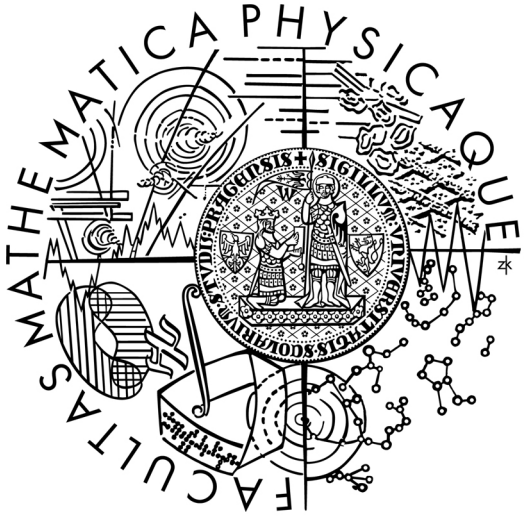
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁRSKA PRÁCA



Dušan Domány

Bezpečnosť informačných systémov

Katedra softwarového inžinierstva

Vedúci bakalárskej práce: Mgr. Jaroslav Tykal
Študijný program: Informatika, Správa počítačových systémov

2008

Ďakujem Mgr. Jaroslavovi Tykalovi za odborné vedenie mojej práce, jeho čas, trpezlivosť, konštruktívne pripomienky a doporučenia, ktoré mi venoval.

Prehlasujem, že som svoju bakalársku prácu napísal samostatne a výhradne s použitím citovaných prameňov. Súhlasím so zapožičaním práce a jej zverejňovaním.

V Prahe dňa 7.8.2008 Dušan Domány

Obsah

Názov práce: *Bezpečnosť informačných systémov*
Autor: *Dušan Domány*
Katedra (ústav): *Katedra softwarového inžinierstva*
Vedúci bakalárskej práce: *Mgr. Jaroslav Tykal*
e-mail vedúceho: *jaroslav.tykal@mff.cuni.cz*

Abstrakt: *Predložená práca pojednáva o rôznych aspektoch zabezpečenia informačných systémov. Rozoberá ciele informačnej bezpečnosti, proces návrhu zabezpečenia informačného systému, najčastejšie formy rizík a niektoré základné metódy ochrany proti nim. Prostredníctvom priloženého programu je možné si vyskúšať návrh zabezpečenia informačného systému fiktívnej spoločnosti a otestovanie tohoto návrhu prostredníctvom simulácie. V práci je uvedený popis tohoto programu zahŕňajúci užívateľskú príručku, popis konfiguračných súborov, štruktúru programu a krátku ukážku.*

Kľúčové slová: *informačná bezpečnosť, informačný systém, bezpečnostné riziká, ochrana informácií*

Title: *Information systems security*
Author: *Dušan Domány*
Department: *Department of Software Engineering*
Supervisor: *Mgr. Jaroslav Tykal*
Supervisor's e-mail address: *jaroslav.tykal@mff.cuni.cz*

Abstract: *Present work studies different aspects of information systems security. It describes the information security goals, the designing process of the information system security, most common forms of risks and some basic methods of protection against them. Through the enclosed program it is possible to try out to design security of information system for an imaginary company and test this design through a simulation. The work contains description of this program including user guide, configuration files description, program structure and a short example of use.*

Keywords: *information security, information system, security risks, protection of information*

Kapitola 1

Úvod

Problematika bezpečnosti je v súčasnej dobe veľmi aktuálna. Po veľkom nadšení z možností, ktoré priniesli informačné technológie, nasledovalo schladenie v súvislosti s množstvom nových problémov a rizík, ktoré tieto technológie priniesli.

Spoločnosť je v súčasnej dobe čoraz viac závislá od správnej a neprerušenej činnosti čoraz zložitejších systémov. Stávajú sa takými zložitými, že nie je v ľudských silách detailne postihnúť súvislosti medzi ich jednotlivými komponentami a následne presne predikovať ich chovanie za okolností odchyľujúcich sa od bežných stavov.

Zložitosť týchto moderných informačných a komunikačných systémov a s ňou súvisiaca vysoká náročnosť na zaistenie primeranej kontroly nad ich činnosťou vytvára množstvo príležitostí pre cielené útoky.

Predložená práca pojednáva o rôznych aspektoch zabezpečenia informačných systémov. Jej prvá kapitola obsahuje tento úvod.

Kapitola dva rozoberá ciele informačnej bezpečnosti. Teda z akého dôvodu je potrebné zabezpečovanie informačného systému.

Kapitola tri sa zaoberá procesom návrhu tohto zabezpečenia. Zahŕňa analýzu rôznych potenciálnych nebezpečenstiev, návrh opatrení a špecifikovanie pravidiel a zásad, ktorých dodržiavanie často výraze znižuje riziko bezpečnostného incidentu. To všetko v súlade so všeobecne uznávanými bezpečnostnými normami, ktorých kritériá hrajú významnú úlohu jak pri samotnom návrhu, tak pri záverečnom hodnotení výsledku.

Kapitola štyri ďalej pojednáva o niektorých základných metódach ochrany, ktoré sa v rôznych podobách využívajú vo väčšine návrhov zabezpečenia. Kokrétne ide o techniky fyzickej ochrany, overenia totožnosti subjektu (autentifikácia), overenie oprávenosti subjektu pristupovať k danému objektu (autorizácia) a šifrovanie.

Kapitola piata rozoberá niektoré najčastejšie formy rizík, na ktoré je vhodné pri každom návrhu zabezpečenia myslieť. Poukazuje nie len na nebezpečenstvo úmyselných útokov, ale aj rôznych zlyhaní, neúmyselných chýb personálu či užívateľov, prírodných katatrof, atď.

Kapitola šiesta popisuje program, v ktorom si užívateľ môže zábavnou formou vyskúšať návrh zabezpečenia informačného systému spoločnosti a otestovanie tohoto návrhu prostredníctvom simulácie. Do simulácie vstupujú štyri typy objektov: Opatrenia nakupované užívateľom na začiatku, ale aj v priebehu simulácie. Hrozby

útočiace na spoločnosť usilujúce sa prekonať opatrenia a vyvolaním tzv. udalostí ju nejakým spôsobom poškodiť. Udalosti sprevádzajúce simuláciu, ktoré sú úzko späté s útočiacimi hrozbami a dodávajú celému priebehu dynamičnosť. A nakoniec samotná spoločnosť, ktorej typ si volí užívateľ na začiatku a určuje tak do istej miery podmienky, za akých bude simulácia prebiehať. Všetky tieto objekty sú načítavané z konfiguračných súborov, kde sú uložené v textovej forme a užívateľ si ich tak môže prispôsobiť podľa vlastných potrieb a predstáv. Program taktiež ponúka prostredníctvom rôznych tabuliek možnosť prehľadného prezerania si atribútov týchto objektov a vzťahov medzi nimi, ako aj sledovania priebehu samotnej simulácie kvôli strategickým rozhodnutiam pri nákupe opatrení. Na konci poslednej kapitoly je uvedená krátka ukážka popisujúca konkrétne použitie programu a poukazujúca na rôzne jeho možnosti a funkcionality.

Posledná kapitola obsahuje záverečné zhrnutie a niekoľko návrhov na ďalšie vylepšenie.

Cieľom tejto práce je poskytnúť jej čitateľovi obraz o tom, čo sa rozumie pod pojmom ochrana informačného systému, čo táto oblasť zahŕňa, aké riziká hrozia informačným systémom v súčasnej dobe a ako je možné sa pred týmito rizikami chrániť. Jedná sa o veľmi obsiahlu oblasť, ktorej pole pôsobnosti siaha od zabezpečenia počítačových sietí na školách po skryté informačné vojny dokonca aj medzi rôznymi národmi. V neposlednom rade je to oblasť, okolo ktorej sa v súčasnej dobe točia nemalé financie. Slovami Mgr. Antonína Beneša, Dr.:

"*Základní princip ochrany výpočetních systému: O peníze jde až v první řade*"

Kapitola 2

Čo zahŕňa ochrana informačného systému

2.1 Spoľahlivosť prevádzky informačného systému

Od spoľahlivej prevádzky informačného systému často závisí schopnosť jeho používateľov vykonávať svoju predpokladanú činnosť, plniť svoje záväzky, ktoré majú k ďalším subjektom, či včas prijímať správne rozhodnutia. Hoci miera ich závislosti od funkčnosti informačného systému závisí od konkrétnych okolností, prerušenie jeho prevádzky či iné odchýlky od jeho projektovanej či očakávanej činnosti (napríklad nesprávne spracovanie údajov) nesporne negatívne ovplyvní výsledky ich práce. V tejto súvislosti je mimoriadne dôležité vziať do úvahy, že dôležitost spoľahlivej prevádzky informačného systému obvykle prudko vzrastá práve v mimoriadnych situáciach, aké vyvoláva napríklad výpadok infraštruktúry či hoci aj odchýlky správania sa dôležitých komponentov systému od normálneho (očakávaného, predpokladaného) stavu.

Zabezpečenie spoľahlivej prevádzky informačného systému znamená vykonanie takých opatrení, ktoré umožnia informačnému systému poskytovať svoje služby používateľom včas a v požadovanej kvalite, a to i pri značných odchýlkách okolia informačného systému od normálneho stavu.

2.2 Ochrana údajov

Podľa OECD Guidelines for the Security of Information Systems [5] sa údajmi rozumie "*reprezentácia faktov, konceptov alebo inštrukcií vo formalizovanom tvare vhodnom pre komunikáciu, interpretáciu alebo spracovanie ľudskými bytosťami alebo automatickými prostriedkami*".

Informácia je potom "*význam priradený údaju prostriedkami konvencií aplikovaných na tento údaj*".

Každý údaj má svoje atribúty, ako napríklad presnosť, správnosť, úplnosť, neprotirečivosť, vierohodnosť zdroja, relevantnosť a podobne. Porušenie niektorého z týchto atribútov sa nazýva bezpečnostný incident.

Zabezpečenie ochrany údajov znamená vykonanie opatrení na zachovanie takých

atribútov predmetných údajov, ktoré sú majiteľom alebo používateľom týchto údajov, prípadne iným subjektom, považované za dôležité.

Hoci voľba skupiny atribútov, ktorú subjekt považuje za dôležité chrániť, môže byť značne individuálna, za najčastejšie chránené atribúty sa považujú:

- dôvernosť - vzťahuje sa na povolenie prístupu k údaju iba vymedzenému okruhu subjektov a zamedzenie prístupu subjektom mimo tento okruh. Pre tento účel sa uplatňujú rôzne autentizačné metódy.
- integrita - znamená, že údaj je celistvý, neporušený, nebol neoprávnene pozmenený. Spája sa s dôverihodnosťou údaju. Strata tohto atribútu znamená, že údaj nezodpovedá skutočnosti, ktorú by mal reprezentovať.
- dosiahnuteľnosť - stav, v ktorom je údaj pripravený pre bezprostredné použitie. Strata tohto atribútu znamená, že údaj nie je k dispozícii tam, kde je očakávaný.

Tieto tri atribúty sú tiež známe pod skratkou CIA, vytvorenou z ich anglických názvov confidentiality, integrity, availability.

Pri formulovaní požiadaviek na zabezpečenie ochrany údajov je mimoriadne dôležité správne určiť, ktoré údaje (a ktoré ich atribúty) konkrétneho systému je potrebné chrániť.

Najčastejšie sa zabúda na potrebu chrániť metaúdaje potrebné pre úspešnú prevádzku informačného systému, ako napríklad prístupové heslá oprávnených používateľov systému, alebo šifrovacie kľúče. Neoprávnená manipulácia s takýmito údajmi však môže mať za následok značné škody.

2.3 Ochrana záujmov používateľov informačného systému

V súčasnej dobe sa pod týmto pojmom chápe predovšetkým ochrana súkromia používateľa v súvislosti s jeho aktivitami v prostredí informačného systému. Sem patrí poskytnutie:

- anonymity - stavu, v ktorom, používateľ môže využívať funkcie informačného systému bez toho, aby bola identifikovateľná jeho totožnosť určitým okruhom subjektov.
- pseudonymity - stavu, v ktorom, používateľ môže využívať funkcie informačného systému bez toho, aby bola identifikovateľná jeho totožnosť určitým okruhom subjektov, pričom používateľ môže byť stále (v prípade potreby) braný na zodpovednosť za svoju činnosť v systéme.
- nespojiteľnosti (unlinkability) - stavu, v ktorom má užívateľ možnosť viacnásobného využívania zdrojov alebo iných služieb informačného systému bez toho, aby iné subjekty boli schopné rozoznať, že všetky tieto aktivity sú spojené s jedným používateľom.

Kapitola 3

Proces vzniku informačného systému

Usilovať sa o dokonale bezpečný informačný systém často nemá význam, pretože sa to skrátka nevyplatí. Snahou je obmedziť hrozby, odstrániť čo najviac slabín a podľa možností čo najviac zamedziť stratám v prípade bezpečnostného incidentu. Avšak len do tej miery, kedy sa to prestane vyplácať. Je treba počítať s tým, že stále zostane nejaké zbytkové riziko. "*Stav bezpečnostného incidentu je nutné brať ako ďalší z prevádzkových režimov informačného systému*" [1]

Z pohľadu návrhu bezpečnosti informačného systému je úplne zásadným krokom vytvorenie si predstavy o tom

- čo je treba chrániť (špecifikovať objekty, ktorých bezpečnosť má byť zaistená).
- pred kým/čím sa to má chránit (aké potenciálne nebezpečenstvo hrozí chránením objektom).
- aké náklady je možné vynaložiť na vybudovanie ochrany.
- aké náklady by mal útočník v prípade úmyselného útoku vynaložiť na prelomenie ochrany.

3.1 Analýza rizík

Cieľom analýzy rizík je charakterizovanie množiny potenciálnych hrozieb a ohodnotenie ich prípadného finančného dopadu. Je pri nej treba zvážiť ako často bude asi k potenciálnej hrozbe dochádzať a aký celkový dopad môže mať na spoločnosť. Niektoré hrozby sa môžu opakovať s pomerne veľkou frekvenciou, avšak s dopadom banálneho charakteru. U iných môže byť pravdepodobnosť, s ktorou nastávajú, úplne mizivá, avšak keď nastanú, môžu spôsobiť krach celej spoločnosti.

Analýza rizík by sa mala zamerať predovšetkým na

- aktíva organizácie (služby informačného systému, údaje, technické prostriedky, programové prostriedky, personál, prostredie v ktorom je informačný systém

prevádzkovaný) a na dôsledky pre organizáciu v prípade, že aktívum je prezradené, modifikované, zničené alebo inak zneužité.

- hrozby, chápané ako javy alebo činnosti ohrozujúce informačný systém, resp. analyzovanú entitu, a na pravdepodobnosť ich výskytu, teda relatívnu "váž-nosť" jednotlivých hrozieb.

- zraniteľnosť informačného systému, resp. analyzovanej entity, teda na slabé miesta a nedostatky bezpečnostných opatrení, ktoré by mohli byť využité touktorou hrozbou.

- ochranné prostriedky, teda na ich účinnosť v zmysle schopnosti redukovať "citlivosť" informačného systému na špecifikované hrozby, a na určenie miery rizika, ktorému je informačný systém vystavený. Miera rizika môže byť vyjadrená kvantitatívne (v penažných jednotkách), alebo kvalitatívne, pomocou jasne definovanej stupnice.

3.2 Návrh opatrení

Spočíva vo výbere takých opatrení, ktoré čo najlepšie pokrývajú jednotlivé slabiny systému. Výsledkom je zoznam navrhovaných opatrení a nástin ročných úspor z ich zavedenia.

3.3 Bezpečnostná politika

Pod pojmom bezpečnostá politika sa rozumie dokument, ktorý má slúžiť pre orientáciu personálu a pracovníkov vo všetkých činnostiach, ktoré majú priamy alebo nepriamy vplyv na úroveň bezpečnosti informačného systému. Vymedzuje kompetencie, zodpovednosť, zásady a princípy, ktorými sa organizácia a jej pracovníci majú riadiť pre dosiahnutie stanovených bezpečnostných cieľov.

3.4 Bezpečnostné normy

Aby bolo možné ohodnotiť bezpečnosť vzniknutého produktu či systému, je potrebné nezávislé odborné posúdenie riadiace sa všeobecne akceptovanými kritériami. Tieto sú spravidla zhrnuté v uznávaných normách a štandardoch.

Ich úlohou je predovšetkým:

- ponúknuť užívateľom vodítko, na základe ktorého môžu sami zhodnotiť úroveň danej bezpečnosti.

- ponúknuť výrobcom a návrhárom smernice pre zabudovanie bezpečnostných prvkov do ich produktov.

- ponúknuť základ pre špecifikovanie bezpečnostných potrieb.

Ďalej:

- zavádzajú jednotnú kultúru a stanovujú zrovnateľné kritériá.
- uľahčujú audit, kontroly, jednanie s partnermi.

Ak systém na základe testovania vyhovie požiadavkám danej normy, môže mu byť v rámci následnej certifikácie vystavený certifikát, ktorý je formálnym vyjadrením zhody s jej požiadavkami.

Uvedené štyri dokumenty sú medzinárodne uznávanými a najznámejšími normami v oblasti informačnej bezpečnosti. Zďaleka však nie jedinými. Jednotlivé štáty môžu mať vlastné kritériá hodnotenia bezpečnosti prispôsobené ich podmienkam, zvyklostiam a právnemu systému.

3.4.1 TCSEC

Prvým pokusom o stanovenie takýchto kritérií boli Trusted Computer Security Evaluation Criteria, známe tiež ako Oranžová kniha Ministerstva obrany USA.

Kritériá sú rozdelené do sekcií a v rámci nich do jednotlivých tried. Tieto kriteriá sa stali základom aj pre niektoré ďalšie v súčasnosti rozšírene používané normy.

- Sekcia D: Minimálna ochrana - Táto sekcia obsahuje iba jednu triedu a je rezervovaná pre systémy, ktoré boli podrobené hodnoteniu, ale nesplnili požiadavky vyšších tried.
- Sekcia C: Voľná ochrana - Užívateľom je poskytnutá určitá miera ochrany, ktorú môžu využiť.
  - Trieda C1: Voľné zabezpečenie - Užívatelia by mali mať možnosť chrániť svoje dáta pred prístupom (čítaním či zapisovaním) ostatných užívateľov.
  - Trieda C2: Kontrolovaný prístup - Užívatelia sa do systému prihlasujú cez svoje účty. Je zabezpečená izolácia zdrojov a ochrana proti reziduám (nesmie sa stať, že užívateľ po skončení svojej činnosti opustí blok pamäte a ten je potom pridelený inému užívateľovi obsahujúc dáta pôvodného užívateľa).
- Sekcia B: Povinná ochrana - Určitý systém ochrany sú užívatelia povinní využívať a nemôzu ho nijakým spôsobom obísť.
  - Trieda B1: Značkovaná ochrana - Zahŕňa požiadavky triedy C2. Naviac musí byť zavedený bezpečnostný model, podľa ktorého musia byť kontrolované subjekty a objekty označené a každý prístup musí byť podľa tohoto modelu kontrolovaný. Akákoľvek závada odhalená pri testovaní musí byť odstránená.
  - Trieda B2: Štrukturovaná ochrana - Musí byť definovaný a zdokumentovaný formálny model bezpečnostnej politiky vyžadujúci voliteľnú aj povinnú kontrolu prístupu z triedy B1 rozšírenú na všetky subjekty a objekty v systéme. Systém musí byť odolný voči prieniku.

  - Trieda B3: Bezpečnostné domény - Musí existovať úplný popis celkovej štruktúry návrhu systému dostatočne jednoduchý na to, aby mohol byť podrobený analýze a testovaniu. Je povinná kontrola každého jedného prístupu subjektu k objektu. Potrebná prítomnosť bezpečnostnej administratívy, auditu, ako aj procedúr pre obnovu systému. Systém musí byť vysoko odolný voči prieniku.

- Sekcia A: Overená ochrana - Je charakteristická formálnymi metódami overovania bezpečnosti.

  - Trieda A1: Overený návrh - Systém sa funkčne nelíši od triedy B3. Musí však naviac obsahovať formálny model bezpečnostných mechanizmov s dôkazom konzistentnosti.

3.4.2 ITSEC

Information Technology Security Evaluation Criteria je pokusom o zosúladenie jednotlivých národných kritérií do medzinárodne platného celku. V roku 1991 bol prijatý ako základ pre hodnotenie bezpečnosti systémov na spracovanie informácií v členských štátoch Európskej únie.

3.4.3 Common Criteria

Metanorma Common Criteria je založená na modely, v ktorom môžu užívatelia špecifikovať svoje vlastné požiadavky na bezpečnosť. Stanovuje princípy a postupy, ako odvodzovať konkrétne technické normy pre vývoj, testovanie, výsledné vlastnosti a prevádzku technických bezpečnostných protiopatrení v rôznych prostrediach. Vychádza z troch historicky najuznávanejších štandardov: ITSEC, TCSEC a CTCPEC (Canadian standard).

3.4.4 BS7799

Jedná sa o britský štandard. Je vytvorená ako referenčný bod identifikácie škály opatrení potrebných vo väčšine situácií. Je vydaný vo dvoch častiach:

- časť 1: Kódex praxe riadenia informačnej bezpečnosti.

- časť 2: Špecifikácia pre systémy riadenia informačnej bezpečnosti.

Kapitola 4

Metódy ochrany

4.1 Fyzická ochrana

Spôsob ochrany, ktorého princíp spočíva vo vybudovaní fyzických bariér oddeľujúcich predmetný objekt od potenciálnych hrozieb alebo použití takých zariadení či opatrení, ktoré pri výskyte týchto hrozieb zamädzia prípadným škodám.

Je to prakticky jediný spôsob ako sa chrániť pred

- záplavami (presun zariadení do bezpečia, použitie nepremokavých krytov,...).
- požiarmi (použitie nehorľavých materiálov, hasiace prístroje, automatické protipožiarne systémy, evakuácia personálu a životne dôležitých komponent systému,...).
- stratami napájania(záložné zdroje,generátory elektrickej energie,zariadenia chrániace pred výkyvmi napätia, bleskami apod.).
- prehriatim kľúčových komponent (chladiace zariadenia,klimatizácia,priestory s prirodzene nižšou teplotou,...).
- prašnosťou, vybráciami, vlhkosťou, atď.

Ku potenciálnym hrozbám prirodzene patria aj ľudský útočníci (zlodeji, vandaly, sabotéri,...).

Má zmysel rozlišovať fyzickú bezpečnosť vo veľkom (budovy, miestnosti, trasy) a v malom (cennosti, listiny, médiá, šifrovacie kľúče). V druhom prípade sa často používajú efektívnejšie spôsoby ochrany, ktoré by v prvom prípade boli neprimerane nákladné.

4.1.1 Ochrana vo veľkom

V tejto oblasti je dôležité si byť vedomý toho, ze celková ochrana je účinná len do tej miery, do akej je odolná jej najslabšia komponenta. Nasadenie mreží na okná a dokonalé zabezpečenie hlavného vchodu zaistí maximálne tak falošný pocit bezpečia

pokiaľ má budova zadný východ s obyčajnými drevenými dverami a zámkom, na ktorého prekonanie stačia dostatočne veľké kliešte.

Jednou z kľúčových otázok je ako zabezpečiť prístupové cesty, aby cez ne prešli iba oprávnené osoby. Taktiež je potrebné zabezpečiť, aby boli tieto osoby v objekte prítomné iba v čase, keď ku tomu majú skutočne oprávnenie. Jedným zo základných prvkov ochrany sú v tomto prípade stráže, ktoré musia byť schopné rozoznať oprávnenú osobu od neoprávnenej. Hoci je možné použitie aj automatického systému ochrany (napr. dvere, ktoré sa otvoria iba pri úspešnej identifikácii osoby, ktorá k nim pristupuje), je vhodné ho kombinovať so strážami. Pre identifikáciu osôb sa využívajú rôzne spôsoby autentifikácie: identifikačné karty, kľúče, magnetické alebo čipové karty, prípadne biometrické metódy.

Okrem uvedených prostriedkov, ktoré pôsobia preventívne, sa používajú aj prostriedky pre detekciu vniknutia do chráneného priestoru. Do tejto kategórie patria kamery, rôzne typy alarmov, senzorov, atď.

4.1.2 Ochrana v malom

Podľa účelu možno ochranu v malom rozdeliť do dvoch kategórií:

- fyzické zabezpečenie dokumentov, médií alebo iných objektov, u ktorých je potrebné, aby k nim bola vytvorená možnosť prístupu oprávneným osobám.
- vytvorenie ochranného krytu, ktorý úplne zablokuje fyzický prístup.

V oboch prípadoch je potrebné použiť konštrukcie a materiály, ktoré sú odolné voči násilnému prieniku.

V prvom prípade sa používajú rôzne schránky, sejfy, a podobne. Celková úroveň ochrany je v podstatnej miere ovplyvnená nutnosťou zabezpečenia legitímneho prístupu k chránenému prvku. Významnú úlohu hrá ochrana kľúčov, hesiel, kódov, atď., ktoré sú používané pre overenie autenticity oprávnenej osoby.

V druhom prípade ide o ochránenie prvku, ktorý je podstatný pre správnu činnosť nejakého zariadenia, pričom v rámci informačného systému sa využívajú rôzne jeho funkcie, avšak nie priamo chránený prvok. V súčasnosti sa fyzická ochrana tohto typu najčastejšie uplatňuje v prípade čipových kariet slúžiacich na úschovu a ochranu šifrovacích kľúčov či autentifikačných údajov (údajov potvrdzujúcich autenticitu čipovej karty a prenesene aj jej držiteľa).

4.1.3 Zálohovanie

Aj pri tej najväčšej snahe o spoľahlivosť dochádza z času na čas v informačnom systéme ku zlyhaniu niektorej jeho komponenty. Následky takéhoto zlyhania môžu spôsobiť odstavenie dôležitej časti informačného systému na niekoľko hodín alebo aj trvalú stratu kľúčových dát, z ktorej sa už nie je možné spamätať.

Zálohy tento problém riešia veľmi dobre. Môže sa jednať o

- záložný hardware, či software, ktorým je možné pokazenú komponentu v krátkom čase nahradiť.

- zálohy dôležitých dát (napríklad údajov o zákazníkoch, zdrojových kódov, štatistík, atď.).

Problémom záloh je, že väčšinu času nerobia nič užitočné a predstavujú iba réžiu naviac. V kľúčových momentoch sa však stávajú nedoceniteľnými. Často nie je možné zálohovať všetko, preto sa treba sústrediť aspoň na podstatné komponenty.

Dôležité záložné kópie by mali byť uložené na bezpečnom mieste vzdialenom od miesta, kde je inštalovaný informačný systém. Oddelené uloženie kópií chráni proti následkom prírodných katastrof, zlodejom, atď. Pre prípad poruchy by mal byť vypracovaný plán obnovy, teda podrobné procedúry, čo je treba vykonať za účelom rýchleho odstránenia následkov.

4.1.4 Likvidácia dát

Pokiaľ by dáta iba pribúdali, časom by sa ich množstvo stalo neúnosným. Aby neužitočné či neaktuálne dáta zbytočne nezaťažovali informačný systém, je potrebné ich vhodným spôsobom likvidovať. Aj takéto dáta sa však môžu stať cieľom potenciálneho útočníka. Proces likvidácie by mal byť teda dôkladný a nevratný. Často sa napríklad zabúda na to, že prosté zmazanie súborov z disku nestačí, pretože pri tejto operácii sa odstránia iba záznamy o existenicii týchto suborov, zatiaľčo samotné dáta sú stále prítomné na disku až do doby kým nie sú prepísané nejakými inými dátami.

Pre likvidáciu papierových dokumentov sa používajú rôzne typy skartovačov. Existujú aj skartovače na diskety, kazety, pásky a iné médiá. Pre mazanie údajov z magnetických médií sa najčastejšie používa viacnásobné prepisovanie. Pre vyšší stupeň spoľahlivosti sa používa degausser, ktorý vygenerovaním silného elektromagnetického impulsu dokáže zničiť pôvodné magnetické pole. V prípade, že nestačí ani použitie degaussera, je možná fyzická likvidácia média.

4.2 Autentifikácia

Autentifikáciou nazývame proces overenia totožnosti. Ide o určitý druh testu, ktorý musí človek či zariadenie zložiť pre získanie oprávnení subjektu, za ktorý sa vydáva (ktorého identifikáciu používa). Tento test by mal byť schopný zložiť iba príslušný subjekt a žiaden iný by nemal byť schopný ho napodobiť. V nasledujúcich troch kapitolách budú rozobraté tri najčastejšie používané prístupy pre unikátnu autentifikáciu subjektu.

4.2.1 Čo subjekt vie

Jedným zo základných prístupov je použitie hesla, teda reťazca (slova, frázy, šifrovacieho kľúča) spojeného s identitou subjektu, ktorý pozná iba daný subjekt. Tento pomerne jednoduchý prístup však so sebou prináša mnoho rizík, ktoré budú podrobnejšie popísané v kapitole Úmyselné útoky:

- odpočutie hesla - heslo by nemalo byť prenášané po komunikačných kanáloch ako také, zvlášť pokiaľ ide o autentifikáciu po sieti. Vhodné je použitie systémov

challenge-response (systém vygeneruje náhodný reťazec a zašle subjektu. Ten použije heslo a reťazec na vygenerovanie odpovede spôsobom, na ktorom je so systémom dohodnutý (napr. reťazec pomocou hesla zašifruje) a zašle odpoveď naspäť systému).

- vyzradenie hesla - týka sa hlavne ľudských subjektov. Zvýšené riziko hrozí v prípade skupinových hesiel. Taktiež v prípade, že si užívatelia systému nedokážu alebo nechcú zapamätať svoje heslá a tak používajú rôzne barličky ako schovávanie poznačeného hesla pod klávesnicu, apod. Je potrebné upovedomiť užívateľov o rizikách (prípadne sankciách) spojených s vyzradením hesla a voliť vhodné kritériá zložitosti hesla, aby bolo možné si ho zapamätať a zároveň aby nebolo príliž jednoduché na uhádnutie.

- uhádnutie hesla - hrozí v prípade príliž jednoduchých hesiel. Heslo by malo mať dostatočnú dĺžku, nemalo by ísť o obvyklé slovo alebo frázu, znaky by mali byť vyberané z dostatočne veľkej množiny a nesmie byť odvoditeľné zo znalosti subjektu, ku ktorému prislúcha.

4.2.2 Čo subjekt vlastní

Jedná sa o rôzne druhy tzv. tokenov. Malo by byť náročné ich falzifikovať a tiež je vhodné zaviesť opatrenia, ktoré by predchádzali ich strate či odcudzeniu. Často sa tokeny kombinujú s heslom, aby samé o sebe nestačili k úplnej autentifikácii. V nasledujúcom zozname sú tokeny zoradené od najmenej bezpečných po najbezpečnejšie:

- rôzne typy preukazov, väčšinou obsahujú fotografiu. Autentifikáciu prevádzajú stráže alebo iné zodpovedné osoby.

- tokeny iba s pamäťou. V pamäti sú uložené dáta potrebné pre autentifikáciu. Jedná sa napríklad o karty s magnetickým prúžkom. Je potrebný špeciálny snímač pre prečítanie obsahu tokenu. V prípade, že sa útočníkovi podarí získať obsah pamäte tokenu, za použitia špeciálneho zariadenia môže pomerne jednoducho vyrobiť falzifikát.

- tokeny s výpočetnou jednotkou. Obsahujú procesor a pamäť, ku ktorej je možný prístup iba cez určité rozhranie. Priame skopírovanie obsahu pamäte teda nie je možné a v prípade použitia vhodnej výpočetnej logiky nie je možné ani jeho odvodenie. Často sa v súvislosti s týmito tokenmi používajú takzvané zero-knowledge proofs.

4.2.3 Čo subjekt charakterizuje ako taký

Jedná sa väčšinou o rôzne typy biometrík (merateľných fyzických či fyziologických charakteristík alebo znakov chovania jedinca):

- verifikácia hlasu - subjekt prečíta systémom náhodne zvolenú frázu. Využívajú sa charakteristiky hlasu, basové a vysoké tóny, vibrácie hlasu a hrdelné a nosné

tóny. Výhodou je vysoká spoločenská prijateľnost a možnosť autentifikácie po telefóne.

- verifikácia dynamiky podpisu - sledujú sa zmeny tlaku, zrýchlenie v jednotlivých častiach, celková rýchlosť, celková dráha a doba pohybu pera na a nad papierom apod. Výhodou je opäť prirozenosť a sociálna akceptovateľnosť, nevýhodou značná variabilita podpisu u niektorých ľudí.

- verifikácia otlačku prstu - robí sa štatistický rozbor výskytu tzv. markant (hrbolkov, slučiek a špirál v otlačku prstu) a ich vzájemnej polohy. Výhodou je vynikajúca variabilita tohoto znaku u ľudí a dobrá spracovateľnosť vstupných dát. Nevýhodou sú možné negatívne asociáce užívateľov (v súvislosti s použitím otlačkov prstov v kriminalistike), a vyššia cena technológie.

- geometria ruky - skúma sa dĺžka a šírka dlane a jednotlivých prstov, bočný profil ruky apod. Metóda je pomerne spoľahlivá avšak dosť drahá.

- obrazy sietnice - snímaný je obraz štruktúry sietnice v okolí slepej škvrny. Obrazy sietnice majú rovnaké charakterizačné vlastnosti ako otlačky prstov. Výhodnou metódy je značná spoľahlivosť a veľmi náročná napodobiteľnosť. Preto ide o metódu vhodnú pre nasadenie v prostredí nejvyššieho utajenia. Nevýhodou je istá subjektívna nepríjemnosť. Opäť ide o veľmi drahú technológiu.

Ďalšie biometriky: rysy tváre, rytmus písania na klávesnici, EEG, EKG, otlačky dlaní a chodidiel, otlačky chrupu, genetické rozbory, ...

Nevýhodou niektorých biometrík je, že môžu byť ovplyvnené stavom jedinca (napríklad choroba môže poznačiť jeho hlas).

Kvalitu biometrík možno hodnotiť na základe nasledujúcich dvoch charakteristík, ktoré je potrebné vhodným spôsobom čo najviac minimalizovať:

- početnosť nesprávnych odmietnutí - autorizovaného subjektu

- početnosť nesprávnych prijatí - útočníka

Je treba voliť vhodnú toleranciu pri snímaní pre optimálnu vyváženosť týchto dvoch charakteristík.

4.3 Autorizácia

Autorizáciou sa nazýva proces overenia oprávnenosti subjektu pristupovať ku danému objektu (súboru, bloku pamäte, procesu,...). Aby proces autorizácie vôbec mohol prebehnúť, systém musí byť schopný rozpoznať vzťah medzi každým subjektom a objektom (teda či a ako môže subjekt ku príslušnému objektu pristupovať). O každom takomto vzťahu teda v systéme musí existovať záznam. Voľba spôsobu ako tieto vzťahy zaznamenávať závisí od požiadaviek na rýchlosť, pamäťových kapacít, pomeru počtu subjektov a počtu objektov, úrovne zdieľania, atď. Nasledujúci zoznam popisuje niektoré z najrozšírenejších spôsobov:

- adresár (Directory)- každému subjektu prislúcha adresár obsahujúci odkazy na objekty, ku ktorým má oprávnenia, vrátane popisu týchto oprávnení.
- zoznam oprávnení (Access Control List) - s každým objektom je udržovaný zoznam informácií, ktoré subjekty k nemu majú aké oprávnenia.
- prístupová matica (Access Control Matrix) - riadky matice zodpovedajú jednotlivým subjektom, stĺpce objektom. V políčkach matice sú záznamy o úrovni oprávnení, ktoré majú subjekty k objektom.
- spôsobilosť (Capability) - subjektom sú prideľované tokeny, ktorých vlastníctvo im zabezpečuje špecifické práva k objektom.

V každom z uvedených prípadov je potrebné dbať na ochranu príslušnej množiny záznamov. Pokiaľ by útočník získal schopnosť túto množinu modifikovať, získal by tak tiež možnosť obísť proces autorizácie.

4.3.1 Úrovne ochrany

Podľa potreby môže systém poskytovať rôzne úrovne ochrany objektov pred neautorizovaným prístupom. Zvolená úroveň závisí predovšetkým od požiadaviek na mieru zdieľania objektov medzi subjektami a mieru špecifikácie operácií, ktoré možno s objektami vykonávať. Najčastejšie sa volí niektorá z nasledujúcich úrovní radených od najnižšieho stupňa ochrany po najvyšší:

- žiadna ochrana - postačujúca ak dochádza ku samovoľnej časovej separácii.
- izolácia - systém zaisťuje úplné oddelenie bežiacich procesov a ich objektov.
- zdieľanie všetkého alebo ničoho - vlastník objektu deklaruje, či je objekt verejný (public), alebo súkromný (private) a teda viditeľný iba pre neho.
- zdieľanie s obmedzenými prístupmi - o každom subjekte a objekte existuje záznam určujúci oprávnenie subjektu k tomuto objektu pristupovať. Testuje sa každý pokus o prístup.
- zdieľanie podľa spôsobilosti - nadstavba predchádzajúceho spôsobu zdieľania. Rozsah oprávnení môže naviac dynamicky závisieť na aktuálnom kontexte.
- limitované použitie objektu - nešpecifikuje sa iba či subjekt smie pristupovať k danému objektu, ale aj operácie, ktoré subjekt smie s objektom vykonávať.

4.3.2 Implementácia

Samotná implementácia sa môže podľa potrieb líšiť. Príkladom implementácie je kontrola prístupu k súborom a adresárom v operačnom systéme Unix, ktorá sa riadi nasledujúcimi pravidlami:

- užívatelia sú zaraďovaní do skupín.

- súbory sú zaraďované do adresárov.
- každý súbor, resp. adresár náleží vlastníkovy a jeho skupine.
- existujú tri základné operácie možné vykonávať: čítanie, zápis a spustenie.
- právo na spustenie adresára zodpovedá právu vstúpiť doň. Právo na zápis v prípade adresára predstavuje právo na mazanie jeho súborov a vytváranie nových súborov.
- u každého súboru, resp. adresára jeho vlastník špecifikuje ktoré z uvedených operácií s ním môže vykonávať on sám, jeho skupina a všetci ostatní.
- správca systému (tzv. root) má schopnosť prístupové práva modifikovať.
- spustiteľné súbory môžu byť spustené s oprávneniami ich vlastníka alebo skupiny.

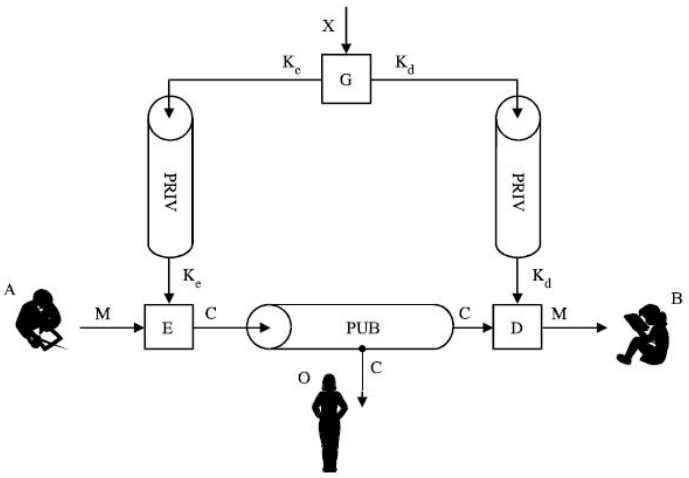
Vzhľadom na to, že právami k adresáru užívateľ čiastočne získava aj práva nad jeho obsahom, zďaleka sa v tomto prípade nemožno spoľahnúť iba na pridelenie prístupových práv k súborom. Môže sa stať, že útočník nebude mať prístupové práva k súboru, avšak bude mať práva na zápis do adresára s týmto súborom, čo mu umožní príslušný súbor vymazať. Ďalej netreba podceňovať prideľovanie práv vlastníka samému sebe vzhľadom na posledný bod v zozname (ak by napríklad niekto spustil súbor s vlastníkovými oprávneniami s príkazmi na mazanie iných jeho súborov) a vzhľadom na to, že každý človek sa z času na čas dopustí nejakej chyby. Z uvedeného vyplýva, že je veľmi dôležité, aby každý užívateľ systému rozumel spôsobu prideľovania práv a usiloval sa podľa neho riadiť.

Podobne ako v systéme Unix, aj v iných systémoch práva prístupu k objektom obvykle prideľujú ich vlastníci alebo administrátor systému. Je žiadúce snažiť sa o systém čo nejmenších oprávnení. Subjekt by mal mať čo nejmenšie možné oprávnenia nutné ku korektnému plneniu jeho úlohy, aby sa znížila možnost prieniku v prípade zlyhania časti ochranného mechanismu. Taktiež dočasne pridelené práva by mali byť prideľované iba na dobu, na ktorú sú skutočne potrebné. Špeciálnu pozornosť treba venovať odobratiu prístupových práv pri rozväzovaní pracovného pomeru. Príslušná osoba by mohla svoje oprávnenia zneužiť v dobe, keď už ich použitie nebude nikým očákavané.

4.4 Šifrovanie

Pri použití bežných komunikačných kanálov je z hľadiska bezpečnosti potrebné vždy predpokladať, že protivník môže získať kópiu akýchkoľvek údajov v nich prenášaných. Šifrovanie môžme voľne chápať ako istú transformáciu originálnych údajov (tzv. otvoreného textu) do iného tvaru (zašifrovaného textu alebo tiež kryptogramu), z ktorého je v ideálnom prípade schopný odvodiť originálne údaje výlučne iba ten subjekt, ktorému sú určené.

Obrázek 4.1: Obrázok znázorňuje základnú schému pre šifrovaný prenos údajov



Subjekt A chce poslať subjektu B správu M (obrázok 4.1). Používa pre to komunikačný kanál PUB, ktorý však môže byť monitorovaný potenciálnym útočníkom O. Preto A použije šifrovací algoritmus E na prevedenie originálnej správy M na zašifrovaný text C. C prenesie kanálom PUB a na druhej strane subjekt B použije dešifrovací algoritmus D, aby previedol C na M. Do algoritmov E a D vstupujú parametre K_e a K_d, ktoré sa nazývajú šifrovacím a dešifrovacím kľúčom. Bezpečnosť celého systému nesmie byť ani približne založená na neznalosti algoritmov E a D. Musí sa počítať s tým, že jediné, čo útočník nepozná, sú kľúče K_e a K_d, ktoré sú vygenerované z náhodného parametra X generátorom kľúčov G a nenapadnuteľnými kanálmi PRIV sú ditribuované ku A a B. Musí platiť E(M, Ke) = C (šifrovanie) a súčasne D(C, Kd) = M (dešifrovanie).

Okrem zabezpečenia ochrany komunikačných kanálov nachádza šifrovanie využitie aj v rôznych iných oblastiach ako napríklad digitálne podpisy, autentifikácia používateľa či špeciálne protokoly pre zabezpečenie elektronických platobných systémov.

4.4.1 Niektoré klasické šifrovacie algoritmy

Potreba utajenia obsahu správy vznikla už za čias staroveku. Okrem rôznych metód ukrývania správ sa už vtedy objavili aj metódy pre ich relatívne jednoduché šifrovanie. Na niektorých takýchto metódach známych z histórie sa dodnes demonštrujú rôzne prístupy ku šifrovaniu.

- Cézarova šifra - všetky znaky správy sú z množiny (abecedy) T, ktorej prvky sú usporiadané, pričom následníkom posledného znaku je prvý znak. Je dané nezáporné číslo k známe iba odosielateľovi a príjemcovi. Šifrovanie prebieha tak, že každý znak je nahradený jeho k-tym následníkom v T. Pri dešifrovaní je každý znak nahradený jeho k-tym prechodcom. Šifru je veľmi jednoduché zlomiť hádaním čísla k, nakoľko každé číslo $k \geq |T|$ je ekvivalentné s nejakým

$k' < |T|$, teda sa stačí obmedziť na množinu všetkých $k < |T|$. Jedná sa o príklad tzv. monoalfabetickej šifry.

- Vigenerova tabuľka - ide o pokročilejšie použitie myšlienky Cézarovej šifry. Je príkladom polyalfabetickej substitúcie. Kľúčom je slovo K dĺžky k. Pri šifrovaní nahrádzame každý znak p_i otvoreného textu príslušným znakom z tabuľky, pričom stĺpec určuje p_i a riadok určuje znak $K_{(i \ mod \ k)}$.

  Tabuľka typicky vyzerá nasledovne:

	A	B	C	...	Z
A	A	B	C	...	Z
B	B	C	D	...	A
C	C	D	E	...	B
...					
Z	Z	A	B	...	X

- One-time pad - na zašifrovanie sa použije kľúč rovnako dlhý ako samotná správa. Šifrovanie môže prebiehať napríklad pomocou Vigenerovej tabuľky. Výhodou tejto metódy je, že zo znalosti šifrovaného textu je nemožné kryptoanalytickými metódami uhádnuť použitý kľúč, pretože bol použitý iba raz. Nevýhodou je značná dĺžka kľúča. Je možné použiť napríklad dlhé sekvencie pseudonáhodných čísel vygenerovaných vhodným generátorom.

4.4.2 Symetrické šifry

Symetrickými šifrovacími algoritmami nazývame také, v ktorých je možné z kľúča K_e pomerne jednoducho (v polynomiálnom čase) odvodiť kľúč K_d a naopak. Ich bezpečnosť je teda závislá na utajení obidvoch týchto kľúčov a zabezpečení ochrany kanálov, po ktorých sú doručené odosielateľovi a príjemcovi. Ich výhodou je predovšetkým veľká rýchlosť a pomerná nenáročnosť, s ktorou sú tieto algoritmy prevádzané.

V praxi býva otvorený text reprezentovaný ako postupnosť jednotlivých bitov. Podľa metódy spracovania tejto postupnosti rozlišujeme:

- blokové šifry - spracúvajú vstup po blokoch určitej dĺžky. Medzi najznámejšie patria DES, Blowfish, IDEA, RC5, Rijndael(AES).

- prúdové šifry - spracúvajú vstup po jednotlivých bitoch. Patria sem napríklad algoritmy RC4 a Fish.

4.4.3 Asymetrické šifry

Asymetrické šifrovacie algoritmy využívajú matematické postupy zaisťujúce, že aj so znalosťou K_e (resp. K_d) predstavuje odvodenie K_d (resp. K_e) veľmi náročnú operáciu (spravidla s exponenciálnou časovou zložitosťou). To umožňuje jeden z týchto kľúčov zverejniť (verejný kľúč) bez obavy z vyzradenia druhého (privátneho) kľúča.

Takto môže napríklad príjemca správy zaslať odosielateľovi verejný kľúč, ktorým má správu zašifrovať. Keďže príjemnca správy je jediným vlastníkom privátneho kľúča, je tiež jediným subjektom schopným správu dešifrovať. Metóda však nie je odolná voči pokusu o podstrčenie falošnej správy.

Iným spôsobom použitia je napríklad pri autentifikácii. Subjekt je jediným vlastníkom privátneho šifrovacieho kľúča. Ktokoľvek si môže overiť autenticitu subjektu nasledujúcim spôsobom:

- vygeneruje náhodnú správu, ktorú si zapamätá. Zašifruje ju príslušným verejným kľúčom a zašle subjektu.
- subjekt správu dešifruje svojim privátnym kľúčom a zašle overovateľovi.
- overovateľ porovná vysledok s originálnou správou.

Medzi najznámejšie asymetrické šifrovacie systémy patria Merkle-Hellman, El Gamal, Rivest-Shamir-Adelman (RSA).

Problémom týchto algoritmov je, že sú spravidla časovo veľmi náročné a preto nie veľmi vhodné pre šifrovanie väčších správ. Často sa využíva postup, pri ktorom je asymetrický algoritmus použitý iba pre výmenu šifrovacích kľúčov a samotné správy sú už šifrované niektorým symetrickým algoritmom.

Kapitola 5

Pred čím sa chrániť

V súvislosti s informačnou bezpečnosťou je veľmi často spájaná ochrana pred úmyselnými útokmi. Teda ochrana pred hackermi, špionážou, zlodejmi a podobne. Informačný systém však oveľa častejšie ohrozujú rôzne chyby, či už hardwaru, softwaru, či samotných užívateľov informačného systému. Tie môžu mať za následok výpadok systému či dokonca stratu dôležitých údajov.

Tabulka 5.1: Tabuľka od spoločnosti Alinean z roku 2004 zobrazuje odhadované straty pre spoločnosť v prípade minútového výpadku pre rôzne typy služieb

Odvetvie	Odhadované straty
dodávateľské služby	11 tisíc dolárov
elektronický obchod	10 tisíc dolárov
zákaznícke služby	3700 dolárov
elektronické platobné systémy	3500 dolárov
správa financií	1500 dolárov
správa ľudských zdrojov	1000 dolárov
komunikácia	1000 dolárov
infraštruktúra	700 dolárov

5.1 Zlyhanie hardware

Medzi príčiny zlyhania hardware patrí výpadok napájania, prehriatie, prašnosť, atď. Príčinou môže byť aj opotrebovanie hardware, ku ktorému časom dochádza aj u tých najkvalitnejších zariadení. Okrem rôznych záložných zdrojov napájania, chladiacich zariadení, ventilačných zariadení , atď., patrí ku kľúčovým metódam ochrany zálohovanie. To sa netýka iba softwaru a dôležitých údajov, ale aj hardwarových komponentov. Poškodené zariadenie je potrebné nahradiť iným, ktoré bude schopné v dostatočnej miere činnosť pôvodného zariadenia vykonávať. V prípade, že dôjde ku zlyhaniu, mali by existovať procedúry umožňujúce rýchlu obnovu systému (výmena zariadenia, nainštalovanie software, konfigurácia, vloženie údajov, ...).

5.2 Zlyhanie software

V prípade software môže dôjsť ku zlyhaniu zvlášť pokiaľ jeho vývojári nepočítali s určitými špecifickými situáciami, vstupmi, nastaveniami, atď. Užívatelia programu sa nie nevyhnutne chovajú v súlade s očakávaniami a často aj neúmyselne môžu spôsobiť úplne nečakané chovanie programu (v optimálnom prípade jeho zrútenie bez vedľajších účinkov). Zvláštne riziko predstavujú veľmi rozsiahle programy. V dôsledku rozsiahlosti ich zdrojového kódu je často veľmi náročné sa v nich zorientovať a odhaliť prípadné chyby, či nedostatky. Naviac sa na ich tvorbe často účastní viacero programátorov, čo môže viesť v prípade nedostatočného porozumenia ku ďalším chybám. Je preto vhodné, aby programátory ovládali a používali overené postupy písania kódu a dokumentácie. Aplikovanie týchto postupov je zvlášť užitočné v prípade, že je program neskôr rozšírovaný o ďalšie funkcie a komponenty.

Občas sa stáva, že programátory do kódu vnášajú kusy kódu, ktoré s jeho funkcionalitou priamo nesúvisia. Tieto dodatočné funkcie často napomáhajú programátorom pri vývoji daného software. Ak sa však v konečnom produkte zabudne na ich odstránenie, môžu predstavovať veľké riziko. Predovšetkým ak sa o nich niekto dozvie a nájde spôsob ako ich zneužiť. Programátory môžu do svojich programov zavádzať aj tzv. trójske kone. Väčšinou sa to týka tzv. freeware programov voľne dostupných na Internete. Autora je v takýchto prípadoch totiž často veľmi náročné vypátrať. Takéto programy väčšinou naozaj výkónavajú uverejnenú funkciu. Môže sa jednať o rôzne editory, hry, apod. Majú však naviac aj skryté funkcie, ktoré užívateľ vôbec nemusí postrehnúť, čo je zvlášť nebezpečné, pokiaľ sú spustené s administrátorskými právami. Výsledkom môže byť napríklad vytvorenie na počítači tzv. backdoor, ktorý môže použiť útočník pre neoprávnené prihlásenie sa ku vzdialenému počítaču. Ďalej môže byť počítač takýmto spôsobom infikovaný vírusom.

5.3 Vírusy a červy

Vírusom sa označuje program, ktorý se dokáže sám šíriť bez vedomia užívateľa. Vkládá sa do iných spustiteľných súborov či dokumentov. Môže sa prejavovať napríklad vytvorením už spomenutého backdoor, ale jeho účinky môžu byť aj oveľa deštruktívnejšieho charakteru. Často sa pojem vírus zovšeobecňuje aj na trójske kone a tzv. červy. Červami sú označované programy schopné sa replikovať v rámci siete. Na rozdiel od vírusov sa však nepotrebujú pripájať ku existujúcim programom.

Aj keď poniektoré vírusy sú vytvárané len zo zábavy alebo čiste s úmyslom škodiť, mnohé vznikajú za účelom obohatenia sa. Príkladom je vírus infikujúci platformu Windows, ktorý po úspešnom infiltrovaní počítača skompromituje niektoré prvky systému a začne so sériou hlásení a falošných antivírových testov, v ktorých užívateľa informuje o tom, že jeho počítač bol úplne ovládnutý vírusmi a hneď aj ponúka možnosť zakúpenia tzv. Windows Vista Antivirus 2008, ktorý má tieto vírusy odstrániť. Zablokuje pritom použitie browserov aj prístup do Task Manager. Na jeho zbavenie sa našťastie postačuje obnova z automatických záloh systému.

Tabulka 5.2: Odhadované škody spôsobené vybranými počítačovými vírusmi a červami, ktoré pred časom uverejnili noviny USA Today

Rok	Vírus alebo červ	Odhadované škody v dolároch
1999	vírus Melissa	80 miliónov
2000	vírus Love Bug	10 miliard
2001	červi Code Red I a II	2,6 miliardy
2001	vírus Nimda	590 miliónov až 2 miliardy
2002	červ Klez	9 miliard
2003	červ Slammer	1 miliarda

5.4 Ľudský faktor

Z uvedeného je však vidieť, že účinok mnohých vírusov závisí od toho, ako k nim užívatelia pristupujú. Keby napríklad niekto uveril, že jedinou cestou ako sa zbaviť vírusov na jeho počítači je zakúpenie uvedeného fiktívneho antivírového programu, dôsledky by mohli byť ešte oveľa horšie. Ľudský faktor je často považovaný za najslabší článok bezpečnosti informačného systému. Útoky na tento článok sa nazývajú sociálnym inžinierstvom. Jedným so svetoznámych expertov na sociálne inžinierstvo je jeden z najhľadanejších hackerov 20.storočia Kevin Mitnick. Vo svojej knihe Umenie klamu uvádza, že na získanie hesiel nikdy nepotreboval použiť žiadne hackovacie či crackovacie nástroje. Kevin Mitnick bol povestný svojou schopnosťou manipulovať ľuďmi. V dnešnej dobe mnohé útoky na bezpečnosť zahŕňajú práve takéto manipulatívne techniky. Medzi tieto útoky patrí aj tzv. spamovanie, teda hromadné rozposielanie elektronickej pošty s klamlivým obsahom. Zneužívaná je dôverčivosť či neopatrnosť niektorých ľudí. Takéto e-maily môžu napríklad obsahovať odkaz na webovú stránku, ktorá si vyžaduje registráciu. Pri registrácii je potrebné uviesť heslo s dostatočnou dĺžkou obsahujúce veľké aj malé písmená a číslice. Pri takýchto kritériách je určitá pravdepodobnosť, že užívateľ uvedie heslo, ktoré používa napríklad v práci, pre prihlásenie ku svojmu počítaču alebo pre príhlasenie ku svojmu mailovému účtu. Určitú mieru ochrany zabezpečujú antispamové programy. Ich úroveň je daná ich schopnosťou rozlíšiť spamové e-maily od inej hromadnej pošty.

Útoky môžu byť realizované aj oveľa priamejším spôsobom. Útočník môže napríklad zatelefonovať administrátorovi systému a vydávať sa za nového zamestnanca, ktorý nedopatrením zabudol svoje heslo. V takomto prípade všetko závisí od opatrnosti, resp. ochoty administrátora, ako aj od presvedčivosti útočníka. Jedná sa o značne cielenejšiu formu útoku.

5.5 Úmyselné útoky

Zvláštny druh ohrozenia vniká v prípade, že sa niekto cielene pokúša o prelomenie bezpečnostných bariér objektu. Útočníkom zďaleka nemusí byť iba jedna osoba. Cieľom útoku môže byť napríklad získanie tajných informácií, špionáž, krádež, narušenie prevádzky,... Metódy útoku sú založené na cieli útočníka, jeho schopnostiach,

vybavení a jeho znalosti zabezpečenia objektu. Patrí sem:

- pokus o fyzické vniknutie do objektu. Obvykle čelí strážam, fyzickým bariéram a rôznym metódam autentifikácie.

- vniknutie do vnútornej počítačovej siete či jej narušenie z vonkajšej siete s využitím chýb a nedostatkov nedostatočne zabezpečeného alebo nevhodne nakonfigurovaného programového či systémového vybavenia. Jednou zo základných metód ochrany je použitie firewall, ktorý filtruje komunikáciu s vonkajšou sieťou.

  V prípade, že je možné s vnútornou sieťou komunikovať pomocou rozhrania (napríklad webového formulára), je treba dôsledne dbať na kontrolu vstupov. Existuje množstvo útokov zameraných práve na nedostatočne kontrolované vstupy.

  Príkladom je útok SQL injection. Užívateľ vyplní formulár. Položky formulára sú následne vložené do SQL dotazu, ktorý je zaslaný databáze. Databáza na základe tohoto dotazu vykoná príslušné operácie, prípadne vráti potrebné informácie. Uvažujme ďalej, že SQL dotaz je tvaru ABC, kde B je výskyt nejakej položky formulára, A je časť príkazu pred touto položkou a C je časť príkazu za touto položkou. Útočník do položky vstupného formulára B zapíše časť SQL príkazu na konci ukončenú dvomi pomlčkami. Za určitých okolností tak vznikne zmysluplný príkaz AB (C bude vďaka dvom pomlčkám na konci B chápané ako komentár) na vykonanie operácie, na ktorú za normálnych okolností užívateľ (útočník) nemá oprávnenie.

  Ďalším príkladom je buffer overflow, pri ktorom útočník zadá vstup väčší než je objem bufferu určeného pre uloženie tohoto vstupu. Pretečenie buffera spôsobí prepísanie oblasti pamäte, ku ktorej by za iných okolností útočník nemal prístup.

- crackovanie hesiel, teda ich systematické skúšanie. Skúšanie úplne všetkých možností je vo väčšine prípadov neefektívne a funguje iba v prípade veľmi krátkych hesiel alebo hesiel, ktorých znaky sú volené z veľmi obmedzenej abecedy.

  Keďže je však pre užívateľov jednoduchšie zapamätať si zmysluplné frázy než náhodné postupnosti znakov, je často výhodné použitie tzv. slovníkového útoku, pri ktorom sa skúšajú rôzne kombinácie slov z daného jazyka. Naviac niektorí užívatelia za účelom zapamätania si hesla používajú slová týkajúce sa nejakým spôsobom ich samých. Znalosť osoby užívateľa teda môže taktiež napomôcť pri crackovaní hesiel.

  Vo väčšine prípadov však tento postup nemožno aplikovať priamo v systéme, pretože vyvoláva značnú odchylku od bežného stavu. Naviac väčšina systémov poskytuje iba obmedzený počet pokusov o prihlásenie, po ktorom je daný účet zablokovaný. V samotnom systéme sa heslá neukladajú v čistej podobe, ale sú prevádzané pomocou tzv. hash funkcie. Tá má tú vlastnosť, že je veľmi jednoduché vytvoriť z hesla jeho hash (pričom tento proces je jednoznačný),

avšak opačný proces je veľmi náročný. Po vložení hesla sa teda heslo prevedie na príslušný hash a ten je porovnaný so vzorom uloženým v systéme. Pokiaľ sa podarí útočníkovy získať "zahashované" podoby hesiel a pozná príslušnú hashovaciu funkciu, môže sa tieto heslá pokúsiť odhaliť pomocou metódy crackovania.

- odpočúvanie - vo väčšine prípadov ide o zachytávanie prúdiacich dát z komunikačných liniek, ktoré majú často oveľa nižšiu úroveň zabezpečenia než koncové uzly. To platí najmä pokiaľ územie, po ktorom komunikácia prebieha, spadá do verejného sektora. Útočník sa môže napojiť na dátový kábel, zachytávať rádiovú komunikáciu, apod. Medzi základé spôsoby obrany patrí šifrovanie komunikácie.

  Medzi ďalšie techniky odpočúvania patrí zrekonštrovanie dátového toku zariadením (napr. crt monitorom) na základe jeho elektromagnetického vyžarovania.

  Známe sú tiež rôzne zariadenia pre odpočúvanie hlasu (napríklad pri útoku na verifikáciu hlasu alebo získavania informácií z rozhovorov).

  Pomocou tzv. keylogeru je možné snímať každé stlačenie klávesy na klávesnici. Môže mať hardwarovú aj softwarovú podobu. Umožňuje napríklad odpočutie hesiel pri ich zadávaní. Vyžaduje si zavedenie keylogeru na príslušnú stanicu. O to sa môžu postarať napríklad niektoré vírusy, ktoré prípadne môžu následne zasielať výsledky von prostredníctvom Internetu.

- sledovanie - špehovanie osôb, získanie otlačkov prstov z pohára, ktorý osoba použila, odpozeranie hesla pri jeho zadávaní, apod. Útočník môže byť pri sledovanom objekte priamo prítomný alebo ho pozorovať pomocou ďalekohľadu, kamery a podobne.

- odvodenie tajných informácií z verejných informácií. Rôzne databázové systémy môžu napríklad poskytovať štatistické údaje ako súčet, medián a podobne, pričom sú zvyčajne nakonfigurované tak, aby odmietali dotazy, ktorých výsledky sú založené na malom počte položiek. Zatiaľčo konkrétne hodnoty niektorých položiek sú verejne dostupné, hodnoty iných položiek môžu byť tajné. Úvážme, že útočník na základe verejne dostupných položiek zistí, že osoba, o ktorú sa mu jedná je jedinou osobou s blond vlasmi ázijského pôvodu. Ďalej chce zistiť jej príjem, ktorý je tajný. Zašle teda databáze dotaz na súčet príjmov všetkých osôb a následne dotaz na súčet príjmov všetkých osôb, ktoré nemajú blond vlasy alebo nie sú ázijského pôvodu. Požadovaný výsledok vypočíta ako rozdiel takto získaných hodnôt.

- podvrhnutie falošných údajov. Týmto spôsobom je napríklad možné narušiť správnu prevádzku alebo zmanipulovať personál či niektoré zariadenia k určitému chovaniu, ktoré by bolo možné zneužiť (napríklad vyvolať falošný poplach). Patrí sem aj tzv. replay attack. Útočník odpočuje komunikáciu (napríklad pri zadávaní hesla, zadávaní platobného príkazu, atď.) a neskôr sa túto komunikáciu pokúsi zopakovať. Účinnú ochranu predstavujú časové známky alebo challenge-response systémy.

- sabotáž - obvykle poškodenie nejakého zariadenia za účelom jednoduchšieho prieniku alebo narušenia prevádzky.
- sociálne inžinierstvo.
- ...

Útok poväčšinou pozostáva z kombinácie niekoľkých takýchto metód.

Zvláštnu hrozbu predstavujú bývalí zamestnanci. Stráže a iní členovia personálu môžu danú osobu stále považovať za zamestnanca spoločnosti. Taktiež jej účet môže byť stále aktívny a použiteľný pre prístup do vnútornej siete. Naviac môže byť dotyčná osoba vzhľadom na vyhodenie z práce k útoku citovo motivovaná. Je teda potrebné dbať na dôsledné rozviazanie pracovného pomeru.

Pre úspešné zaistenie bezpečnosti informačného systému proti úmyselným útokom je vhodné uvažovať rôzne typy opatrení:

- odstrašujúce, zamerané na to, aby potenciálny protivník upustil od úmyslu útočiť na informačný systém. Základným prvkom sú predovšetkým ustanovania trestného zákona. Je však dobré si byť vedomý toho, že to čo útočníka odstraší väčšinou nie je samotná existencia legislatívnych noriem, ale existencia a účinnosť iných opatrení a prostriedkov, ktorých správna činnosť vo svojom dôsledku umožní tieto normy aplikovať.
- preventívne, zamerané na zabránenie vykonania útoku na informačný systém. Patrí sem izolácia objektu a použitie rôznych bariér a iných prostriedkov fyzickej ochrany pre zabránenie neoprávneného prístupu k objektu.
- detekčné a reakčné, zamerané na včasné odhalenie príznakov útoku na informačný systém a na rýchle vykonanie vhodných obranných akcií. Patria sem rôzne druhy alarmov, kamerové systémy a iné detekčné zariadenia. Taktiež sem patria rôzne druhy softwaru skúmajúce odchýlky od bežného stavu vo vnútornej sieti. Útoky často neprebiehajú naraz. Úspešné detekovanie útoku ešte predtým než sa prejavý v plnom rozsahu umožní vykonanie príslušných opatrení a uchránenie systému. Takto je možné útok úplne zablokovať alebo mu nechať zdanlivo voľný priebeh a pripraviť sa na zadržanie útočníka.
- korekčné, zamerané na rýchle a podľa možnosti úplné zotavenie sa informačného systému z následkov úspešného útoku. Sem patria predovšetkým už spomenuté zálohy a dopredu pripravené procedúry pre obnovu systému.

5.6 Ďalšie hrozby

Medzi ďalšie hrozby patria povodne, požiar, zemetrasenia, búrky, zmeny teploty, vandalizmus a mnoho ďalších. Bezpečnosť informačného systému má komplexný charakter a snaha o dokonalé zabezpečenie väčšinou ani nie je jej cieľom. Má zmysel uvažovať iba také dokonalé zabezpečenie informačného systému, aké sa z hľadiska veľkosti rizika potenciálnych hrozieb oplatí zaviesť.

Kapitola 6

Popis programu

Cieľom programu je umožniť jeho užívateľovi definovaním rôznych rizík, opatrení a tzv. udalostí vytvoriť prostredie, v ktorom je možné hravou formou získať predstavu o týchto rizikách a príslušných opatreniach. Jedná sa o diskrétnu simuláciu, pri ktorej je fiktívny informačný systém vystavovaný jednotlivým útokom. Jeden krok simulácie predstavuje zmenu stavu (vyvolanie nejakej udalosti) v dôsledku narušenia bezpečnosti. Užívateľ do simulácie vstupuje nákupom jednotlivých opatrení za kredit (financie), ktorý mu pribúdajú pravidelne počas simulácie. Okrem kreditu pribúda pravidelne aj skóre, ktoré je v dôsledku jednotlivých rizík znižované (v prípade, že nie sú v dostatočnej miere nakúpené príslušné opatrenia). To na konci simulácie predstavuje hodnotenie toho, ako si užívateľ počínal. V programe sú prítomné štyri základné typy objektov, ktorých definície sú ukryté v samostatných konfiguračných súboroch.

- Spoločnosť - jej najzákladnejším atribútom je jej veľkosť. Tá má vplyv na riziká (ďalej budem používať pojem hrozby), ktoré spoločnosť ohrozujú. Ďalšími atribútmi sú kredit na nákup opatrení do začiatku a prírastok ku kreditu za jeden deň. Užívateľ si na začiatku zvolí jednu z ponúkaných spoločností, ktorých definície sú načítané z konfiguračného súboru companyTypes.txt. Tá sa po zbytok simulácie nemení.

- Udalosti - pokiaľ sú vyvolané niektorou hrozbou, zostávajú po určitú vopred danú dobu (meranú v dňoch) aktívne v simulácii. Po túto dobu ovplyvňujú silu niektorých hrozieb. O týchto hrozbách hovorím, že sú na príslušných udalostiach závislé alebo že sú nimi ovplyvnené. Taktiež po túto dobu každý deň znižujú skóre o vopred stanovenú hodnotu. Aj keď je simulácia diskrétna, zaznamenáva sa počas nej počet dní medzi jednotlivými krokmi, aby bolo možné kontrolovať, ktoré udalosti už nie sú aktívne. Nikdy nie sú aktívne dve rovnaké udalosti.

- Opatrenia - chránia spoločnosť proti hrozbám. Ich kvalita je daná ich úrovňou (nezápornou číselnou hodnotou, kde 0 znamená nezakúpené opatrenie). Sú definované silou za úroveň, maximálnou možnou úrovňou a cenou za úroveň. Ich skutočná sila je daná ako súčin zakúpenej úrovne a sily za úroveň.

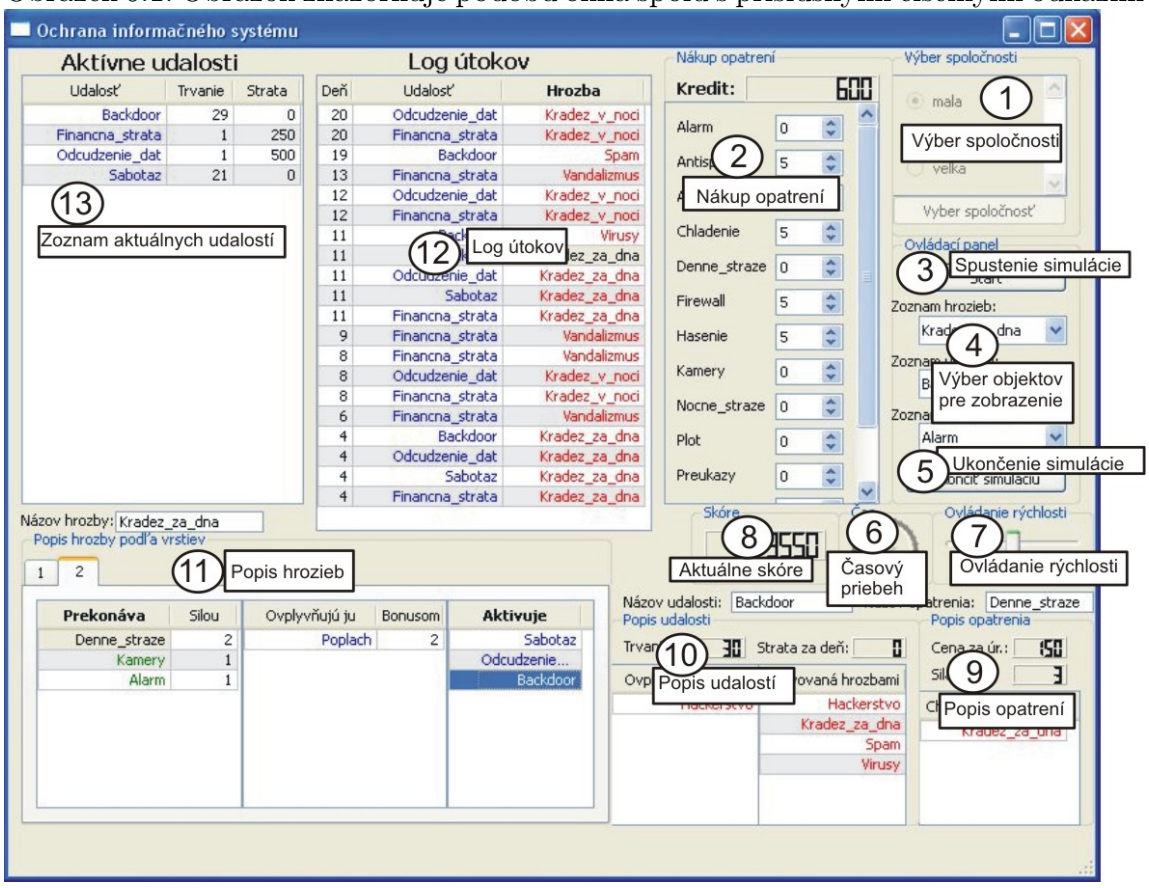
Majú rovnakú silu proti všetkým hrozbám, proti ktorým spoločnosť chránia. Rôzne hrozby však môžu mať rôznu silu proti opatreniam, ktoré prekonávajú.

- Hrozby - ich cieľom je útočiť na spoločnosť, čo sa v prípade ich úspechu prejavuje nastavením udalostí (a v konečnom dôsledku obvykle znížením skóre). Dôležitým atribútom je perióda (v dňoch), s ktorou približne útočia na spoločnosť. Ďalej sú definované po tzv. vrstvách, v ktorých prebieha ich útok. Na každej vrstve je záznam o tom
  - na ktorých udalostiach je daná hrozba na tejto vrstve závislá a v akom rozsahu.
  - ktoré udalosti hrozba vyvoláva v prípade úspešného prekonania vrstvy.
  - ktoré opatrenia musí hrozba prekonať, aby prekonala danú vrstvu a aká je jej sila proti jednotlivým opatreniam.

  Útok hrozby končí v prípade, že niektorú vrstvu neprekoná (neprekoná niektoré opatrenie na nej) alebo prekoná všetky vrstvy.

Ďalej nasleduje popis užívateľského okna:

Obrázek 6.1: Obrázok znázorňuje podobu okna spolu s príslušnými číselnými odkazmi



Okno programu obsahuje blok pre výber typu spoločnosti (1), blok pre nákup opatrení (2), tlačítko pre spustenie a zastavenie simulácie (3), tlačítko pre ukončenie simulácie (5), časový priebeh (6), ovládanie rýchlosti simulácie (7) a displej pre zobrazenie skóre (8) - viď obrázok 6.1.

Aby bolo možné sa strategicky rozhodovať, v spodnej časti okna programu sú umiestnené tri tabuľky pre zobrazovanie definicií jednotlivých opatrení (9), udalostí (10) a hrozieb (11). Každej tabuľke prísluší v pravej časti okna combobox (4), z ktorého je možno vybrať opatrenie, udalosť, resp. hrozbu, ktorej definícia sa má zobraziť. Program ďalej obsahuje tabuľku s históriou (logom) útokov (12) a tabuľku so zoznamom aktívnych udalostí (13). Väčšina políčok v tabuľkách je klikateľných a po kliknutí na ne sa zobrazí definícia príslušného objektu, ktorý je uvedený v tomto políčku.

6.1 Užívateľská príručka

Na začiatku si užívateľ volí typ spoločnosti, ktorý bude chrániť - viď blok (1) na obrázku 6.1. Všetky ostatné časti okna sú v tejto chvíli neaktívne. Od zvoleného typu spoločnosti budú závisieť financie na nákup opatrení a sila hrozieb. Tieto parametre však nie sú užívateľovi zverejnené. Pomenovanie typov spoločností by malo v dostatočnej miere vypovedať o ich charaktere.

Po vykonaní voľby sa blok (1) deaktivuje a aktivujú sa zvyšné časti okna. Užívateľ by v tejto chvíli mal upriamiť svoju pozornosť predovšetkým na blok pre nákup opatrení (2). Úroveň všetkých opatrení je 0, čo je minimálna úroveň. V tomto stave nie sú zakúpené žiadne opatrenia a v prípade útoku hrozby ju nebudú žiadnym spôsobom blokovať. Šípkami napravo od každého opatrenia je možné zvyšovať jeho úroveň, čo sa prejavý znížením kreditu v závislosti od ceny opatrenia. V prípade, že hodnota kreditu je nižšia ako 0, nie je možné spustiť simuláciu a ak sa o to užívateľ pokúsi, objaví sa mu chybová správa. V záujme zvýšenia kreditu je možné úroveň opatrení aj znižovať. Kredit je pritom navýšený o cenu opatrenia bez akýchkoľvek penalizácií.

Ku rozhodovaniu, ktoré opatrenia nakúpiť, môže dopomôcť combobox s výberom opatrení v bloku (3). V tomto bloku sú tiež comboboxy s výberom udalostí a hrozieb. Po výbere opatrenia sa jeho popis zobrazí v bloku (9). Tento popisuje cenu opatrenia, jeho silu a obsahuje tabuľku s hrozbami, proti ktorým toto opatrenie chráni.

Kliknutím na hrozbu v tabuľke sa zobrazí jej popis v bloku (11). Pre výber hrozby je tiež možné použiť combobox z bloku (3). Popis je rozdelený do záložiek, ktoré reprezentujú jednotlivé vrstvy útoku danej hrozby. Každá záložka obsahuje tabuľku so zoznamom opatrení, ktoré hrozba na danej vrstve prekonáva (spolu s jej silou proti týmto opatreniam), udalosti, na ktorých na tejto vrstve závisí (spolu s bonusom, ktorý jej pridávajú k sile) a udalosti, ktoré po prekonaní tejto vrstvy aktivuje. Kliknutím na opatrenie sa zobrazí jeho popis v bloku (9).

Kliknutím na udalosť sa zobrazí jej popis v bloku (10). Pre výber udalosti je tiež možné použiť combobox z bloku (3). Popis pozostáva z trvania udalosti, straty za deň (ktorá sa odčítava od skóre), zoznamu hrozieb, ktoré na nej závisia a zoznamu

hrozieb, ktoré ju aktivujú. Na hrozby je opäť možné klikať a ich popis sa objaví v bloku (11).

Po nákupe opatrení užívateľ spustí simuláciu tlačítkom Štart (3). Rovnakým tlačítkom je možné ju pozastaviť. Počas behu simulácie pribúda kredit v závislosti na zvolenom type spoločnosti. Kedykoľvek môže užívateľ beh pozastaviť a zvýšiť úroveň opatrení. Počas simulácie sa v každom kroku aktualizuje log (história) útokov. Ten zaznamenáva posledných 20 vyvolaných udalostí. Ku každej je uvedený deň kedy bola vyvolaná a hrozba, ktorá ju vyvolala. Môže sa stať, že hrozba naraz vyvolala niekoľko udalostí. V tom prípade sú tieto udalosti uvedené za sebou a majú pri sebe uvedený rovnaký deň a tú istú hrozbu. Na hrozby aj udalosti je možné klikať a ich popisy sa zobrazia v blokoch (11) a (10). Okrem logu útokov sa obnovuje aj tabuľka aktívnych udalostí. Tá obsahuje zoznam udalostí, ktoré sú práve aktívne a ku nim ich trvanie (koľko dní budú ešte aktívne) a stratu na skóre, ktorú spôsobia za jeden deň. Udalosti sú opäť klikateľné a ich popis sa zobrazí v bloku (10).

Počas simulácie užívateľ môže sledovať v bloku (8) svoje aktuálne skóre a v bloku (6) časový priebeh. V bloku (7) môže meniť rýchlosť simulácie - posunom doprava rýchlosť zvýšiť, posunom doľava zasa znížiť.

Simulácia končí prvým narušením bezpečnosti po uplynutí časového limitu 500 dní. Hodnota limitu je v programe nastavená ako konštanta. Po skončení simulácie sa užívateľovi zobrazí správa s výsledným skóre a ďalej už nie je možné v simulácii pokračovať. Zavrieť program je možné tlačítkom Ukončiť simuláciu (5).

6.2 Popis kofiguračných súborov

Objekty sú pri iniciácii programu načítané z konfiguračných súborov umiestnených v rovnakom adresáry ako samotný program.

Formát súborov:

Mriežka na začiatku riadku znamená komentár. Položky sú oddelené aspoň jedným bielym znakom. Každý objekt má svoje meno (v prípade typu spoločnosti je to veľkosť), ktoré predstavuje jeho identifikátor. Identifikátory sa nesmú opakovať. Na obrazovku sa vypisuje tzv. štítok objektu. Ten by mal byť dostatočne krátky (okolo 10 znakov) a zároveň by mal dostatočne vystihovať, o aký objekt ide. Ostatné položky už boli popísané vyššie. Žiadna položka nesmie obsahovať medzery ani iné biele znaky.

6.2.1 Udalosti

Udalosti sa načítavajú z konfiguračného súboru events.txt

Vzor súboru pre udalosti:

Meno Stitok Trvanie_v_dnoch Strata_za_jeden_den

Príklad:

vypnuty_system Vypnuty_system 1 250

6.2.2 Opatrenia

Opatrenia sa načítavajú z textového súboru protections.txt

Vzor súboru pre opatrenia:

Meno Stitok Sila_za_uroven Maximalna_uroven Cena_za_uroven

Príklad:

plot Plot 1 3 100

6.2.3 Typy spoločnosti

Jednotlivé typy spoločnosti sa načítavajú z textového súboru companyTypes.txt. Na každom riadku je definovaná jedna úroveň veľkosti spoločnosti.

Vzor súboru pre typy spoločnosti:

Velkost Stitok Kredit_do_zaciatku Zisk_za_den

Príklad:

1 mala 400 3

6.2.4 Hrozby

Hrozby sa načítavajú z textového súboru dangers.txt.

Vzor súboru pre hrozby:

Meno Stitok Perioda

Ďalej nasledujú riadky predstavujúce jednotlivé vrstvy útoku.

Riadok je rozdelený do troch častí znakmi |

V prvej časti sú uvedené identifikátory udalostí, na ktorých hrozba na danej vrstve zavisí spolu s príslušnými bonusmi k sile hrozby v tvare:

udalost_1 bonus_za_udalost_1 udalost_2 bonus_za_udalost_2 ... |

V druhej časti sú uvedené identifikátory udalostí, ktoré hrozba na danej vrstve aktivuje v tvare:

udalost_1 udalost_2 udalost_3 ... |

V tretej časti sú opatrenia, ktoré musí hrozba na danej vrstve prekonať spolu s jej silou proti týmto opatreniam v tvare:

opatrenie_1 sila_proti_opatreniu_1 opatrenie_2 sila_proti_opatreniu_2 ...

Definícia hrozby je ukončená samostatným riadkom obsahújucim na začiatku znak ';'

Priklad:

kradez_v_noci Kradez_v_noci 10

poplach 2 | financna_strata | plot 1 nocne_straze 1

| sabotaz odcudzenie_dat backdoor | nocne_straze 1 kamery 1 alarm 1

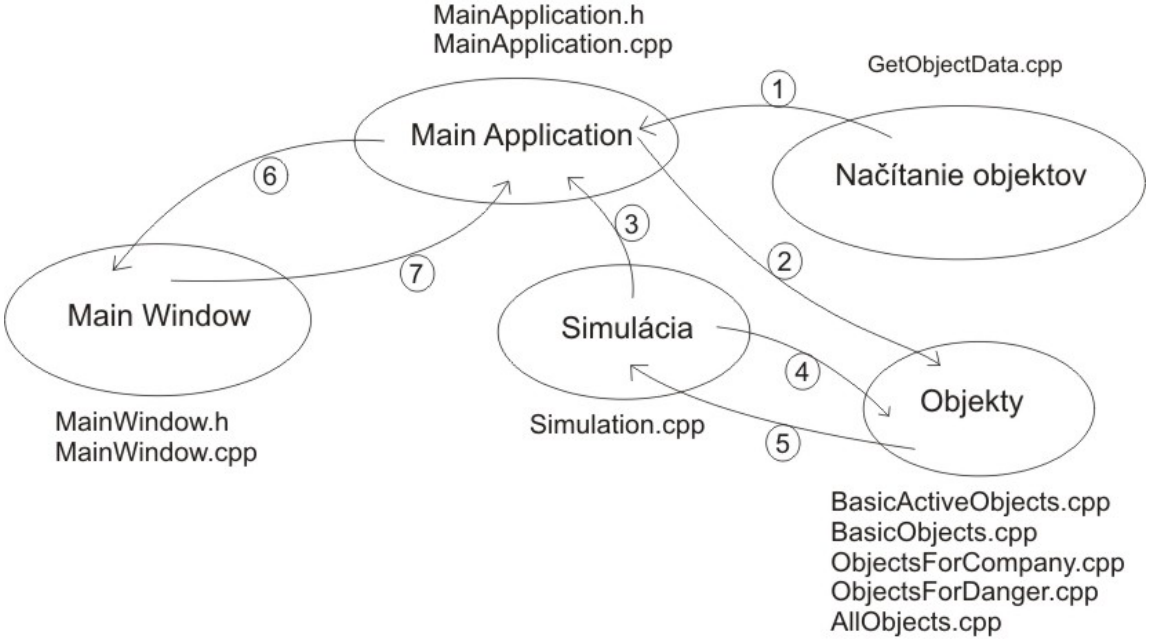
;

6.3 Programátorská dokumentácia

Program bol vyvýjaný vo vývojovom prostredí Microsoft Visual Studio 2005 pod platformou Microsoft Windows XP, na ktorej bol aj testovný. Použitý programovací jazyk je C++. Boli použité niektoré štandardné knižnice pre kontajnery (std::vector, std::map) a textové reťazce (std::string). Pre grafický výstup a interakciu s užívateľom bola využitá knižnica QT, ktorá je pre nekomerčné účely voľne použiteľná.

Nasleduje náčrt štruktúry programu:

Obrázek 6.2: Diagram zachycuje hrubú štruktúru programu



Trieda MainApplication je bázou celého programu. Je odvodená od triedy QApplication knižnice Qt. Jej inštancia je vytvorená a "spustená" funkciou main hneď na začiatku. Spracúva signály zo vstupov od užívateľa, uchováva kontajnery s objektami a riadi beh celého programu. Pre väčšiu prehľadnosť sú niektoré časti kódu presunuté do knižníc. Každá knižnica je tvorená jednou veľkou triedou, s ktorou MainApplication komunikuje prostredníctvom jej metód.

Komunikačný kanál (1) na obrázku 6.2 znázorňuje načítanie atribútov udalostí, hrozieb, opatrení a typov spoločností z konfiguračných súborov prostredníctvom metódy getAllData triedy GetObjectsData v súbore GetObjectsData.cpp. Vzápätí sú vytvorené objekty s príslušnými atribútmi - kanál (2). Aj keď sú tieto objekty prakticky uložené v MainApplication, v diagrame sú znázornené oddelene, pretože obsahujú množstvo vlastných metód a atribútov, ktoré sa MainApplication priamo netýkajú. Naviac s nimi MainApplication komunikuje taktiež iba prostredníctvom ich metód.

Samotná simulácia sa prevádza prostredníctvom volania metódy runSimulation triedy Simulation v súbore Simulation.cpp - kanál (3). MainApplication tejto metóde odovzdá referencie na všetky potrebné objekty (kontajnery s objektami). Trieda

Simulation ďalej volá metódy objektov a výsledky používa pre vyhodnocovanie simulácie - kanál (5). Taktiež môže beh simulácie spôsobiť zmenu atribútu niektorého objektu (čo sa deje predovšetkým v prípade udalostí). Zmena atribútov je realizovaná opäť prostredníctvom metód objektov - kanál (4).

Nakoniec trieda MainWindow sa stará o vykresľovanie samotného okna. Obsahuje väčšinu grafických objektov. Zachytáva signály zo vstupov užívateľa a odovzdáva ich MainApplication - kanál (7). Niektoré signály môžu mať za následok zmenu atribútov niektorých objektov. Tieto sú taktiež spracované triedou MainApplication a zmena je uskutočnená kanálom (2).

MainWindow nemá predstavu o udalostiach, hrozbách a opatreniach prítomných v programe. Avšak niektoré bloky okna (ako napríklad blok pre nákup opatrení) sú od objektov závislé. MainApplication sa stará o postupné vykresľovanie takýchto blokov volaním špecifických metód triedy MainWindow - kanál (6).

6.3.1 Popis objektov simulácie

Objekty simulácie sú rozdelené do dvoch kategórií:

- pasívne objekty, ktorých atribúty sú načítavané z konfiguračných súborov. Sem patria Event (udalosť),Protection (opatrenie),Danger (hrozba),CompanyType (typ spoločnosti). Tieto sa ukladajú do kontajnerov bagOfEvents, bagOfProtections, bagOfDangers a bagOfCompanyTypes. Tieto kontajnery sú typu map, aby v nich bolo možné rýchlo vyhľadávať.

- aktívne objekty, ktoré sú odvodené od svojich pasívnych ekvivalentov. Aktívne objekty vstupujú do simulácie, ich atribúty môžu byť ovplyvnené vstupmi od užívateľa, náhodou, či behom simulácie. Ovplyvňujú priebeh simulácie. Hrozby (danger) nemajú aktívnu verziu. Ich pasívna verzia slúži aj ako aktívna. Aktívne objekty sú taktiež ukladané do kontajnerov typu map.

Všetky objekty obsahujú konštruktor. Jeho parametrami sú v prípade pasívnych objektov hodnoty jednotlivých atribútov. V prípade aktívnych objektov je to referencia na príslušný pasívny objekt, z ktorého sú základné atribúty skopírované. Atribúty v zásade nie sú verejné, preto každý objekt obsahuje ku svojim atribútom metódy, ktoré vracajú kópiu týchto atribútov (v ojedinelých prípadoch referenciu na ne). Názov takejto metódy je zložený zo slovíčka "get" a mena príslušného atribútu.

6.3.2 Priebeh simulácie

Po stlačení tlačítka štart sa zavolá metóda MainApplication::startSimulationSlot().

- štruktúra MainApplication::startSimulationSlot():
  - ak je kredit nižší ako 0, užívateľovi sa zobrazí chybová hláška a simulácia ďalej nepokračuje.
  - blok s nákupom opatrení je deaktivovaný. Nápis na štartovacom tlačítku je zmenený na Stop.

  - je nanovo vytvorený zoznam aktívnych opatrení na základe navolených úrovní.
  - v pravidelnom časovom intervale je spúšťaná metóda MainApplication::runSimulation() až do pozastavenia alebo ukončenia simulácie.

- štruktúra MainApplication::runSimulation():
  - v prípade, že uplynul stanovený počet dní určujúci dĺžku simulácie, simulácia ďalej nepokračuje.
  - opakovane je spúšťaná metóda simulation::runSimulation() až kým nedôjde ku aktivovaniu novej udalosti. Pred každým spustením metódy je inkrementovaný počet uplynutých dní.

- štruktúra simulation::runSimulation():
  - zavolá sa activeCompany.addIncomeToCredit() - kredit je navýšený o denný prírastok.
  - zavolá sa activeCompany.addDailyScore() - skóre je navýšené o denný prírastok.
  - zavolá sa runActiveEventsForDay() - skóre je znížené za jednotlivé aktívne udalosti. Zostávajúce trvanie je aktívnym udalostiam znížené o 1. Tie, ktorým klesne táto hodnota na 0, sú odstránené z kontajnera aktívnych udalostí.
  - postupne pre jednotlivé hrozby je zavolaná metóda simulateAttackOfDanger().

- štruktúra simulateAttackOfDanger():
  - náhodne v závislosti od periódy hrozby je rozhodnuté, či táto hrozba daný deň zaútočí.
  - zavolá sa metóda útočiacej hrozby attackActivatedSomeEvents() - prevedie útok a vráti či bola počas neho aktivovaná nejaká udalosť.

- štruktúra attackActivatedSomeEvents():

  Pre každú vrstvu útoku hrozby sa vykonajú nasledujúce kroky:
  - spočíta sa bonus k sile hrozby z veľkosti spoločnosti a aktuálnych udalostí.
  - zavolá sa layerIsPenetrated() - prevedie sa simulácia útoku na danej vrstve a vráti sa, či bola vrstva prekonaná.
  - ak bola vrstva prekonaná, potom sú aktivované udalosti zo zoznamu udalostí, ktoré hrozba aktivuje na danej vrstve.

- štruktúra layerIsPenetrated():

  Pre každé protiopatrenie (objekt nesúci informáciu o sile danej hrozby proti nejakému opatreniu, ktoré prekonáva) na danej vrstve sú vykonané nasledujúce kroky:

  - ak nie je aktívne opatrenie, ku ktorému sa dané protiopatrenie vzťahuje, potom je toto opatrenie prekonané automaticky.
  - zistenie sily protiopatrenia a príslušného opatrenia.
  - zavolá sa contraProtectionBreaksProtection() - prevedie simuláciu útoku na jedno opatrenie a vráti či bolo prekonané.

  V prípade, že niektoré opatrenie nebolo prekonané, metóda okamžite končí s návratovou hodnotou false.

- štruktúra contraProtectionBreaksProtection():
  - je zvolené náhodné číslo od 0 do veľkosti sily protiopatrenia.
  - je zvolené náhodné číslo od 0 do veľkosti sily opatrenia.
  - návratová hodnota je true ak je prvé náhodné číslo väčšie ako druhé. V opačnom prípade je to false.

6.4 Ukážka

Nasledujúca ukážka má za úlohu demonštrovať použitie programu na konkrétnych objektoch a poukázať na jednotlivé funkcionality programu.

Uvedené dve tabuľky popisujú objekty použité v ukážke. Jednotlivé vrstvy útoku sú popísané na samostatných riadkoch. Jedná sa iba o príklad. Pre súlad s realitou by bolo potrebné vykonať dôkladnú analýzu založenú na rôznych štatistikách a popis by musel byť oveľa podrobnejší.

Tabulka 6.1: Vzťah hrozieb a opatrení

Hrozba	Opatrenia
Krádež za dňa	Preukazy, Denné stráže Kamery, Alarm, Denné stráže
Krádež v noci	Plot, Nočné stráže Kamery, Alarm, Nočné stráže
Výpadok prúdu	Záložný zdroj
Prehriatie	Chladiace zariadenie
Požiar	Hasiace zariadenie
Vandalizmus	Plot,Nočné stráže
Hackerstvo	Firewall Školenia, Firewall
Vírusy	Školenia, Antivírus
Spam	Školenia, Antispam

Tabulka 6.2: Vzťah hrozieb a udalostí

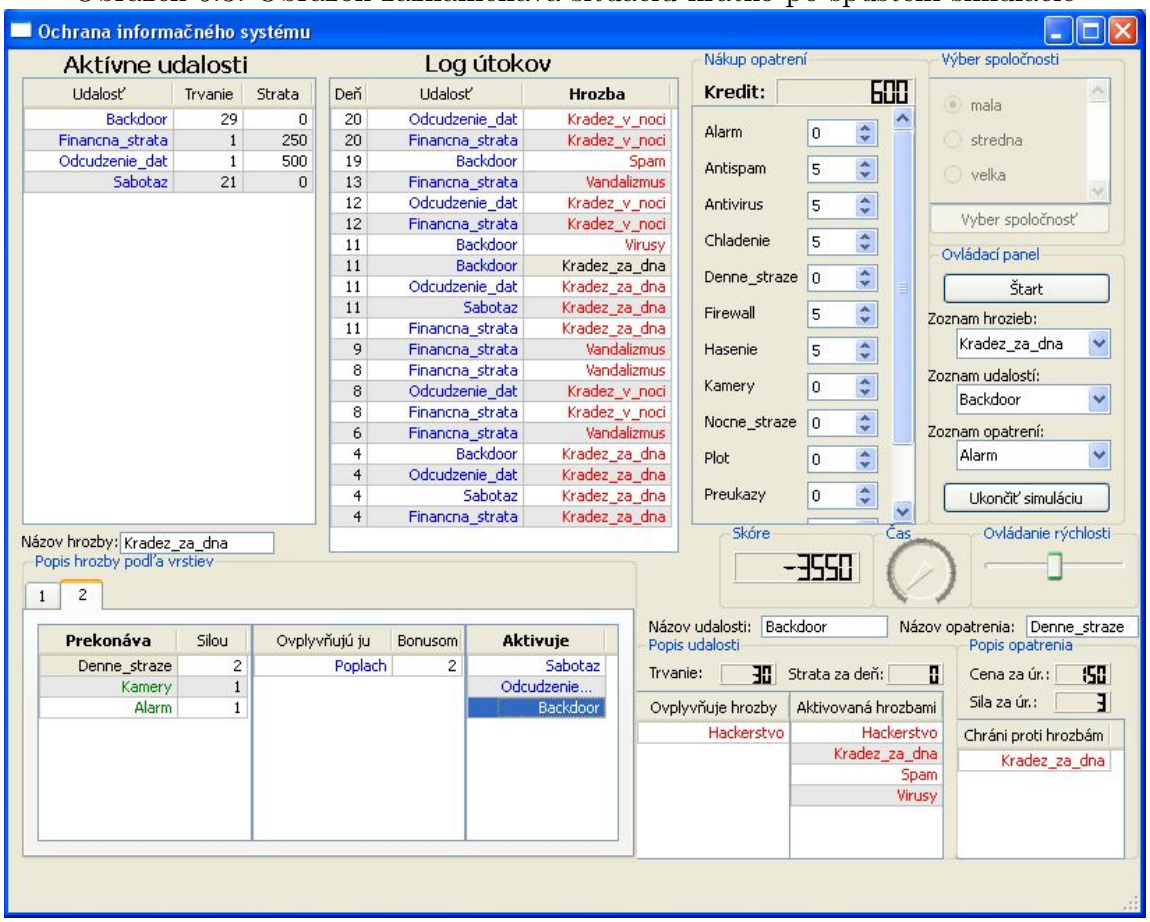
Hrozba	Závislosť na udalostiach	Aktivuje udalosti
Krádež za dňa	Poplach	Finančná strata Sabotáž, Odcudzenie dát, Backdoor
Krádež v noci		Finančná strata Odcudzenie dát
Výpadok prúdu	Sabotáž	Vypnutý systém
Prehriatie	Sabotáž	Vypnutý systém
Požiar	Sabotáž	Vypnutý systém, Poplach
Vandalizmus		Finančná strata
Hackerstvo	Vypnutý systém, Backdoor Vypnutý systém	Odcudzenie dát, Backdoor Vypnutý systém
Vírusy	Vypnutý systém	Backdoor
Spam		Backdoor

Prvým krokom simulácie je voľba typu spoločnosti. Od tejto voľby bude závisieť kredit na nákup opatrení a sila hrozieb. Zvolím typ spoločnosti "malá", čo znamená, že na začiatku mám k dispozícii pomerne nízky kredit v hodnote 3000, ktorý sa bude v priebehu simulácie len pomaly zvyšovať. Až však budem mať nakúpenú dostatočnú

úroveň opatrení, dá sa očakávať, že s vysokou pravdepodobnosťou zablokujú väčšinu útočiacich hrozieb.

V ďalšom kroku nakúpim niekoľko náhodne zvolených opatrení a spustím simuláciu tlačítkom Štart. V logu útokov a tabuľke aktívnych udalostí sa začínajú objavovať jednotlivé záznamy o vyvolaných udalostiach.

Obrázek 6.3: Obrázok zaznamenáva situáciu krátko po spustení simulácie



V logu útokov sa pomerne často vyskytuje hrozba Krádež za dňa - viď obrázok 6.3. V skutočnosti k jej útoku došlo iba dvakrát, avšak zakaždým vyvolala až 4 udalosti, z ktorých každá bola do logu zaznamenaná. Kliknutím na hrozbu Krádež za dňa v logu sa mi zobrazí jej popis. Kliknutím na záložku s číslom 2 si prezriem popis druhej vrstvy jej útoku. Všimnem si tiež, že udalosti, ktoré táto hrozba aktivuje sa skutočne nachádzajú v zozname aktivovaných udalostí. Kliknutím na udalosť backdoor sa zobrazí jej popis. Táto udalosť sama o sebe žiadne škody nespôsobuje, avšak ovplyvňuje (pravdepodobne posilňuje) hrozbu Hackerstvo. Kliknutím na hrozbu Hackerstvo sa mi zobrazí jej popis. Zisťujem, že pokiaľ je udalosť Backdoor aktívna, posiluje hrozbu Hackerstvo o 1 na prvej vrstve. Všimnem si tiež, že táto hrozba je značne negatívne ovplyvnená udalosťou Vypnutý systém (znižuje jej silu o 100). To zachytáva fakt, že ak je systém vypnutý, je veľmi nepravdepodobné, že by doň niekto takýto spôsobom prenikol. Kliknutím na udalosť Vypnutý systém však tiež zistím, že aktívnosť tejto

udalosti značne znižuje skóre.

Pri opätovnom nahliadnutí do logu útokov si všimnem, že najčastejší výskyt má v skutočnosti hrozba Vandalizmus, ktorá vyvoláva iba jednu udalosť - Finančná strata. Nemusím ani klikať na udalosť Finančná strata a v tabuľke aktívnych udalostí si prečítam, že aj dopad tejto udalosti na skóre je značný. Kliknem teda na hrozbu Vandalizmus a zisťujem, že proti nej pôsobia opatrenia Plot a Nočné stráže. Kliknutím na opatrenie Plot zisťujem, že stojí 100 kreditu za úroveň a má silu 2 za úroveň. V prípade Nočných stráží je cena 200 kreditu za úroveň a sila 3 za úroveň. Za ten istý kredit môžem teda dosiahnuť u opatrenia Plot väčšiu silu. Je treba tiež vziať do úvahy silu hrozby Vanadalizmus proti jednotlivým opatreniam. Tá je však v tomto prípade rovnaká. Za kredit 600 teda zvýšim úroveň opatrenia Plot z 0 na 6. Než však budem pokračovať v simulácii, všimnem si, že toto opatrenie chráni ešte pred jednou hrozbou - Krádež v noci. Tá sa v logu útokov taktiež nachádza pomerne často. Kliknutím na túto hrozbu sa mi zobrazí jej popis. V ňom si všimnem, že sa na prvej vrstve chová podobne ako hrozba Vandalizmus, avšak má aj druhú vrstvu útoku, na ktorej aktivuje udalosť Odcudzené dáta. Táto udalosť taktiež spôsobuje nemalé straty na skóre. Taktiež si všimnem, že zatiaľčo Plot čelí tejto hrozbe iba na prvej vrstve, opatrenie Nočné stráže jej čelí na oboch vrstvách. Znížim teda úroveň opatrenia Plot naspäť na nulu, nakúpim miesto neho opatrenie Nočné stráže a opäť stlačím tlačítko Štart.

Naďalej si všímam log útokov, pozastavujem simuláciu a nakupujem ďalšie opatrenia. Rozostupy medzi dňami kedy boli udalosti vyvolané sa pomaly zväčšujú, pretože vďaka novým opatreniam stále menej dochádza ku narušeniu bezpečnosti. Klesanie skóre pomaly prechádza na jeho rast vďaka každodenným prírastkom a stále sa zmenšujúcemu počtu bezpečnostných incidentov. Nakoniec mám nakúpené všetky opatrenia a čakám kým simulácia dobehne. Ovládaním rýchlosti v pravej časti okna jej priebeh urýchlim. Prvý bezpečnostný incident, ktorého deň je väčší ako 500, ukončí simuláciu. V mojom prípade je to vyvolanie udalosti Vypnutý systém hrozbou Prehriatie v deň 839. Výsledné skóre je -6080.

Kapitola 7

Záver

Práca načrtáva základné aspekty návrhu a prevádzkovania zabezpečenia informačného systému. Zďaleka nekončí iba návrhom opatrení určených na ochranu pred potenciálnymi hrozbami. Bezpečnostný odborník musí rozumieť vzájomnému vplyvu týchto opatrení a hrozieb, byť schopný analyzovať konkrétnu situáciu a vziať do úvahy aj niektoré menej predvídateľné aspekty, medzi ktoré patrí napríklad aj ľudský faktor.

Zďaleka sa nejedná o vyčerpávajúcu príručku. Oblasť informačnej bezpečnosti je veľmi obsiahla a zahŕňa veľa ďalších tém ako sú špecifiká bezpečnosti v sieťach, bezpečnostné modely, bezpečnostný audit, testovanie, etický hacking, právny systém a mnoho ďalších.

Práca v úvodnej časti obsahuje popis cieľov informačnej bezpečnosti. Ďalej sa zaoberá procesom návrhu zabezpečenia informačného systému, konkrétne analýzou rizík, návrhom opatrení a bezpečnostných postupov, ako aj najznámejšími bezpečnostnými normami. V ďalšej časti pojednáva o niektorých elementárnych metódach ochrany, ktoré sa v rôznych podobách vyskytujú vo väčšine návrhov zabezpečenia ochrany informácií. Patria sem rôzne metódy fyzickej obrany, autentifikácia, autorizácia a šifrovanie. Práca tiež popisuje najčastejšie formy rizík, ktoré informačné systémy ohrozujú, ako napríklad zlyhania hardwaru, či softwaru, chyby personálu a užívateľov, prírodné katastrofy, ale aj úmyselné útoky.

K práci je priložený program umožňujúci užívateľovi prostredníctvom simulácie výskúšať si návrh zabezpečenia vybranej spoločnosti. Medzi ďalšie vylepšenia programu by mohlo patriť vytvorenie grafického editoru objektov vstupujúcich do simulácie, ako aj lepšie ošetrenie reakcií programu na syntaktické chyby v konfiguračných súboroch.

Literatura

[1] Mgr. Antonín Beneš, Dr.: *Ochrana informací I, II - prednáška a učebné materiály, 2006/2007*

[2] Jozef Vyskoč: *Bezpečnosť informačných systémov, 1999*

[3] Shon Harris, Allen Harper, Chris Eagle, Jonathan Ness, Michael Lester: *Manuál Hackera, 2005*

[4] Kevin Mitnick, William Simon: *Umění klamu, 2002*

[5] Trusted Computer System Evaluation Criteria, DOD 5200.28

[6] British Security Standard BS7799-1, BS7799-2

[7] OECD Guidelines for security of information

[8] Specialista.info: http://www.specialista.info/view.php?cisloclanku=2005100401

[9] Security-portal.cz: http://www.security-portal.cz/