Základní princip ochrany výpočetních systémů.
O peníze jde až v první řadě.

→ Chráněné objekty mají svoji cenu, pro kterou jsou chráněny. Cena může být různá pro majitele a útočníka.
→ Ochrana není zadarmo.

Několik základních pojmů

Informačním systémem rozumíme soubor hardwaru, softwaru, záznamových medií, dat a personálu, který daná organizace používá ke správě svých informací.

Korektní stav IS odpovídá situaci, kdy systém je schopen v definovaném rozsahu poskytovat zajišťovat všechny požadované vlastnosti zpracovávaných informaci, či poskytovaných služeb

- utajení
- dostupnost
- integrita
- nepopiratelnost
- včasnost
- současnost
- autenticita
- anonymita
- pseudonymita
- …

Bezpečnostní incident je stav, kdy došlo k porušení alespoň jedné z požadovaných vlastností

Princip nejsnazšího průniku.
Je třeba očekávat, že útočník použije libovolný způsob průniku. Nemusí to být nejzřejmější metoda a útok nemusí být veden proti nejsilnějšímu místu ochrany výpočetního systému.

Expozice je místo potenciálního poškození nebo ztráty informací, či funkčnosti systému. (např. odhalení utajovaných dat, jejich neoprávněná modifikace, odmítnutí autorizovaného uživatele).

Zranitelnost je nedostatek bezpečnostního systému, může být použit k poškození nebo zcizení informací.

Hrozba = externí skutečnosti, které potenciálně mohou vést k poškození informací. (požáry, hackeři, …). Dopadem hrozby na expozici se rozumí kvantifikace škod, které utrpíme v souvislosti s realizací příslušného incidentu.

Riziko vyplývá z případné realizace hrozby. Je dopadem hrozby, do kterého se zahrne pravděpodobnost výskutu příslušného incidentu.

Zdroje bezpečnostních požadavků

organizace musí určit své požadavky na bezpečnost na základě

- požadavků zákonů, vyhlášek a dalších legislativních instrumentů
- norem a jiných oborových předpisů
- smluvních závazků
- vlastního hodnocení rizik
- dalších principů

Identifikace aktiv

z 4eho se skládá
co to dělá

Hodnocení rizik

míra rizika se určuje na základě modelu hrozeb s ohledem na

- nemožnost normálně operovat až do doby zotavení
- nákladů na zotavení
- pravděpodobnosti realizace hrozby

Nezbytná periodická revize

- určení změn obchodních požadavků
- zahrnutí nových hrozeb
- potvrzení vhodnosti opatření

Model hrozeb

Každý si musí definovat pro něj relevantní systém hrozeb, neexistuje univerzální. Model se odvíjí od

- povahy činnosti organizace
- ceny dat pro útočníka
- ...

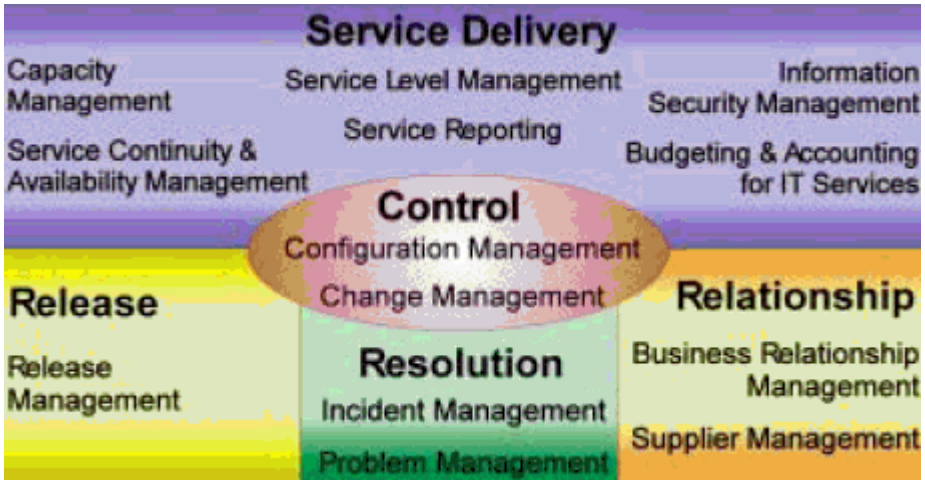
- míry paranoiy

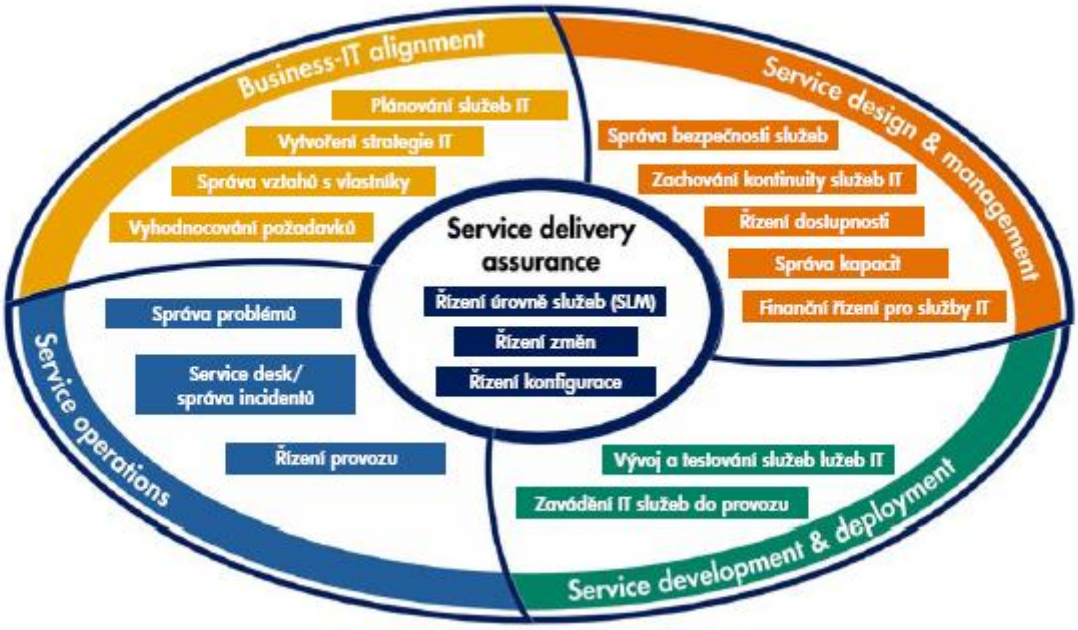
Příklad:
1. *Tupá síla* – vlivy, které při svém působení neinterpretují stav systému (povodně, požáry, globální konflikty ...)
2. *Amatérský oponent* – útočník reaguje na stav systému, může mít rozsáhlou znalost, omezené prostředky, simultální působení více útočníků (hacker, matfyzák, nešikovný uživatel ...)
3. *Profesionální oponent* – podobně jako amatérský útočník, ale se schopností koncentrovat rozsáhlé zdroje na provedení útoku (tajná služba ...)
4. *Autority* – schopnost působit nepřímo prostřednictvím obecně závazných pokynů bez nutnosti lokalizovat systém (soudy, náboženské autority, státní moc ...)

Normosloví

Pozice IT (a bezpečnosti) v rámci organizace

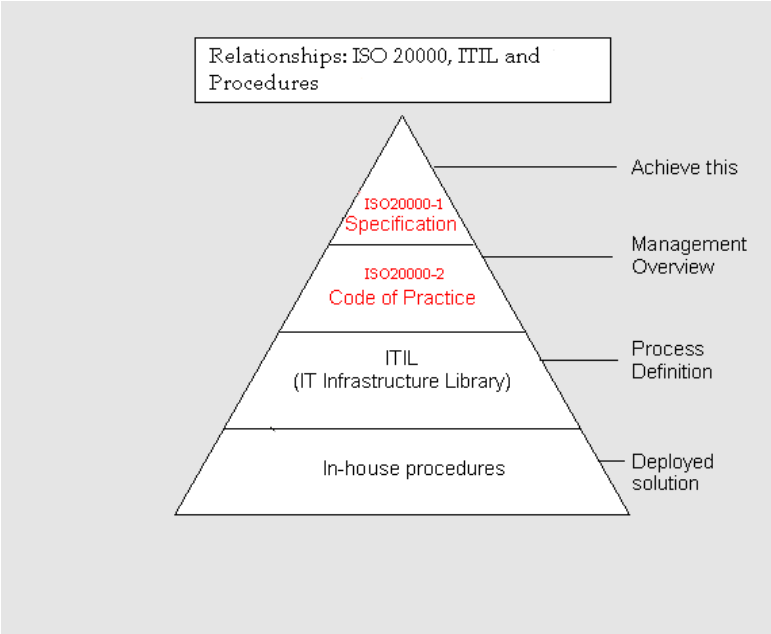
IT je chápáno jako vnitřní dodavatel služby (zhruba řečeno dodávka služeb informačního systému pro podporu operací organizace)
„zákazníkem“ IT je v tomto modelu vnitřní uživatel





Pro harmonizaci s dalšími standardy byla provedena kosmetická úprava BS15000 spočívající v zahrnutí PDCA principu:

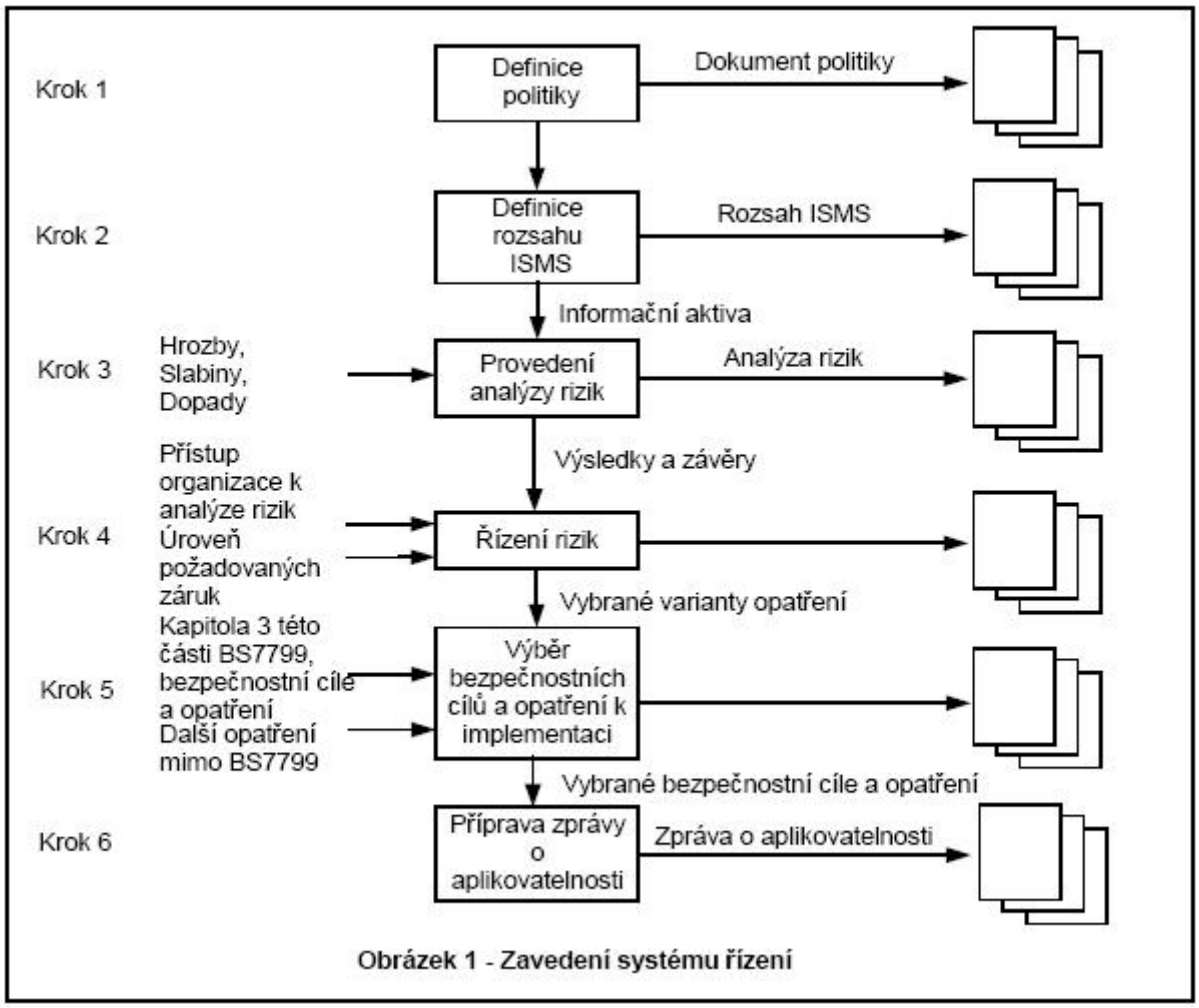
Souvislost jednotlivých norem ukazuje následující obrázek



Zavedení bezpečnosti dle BS7799, ISO2700*

Kritické faktory úspěchu

- existence bezpečnostní politiky
- implementace BP v souladu s kulturou organizace
- podpora na všech úrovních
- pochopení bezpečnostních cílů
- efektivní vnitřní marketing bezpečnosti
- znalost norem a směrnic bezpečnosti
- systém sankcí za nedodržování bezpečnosti



Obrázek 1 - Zavedení systému řízení

Bezpečnostní politika

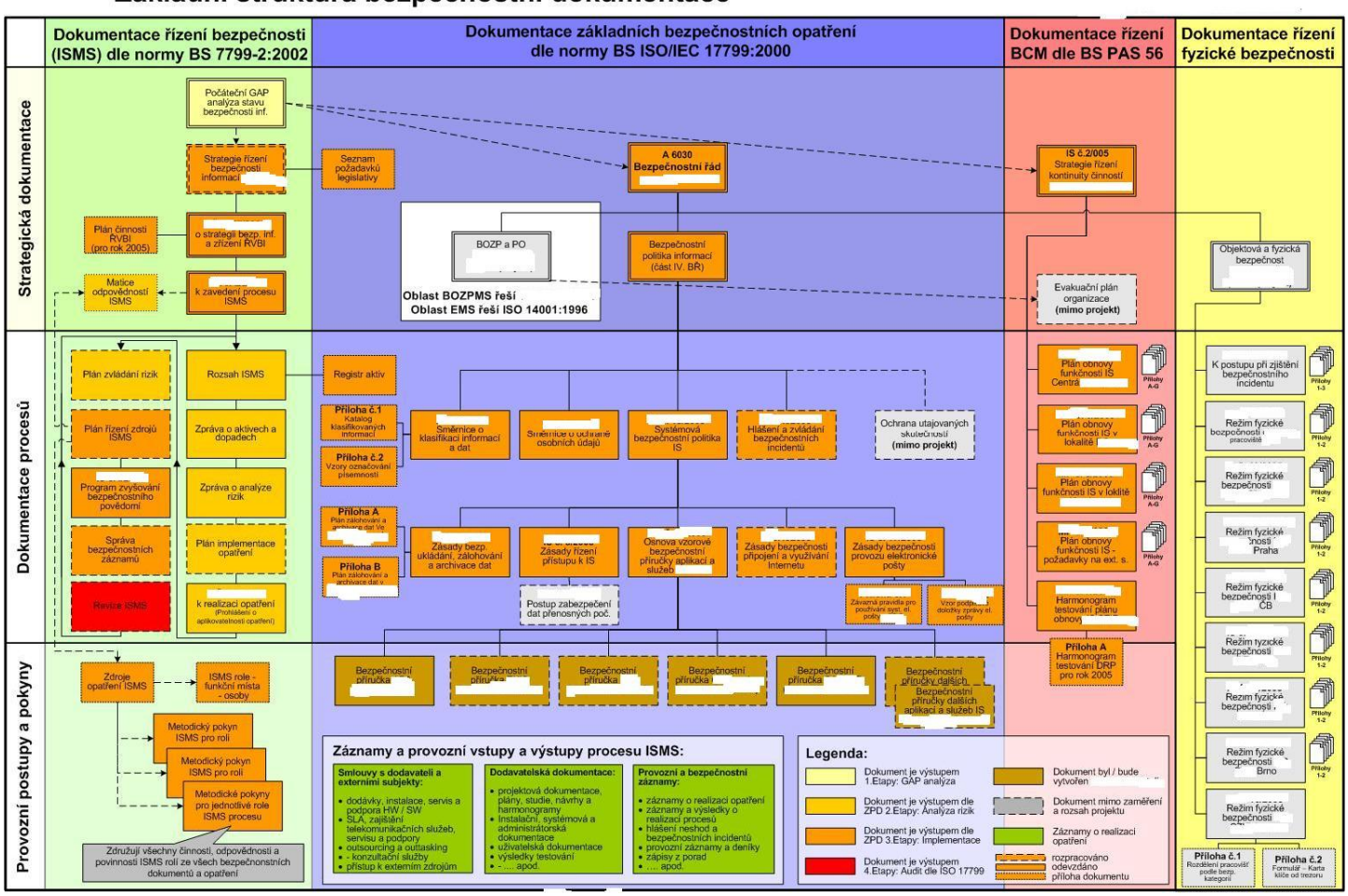
cílem je definovat směr a vyjádřit podporu bezpečnosti

Dokument bezpečnostní politiky

musí být schválen a vydán vedením
obsahuje:

- definice, cíle, rozsah a důležitost bezpečnosti
- prohlášení vedení organizace (často samostatně)
- stručný výklad hlavních zásad, principů, norem a procesů
- stanovení odpovědností

- odkazy na podřízené dokumenty (lokální BP pro jednotlivé oblasti, procedury, ...)



Revize a hodnocení

BP musí mít garanta odpovědného za aktualizaci
Plán revizí kontroluje

- efektivitu politiky
- ceny a dopad opatření
- dopad změn technologie

Řízení bezpečnosti

musí být formálně vytvořen řídící rámec pro implementaci bezpečnosti a kontrolu
organizace potřebuje metodický zdroj bezpečnosti (lze zvládnout i smluvně)

Řídící fórum bezpečnosti

Působnost:

- revize a zdokonalení bezpečnosti
- definice rolí v rámci bezpečnostního týmu
- sledování změn a navazujících zranitelností

- sledování incidentů
- schvalování hlavních opatření

Odpovědnost

Obvykle bývá jmenován vedoucí odpovědný za bezpečnost, dále vlastníci jednotlivých aktiv se zodpovědností za bezpečnost příslušného aktiva.
V rámci vymezení odpovědnosti je třeba

- identifikovat a definovat aktiva
- určit konkrétní odpovědnost za aktivum
- určit a zdokumentovat úroveň oprávnění

Další kroky

Musí existovat proces schvalování zařízení zpracovávajících informace

- odsouhlaseno příslušným vedoucím
- kontrola kompatibility

Je vhodné udržovat kontakty s orgány prosazování práva, regulačními orgány, poskytovateli služeb, operátory z důvodu rychlého řešení incidentu.

Implementace bezpečnosti má být nezávisle posouzena (interní audit, externí dodavatel)

Řízení aktiv

cílem udržení přiměřené ochrany aktiv
nezbytné stanovení odpovědnosti, implementaci lze delegovat, odpovědnost nikoliv
základem je provedení evidence všech aktiv

- každé aktivum musí být určeno
- musí být stanoven vlastník
- stanovena bezpečnostní klasifikace

Klasifikace aktiv

popisuje potřebnost a důležitost aktiva
základem pro určení adekvátní ochrany a způsobu zacházení
klasifikace není neměnná
pro zacházení s aktivy je třeba definovat soustavu postupů

Personální bezpečnost

cílem snížit riziko lidské chyby či selhání
je třeba zahrnout do procesu přijímání nových pracovníků i sledování stávajících (zvl. na kritických postech)
zvýšený dohled nad novými zaměstnanci
smlouva o zachování důvěrnosti má být součástí nástupních podmínek
nezbytné stanovit povinnosti zaměstnance v oblasti bezpečnosti a zajistit odpovídající proškolení

Reakce na incidenty

zaměstnanci musí znát postup hlášení incidentů
má být postup po přijetí hlášení incidentu
je nezbytné monitorovat a kvantifikovat typy, rozsah a cenu incidentů
má existovat formalizované disciplinární řízení

Fyzická bezpečnost a kontrola prostředí

cílem je předcházení neautorizovanému přístupu
bezp. perimetr je cokoliv, co vytváří bariéru, musí být jasně definován a v řádném stavu, s kontrolou přístupu
nezbytné opatření pro kontrolu pohybu osob s viditelnou identifikací oprávněných a reakcí na výskyt neoznačené osoby

Opatření

vhodné situování důležitých opatření
detekční systémy, uzavření prostor, zejména prázdných
zvážit, kde jsou veřejně přístupné prostory
zcela nezbytné vymezení bezpečných zón, včetně odpovídajících pravidel pro pohyb v nich
zajištění dodávek energií v potřebném rozsahu a kvalitě (napájení, chlazení, ...)
bezpečnost kabeláže by měla být zajištěna vhodnou pokládkou
pravidelná údržba
nutno řešit bezpečnost zařízení mimo objekt a vhodnou formu likvidaci, nebo znovupoužití zařízení
zásada prázdného stolu

Řízení komunikací a provozu

Cílem zajistit správný a bezpečný provoz prostředků pro zpracování informací.

stanoveny odpovědnosti a postupy pro řízení a správu včetně provozních instrukcí a postupů při incidentech.
měl by být uplatněn princip oddělení funkcí, aby se snížilo riziko úmyslného zneužití systému nebo zneužití z nedbalosti.

Opatření

dokumentace provozních postupů včetně časových návazností, reakcí na chyby a mimořádné stavy
postupy pro řízení bezpečnostního incidentu (identifikace příčiny, plán oprav, zajištění stop, komunikace s okolím, hlášení)
oddělení vývoje a provozu včetně pravidel pro přenos změn, nedosažitelnost vývojových nástrojů z produktivního prostředí
oddělení povinností (separation of duties)
správa externích zařízení a služeb, identifikace kritických aplikací, které nelze outsourcovat, smlouvy
plánování a akceptace systému, plánování kapacit (i v čase), akceptace systému
ochrana proti škodlivým programům, formální pravidla použití SW, aktualizace antivirových opatření, content scanning, plánu kontinuity
správcovství: zálohy, operátorský deník, incident list
správa sítě
bezpečnost při zacházení s médii, správa a likvidace (vyměnitelných) médií, postupy pro manipulaci s informacemi, bezpečnost dokumentace
výměna informací a programů mezi organizacemi, bezpečnost médií při přepravě,
bezpečnost el. obchodu, el. pošty, kancelářských systémů, veřejně přístupných systémů, standardy pro jiné formy výměny informací (hlas, fax, video, ...)

Řízení přístupu

Cílem řídit přístup k informacím na základě provozních a bezpečnostních požadavků v souladu s pravidly a postupy organizace, předcházení neoprávněnému přístupu

Opatření

Musí být definována politika řízení přístupu, provozní požadavky a pravidla, need_to_know, standardní přístupové profily, vše_co_není_povoleno_je_zakázáno, proces registrace uživatele, použití unikátního ID, řízení privilegií a kontrola přístupových práv, správa hesel a zacházení s nimi, definování odpovědnosti uživatele

zásady použití síťových služeb, vynucení stanovené cesty, autentizace uživatele externího připojení, autentizace uzlů,
ochrana portů, oddělení v sítích, řízení síťových prostředí, řízení směrování, bezpečnost síťových služeb
řízení přístupu k OS, identifikace terminálu, identifikace a autentizace uživatelů, identifikace přihlášení pod nátlakem, omezení doby spojení a doby neaktivity
řízení přístupu k aplikacím
monitorování přístupu k systému a použití, zaznamenávání událostí, monitorování použití systému, synchronizace času
mobilní výpočetní prostředky, práce na dálku

Vývoj a údržba

Řízení kontinuity

Soulad s požadavky

Místa zranitelnosti

1. *utajení* - objekty systému jsou přístupné pouze autorizovaným subjektům
2. *integrita* - objekty mohou být modifikovány pouze oprávněnými subjekty
3. *dosažitelnost* - objekty jsou dostupné pro autorizované subjekty

Objekty ochrany - aktiva

Technická zařízení

nejrůznější problémy počínaje ukradením daného zařízení, konče klávesnicí prolitou džusem či kabely překousanými od myší, záměrné poškození komponent systému, přírodní katastrofy

Programy

Dostupnost - úmyslná/náhodná ztráta softwaru se stane zřejmou až při pokusu o spuštění. Pokud systém poskytuje rozumnou *správu konfigurací*, lze snížit riziko náhodné ztráty.
Modifikace - nemusejí být poznatelné, určení jejich rozsahu a následků je obtížné.
Krádež - programy bývají cennou součástí systému, krádeže jsou těžko detekovatelné. Právní problémy.

Data

- těžko vyčíslitelná, povětšinou však značná hodnota, schopnost udržet data v tajnosti je často životně důležité, hodnota může být v čase značně proměnná.Služby
externí používané služby, dodávaná data

Princip časové závislosti.
Ochrana jednotlivých objektů by měla trvat pouze do doby, než pozbydou svoji hodnotu.

→ použití adekvátních metod ochrany

Utajení - data mohou být kompromitována celou řadou způsobů, od podplacení osob majících legální přístup až po monitorování el.mag. záření.

Integrita - Problémy mohou způsobovat chybné programy, technické zařízení atd.
Vhodně provedené úmyslné úpravy prakticky neodhalitelné. Pokusy o znovupoužití některých dat.

Záznamová media

nutný vhodný plán tvorby a správy záložních kopií

Sítě

přinášejí specifický problém komunikace jednotlivých uzlů, vzájemné identifikace, ochrany přenosových medií

Přístup

Jde o neoprávněné získání strojového času případně služeb poskytovaných systémem. Dalším následkem může být poškození dat, nebo znepřístupnění služeb pro legitimní uživatele.

Klíčoví lidé

Provoz celého systému může být závislý na velmi malém počtu lidí, kteří jsou schopni ho udržovat. Tito lidé mívají rozsáhlé pravomoci, je nutné je vybírat opatrně.

Zdroje ohrožení

1. vyšší moc (požár, povodeň, zemětřesení, blesk, …)
2. závady technického zařízení
3. neúmyslné lidské chyby
4. záměrné útoky

Klasifikace možných útočníků

klasifikovat lze dle mnoha kriterií, zejména dle

I. způsobu, jak se projeví způsobená škoda
   A. ztráta integrity
   B. ztráta dosažitelnosti
   C. ztráta autenticity …
II. druhu způsobené ztráty
   A. neautorizované použití služeb
   B. přímá finanční ztráta
   C. fyzické poškození, vandalismus
III. role, kterou výpočetní technika hraje v tomto konání
   A. objekt útoku
   B. nástroj
   C. prostředí
   D. symbol
IV. použitých prostředků
   A. opisování údajů
   B. špionáž
   C. vkládání falešných dat
   D. krádež

E. odposlech
F. scanování, prohledávání - kupříkladu hledání hesel zkoušením, hledání tfn. linek, které vedou k počítači, …
G. piggybacking, tailgating - útočník se snaží projít vstupní kontrolou zároveň s autorizavanou osobou, nebo pokračovat v započaté session
H. trojské koně - programy, vykonávající skrytou funkci
I. viry
J. trapdoors - skryté vstupy do systému, utajené příkazy umožňující přeskočit některé části procesu
K. logické bomby - části kódu spouštěné výskytem určitých okolností - čas, dosažený obrat, stav systému
L. salami attack - využívání zaokrouhlovacích chyb, drobné úpravy na hranici přesnosti zpracovávaných dat
M. prosakování dat
N. pirátství

Způsoby ochrany

Cílem ochrany je zajistit utajení, integritu a dostupnost všech objektů. Některé metody zajišťují prevenci před útoky, jiné pouze detekují napadení.

Šifrování

Zakódování dat tak, aby nebyla běžnými prostředky čitelná. I v případě odcizení takto zakódovaných dat nedojde k úniku informací.
Dále lze použít k zajištění integrity dat, nebo k vytvoření speciálních protokolů pro výměnu informací.
Elektronické podpisy (nejen) elektronických dokumentů.

Softwarové kontroly

Programy musí být bezpečné a spolehlivé. Protože SW kontroly přímo ovlivňují přístup uživatele k systému, musí být navrženy tak, aby neznemožňovaly práci.Jakožto nástrojů používaji kryptografie, hardwarových součástek apod.
Zahrnují:
1. Kontrola vývoje - soubor standardů, jak vytvářet, testovat a udržovat programy pro správu chráněných dat.

2. Kontroly operačního systému - různá omezení vynucená operačním systémem, jejichž cílem je chránit jednotlivé uživatele navzájem.
3. Interní programové kontroly - omezení vynucená samotným programem, např. omezený přístup do jednotlivých částí databáze.

Kontroly hardwaru

Technická zařízení používaná ke zpracování utajovaných dat musí vyhovovah specifickým normám. Dále je nutná jejich vhodné zajištění proti útokům a celkové zabezpečení přístupu k nim.

Bezpečnostní politika

Velmi účinná bývají nejjednodušší bezpečnostní opatření. Vysvětlit sekretářce, že si nemá svůj hardwarový klíč nechávat v horní zásuvce psacího stolu, přimět uživatele k občasným změnám hesel.
Je vhodné uživatelům vštěpovat postupy vedoucí k zajištění bezpečnosti a základy etiky ve vztahu k počítačům.
Toto působení na uživatele by mělo být ucelené co do formy a obsahu.

Fyzické kontroly

Obyčejné zámky, stráže, záložní kopie dat a programů, náhradní technické vybavení, ale i plánování umístění jednotlivých komponent systému.
Fyzické kontroly bývají velmi účinné, bohužel jsou však často přehlížené.

Efektivita ochrany

Znalost problému

Lidé lépe dodržují daná pravidla, pokud chápou jejich smysl a cíl.

Pravděpodobnost použití

Budou-li bezpečnostní opatření příliš "překážet", uživatelé se budou pokoušet je obcházet.

Periodické ověřování

Je nutné periodicky ověřovat, zda přijatá bezpečnostní opatření stále odpovídají reálné situaci.
Rovněž uživatelům třeba občas připomenout, jaká opatření dodržují.

Princip efektivity.
Použité způsoby ochrany musí být efektivní. Je nutné, aby byly výkonné, přiměřené a aby nepřekážely.

Bezpečnostní politika

stejně jako každá činnost, i provozování systému pro správu informací je spojeno s jistým rizikem (chyba zařízení, obsluhy, programu, vandalismus, krádež, …)
provedení kvalifikovaného odhadu rizik přináší:

- zlepšení obecného povědomí - pracovníci si problém uvědomí a mají šanci jej pochopit
- identifikace hodnot, slabin a možných kontrol celého systému - ne vždy je jasné, které části systému mají největší hodnotu, odkud pramení největší nebezpečí
- zlepšení východiska pro strategická rozhodnutí - některé ochranné a kontrolní mechanismy velmi snižují produktivitu systému přičemž jejich přínos není zřejmý, různé druhy nebezpečí jsou různě reálné a představují mnohdy daleko větší hrozbu, než by se dalo očekávat
- lepší rozložení výdajů na bezpečnost - některé velmi drahé ochranné mechanismy poskytují pouze malé zvýšení bezpečnosti a popřípadě i naopak

Vlastní provedení odhadu rizik lze rozdělit do několika kroků:

1. Identifikace hodnot
2. Určení slabin
3. Odhad pravděpodobnosti zneužití
4. Výpočet očekávaných ročních ztrát
5. Přehled použitelných ochranných mechanismů
6. Nástin ročních úspor ze zavedení ochranných mechanismů

ad) Identifikace hodnot

přesnější výsledek docílíme sčítáním po jednotlivých kategoriích, např

- ♦ hardware - počítače, monitory, pásky, tiskárny, disky, komunikační media, …
- ♦ software - operační systém, koupené programy, vlastní zdrojové kódy, knihovny
- ♦ data - vlastní uložená data, logy, archivní kopie, listingy, …
- ♦ lidé - pracovníci potřební k správnému chodu systému, správci, programátoři
- ♦ dokumentace - programů, technického vybavení, systému, administrativní postupy
- ♦ spotřební materiál - papír, diskety, tonery, pásky do tiskáren, …

v podstatě jde i zevrubnou inventarizaci celéh systému, cena některých částí může být pouze velmi přibližně odhadnuta a i takový odhad může být velmi obtížný

ad) Určení slabin

- ♦ dopad přírodních katastrof - požár, vichřice, záplavy, výpadky napájení, selhání techniky
- ♦ poškození třetími osobami - přístupy po síti, vytáčená spojení, hackeři, kolem-jdoucí, lidé zkoumající odpad firmy
- ♦ následky zlomyslných pracovníků - zklamaní pracovníci, úplatkářství, zvědavci
- ♦ důsledky neúmyslných chyb - zadání špatných příkazů, vadných dat, skartace špatných dokumentů, kompromitace tajných materiálů

zjišťování těchto faktů lze provádět formou dotazníku, který vyplní zainteresovaní pracovníci:

Dotazníček			
Hodnota	*Utajení*	*Integrita*	*Dostupnost*
Hardware		přetížení, zničení, poškození	
Software	odcizen, kopírován	modifikován	smazán, přesunut
Data	zpřístupněna vně firmy	zničena chybou SW ; HW ; lidí	smazána
Lidé			únava, nemoc
Dokumentace			ztracena, odcizena
Materiál			odcizen, zničen

ad) Odhad pravděpodobnosti zneužití

jde o to zjistit, jak často dojde ke zneužití některé z expozic systému
učinění těchto odhadů může být velmi obtížné, lze použít některou z metod:

- Odhad na základě obecných dat - např. pojišťovny mají rozsáhlé záznamy o počtu katastrof a o průměrných způsobených škodách, o počtu vloupání, podvodů. Výrobci mají přehled o životnosti a počtu selhání zařízení, …
- Odhad na základě vlastních dat - za dobu činnosti firmy vzniklé záznamy o závadách zařízení, počtech vadných loginů, …
- Odhad počtu výskytů události za určité časové období - např, na základě počtu výskytů této události za polední dva roky
- Bodovací systém počtu výskytů události - např dle tabulky

Frekvence	*Hodnocení*	*Frekvence*	*Hodnocení*
více než 1 x za den	10	1 x za měsíc	5
1 x za den	9	1 x za 4 měsíce	4
1 x za 3 dny	8	1 x za rok	3
1 x za týden	7	1 x za 3 roky	2
1 x za 2 týdny	6	méně než 1 x za 3 roky	1

- *Delfská metoda* - okruh hodnotitelů provede hodnocení dané veličiny. Poté je každý seznámen s výsledky ostatních a upraví své hodnocení. Pokud jsou upravená hodnoccení podobná, máme výsledek, v opačném případě výsledek vznikne dohodou hodnotitelů.

ad) Výpočet očekávaných ročních ztrát

je nejproblematičtější krok analýzy, zatímco cenu výměny součástek lze snadno zjistit, je daleko obtížnější vyčíslit nedostunost (i jen dočasnou) části dat
mnohé fitmy udržují o svých zákaznících velmi důvěrná osobní data (nemocnice, banky, pojišťovny), je obtížné odhadnout ztráty způsobené vyzrazením těchto dat
je takřka nemožné vyčíslit ztrátu způsobenou nedostupností obsluhy v okamžiku selhání systému udržujícího životní funkce pacienta
je třeba najít odpověď na následující okruhy otázek:

- ♦ Jaké právní normy chrání utajení a integritu dat?
- ♦ Může uvolnění daných dat představovat poškození osoby, nebo organizace?
- ♦ Může neautorizovaný přístup k datům způsobit ztrátu obchodních příležitostí? Může tak útočník získat výhodu, kolik představují očekávané ztráty?
- ♦ Psychologický efekt ztráty dostupnosti? Ztráta důvěryhodnosti, dobrého jména, … Kolika zákazníků se záležtost týká, jaký je jejich přínos pro firmu?
- ♦ Jaká je cena přístupu k programům, lze počítání odložit, nebo provést jinde? Cena tohoto řešení?

- Kolik je útočník ochoten zaplatit za získání přístupu k našim datům a programům?Jakou pro něho představují hodnotu?
- Dopad ztráty dat: co tostojí, lze data nahradit nebo rekonstruovat, za jak dlouho, za kolik?

Kvalifikovaný odhad ztrát bývá vyšší, než se obvykle předpokládá, může problému ochrany zajistit potřebnou pozornost. LZe rovněž vytyčit okruhy bezpečnosti, kterým je třeba se zvláště věnovat.
výpočet je na základě předchozích zkoumání, vždy násobíme pravděpodobnost některé ze ztrát s její hodnotou, výsledný součet těchto násobků představuje odhad ročních ztrát

ad) Přehled použitelných ochranných mechanismů

pokud vyčíslený odhad ztrát je příliš vysoký, je třeba zavést nové ochranné mechanismy
můžeme probrat jednotlivé expozice systému a zkoumat možnosti jejich pokrytí, nebo naopak mezi všemi ochrannými mechanismy hledat nějaký, který by řešil náš problém
výsledkem je seznam navrhovaných opatření

ad) Nástin ročních úspor ze zavedení ochranných mechanismů

můžeme spočítat, o kolik se sníží odhad očekávaných ztrát, víme, jaká je cena zavedení nových ochranných mechanismů, z těchto hodnot lze získat odhad celkových úspor.

Nedostatky odhadu rizik

nedostatečně přesný - velká část zpracovávaných hodnot může být pouze zhruba odhadnuta, výsledky jsou pouze statistické
klamný pocit přesnosti - absolutní velikot vlastních vypočtených hodnot bývá přeceňována, důležitější je jejich vzájemný vztah
nepružnost - analýza rizik by měla být prováděna opakovaně, je však tendence i při nových zpracováních používat hodnoty obdobné hodnotám z minulých let

Návrh bezpečnostního plánu

bezpečnostní plán popisuje, jak daná organizace přistupuje k otázkám bezpečnosti
plán musí být dostatečně často revidován a musí být zkoumáno jeho dodržování

vypracováním plánu bývá pověřena skupina odborníků pokud možno ze všech důležitých organizačních struktur firmy, velikost a struktura tohoto týmu závisí na velikosti firmy
součásti bezpečnostního plánu:

Bezpečnostní politika

vyjadřuje vůli pracovat na dosažení jistého stupně bezpečnosti

- popis celkových cílů bezpečnostních aktivit - např ochrana dat před katastrofami, před úniky mimo organizaci, apod.
- kdo má zodpovědnost za udržení bezpečnosti - pověřený pracovník, vedení, všichni
- závazky organizace na udržení bezpečnosti - počet vyčleněných pracovníků, minimální výdaje do této oblasti

Popis současného stavu

popis obsahuje seznam hodnot systému, soupis hrozeb pro tyto hodnoty a používané ochranné mechanismy
dále je popsán způsob získávání a vstupní validace dat, případně předpoklady o jejich vlastnostech
měly by být popsány metody odhalování slabin systému, popisy akcí, které je třeba podniknout v případě odhalení nové slabiny

Doporučení

seznam dalších bezpečnostních opatření, které je třeba přijmout k doplnění, nebo nahrazení sočasných mechanismů
součástí by měl být rozbor nákladů a ztrát
seznam by měl být seřazen podle naléhavosti navrhovaných opatření, navrhována by měla být pouze opatření, jejichž celkový efekt není záporný

Odpovědnost za implementaci

je třeba určit konkrétní osoby zodpovědné za zavedení a provozování konkrétních bezpečnostních mechanismů, těmto lidem důkladně vysvětlit jejich úkol a důvody
též je nutné navrhnout způsob hodnocení splnění těchto úkolů
možné rozdělení zodpovědnosti:

- uživatelé osobních počítačů - každý ručí za svůj počítač
- administrátor databázového systému - zodpovídá za přístup k datům a jejich integritu

- firma může pověřit zvláštního pracovníka zodpovědného za vytvoření obecných pravidel práce s daty a jejich uvolňování či rušení
- pracovníci osobních oddělení zodpovídají za přijetí důvěryhodných a spolehlivých pracovníků

Časový rozvrh

některá opatření mohou být příliš nákladná, nebo složitá, než aby mohla být zavedena naráz
musí existovat plán, do kdy budou která opatření zavedena, případně nejzajší termíny splnění jednotlivých fází bezpečnostního plánu
též pořadí zavádění opatření může být důležité

Soustavná pozornost

je třeba již v plánu stanovit termín, kdy musí být provedeno nové zhodnocení bezpečnostní situace a ověření funkčnosti bezpečnostních aktivit
získaná ocenění hodnot a bezpečnostních rizik musí být průběžně aktualizována

Závazek dodržování bezpečnostního plánu

všichni pracovníci by měli být s bezpečnostním plánem seznámeni a měla by jim být vysvětlena jeho důležitost i jejich role v rámci plánu
podstatné je, aby vedení organizace přijalo závazek, že bude poskytovat dostatečnou podporu provádění bezpečnostního plánu

Meet-in-the-middle security

tohle je můj soukromý nápad, nehledejte pod tím nic oficiálního

Každý má svůj informační systém, který je zpravidla vybaven nějakými bezpečnostními mechanismy, kterého se určitě nebude zbavovat. Proč tedy neudělat inventuru bezpečnostních mechanismů, které tyto systémy nabízejí, zatrhnout si ty, které jsou v mé konkrétní situaci relevantní, vymyslet co nejlepší nastavení a podle tohoto seznamu je zprovoznit.

Nejzákladnější bezpečnostní mechanismy:

- *systém hesel (šířeji mechanismus autentizace) a jeho nastavení*
- *autorizační mechanismus*
- *ochrana komunikace*

- *auditní záznamy systému*
- *zálohování a obnova*
- *kontrola komunikace*
- *antiviry*

Esoteričtější mechanismy:

- *Replikace dat*
- *Clustery a další mechanismy v oblasti fault tolerance*
- *IDS a IPS systémy*
- *PKI, ...*

Protože bezpečnost je ve skutečnosti spíše o lidech, vytvořte seznam nejdůležitějších procesů, ověřte, zda jsou skutečně implementovány a hlavně používány v souladu s popisem.

Nejzákladnější procesy:

- *zakládání a rušení uživatelů,*
- *změna oprávnění uživatele,*
- *řízení změn vlastního IS (change management),*
- *plánování odstávek,*
- *proces rutinní administrace,*
- *monitoring a alerting.*

Esoteričtější procesy:

- *audit systému,*
- *evaluace bezpečnostních mechanismů a předpisů.*

po tomhle jste připraveni na velký projekt. Ten by měl učinit inventuru a provést sjednocení a učesání dosaženého stavu.
Až tak prosté to je.