Ochrana informací 1

Karel Velička

6. února 2025

Beneš Antonín, RNDr., Ph.D.

Obsah

1 Úvod

Informačním systémem (IS) prostředek, který se používá ke správě svých informací

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

Zranitelnost nedostatek bezpečnostního systému.

Dopad finanční vyjádření incidentu
Celkově snaha minimalizovat investici, provozní náklady, očekávané ztráty

Komponenty bezpečnosti

- Zákony
- Normy
- Politika
- Bezepčnostní cíle
- Kontrola prostředí
- Autentizace + Autorizace
- Separace - fyzická, časová, logická, kryptografická
- Integrita, dostupnost, auditabilita

Možné hrozby

- Přerušení - šást ztracena/ nedosažitelná
- Zachycení - útočník má přístup do systému
- Modifikace - útočník může měnit
- Fabrikace - neautorizované vytvoření nového objektu

2 Řízení bezpečnostních rizik

3 Aktiva

Jakýkoliv zdroj hodnoty (hmotný/ nehmotný)
Normy GDPR, FIPS 199, SIA (Security of Information Act)

Klasifikace dat

Abychom mohli pro jednotlivé kategorie navrhnout odpovídající bezpečnostní mechanismy (ty jsou založené na kontextu, obsahu, uživateli)
U klasifikace obecných aktiv je cílem „inventurní seznam“ aktiv. Pro každou třídu se stanoví minimální sada bezpečnostních opatření.

Kategorizace dat

Seskupení typů dat na základě obdobných nároků na zabezpečení
Dělí se na kategorizace dle *senzitivity, kritičnosti (nepostradatelnosti), hodnoty*

Požadavky na nakládání s aktivy a informacemi

- Označování - viditelné etikety na zařízení značící důležitost, bezpečnostní úroveň, ... v záhlaví/ zápatí dokumentu
- Zpracování - politika, pravidla a postupy používání senzitivních dat a kritických aktiv - důležitost školení
- Uložení - lokace a zabezpečení uložených dat, šifrování, použití HW prostředků
- Deklasifikace - úorava přiřazené klasifikace - musí se dokumentovat, ideálně schválit

Role spojené se správou dat

- Vlastník - odpovědný za stanovení, jak a kým budou data používána; rozhoduje o udělení/ odebrání přístupu; plně odpovědný za data
- Regulátor - osoba/ agentura/ společnost určující účel a způsoby zpracování dat; odpovědný za dodržování principů, pravidel, legislativy
- správce - odpovědný za údržbu dat a technických prostředků zpracování
- Zpracovatel - odpovědný za nakládání s daty jménem vlastníka
- Uživatel - konzumenti dat
- Subjekt - ten, o kom data vypovídají

Správa dat

- Umístění - požadavky na geografické omezení zpracování a uložení dat
- Údržba - zpracování, analyzování a sdílení dat; řídí přístup; least priviledge prinicp
- Uchovávání - třeba stanovit pro každý typ dat
- Likvidace - zvážit schválení; třeba likvidace i nosičů (fyzicky - drcení)
- Remanence - smazaná data lze získat zpětně z nosičů; na cloud nelze zajistit - ukládat šifrovaně

Opatření pro zajištění bezpečnosti dat

- Technická - firewally, filtry, šifrování
- Administrativní - politiky, standardy, postupy
- Fyzické - stráž, recepce

4 Architektura

Systémy a aplikace procházejí fázemi - návrh, vývoj, testing, nasazení, údržba, vyřazení
Používají se obvykle konkrétní standardy ISO, STRIDE, PASTA

Obecné principy

Separace domény

Doména je soubor souvisejících komponent se společnými bezpečnostními atributy
Komunikace je omezená na kanály

Vrstvení (layering)

Hierarchické strukturování systému - vyšší závisí na nižších
Je to dekompouzice $\implies$ napomáhá srozumitelnosti, atd.

Zapozdření (encapsulating)

Objekty nezpřístupňuí data, ale metody - lepší kontrola přístupu a integrita

Redundance replikace komponent, paralelní zpracování, vyšší odolnost

Virtualizace separace; snazší zotavení

Nejmenší oprávnění (least priviledge) služby, informace dostupné na základě aktuální potřeby *(need-to-know princip)*

Attack surface (plocha pro útok) souhrn všech expozic

Hardening obecně zabezpečení - vypnutí nepotřebných služeb, odstranění standardních účtů, portů, aplikací apod.

Bezpečné výchozí hodnoty, havarování po spuštění/ havarování musí mít systém bezpečné výchozí hodnoty

Fail safe/open blokuje se přístup/ zachová se dostupnost (snaha)

Důvěra

Keep-it-simple jednoduchost...

Důvěřuj, ale prověřuj (trust but verify) ověřujte cokoliv, co přichází z vnějšího prostředí

Zero trust nevěří se ničemu; všichni jsou hrozba - všechny vstupy se validují, přístupy autentizují atd.

Bezpečnostní modely obecně

První fází tvorby bezpečného IS je volba vhodného bezpečnostního modelu. Základní požadavky bezpečnosti jsou *utajení, integrita, dostupnost, anonymita.* Předpokládejme, že umíme rozhodnout, zda danému subjektu poskytnout přístup. *Modely poskytují pouze mechanismus pro rozhodování!*

- **Jednoúrovňové modely** jsou vhodné pro případy, kdy stačí jednoduché *ano/ne rozhodování,*zda danému subjektu poskytnout přístup k požadovanému objektu a *není nutné pracovat s klasifikací dat.*
- **Víceúrovňové modely** Může existovat několik stupňů senzitivity a "oprávněnosti". Tyto stupně senzitivity se dají použít k algoritmickému rozhodování o přístupu daného subjektu k cílovému objektu, ale také k řízení zacházení s objekty. Víceúrovňový systém *"rozumí" senzitivitě dat* a chápe, že s nimi musí zacházet v souladu s požadavky kladenými na daný stupeň senzitivity. Rozhodnutí o přístupu pak nezahrnuje pouze prověření žadatele, ale *též klasifikaci prostředí, ze kterého je přístup požadován.*

Modely pro speifické účely

Chinese wall model

Dynamický model, pravidla generována až v okamžiku používání.
Konzultant nesmí radit konkurenci, ale může radit nekonkurenci.
Objekty jedné organizace tvoří *dataset*, datasety rozčleněny do *tříd* (conflict of interest classes)
Sanitizovaná informace – odstraněny ty části, které umožňují identifikovat konkrétního vlastníka
Subjekt na počátku univerzální práva (ke všem objektům)
Přístup je povolen, pokud je ve stejném datasetu/ náleží do jiné třády.
Zápis je povolen, pokud je umožněn přístup/ není čten objekt s informacemi z jiného datasetu.

Clark-Willson model

Potřebám komerčních organizací dobře vyhovuje např. Clark-Wilson model, který přejímá postupy běžné v účetnictví.

Základní principy Clark-Wilson modelu:

1. Dobře formované transakce (konzistentní data → konzistentní data)
2. Separace operací - žádnou operaci nesmí být schopen korektně provést jediný subjekt.

Pravidla modelu jsou dále rozdělena na požadavky na vynucení (E) a korektnost (C).

- E1 – Systém musí zajistit, že pouze procedury vyhovující požadavku C2 mohou pracovat s chráněnými objekty.
- E2 – Systém musí udržovat seznam relací popisující, který subjekt smí spouštět které transformační procedury a musí zajistit dodržování těchto relací.
- E3 – Systém musí autentizovat každý subjekt pokoušející se spustit transformační proceduru.
- E4 – Pouze administrátor provádějící certifikaci entit může provádět změny relací. V žádném případě nesmí mít právo spustit žádnou z procedur, které administruje.
- C1 – Všechny procedury testující validitu dat musí zajistit, že pokud doběhnou, všechna chráněná data jsou korektní.
- C2 – Všechny používané transformační procedury musí být certifikovány, že po zpracování korektních chráněných dat zanechají chráněná data opět v korektním stavu.
- C3 – Seznam popsaný v E2 musí splňovat pravidlo separace operací.
- C4 – Všechny transformační procedury musí zapisovat do append-only objektu (log) veškeré informace nezbytné pro rekonstrukci povahy provedené operace.
- C5 – Každá transformační procedura zpracovávající nechráněná data musí buď skončit s tím, že chráněná data jsou v korektním stavu, nebo nesmí provést žádnou změnu.

Obr. 1: Clark-Willson model - zdroj: Tahak_Ochrany_Informace.pdf

Take-Grant systém

Systém přidělování a odebírání oprávnění; Efektivních vyhodnocování práv (v $O(n)$)
Čtyřmi základními primitiva: *create, revoke, take, grant*

Military security model

Řazení do disjunktních kategorií utajení - *unclassified, confidental, secret, top secret*
Uplatnění least priviledge principu.

Svazový model (Lattice model)

Military je případem tohoto modelu. Uplatnění relace $\leq$. Rozdělení do kategorií podle utajení.

Graham-Denning model

popisuje proces tvorby objektů a subjektů a bezpečného přidělování oprávnění i v distribuovaném prostředí
model pracuje s množinou subjektů *S,* množinou objektů *O*, množinou práv *R* a přístupovou maticí *A*.
Každý objekt má přiřazen jeden subjekt nazývaný *vlastník,* každý subjekt má přiřazen jiný subjekt nazývaný *kontroler*.
Model definuje následující práva:

- *vytvořit objekt* - povoluje subjektu vytvořit v systému nový objekt
- *vytvořit subjekt*, *zrušit objekt*, *rušit subjekt* - obdobně jako předchozí
- *číst přístupová práva* - povoluje subjektu zjistit aktuální přístupová práva jistého subjektu k určitému subjektu
- *přidělit přístupová práva* - dovoluje vlatníku objektu přidělit jistá práva k objektu určitému subjektu
- *zrušit přístupová práva* - dovoluje vlastníku objektu resp. kontroleru subjektu odebrat danému subjektu jistá práva k objektu resp. subjektu
- *předat přístupová práva* - dovoluje subjektu předat některé ze svých práv jinému subjektu (každé oprávnění může být předatelné či nikoliv, obdrží-li subjekt předatelné právo, může jej dále předat jako předatelné či nepředatelné).

Obr. 2: Graham-Denning model

Bell-LaPadula model

Popisuje povolené přesuny informací takové, aby bylo zajištěno jejich utajení. Pro každý subjekt S a objekt O je v systému definována bezpečnostní třída $C(S)$, $C(O)$.

- *Vlastnost jednoduché bezpečnosti:* Subjekt S může číst objekt O právě tehdy, když $C(O) \leq C(S)$.
- **-vlastnost:* Subjekt S mající právo čtení k objektu O může zapisovat do objektu P právě tehdy, když $C(O) \leq C(P)$.

Obyčejně nepotřebujeme tak silná omezení, která klade *-vlastnost. Často je tato vlastnost poněkud oslabena v tom smyslu, že systém povolí zápis do objektu nižší bezpečnostní třídy, pokud zapisovaná data nezávisí na čtených údajích. Model je používán v systémech, které paralelně zpracovávají informace různého stupně utajení.

Obr. 3: Bell-LaPadula model - zdroj: Tahak_Ochrany_Informace.pdf

Biba model

Biba model je duálním modelem k Bell-LaPadula modelu. Bell-LaPadula model se vůbec nezabývá integritou dat. Nechť pro každý subjekt S a objekt O je v systému definována integritní bezpečnostní třída $I(S)$ a $I(O)$. Obdobně jako v Bell-LaPadula modelu definujeme:

- *Vlastnost jednoduché integrity:* Subjekt S může modifikovat objekt O právě tehdy, když $I(O) \leq I(S)$.
- *Integritní *-vlastnost:* Subjekt S mající právo čtení k objektu O může zapisovat do objektu P právě tehdy, když $I(O) \geq I(P)$.

Biba model se zabývá zajištěním integrity a tedy i důvěryhodnosti dat. Bezpečnostní třída entity popisuje míru její důvěryhodnosti pro ostatní. Tento model vůbec neřeší utajení dat.

Obr. 4: Biba model - zdroj: Tahak_Ochrany_Informace.pdf

5 Mechanismy

6 Sítě

Firewall

Personální firewally filtry - analýza a odstraňuje nežádoucí objekt

Aplikační firewally (proxy brány) musí existovat specializovaná „proxy“ pro každý přenášený protokol

Síťové IDS, IPS hlídá známe vzory chování odpovídající útoku (IDS - detekuje, IPS - reaguje)

Protokoly

SSL Struktura - handshake, cipher, alert, application protocol (HTTP), record, TCP, IP

IpSec dvojice nezávislých protokolů:

AH (appliation header)	integirita packetů, HMAC; MD5
ESP (encapsulated security payload)	integrita + utajení dat, HMAC blokové šifry (AES, Blowfish)

Internal Security Gateway (ISG)

- Ověřuje soulad se standardy
- Kontroluje použití očekávaných mechanism
- Hlídá hazardní operace aplikací
- Analyzuje nebezpečný kód

7 IAM

8 Provoz

9 Hodnocení

≡ vyhodnocení vlastnosti objektu (pravděpodobnost, předpokládaná velikost, ...); výstupem je report s nálezy a zkoumáním

Návrh a validace - strategie testování

Explicitní stanovení rozsahu a cílů zkoumání - jasně definovat, volit vhodnou metodologii (umožňuje srovnání)

Audit porovnání reálného stavu organizace s deklarovaným stavem (standardy, smluvní závazky, cíle).

Standardy pro audit Doporučuje se ISO/IEC 15408, ISO/IEC 27006, NIST 800-53A atd.

Interní audit

- Někým jiným než autorem politiky.
- Výhody: znalost prostředí, kultury a možnost častějšího provádění.
- Vhodný pro hledání slabin, rutinní kontroly patchů, ...
- Ideální příprava na externí audit, omezení dopadu na obchodní aktivity v případě neúspěchu auditu.

Externí audit

- Nezávislý + pohled zvenčí.
- Větší zkušenosti, ale menší znalost objektu
- Jediná možnost pro angažování dostatečně erudovaných pracovníků.

Audit třetí stranou

- Provádí zákazník/ jiný obchodní partner $\implies$ odpovědnost vlastníka
- Zaměření na provozní postupy, správa procesů, zabezpečení dat

Testování bezpečnostních opatření

Slouží k identifikaci slabých míst a rizik v systému.
Kontroly logů + kódu + testů; testování zneužití, rozhraní; analýza pokrytí testů; Simulace narušení a útoku

Hodnocení slabin

Hledat v kritických komponentách; Po nalezení provést hodnocení dopadu, relevanci a stanovit priority oprav.

Penetrační testování

Kodex etického hackera. Snaha najít známe slabiny a zmapovat dopad + rozsah. Výsledkem je report.
Obvykle - průzkum, sken, využití poznatků, průnik, report

Syntetické transakce

simulované aplikační transakce, kterými se ověřuje funkčnost cílových systémů a kontroluje se, že systém odpoví očekávanou odezvou

Shromažďování dat o bezpečnostních procesech

Založeno na průběžném monitoringu.
Cílem je hodnocení stavu a provozu bezpečnostních opatření.
Vychází z hodnocení rizik a návrhu programu bezpečnosti - díky tomu stanoví strategie tvorby a zpracování logů.
Logování + zavede se centralizace zpracování + automatizace monitoringu.
Nasazení pokročilých metod automatického vyhodnocování (trendy, clustery, AI...)

Administrativní opatření

Politika, pravidla; záznamy o obchůzkách, vydané ceritifikáty... Hodnotí se dopad politiky, efektivita ...

Správa účtů Administrativní + techická opatření

Klíčové indikátory výkonu a rizika

Je vhodné se zamýšlet nad budoucím vývojem

KPI hodnocení stávajících opatření na základě vhodných metrik

KRI povědomí o nadcházejících hrozbách a vývoji rizik
Dobré obstarávat bezpečnostní skóre (# malware, # oprav SW, neúspěšná přihlášení apod.), a sledovat návratnost investic (vyplatilo se opatření?),
Dále kontrola a schválení managementem; Kontrola shody (ISO, ...); Kontrola záloh; Školení a povědomí; Náprava chyb; Obnova po katastrofě