# Bezpečnosť informačných systémov a TMN





## Čo by malo byť chránené

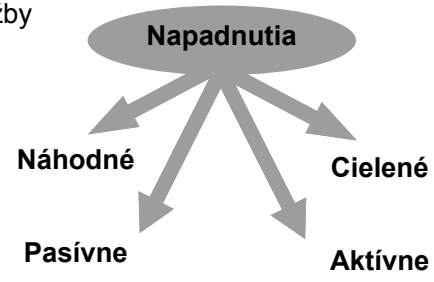
- Informácie a dáta
- Komunikačné služby a služby spracovania dát
- Zariadenia





## Možné napadnutia dátového komunikačného systému

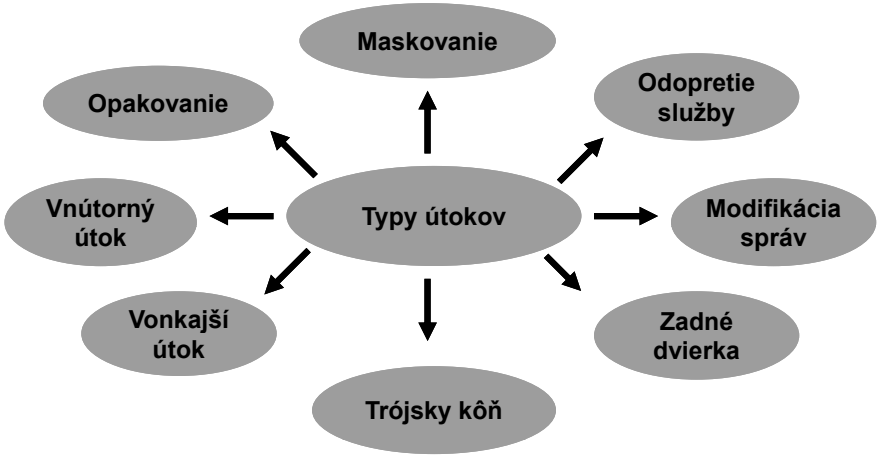
- Zničenie informácie alebo iných zdrojov
- Narušenie alebo modifikácia informácie
- Krádež, zmazanie alebo strata informácie alebo iných zdrojov
- Prezradenie informácie
- Prerušenie služby








## Typy útokov



# Ochrana pred vnútorným útokom

- Dôkladná kontrola zamestnancov
- Skúmanie technického vybavenia, programového vybavenia, bezpečnostnej politiky a konfigurácie systému
- Pravidelné kontroly na zvýšenie možnosti detekcie prípadných útokov





# Techniky používané pri vonkajších útokoch

- Priame pripojenie na vedenie (aktívne alebo pasívne)
- Rušiace emisie (napr. elektromagnetické rušenie)
- Vydávanie sa za autorizovaného používateľa systému (maskovanie) alebo za komponent systému
- Obídenie kontroly prístupového mechanizmu





# Bezpečnostná politika

Prvým krokom na zisťovanie bezpečnostných útokov je odhadnutie bezpečnostných rizík.

**Predpokladanie napadnutí zahŕňa**

- Identifikovanie zraniteľných miest systému
- Analyzovanie pravdepodobnosti napadnutia s cieľom využiť zraniteľné miesta
- Stanovenie dôsledkov, ak napadnutie bude úspešné
- Odhadnutie nákladov každého útoku
- Vyčíslenie nákladov potenciálnych protiopatrení
- Výber bezpečnostného mechanizmu, ktorý obsiahne všetky požiadavky





# Bezpečnostná politika *(pokr.)*

Pre stanovenie bezpečnostnej politiky je potrebné vypracovať *Analýzu bezpečnostných rizík*.

***Analýza bezpečnostných rizík***

Postupnosť krokov:

1. Vykonanie ohodnotenia rôznych typov útokov.
2. Určenie potenciálnych rizík podľa jednotlivých bezpečnostných útokov.
3. Určenie priorít, ktorým rizikám sa treba venovať a ako často.
4. Vypravovanie *Správy o odhade rizík*.

# Správa o odhade rizík

**Tvorí základ pre ďalšie analýzy bezpečnostných rizík, každé riziko je ďalej vyhodnocované s cieľom určiť:**

- pravdepodobnosť, že slabina bude odhalená,
- náklady a vynaložené úsilie potrebné na odstránenie slabiny,
- potenciálne výhody získané votrelcom z využitia slabiny,
- potenciálne škody pre firmu a jej zákazníkov.

- ***Výstup analýzy rizík*** by mal poskytovať dostatok informácií pre návrh ***bezpečnostných prístupov*** na zisťovanie útokov a minimalizovanie bezpečnostných rizík.
- Bezpečnostný prístup by mal obsahovať ***bezpečnostný profil*** pre jednotlivé aplikácie na TMN rozhraniach.
- Profil obsahuje množinu požiadaviek, ktoré sú považované za dôležité a potrebné pre zisťovanie útokov a minimalizovanie rizík.





# Bezpečnostné mechanizmy

## Všeobecné bezpečnostné mechanizmy:

1. Identifikácia
2. Autentifikácia
3. Riadenie prístupu
4. Utajenie
5. Integrita
6. Neodmietnuteľnosť
7. Bezpečnostný audit





# Požiadavky na identifikáciu

- TMN má poskytovať adekvátne možnosti pre identifikáciu TMN používateľov. Tieto možnosti môžu byť vyžadované na podporu overiteľnosti všetkých činností používateľov a aktivít siete a na podporu mechanizmov pre autentifikáciu a riadenie prístupu.

- **Základné bezpečnostné požiadavky pre identifikáciu:**
  - používateľ siete má mať globálne jednoznačné meno (alebo používateľské ID) pre účely identifikácie z dôvodu podpory individuálnych kont a auditu,
  - TMN musí pri komunikácií cez domény, alebo jurisdikčné hranice posielať meno používateľa a identifikátor TMN.





# Požiadavky na autentifikáciu

- TMN má umožňovať adekvátne overenie totožnosti používateľov.

- Požiadavka na autentifikáciu je povinná v prípade, ak sa používa komutovaná sieť.

- V prípade realizácie prostredníctvom prenajatej siete v rozsahu koniec-koniec môže byť autentifikácia vyžadovaná voliteľne .

# Požiadavky na autentifikáciu

- TMN musí byť schopná zabezpečiť autentifikáciu používateľov.
- TMN nesmie podporovať mechanizmy, ktoré by umožňovali obídenie autentifikácie.
- Dôvernosť všetkých tajných autentifikačných informácií musí byť chránená TMN .
  - V prípade, že sú autentifikačné informácie uložené interne v TMN, musia byť chránené pred neautorizovaným prístupom.
  - Niektoré autentifikačné informácie (napr. heslo) nesmú byť prístupné v čistej textovej podobe, dokonca ani pre používateľov s najvyššou prioritou.





# Požiadavky na autentifikáciu

- Každý používateľ TMN musí mať jedinečnú autentifikačnú informáciu.
- Autentifikačná informácia nesmie byť posielaná v čistej textovej podobe v rámci TMN, alebo medzi TMN, okrem prípadu, keď je to nariadené príslušným autentifikačným mechanizmom.
- Integrita všetkých interne uložených autentifikačných informácií musí byť chránená TMN.
- TMN musí byť schopná zabezpečiť dôkladnú autentifikáciu používateľov, ktorí požadujú vykonanie “kritických” administračných a OAM&P operácií.
- TMN musí byť schopná obsiahnuť a podporovať autentifikačné schémy vrátane tých, ktoré sú založené na jednoduchých bilaterálnych dohodách, využití autentifikačných serverov tretích strán, ako aj tie, ktoré sú založené na jednoduchom hesle.





# Požiadavky na riadenie prístupu

- TMN musí mať možnosti na riadenie (povolenie, alebo zamietnutie) prístupu k rôznym telekomunikačným zdrojom na základe správne autentifikovaných používateľských identít.
- Požiadavky na využitie procedúr riadenia prístupu závisia na aktuálne ponúkanej manažmentovej službe.





# Riadenie prístupu znamená

- TMN nesmie:
  - umožniť používateľovi prístup k žiadnemu systému, alebo sieťovému zdroju, pokiaľ nie je správne identifikovaný a autentifikovaný.
- TMN musí:
  - poskytovať možnosti na riadenie prístupu k zdrojom TMN na všetkých úrovniach.
  - byť schopná podporovať riadenie prístupu pre rôzne triedy používateľov, vrátane individuálnych používateľov, skupín a proxy.
  - mať možnosť chrániť prístup k zdrojom založený na ľubovoľnej kombinácií zdrojovej entity, adresy žiadateľa, požadovanej operácie, cieľovej entity, adresy, ako aj autorizačného profilu.
  - TMN musí byť schopná obsiahnuť a podporovať mechanizmy na poskytnutie, alebo zamietnutie prístupu na základe ľubovoľnej kontextuálnej informácie (napr. čas).
  - TMN musí byť schopná riadiť prístup k aplikáciám, ktoré ovplyvňujú smerovanie, konfiguráciu a riadenie toku.

# Požiadavky na utajenie

Požiadavky na utajenie majú byť podporované z dôvodu zaručenia, že dôverné informácie nie sú prezradené.

**Základné požiadavky na utajenie zahŕňajú:**

- schopnosť TMN zakódovať citlivé informácie prenášané v rámci TMN, alebo medzi TMN sieťami, ako aj citlivé informácie uložené interne v TMN,
- schopnosť TMN podporovať end-to-end dôverný prenos údajov v rámci, alebo medzi TMN,
- schopnosť TMN zakódovať citlivé informácie v prípade použitia všesmerovej technológie,
- schopnosť TMN podporovať bezpečnú distribúciu a manažment kľúčov.





# Požiadavky na integritu

- TMN musí byť schopná spoľahlivo asociovať ľubovoľný sieťový zdroj (údaj, proces) s jeho pôvodcom/vlastníkom.
  *(Okrem špecifického prípadu, keď musí byť zaručená anonymita používateľa).*
- TMN musí spoľahlivo asociovať komunikačné dáta s ich pôvodcom.
- TMN musí byť schopná zabezpečiť end-to-end integritu dátovej komunikácie v rámci aj mimo TMN.
- TMN musí poskytovať mechanizmy na ochranu proti opakovaným útokom.
- TMN musí chrániť integritu TMN dát.





# Požiadavky na bezpečnostný audit

- TMN má poskytovať prostriedky na overenie korektnosti bezpečnostných mechanizmov (napr. aktivovanie bezpečnostných záznamov).
- Bezpečnostný záznam (*log*), bezpečnostný audit, ako aj iné bezpečnostné funkcie poskytované v rámci TMN nesmú byť negatívne ovplyvnené reinicializáciou systému.





# Manažment bezpečnosti

- TMN musí poskytovať adekvátne možnosti umožňujúce zisťovanie, audit, detegovanie a analyzovanie aktivít v reálnom čase tak, aby mohli byť včas vykonané potrebné opatrenia.
- Pre potreby bezpečnostného auditu je potrebné zaznamenávať udalosti, ktoré majú vzťah k bezpečnosti do bezpečnostných záznamov.

# Manažment bezpečnosti

**Hlavné zásady:**

- Bezpečnostné záznamy majú byť vytvorené a spravované vo vnútri TMN
- Bezpečnostné záznamy majú byť chránené pred neoprávneným prístupom a ich modifikácie nemajú byť povolené





# Manažment bezpečnosti

**Hlavné zásady** *(pokr.)* **:**

- Bezpečnostné záznamy majú uchovávať minimálne nasledovné udalosti:
  - *neúspešné pokusy o autentifikáciu,*
  - *všetky typy neoprávnených pokusov o prístup k zdrojom TMN,*
  - *zmeny prístupových práv používateľov,*
  - *reinicializácia,*
  - *vymazanie záznamu,*
  - *zmeny bezpečnostných atribútov prináležiacich TMN zdrojom.*





# Manažment bezpečnosti

**Hlavné zásady** *(pokrač.):*

- Pre každú zaznamenanú udalosť má bezpečnostný záznam obsahovať minimálne nasledovné parametre:
  - *dátum a čas udalosti v UTC (Universal Time Coordinated),*
  - *dentifikácia používateľa vrátane sieťovej adresy (ak je známa),*
  - *typ udalosti,*
  - *meno sprístupneného TMN zdroja,*
  - *úspešnosť/neúspešnosť udalosti,*
- Zaznamenávanie zrejmých narušení bezpečnosti a zaznamenávanie “normálnych” udalostí, ako je prihlásenie sa do systému.





# Hlásenie poplachov

- Bezpečnostné poplachy sú typy hlásení o udalostiach, ktoré by mali byť vždy zaznamenané.
- Hlásenie o bezpečnostných poplachoch slúži na upovedomenie entity o narušení, alebo predpokladanom narušení bezpečnosti.

# Hlásenie poplachov *(pokr.)*

**Platí:**

- TMN má poskytovať mechanizmus na upovedomenie (alarm, on-line správa) administrátora, ak sa nepodarí zaznamenať udalosť, ktorá má byť zaznamenaná.
- Upovedomenie o takomto zlyhaní by malo byť realizované v reálnom čase.
- TMN má tiež poskytovať možnosti na uchovanie informácií pre potreby auditu na pamäťové médium, aby nedošlo k ich prepísaniu.





# Administratívne požiadavky

**TMN má poskytovať:**

- Mechanizmus ktorý umožní administrátorovi zodpovednému za bezpečnosť:
  - v ľubovolnom okamžiku zobraziť všetkých aktívnych používateľov,
  - nezávisle a selektívne prehliadať operácie požadované ľubovoľným používateľom, vrátane privilegovaných používateľov, na základe jedinečnej identity používateľa,
  - blokovať špecifickú komunikačnú cestu prostredníctvom ovládania portov smerovačov a im podobných zariadení,
  - zakázať identifikácie používateľov, ktoré neboli počas špecifikovaného času použité,
  - resetovať autentifikačné informácie používateľov, alebo zrušiť používateľské kontá.





# Administratívne požiadavky

**TMN má poskytovať (pokr.):**

- Mechanizmus na automatickú aj manuálnu kontrolu zahltenia, aby sa zabránilo útokom na zamietnutie služby, (napr. medzinárodné záplavové útoky, ktoré môžu postihnúť TMN generovaním množstva žiadostí na operácie a odpovede),
- Mechanizmus ktorý v prípade zlyhania bezpečnosti poskytuje možnosti na opravu a obnovenie funkcionality OAM&P sieťových služieb, napr. poskytnutím schopností na obnovenie a reinicializáciu sytému,





# Administratívne požiadavky

**TMN má poskytovať (pokr.):**

- Možnosti na generovanie alarmov pre špeciálne bezpečnostné udalosti, vrátane narušenia integrity (napr. opakovania) a fyzického narušenia,
- Administrátorovi zodpovednému za bezpečnosť nástroje na analýzu zozbieraných informácií pre účely auditu, ktoré môžu generovať mimoriadne správy, súhrnné správy a detailné správy o špecifických položkách siete a používateľoch,
- Ochranu nástrojov pre operátora pred neoprávneným prístupom.

# Manažment kľúčov

- Bezpečnosť je založená na dostupnosti a používaní kľúčov na zakódovanie dát.
- Manažment kľúčov zahŕňa generovanie, uchovávania, distribúciu, rušenie, archivovanie a používanie materiálov týkajúcich sa kľúčov a bezpečnostnej politiky.
- Manažment kľúčov predstavuje kritický prvý krok v poskytovaní a zaisťovaní spoľahlivosti bezpečnostných služieb.





# Minimálne požiadavky kladené na manažment kľúčov

- Spravovanie materiálov týkajúcich sa kľúčov počas celej ich životnosti, aby sa zabránilo ich neoprávnenému odhaleniu, modifikovaniu, alebo výmene,
- Distribúciu materiálov, týkajúcich sa kľúčov s cieľom zabrániť nekompatibilite šifrovacích zariadení,
- Zaručenie integrity materiálov, týkajúcich sa kľúčov počas všetkých fáz ich existencie, vrátane ich generovania, distribúcie, uloženia, zadávania, použitia a zničenia,
- Obnovenie v prípade zlyhania procesov manažmentu kľúčov, keď je integrita materiálov týkajúcich sa kľúčov diskutabilná.





# Havarijný plán

- Určuje, čo robiť po odhalení útoku (bezpečnostného incidentu) a ako postupovať, aby sa udržala kontinuita činnosti organizácie.
- Určuje miesta skladovania a počty náhradných dielov, miesta skladovania a spôsob organizácie záloh dát, obsah pohotovostného skladu technických a softvérových náhrad, metodiku určovania aktuálnosti stavu skladov dát, softvéru, hardvéru a metodiku aktualizácie a testovania hardvéru.





# Havarijný plán

Súčasťou havarijného plánu sú návody, ako postupovať po zistení útoku:

**1. Plán činnosti po útoku**

- Je súborom akčných plánov pre rôzne situácie, (podľa typu straty vybavenia).
- Po vyriešení incidentu je treba prijať záver:
  - či bol plán činnosti po útoku riešiteľom dostupný,
  - či bol efektívny,
  - čo robiť nabudúce inak
  - či je potrebné plán modifikovať.

# Havarijný plán

**2. Priebeh reakcie na incident**

- Ako prvé reagujú ***„tímy prvej reakcie“*** - majú plán činnosti v stave núdze (zoznam adries, tel. čísiel).
- Potom nastupujú ***„tímy pre riešenie incidentu“*** – majú smernice definujúce postupy riešenia.
- Ako tretie nastupujú ***tímy pre obnovu*** – uvedú systém do štandardného stavu.





# Plán obnovy

- Musí obsahovať kritéria definujúce:
  - čo sa chápe ako havária,
  - zodpovednosť za aktiváciu obnovy,
  - zodpovednosť za aktiváciu čiastkových činnosti podľa plánu obnovy
  - návody k vykonaniu činností podľa plánu obnovy.





# Plán obnovy

**Zásady pre plán obnovy:**

- Je potrebné vykonať segmentáciu informačných zdrojov podľa priority obnovy, napr.:
  - obnova činnosti najkritickejších systémov do 30 min,
  - obnova činnosti všetkých kritických systémov do 120 min,
  - obnova činnosti všetkých systémov do 24 hod.
- Vyhodnocovanie kritickosti a priority viacužívateľských aplikácií sa vykonáva aspoň raz za rok – vypracovávajú sa zoznamy kritických aplikácií triedených podľa priority obnovy





# Plán obnovy

**Zásady pre plán obnovy** *(pokr.)***:**

- Vypracovanie plánu činnosti organizácie v stave núdze
- Udržovanie „tímov prvej reakcie“ v pohotovosti
- Definovanie činnosti pri podozrení na prienik do systému
- Zavedenie (udržovanie a pravidelné testovanie) varovného systému informujúceho o podozrení na prienik útočníka či iné narušenie bezpečnosti
- Archivovanie

# Plán obnovy

**Zásady pre archiváciu:**

- Zavedenie periodicity archivácie dát – rotácia archivačného média
- Zavedenie systému prístupu k archívnym kópiám – koncový užívateľ nemôže mať možnosť využiť archivačný systém
- Musí byť zavedený systém evidencie archivačných kópií
- Ošetrenie problematiky archivácie dát na mobilných počítačoch – potreba vykonať archiváciu pred cestou
- Ekonomická efektivita archivácie – cena za vyhotovenie kópie vs. hodnota stratených informácii
- Zálohovanie dokumentácie (manuálov)