Systémová bezpečnost

PK-PT2 přednáška 3

České vysoké učení technické v Praze
Fakulta informačních technologií

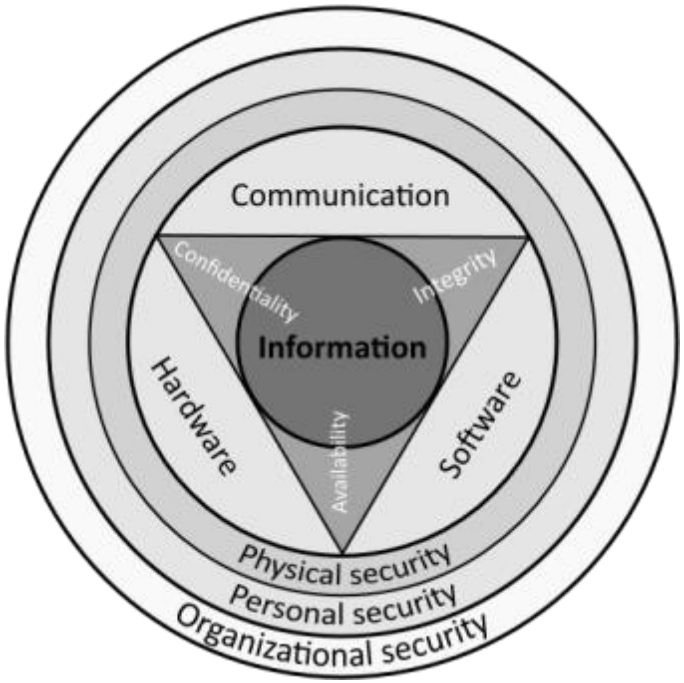
Co je to systémová bezpečnost?

- Ochrana počítačových systémů a sítí před útočníky, kteří chtějí ohrozit důvěrnost, integritu nebo dostupnost dat v systému uložených.
- Důvěrnost (Confidentiality) — k datům mohou přistupovat pouze oprávnění aktéři (lidé, procesy, atd.) a pouze takovým způsobem, jak je to očekáváno. Pokud by se o přístup pokusil neoprávněný akter, bude mu v tom zabráněno.
- Integrita (Integrity) — data jsou po celou dobu své existence úplná a přesná, nemůže dojít k jejich nedetekovanému pozměnění neautorizovanými aktéry. Neautorizovaným aktérem je v tomto smyslu i oprávněný uživatel, který ale změní data nechtěným způsobem (např. v důsledku omylu).

- Dostupnost (Availability) — data jsou oprávněným aktérům dostupná v takové kvalitě, jak mohou rozumně očekávat.
- Součástí systémové bezpečnosti je také vybudování takového prostředí, ve kterém bude možné minimalizovat dopady případných narušení bezpečnosti, až/pokud k nim dojde.

Proč "systémová" bezpečnost?

- Bezpečnost je třeba řešit na všech úrovních systému, protože tyto spolu interagují a nedostatečné řešení na jedné úrovni může ohrozit bezpečnost informací na úrovni jiné.


Communication
Confidentiality
Integrity
Information
Availability
Hardware
Software
Physical security
Personal security
Organizational security

Zdroj: [1]

Útočník

- Systémová bezpečnost předpokládá existenci útočníka.
- Útočník je osoba, proces nebo entita, která se cílevědomě snaží o narušení jedné nebo více bezpečnostních charakteristik.
- Ve srovnání s náhodným poškozením dat např. v důsledku selhání hardware musíme očekávat:
  - Činnost útočníka je cílevědomá, ne náhodná.
  - Útočník aktivně vyhledává slabá místa.
  - Útočník může zasahovat do chování různých částí systému tak, aby dosáhl svého cíle. Zejména může kombinovat slabá místa různých vrstev systému pro maximalizaci svého užitku.
    Útočník může mít i značné prostředky, nelze se spoléhat na to, že něco nezná.

- Útočníkem může být i osoba, která je jinak legitimním uživatelem systému.
- Útočníků může být více, každý s odlišnými možnostmi a cíli.
- Bezpečný systém by měl splňovat požadované charakteristiky i v prostředí s aktivními útočníky.

Bezpečnost je velmi obtížná

- Bezpečnost je nesmírně rozsáhlý koncept.
- Pro dosažení bezpečnosti je nutné zabezpečit všechno.
- Obvykle však ani neumíme rozhodnout, zda je systém bezpečný.
  - Umíme (někdy) pouze rozpoznat, že bezpečný není.
- Úvahy o bezpečnosti vycházejí z aktuálního stavu poznání a ze stanovených bezpečnostních předpokladů.

Tento stav a tyto předpoklady se ale v čase mění. Mnohdy to, co bylo považované za bezpečné, už s uplynulým časem bezpečné není.

- Nebezpečné jsou programy vs. nebezpečné je všechno.
- Politiky pro tvorbu hesel.

Bezpečnost je iterativní proces.

Řízení rizik I

- **Aktivum** je cokoliv, co organizaci přináší hodnotu a mělo by tedy být chráněno.
- **Riziko** je pravděpodobnost, že aktivum bude poškozeno nebo zničeno.
- **Hrozba** je potenciální příčina nežádoucího incidentu, který může mít za následek poškození systému nebo organizace.[2]
- **Zranitelnost** je slabé místo aktiva nebo skupiny aktiv, které může být využito jednou nebo více hrozbami.[2]
- **Opatření** je cokoliv, co odstraňuje nebo zmenšuje hrozbu či zranitelnost.
-

Dopad je vyjádření škody, kterou aktivum utrpí v důsledku úspěšně realizace hrozby.

Řízení rizik II

- **Řízení rizik** je proces, ve kterém organizace identifikuje hrozby pro svá aktiva a jejich zranitelnosti a rozhoduje se, jaká opatření přijme proto, aby došlo ke snížení rizika či jeho dopadu na přijatelnou úroveň.
  - Řízení rizik není jednorázová činnost, ale permanentní iterativní proces, ve kterém neustále iterativně zjišťujeme a vyhodnocujeme hrozby a rizika ve vztahu k měnícím se okolnostem.
  - Při rozhodování o opatřeních nelze akcentovat jen jednu vlastnost, je nutné vyvažovat přínosy a náklady každého opatření (např. na využitelnost aktiva pro jeho zamýšlený účel nebo náklady na opatření ve srovnání se způsobeným dopadem.).

Postup pro řízení rizik

1. Identifikace aktiv a stanovení jejich hodnoty.
2. Provedení analýzy hrozeb pro všechna identifikovaná aktiva.
3. Provedení analýzy zranitelností vztažených k nalezeným hrozbám.
4. Vyhodnocení nalezených zranitelností vzhledem k jejich riziku a dopadu.
5. Analýza, výběr a implementace opatření.
6. Vyhodnocení efektivity přijatých opatření.
7. Zpět na krok 1.

Standardní způsoby řešení rizik I

- Odstranění nebo zmenšení hrozby
  - Např. použití biometrie místo hesla odstraňuje hrozby spojené s heslem (uhádnutí hesla, odpozorování hesla, vylákání hesla z uživatele).
- Přesun hrozby
  - Např. využitím přihlášení pomocí Google/Facebooku/myID přesouváme hrozby spojené s autentizací na jinou společnost.
- Přijetí rizika
  - Vědomě akceptujeme riziko, např. proto, že ostatní způsoby řešení jsou dražší než očekávaný dopad.

Hlavní skupiny opatření

- Administrativní opatření
- Fyzická opatření
- Logická (technická) opatření

Administrativní opatření

- Jde o stanovení politik, standardů, postupů a doporučení, která umožní dosáhnout bezpečnostních cílů organizace.
- Zaměřují se na personál a vedení businessu, vytváří základní kostru jednání organizace.
- Mohou být interní nebo i vynucená zvnějšku (např. prostřednictvím zákonů nebo standardů).
- Zahrnují např.:
  - Politika vytváření, ukládání, využívání a ničení dat.
    - Klasifikace dat podle citlivosti.
    - Určení přístupu k nim.
  - Způsob přijímání a propouštění pracovníků.
  -
  -
  -
  -

Rozdělení povinností a zodpovědnosti, princip čtyř očí.
Vzdělávání pracovníků.
Bezpečnostní audity.
Politika čistého stolu.

Fyzická opatření

- Cílem je řízení fyzického prostředí, ve kterém jsou informační systémy umístěny, tak, aby byla minimalizována rizika.
- Zahrnuje např.:
  - protipožární systémy,
  - dveře a zámky,
  - monitorovací kamery,
  - strážní službu
- Důležité i pro jednotlivce (např. šifrování disku vs. fyzický přístup).

Logická (technická) opatření I

- Velmi rozsáhlá oblast.
- Používá softwarové a hardwarové prostředky k vynucení stanovených požadavků.
- Vyžaduje se tzv. defense in depth: Každá vrstva počítačového systému musí mít svoji vlastní sadu logických opatření, která se vzájemně překrývají a doplňují.
- Nutno počítat s tím, že každé jednotlivé opatření může být překonáno.

Logická (technická) opatření

II

- Opatření na všech úrovních:
  - Řízení přístupu k prostředkům.
  - Vhodné mechanismy pro autentizaci (kdo k prostředku přistupuje).
    - Jaké faktory autentizace se používají (hesla, čipové karty, biometrie)?
    - Jsou požadované jejich kombinace?
    - Pokud se používají hesla, jaké jsou politiky pro jejich vytváření. Zahrnutí
    - času a místa do rozhodnutí o autentizaci.
  - Vhodné mechanismy pro autorizaci (co s prostředkem smí dělat).
  - Vhodné logování a auditování kritických operací.
    - Logování ukládá informace o událostech v systému. Následně dovolí zpětně dohledat, co se v systému dělo.
    -

Logická (technická) opatření

Auditování porovnává vztahy v logovacích záznamech a hledá neobvyklé situace. Tyto mohou signalizovat pokus o zneužití.

III

- Důsledné dodržování principu nejmenších oprávnění.
  - Stanovit, jakou minimální sadu operací smí uživatel či proces provádět, aby ještě byl schopen plnit cíle organizace.
  - Stanovit, jaká minimální oprávnění musí uživatel/proces mít, aby toto operace dokázal použít.
  - Nastavit právě tato oprávnění pro všechny uživatele.
  - Nikdy nedávat uživateli administrátorská práva; pokud je musí mít, tak v rámci samostatného účtu se striktnějšími pravidly (jak na autentizaci, tak organizačních — které operace a jak je uživateli dovoleno s tímto účtem provádět).

Logická (technická) opatření IV

- Opatření na úrovni síťové infrastruktury:
  - Fyzické odpojení kritického počítače od zbytku sítě (tzv. “Air Gap”).
    - Vhodné např. pro centrální certifikační autoritu organizace. Rozdělení
  - počítačů do logických skupin podle míry citlivosti např. za použití podsítí nebo VLAN či VPN, řízení přístupu mezi nimi.
    - Uživatelské počítače by neměly být ve stejné síti jako servery.
    - Možnost využití “přestupních stanic”.
  - Firewally, proxy servery, brány.
  - IDS (Intrusion Detection System), IPS (Intrusion Prevention System).
  -

Logická (technická) opatření

Zablokování adres, portů, protokolů, které nutně nepotřebujeme.
Zahrnuje např. vynucení šifrovaných protokolů se silným nastavením kryptografie.

V

Logická (technická) opatření

- Opatření na úrovni jednotlivého počítače:
  - Heslo pro přístup do nastavení BIOS/UEFI.
  - Aktivní Secure Boot.
  - Šifrování celého disku.
  - Zvlášť šifrování nejdůležitějších dat.
  - Bezpečný operační systém.
  - Lokální antivirus.
  - Lokální firewall.
  - Automatické aktualizace pro operační systém a ideálně i pro všechny aplikace.
  - Pokud možno automatické zamykání stanice v okamžiku, kdy u ní uživatel není přítomen.

Logická (technická) opatření

VI

- Vyřešené zálohování a archivace.
  - Důležité jak pro servery, tak pro koncové stanice.
  - Účelem zálohování je ukládat data tak, aby mohla být v případě ztráty obnovena.
  - Účelem archivace je ukládat historická data pro případ, že by byla někdy potřeba → menší nároky než u zálohování.
  - Zálohy by měly být ukládány jinam, než kde leží originální data, pro případ selhání zdrojového systému.
  - Pozor na zajištění ochrany důvěrnosti a integrity samotných záloh! U záloh je nezbytné mít ověřené postupy pro obnovu a tyto postupy dále pravidelně testovat!

Logická (technická) opatření

RAID není záloha, i když dokáže ochránit data před některými typy poškození!

Reakce na incidenty

- Součástí systémové bezpečnosti je také připravený plán reakce na incident.
- Legislativa může takový plán vyžadovat a může určovat některé jeho kroky (např. hlášení incidentu NÚKIBu).
- Plán se aktivuje v okamžiku, kdy bylo detekováno narušení bezpečnosti.
- Může zahrnovat:
  - Založení a udržování týmu lidí, kteří budou na incident reagovat.
  - Popis reakce v případě podezření na incident.
  - Popis okamžitých kroků v případě potvrzeného incidentu. Snahou je co nejrychleji zastavit případný dosud trvající incident, identifikovat a

izolovat napadené systémy a přitom zachovat informace, které budou potřeba pro úplné vyšetření incidentu.

- Odstranění aktivních činitelů incidentu (např. smazání nainstalovaného malwaru nebo aktualizace zranitelné služby, která útok umožnila).
- Kontrola a návrat systémů do běžného provozu.
- Poučení do budoucna.

Literatura I

Bakni M.: *Information Security, CIA triad. Confidentiality, Integrity, Availability. Second version*, Wikipedia, 2022, https://en.wikipedia.org/wiki/File:CIAJMK1209-en.svg.

ISO/IEC 27002: *Information technology — Security techniques — Code practice for information security management*, 2005.