BEZPEČNOST DAT V ORGANIZACI A IS

Dagmar Brechlerová

KIT PEF ČZU, Kamýcká, 165 21, Praha 6, ČR, brechlerova@pef.czu.cz

Abstrakt

Computer security consists of maintaining three chracteristics: confidentality, integrity, availability. There are threats to hardware, software and data. The threats to data are the most dangerous because data are the most important for us. There are several reasons why to be care about data. Secure policies are discussed here.

l. Základní pojmy bezpečnosti

Pojem bezpečnost IT bývá různě chápán. Obvykle se pod tímto termínem rozumí bezpečnost jak IS, tak informací v něm uchovávaných, přenášených, zpracovávaných. Patří sem tedy dále i komunikační bezpečnost, fyzická bezpečnost, personální, ochrana před přírodními hrozbami apod. Často bývá tato bezpečnost zužována pouze na ty části IS, který je provozován s pomocí výpočetní techniky. To je ovšem velmi nebezpečné, neboť na co nám je skvěle zabezpečený výpočetní systém, když u faxu se volně povalují došlé zprávy.

Abychom si uvědomili, o jak komplexní problém se vlastně jedná, musíme si definovat, co se dnes pod pojmem bezpečnost IT vlastně rozumí. Za bezpečný IS se považuje *IS zajištěný fyzicky, administrativně , logicky a technicky.*

Za zajištění bezpečnosti se považuje zajištění těchto složek bezpečnosti:
celistvost tj. integrita a autenticita + dostupnost + důvěrnost.

Důvěrnost znamená přístup k aktivům pouze pro autorizovanou stranu - subjekt, zde jde o určení toho, kdo smí provádět operace typu read, print, view, nebo pouze vědět o existenci objektu. Někdy se také nazývá tajemnost (secrecy, privacy). Problém je s určením, kdo je důvěryhodný, a co to je porušení důvěrnosti, zda vidět např. bit, byte, kus textu atd.

Integrita a autenticita - modifikace aktiv (HW, SW, data) pouze autorizovanou stranou. Jen ta smí např. psát, měnit, měnit status, mazat, vytvářet. Autenticita - lze zjistit původce informací. *Přístupnost, dostupnost* - autorizovaná strana musí mít přístup k aktivům, nedojde k odmítnutí služby, tj. nemohu např. zajistit důvěrnost tak, že k datům není přístup, že je nikdo nesmí číst.

Tyto tři výše uvedené cíle se mohou překrývat ale i vylučovat, je tedy nutno vždy určit nějaký přijatelný kompromis. Pro různé organizace je tento kompromis různý, záleží na tom, co preferují, např. rychlost poskytování informací atd. Jiné preference bude mít prodejce letenek a jiné některá ze složek armády či Národní bezpečnostní úřad.

l.l Typy útoků

Každý systém má nějakou slabinu, nějaké zranitelné místo. *Útok je využití tohoto zranitelného místa.* Mezi základní bezpečnostní incidenty (útoky) obvykle počítáme následující útoky: *Přerušeni, odposlech, změnu a přidání nové hodnoty.*

Co se pod těmito pojmy obvykle rozumí:
Přerušení, zničení: zde se jedná o určité ukončení dostupnosti něčeho trvalé či dočasné, jedná se o *aktivní útok* na dostupnost HW, SW či dat, tj. např. vymazání dat, vymazání SW, poškození dat, ztráta HW, porucha HW či porucha operačního systému apod. - ztráta dat, dojde ke špatnému ukládání na disk, přestane být něco dostupné, toto je poškození aktiv. U tohoto útoku obvykle brzy zjistíme, že k útoku došlo.

Odposlech: Při odposlechu se jedná o útok pasivní a na rozdíl od předcházejícího typu se o něm nikdy nemusíme dozvědět, např. tiché kopírování dat a programů. Zde j sou typické příklady: odposlech na Internetu či jiné síti, kopírování dat či SW, *odposlech - zachycení,* neautorizovaná strana získá přístup, může to být osoba, program, počítačový systém, *toto je útok na důvěrnost*, získání dat ze sítě, velmi často se na to nepřijde.
Útoky tohoto typu j sou velmi zákeřné právě tím, že nemusí být dlouhou dobu případně nikdy, pozorovány.
Změna, modifikace: opět jde o útok aktivní obvykle na integritu tj. celistvost dat či SW, např. přidání funkce do programu, změna dat, útočník nejen pronikne ale i mění, např. mění data zaslaná Internetem, mění data v databázi, některé věci se dají změnit velmi *rychle.*
Přidání hodnoty, vyrobení nové hodnoty - podvržení, *útok na integritu, autenticitu*, vyrobení podvržené transakce na Internetu, vyrobení nových záznamů do databáze. Proto například při e- komerci nebo e -bankovnictví musíme používat velmi zabezpečený systém jak objednávání zboží tak placení, neboť jinak hrozí mnoho útoků na objednávky, na platby atd.
Je nutno si uvědomit, že na HW, SW a data jsou útoky různého druhu a také mohou způsobit různou škodu a různě se jim bráníme.

Útok na HW:
přerušení - přírodní havárie, poškození, destrukce, krádež
odposlech - krádež času procesoru, místa v paměti
přidání hodnoty - změna režimu činnosti
Útokům na HW obvykle jde zabránit různými bezpečnostními systémy, mřížemi, střežením, alarmy atd. Navíc proti těmto útokům (například krádeži) jde někdy pojistit.
Útok na SW:
přerušení - úmyslné a neúmyslné vymazání SW, chyby
odposlech - kopírování, porušení autorského práva
změna - využití tzv. zadních vrátek
přidání hodnoty - viry atd.
Tento útok obvykle provádí osoba na určité profesionální úrovni a lze ji takový útok alespoň ztížit.
Útok na data:
přerušení - vymazání dat, úmyslné a neúmyslné
odposlech - porušení důvěrnosti, krádež kopie dat
změna - porušení integrity, modifikace dat
přidání hodnoty - generování transakcí
Útoky na data může provést kdokoliv a to velmi rychle. Pokud nejsou data zašifrovaná, jsou pro kohokoliv čitelná. Zatímco HW i SW lze nahradit, data mohou být nenahraditelná. Proto se soustředím zejména na ochranu dat, pro kterou je řada důvodů. Navíc útok na data často provádí útočník zevnitř organizace (cca 80%), kterému lze těžko v práci s daty zabránit, neboť je to jeho náplň práce, např. operátorky.

2. Důvody pro ochranu dat

Proč vlastně data ochraňovat? Důvodů pro ochranu dat je několik, buď jsme k tomu přinuceni některým zákonem nebo si uvědomujeme, že jsou data pro nás cenná.

2.1 Zákon o ochraně osobních údajů

Pokud se data, které j sou v námi užívaném nebo námi navrhovaném IS, dají považovat za osobní či citlivé údaje, pak se na tento IS vztahuje zákon *101/2000 Ochraně osobních údajů a o změně některých zákonů.* [1] Je nutno si uvědomit, že dle tohoto zákona platí (dále citace ze zákonů jsou kursivou): „*…osobním údajem jakýkoliv údaj týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze na základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho identitu. O osobní údaj se nejedná, pokud je třeba ke zjištění identity subjektu údajů nepřiměřené množství času, úsilí či materiálních prostředků...“*. I když zatím kolem výkladu určitých částí tohoto zákona trvají rozpory, které se projevily při proběhlém sčítání lidu 2001, je stejně jisté, že IS obsahujícímu jakékoliv údaje o osobách je nutno věnovat zvýšenou pozornost. Ještě větší pozornost je pak nutno věnovat tzv. citlivým údajům, kdy citlivým údajem je dle tohoto zákona: *"...citlivým údajem osobní údaj vypovídající o majetku a majetkových poměrech, národnostním, rasovém nebo etnickém původu, politických postojích, členství v politických stranách či hnutích nebo odborových či zaměstnaneckých organizacích, náboženství a filozofickém přesvědčení, trestné činnosti, zdravotním stavu a sexuálním životě subjektu údajů...".*

Důležité je uvědomit si, jaké činnosti se daný zákon vlastně týká. Je to jednak spravování dat a dále operace při zpracování osobních údajů. Pojem zpracování je zde velmi široký a zahrnuje řadu operací*: „zpracováním osobních údajů jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace“*. Je nutno si uvědomit, že odpovědnost za ochranu dat nese správce a zpracovatel, neboť: *„….Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.“*
Zde při nedbalé ochraně dat mohou hrozit i velké problémy, neboť na rozdíl od jiných trestných činů souvisejících s IT, je zde možný i nedbalostní trestný čin neboť: *„Neoprávněné nakládání s osobními údaji ... ...Kdo, byť i z nedbalosti, neoprávněně sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje o jiném v souvislosti s výkonem veřejné moci, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti nebo peněžitým trestem."*
Uvedenému zákonu zde věnuj i zvýšenou pozornost z toho důvodu, že vešel v platnost poměrně nedávno v roce 2000 a řada organizací si vůbec neuvědomuje, že by se na ní resp. na odpovědné pracovníky mohly vztahovat výše uvedené sankce.

2.2 Zákon o ochraně utajovaných skutečností

Situace je ještě komplikovanější, pokud se organizace nějakým způsobem dotýká *Zákon o ochraně utajovaných skutečností 148/ 1998* a řada prováděcích vyhlášek. Plné znění zákona a navazujících vyhlášek možno najít např. na stránkách Národního bezpečnostního úřadu [2].

Délka příspěvku a složitost celé problematiky neumožňuje se více tímto zákonem a danou problematikou zabývat, ale je nutno si uvědomit, že pokud organizace pod pravomoc příslušné právní normy spadá, znamená to pro ni zabývat se bezpečností dle přísných pravidel uvedených v uvedeném zákoně včetně prověření osob pro dané stupně utajení. Je nutno si dále uvědomit, že mezi organizace, pro které platí Zákon o ochraně utajovaných skutečností patří i dodavatelé služeb a zboží např. pro ozbrojené síly a v literatuře [3] je uveden jako ilustrativní příklad firma, která dodává kožešinové límce pro armádu. Pro organizaci z toho plyne, že pokud v budoucnu hodlá dodávat zboží či služby právě třeba armádě, měla by se v předstihu na danou situaci připravit, neboť bezpečnostní prověrky trvají určitou dobu.

2.3 Ostatní důvody pro ochranu dat

Ale ani pokud IS, který vytváříme či již provozujeme nebude uchovávat či zpracovávat ani utajované skutečnosti ani osobní data, stále musíme bezpečnosti věnovat velkou pozornost.

Jde o ochranu dalších informací pro firmu či organizaci zásadních. Zničení dat (bez skutečně kvalitně prováděných záloh) či prozrazení dat konkurenci může pro firmu či jinou organizaci znamenat v krajním případě i zánik. Proto i v případě, že se jedná o „pouze“ firemní informace, je potřeba chránit data zásadní a přesto dle zkušeností autorky stále v řadě organizací vysoce podceňovaná záležitost. Jak je již uvedeno výše hardware i software jde obvykle nahradit, pro konkurenci není znalost toho, jaký HW či SW používáme obvykle nijak zásadní, ale znalost našich dat může být zásadní. Zde nutno poznamenat, že přenosné počítače jsou dnes kradeny obvykle kvůli datům a ne kvůli samotnému počítači a proto se doporučuje mít data na nich trvale zašifrována.

3. Bezpečnostní politika

Zde je nutno podotknout, že bezpečnost dat v organizaci není věcí pouze IS v počítačové podobě, ale jedná se o mnohem rozsáhlejší problematiku. Zásadním dokumentem pro řešení bezpečnosti v organizaci je tzv. bezpečnostní politika, dále BP.

BP obecně musí určit, co vlastně budeme chránit, proti jakým hrozbám, jakým způsobem. Rozlišuje se celková BP a systémová BP. Jak jsem již výše uvedla, existuje několik požadavků na bezpečnost. Proto BP musí řešit, jak zajistit důvěrnost (utajení) informací. Jedná se tedy o to, zda a kde užívat šifrování, na jaké úrovni. Dále můžeme utajení realizovat například pomoci řízení přístupu. Dále bude bezpečnostní politika řešit, jak zajistit integritu, tj. zda užívat elektronické podpisy, kontrolní součty atd. Dalším z cílu bezpečnosti je autenticita, tj. možnost prokázat, kdo je komunikujícím partnerem a nepopiratelnost, tj. není možnost popřít účast v nějaké transakci. Dalším cílem bezpečnosti ovsem musí byt opatření trvale dostupnosti, tj. nemohu třeba dosažením sice totálního utajení dosáhnout nedostupnosti dat. Tvorba bezpečnostní politiky vyžaduje řadu specifických znalostí. Některé organizace si vytvoří BP sami, jiné tuto tvorbu celou zadají externí firmě a někdy dojde k určité dělbě práce mezi interními řešiteli a externí firmou. Záleží samozřejmě na velikosti organizace apod. Vzhledem k tomu, že není možno „koupit“ BP hotovou někde v obchodě, protože je pro každou organizaci jiná, jedná se často o velmi složitou záležitost a nákladnou záležitost. Je ale nutno si uvědomit, že řešení bezpečnosti bez vytvoření BP nemá žádný skutečný dlouhodobý smysl a v konečné fázi se může nevyplatit jak finančně, tak i možností bezpečnostních incidentů.

3.1 Celková bezpečnostní politika

Dále se krátce zmíním o tom, co to BP je, podrobnější informace možno najít v uvedené literatuře.
Rozlišuje se BP *celková a systémová*. Celková BP (dále CBP) určuje kdo, která funkce za co odpovídá. Kdo data specifikuje, kdo definuje jejich důležitost pro organizaci. Tato BP specifikuje omezení, která se organizace týkají. Specifikuje právní rámec, platící pro organizaci. Tento dokument by měl platit delší dobu asi 5 až 10 let, pravdou je, že v našem zatím neustáleném právním prostředí to asi bude kratší doba. Jedná se o písemný dokument, stručný, který neřeší právě užívané informační technologie. Určuje odpovědnosti, pravomoc a práva. Musí ji schválit vedení organizace, jinak její tvorba nemá vcelku smysl, neboť ji nikdo nerespektuje.

Samotná BP má zhruba následující strukturu:
Popis organizace, poslání, koncepce IT.
Plán a harmonogram budování CBP,cíle CBP.
Vypracování bezpečnostní infrastruktury organizace- role, funkce.
Identifikace aktiv, zejména citlivých dat, identifikace obecných hrozeb.
Orientační analýza rizik.
Popis současného stavu bezpečnosti.
Orientační popis navrhovaných bezpečnostních opatření.
Strategie havarijních plánů.
Školení - plán a koncepce.

Někdy se samozřejmě můžeme setkat s poněkud jinou strukturou obsahující další body, ale podstatou je, že nejde ještě o konkrétní opatření, ale více o koncepci budování bezpečnosti v organizaci.

3.2 Systémová bezpečnostní politika

Konkrétní implementaci CBP v daném technologickém prostředí určuje tzv. systémová bezpečnostní politika, déle SBP.

Ta se již vypracovává pro mnohem kratší období několika let, tak jak rychle se mění technologie.

Je to soubor *principů a pravidel pro ochranu IS a jím poskytovaných služeb*. Řeší se bezpečnost elektronické části, ale pokud by i neelektronická část mohla ovlivňovat bezpečnost elektronické části, je nutno řešit i tu.

Zde jde již o konkrétní opatření, konkrétní cíle, konkrétní hrozby. Tvorba SBP je u rozsáhlé organizace či rozsáhlého systému natolik složitá, že se často dělí na několik částí: SBP fyzické ochrany, SBP technické ochrany, SBP personální, SBP komunikační. Konkrétní informace o budování jednotlivých politik poskytuje například literatura. [4]

Pro realizování a prosazování BP musí mít organizace zvláštní pracovníky. Rozhodně by to neměl být správce sítě, jak se někdy u nás děje. V literatuře [3], [4] je navržena určitá bezpečnostní infrastruktura tzv. *bezpečnostní management*. V jejím čele stojí bezpečnostní ředitel, dále jsou zde specializovaní bezpečnostní specialisté.

V jaké fázi vývoje IS by měla vznikat nová systémová politika? Samozřejmě nejlepší by bylo, kdyby souběžně s vývojem IS se zpracovávala systémová bezpečnostní politika a systémová bezpečnostní politika se rovnou implementovala. Tím by se i při vývoji mohlo jednak zabránit různým možným bezpečnostním incidentům, které mohou nastat již při testování systému a dále by nedocházelo k tomu, že na již vyvinuté části IS se bezpečnostní prvky později „roubují". Již při analýze a projektu IS je nutno hledět na možnost oddělit data různé citlivosti, používat takové systémy, které umožňují diferencovat jak data tak i uživatele. Pokud již organizace má strukturu bezpečnostních pracovníků (což z vlastní zkušenosti musím říci, že kromě bank a telekomunikačních firem je situace spíše ojedinělá) při vývoji nového nebo či částečně inovovaného IS jistě někteří tito pracovníci mohou z hlediska bezpečnosti spolupracovat. Bohužel zatím je situace obvykle taková, že až po nějakém významném bezpečnostním incidentu začne vedení organizace bezpečnosti věnovat pozornost. A poté často bez jakékoliv BP je zakoupeno nějaké bezpečnostní zařízení např. firewall, jehož nevhodné nasazení může naopak bezpečnost organizace snížit.

4. Závěr

Na závěr nutno říci, že význam bezpečnosti stále vzrůstá. Důvodem je jednak zvyšující se závislost celé společnosti na IT a dále prakticky absence jakékoliv výchovy v dané oblasti u dětí a dospívajících, takže například činnost hackerů je často považována za hrdinský čin a ne za trestnou činnost a napadání systémů patří téměř k módě.

Špatnou službu zde konají také sdělovací prostředky, kde sice problematika bezpečnosti IT je častým námětem, ale odborná úroveň těchto článků či pořadů bývá minimální. Příkladem nám může být nedávno proběhlá mediální „akce" prolomení PGP, kdy bylo vidět, že pisatelé článků nemají o dané problematice nejmenší potuchu.

Vzdělávání v oblasti bezpečnosti IS zatím u nás nepatří k běžné součásti výchovy informatiků. Na základě zkušeností z poskytování konzultací v dané oblasti a výuky předmětu s touto problematikou na vysoké škole, se autorka příspěvku domnívá, že určité znalosti z oblasti bezpečnosti IT by měl mít každý absolvent studia informatiky.

Literatura

1. www.uoou.cz
2. www.nbu.cz
3. Staša, P., Rodyryčová, D.: Bezpečnost informací jako prosperita firmy. Grada, 2000, 144 str. ISBN 80-7169-144-5
4. Kovacich, G.: Průvodce bezpečnostního pracovníka informačních systémů, UNIS, 2000, 200 str. ISBN 80-86097-42-0