebné počítať s časom na ich začlenenie do riešenia. Objektívne posúdenie naplnenia požiadaviek zákazníka bolo výsledkom akceptačných testov, ktoré robili výhradne zamestnanci zákazníka podľa vytvorených testovacích scenárov.

Implementácia produktu forenznej analýzy

Špecifickou etapou projektu bola implementácia riešenia pre forenznú analýzu údajov. Vybraný produkt, eTrust Network Forensics, určený primárne na analýzu údajov zaznamenaných zo sieťovej komunikácie, bol v tomto prípade využitý aj ako nástroj na podporu procesov identifikácie neštandardných obchodných operácií. Vzhľadom na vypustenie monitorovania sieťových komponentov a výstupov zo systému na detekciu narušenia zo strany zákazníka, úloha eTrust Network Forensics spočívala v:

- podpore systému na identifikáciu neštandardných obchodných operácií;
- analýze podozrivých finančných tokov;
- vizualizácii realizovaných finančných transferov a väzieb medzi účastníkmi transakcií.

Proces implementácie pozostával z nasledujúcich fáz. V prvej fáze prebehla analýza požiadaviek kladených na výstupy z eTrust Network Forensics potrebných pre podporu identifikácie neštandardných obchodných operácií. Výstupy mali hlavne zefektívniť hľadanie väzieb medzi podozrivými účtami a transfermi smerujúcimi do daňových rajov. Ďalšia fáza definovala požiadavky na výstupy z finančnej aplikácie, ktoré slúžili ako vstupy do analytického produktu. Ideálnym zdrojom konsolidovaných výstupných údajov by bol dátový sklad, ale zákazník ho v čase implementácie riešenia nemal k dispozícii. Ťažiskovou úlohou v tejto fáze bolo:

- určenie rozsahu požadovaných výstupov;
- určenie periódy ich vytvárania;
- určenie spôsobu odovzdávania analytickému riešeniu;
- postavenie štruktúry výstupného súboru;
- definovanie pravidiel na odfiltrovanie „šumových transakcií" (napr. poplatkové transakcie, transakcie interného zúčtovania apod.).

V poslednej fáze bola vytvorená externá aplikácia na normalizáciu a selekciu výstupných údajov z finančnej aplikácie do formátu spracovateľného analytickou časťou eTrust Network Forensics. Okrem toho bola realizovaná aj zmena štandardnej konfigurácie eTrust Network Forensics tak, aby bolo možné spracovanie finančných transakcií.

Úprava konfigurácie eTrust Network Forensics pozostávala z definície vlast-

ZDROJE INFORMÁCIÍ:

[1] *http://www3.ca.com/solutions/Product.aspx?ID=4351.*
[2] *http://www3.ca.com/solutions/Product.aspx?ID=4856.*
[3] Nicolett M., Williams A. T. Security Information and Event Management Leaders, 2H05. Gartner Research, June 3, 2005.
[4] *http://www.occ.treas.gov/moneylaundering2002.pdf.*

ných entít, typických pre finančné transakcie, vytvorenia nových profilov zohľadňujúcich špecifiká finančných údajov a úpravy zobrazovania výstupných parametrov v slovenskom jazyku.

Pre ilustráciu je na obr. 3 zobrazený jeden z výstupov riešenia. (Poznámka: Štruktúra údajov použitých v tomto článku bola postavená na báze spracovaných údajov, ale ich obsah bol modifikovaný tak, aby nemali vzťah k reálnym organizáciám alebo osobám). V tomto prípade bolo cieľom analýzy identifikovať transfery do daňových rajov a výstup použiť pre koreláciu s ďalšími výstupmi.

V hornej časti vizualizácie na obr. 3 je vidieť zdroje platieb (účty, alebo návestia na ne) smerujúcich do daňových rajov, v dolnej časti zase jednotlivé prijímajúce krajiny. Cieľom nebolo identifikovať prijímajúcu stranu, ale účty, ktoré realizujú finančné transfery do daňových rajov. Spojnice medzi účtami a krajinami predstavujú menu realizovanej transakcie a detailné informácie o nej. Ukážka detailu transferu je na obr. 4.

Výhodou popísaného výstupu oproti normálnemu reportu v podobe výpisu účtov, transferov a krajín je v možnosti jeho jednoduchej korelácie s inými výstupmi, napr. bežnými dennými transfermi, priamo v dodávanom produkte. Touto efektívnou a jednoduchou koreláciou viacerých výstupov boli oveľa rýchlejšie získané informácie o väzbách medzi podozrivými účtami a jednotlivými transfermi. Zároveň môže korelovaný výstup, spolu s ďalšími údajmi, poslúžiť aj ako podklad pre vyšetrovanie finančnej polície.

PRÍNOSY PROJEKTU

Implementáciou riešenia pre centrálne monitorovanie bezpečnosti získava zákazník prehľad o aktuálnej bezpečnostnej situácii v organizácii. Riešenie zároveň umožňuje efektívnejšie riadiť bezpečnostné riziká a zlepšiť možnosti vyšetrovania a prijatia následných opatrení pre identifikované bezpečnostné incidenty. V konečnom dôsledku vytvára predpoklady na prepojenie Network Operations Centers (NOC) a Security Operations Centers (SOC).

Implementácia produktu forenznej analýzy ako riešenia na podporu procesov identifikácie neštandardných obchodných operácií zefektívnila proces analýzy podozrivých transakcií a významne zjednodušila korelovanie a hľadanie väzieb medzi podozrivými účtami a realizovanými transfermi.

K primárnym prínosom projektu sa radí aj splnenie legislatívnych požiadaviek a priblíženie sa k medzinárodným bezpečnostným štandardom. Sekundárnym prínosom sa stal rozvoj internej metodiky a procesov na identifikáciu neobvyklých obchodných operácií.

RIEŠENÉ PROBLÉMY A RIZIKOVÉ FAKTORY PROJEKTU

Hlavným problémom pri implementácii produktu na podporu procesov identifikácie neštandardných obchodných operácií bola absencia jednoznačnej metodiky. Zo strany legislatívy a regulačných orgánov existujú len základné rámce a požiadavky na identifikovanie neštandardných obchodných operácií. Zákazník tento problém vyriešil vytvorením vlastnej metodiky vo forme interného predpisu.

Vychádzajúc zo skúseností získaných počas implementácie, hlavnými rizikovými faktormi, ktoré významným spôsobom môžu ovplyvniť priebeh projektu a prevádzku riešenia sú:

- nedostatok interných ľudských zdrojov na implementáciu a prevádzku riešenia;
- podhodnotenie finančných nárokov na projekt zo strany zákazníka;
- nedostatočná dokumentácia aktuálne prevádzkovaného IS, hlavne jeho aplikácií a kontrolných funkcií.

Kvalitu a vypovedaciu schopnosť konečného riešenia môže negatívne ovplyvniť aj absencia zdroja a synchronizácie presného času v IS a absencia jednoznačnej identifikácie komponentov a používateľov IS.

ČO BUDE ĎALEJ

Implementácia riešenia pre centrálne monitorovanie bezpečnosti a nástroja forenznej analýzy nie je jednorazovou aktivitou. Integrovanie sieťových komponentov, systému detekcie narušenia a rozšírenie forenznej analýzy o sieťovú prevádzku bude predmetom druhej časti projektu. S rozvojom a zmenami informačného systému bude potrebné rozšíriť aj monitorovanie o nové zdrojové systémy, hlavne aplikácie. Na základe skúseností z prevádzky riešenia vznikla potreba úprav pravidiel pre zber udalostí a štandardných výstupných reportov podľa potrieb zákazníka. Samostatnou kapitolou bude rozvoj internej metodiky a procesov na identifikáciu neobvyklých obchodných operácií. Zákazník prejavil záujem o vývoj špecializovanej aplikácie určenej pre podporu procesov na identifikáciu neobvyklých obchodných operácií, ktorá bude kooperovať s nástrojom forenznej analýzy a internými bankovými systémami. Dôvodom takého rozhodnutia bolo vytvorenie aplikácie presne podľa zákazníkových požiadaviek a ním spracovanej metodiky.

IVAN MASNÝ
masny@emm.sk

ING. IVAN MASNÝ, CISM
Po ukončení Elektrotechnickej fakulty STU, odbor Technická kybernetika v roku 1992, pôsobil vo Všeobecnej úverovej banke, a.s. a Poštovej banke, a.s. v rôznych funkciách spojených s implementáciou, prevádzkou a bezpečnosťou bankového IS. Od roku 2003 pracuje vo firme EMM, spol. s r.o. v pozícii analytika a architekta IT bezpečnosti hlavne pre zákazníkov z finančného a štátneho sektora.

MANAGEMENT SUMMARY

Štúdia sa venuje implementácii riešenia centrálneho monitorovania bezpečnosti doplnenému o nástroj pre forenzné analýzy vo finančnej inštitúcii, popisuje praktické skúsenosti z realizovaného projektu a upozorňuje na problémové oblasti.