Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Bezpečnosť prevádzky

Erik Saller, Ivan Oravec

KPMG
cutting through complexity™

Obsah

- Rozsah bezpečnosti prevádzky
- Význam a základy ochrany proti škodlivému kódu
- Narábanie s pamäťovými médiami
- Zálohovanie a obnova
- Redundancia sieťovej infraštruktúry
- Logovanie a monitoring bezpeč. incidentov
- Používanie mobilných zariadení a vzdialená práca
- Bezpečná správa IKT

Rozsah bezpečnosti prevádzky a vzťahy s inými oblasťami

Rozsah bezpečnosti prevádzky

- Kontroluje spôsoby, akými je k dátam pristupované a ako sú spracovávané
- Zaisťuje kontrolu nad hardvérom, médiami, rolami operátorov a administrátorov, ktorí majú prístup k zdrojom
- Pre všetky dátové centrá, serverové miestnosti a operačné výpočtové strediská

Aktivity v rámci bezpečnosti prevádzky

- Riadenie prevádzky
- Manažment problémov
- Manažment úrovne služieb
- Aplikačná podpora
- Manažment kapacít a výkonu
- Riadenie zmien
- Konfiguračný manažment
- Kontrola nad softvérom a jeho distribúcia
- Spoľahlivosť a kontinuita prevádzky

Rozsah bezpečnosti prevádzky a vzťahy s inými oblasťami (pokr.)

Požiadavky na bezpečnosť prevádzky

- Ochrana zdrojov – ochrana výpočtových zdrojov organizácie pred stratou a kompromitáciou
- Kontrola nad privilegovaným prístupom – používatelia na sieti majú určitú úroveň prístupu
- Kontrola nad hardvérom – riziko útokov priamo na hardvér

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Rozsah bezpečnosti prevádzky a vzťahy s inými oblasťami (pokr.)

Ochrana zdrojov

- Redukcia zraniteľností, ktoré by mohli viesť ku kompromitácii dostupnosti, integrity a dôvernosti
- Vyváženie používateľskej prístupnosti s potrebou kontroly nad používateľskými právami
- Zabezpečenie zosúladenia s legislatívnymi požiadavkami a priemyselnými normami
- Ochrana zdrojov dátového spracovania

KPMG
cutting through complexity™

Rozsah bezpečnosti prevádzky a vzťahy s inými oblasťami (pokr.)

Kontrola nad privilegovaným prístupom

- Používateľ s privilegovaným prístupom má možnosť modifikácie kontroly prístupu, auditných logov a detekcie incidentov

Kontrola nad hardvérom

- Nielen fyzická a softvérová bezpečnosť je dôležitá
- Neautorizované pripojenie zariadenia k procesoru, alebo k telekomunikačnej linke môže vystaviť dáta neautorizovanému vyzradeniu
- Prístup k systémovým zdrojom je definovaný operačným systémom, ale zariadenia pripojené k tomuto systému môžu tiež umožniť útočníkovi prístup

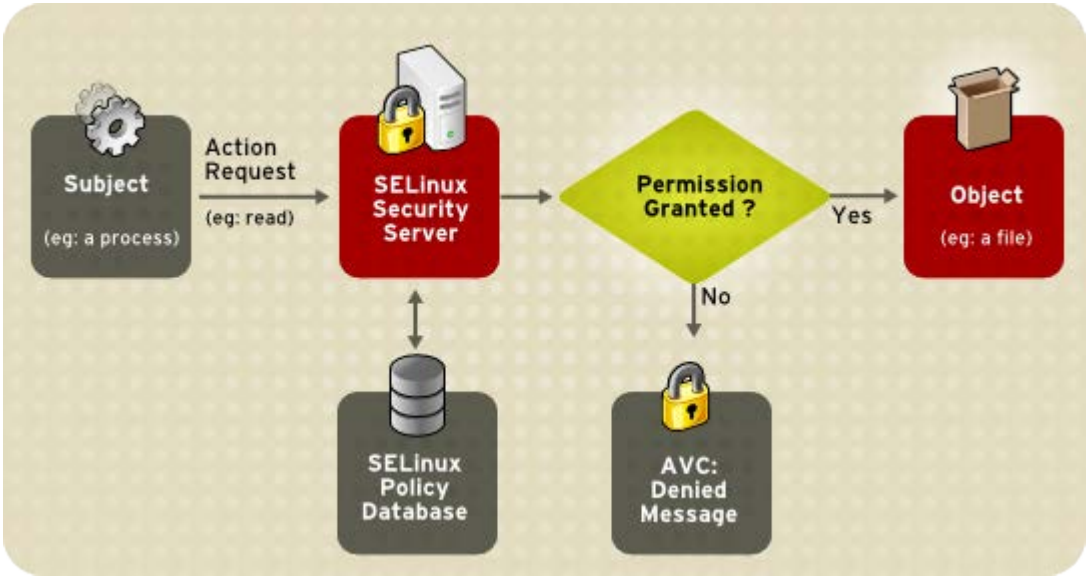
Príklady konkrétnych riešení a technológií

Selinux

- Riadenie prístupu na úrovni operačného systému

- Požiadavka na sprístupnenie zdroja je najprv posudzovaná oproti bezpečnostnej politike

- V prípade, že sú podmienky splnené => objekt sprístupnený



Rozsah bezpečnosti prevádzky a vzťahy s inými oblasťami (pokr.)

Spoľahlivá obnova

- Udržovanie bezpečnostných a zaznamenávacích (accounting) vlastností systému s ohľadom na chyby a prerušenia v prevádzke

Počítačová inštalácia

- Akýkoľvek systém ktorý podporuje jeden, alebo viac biznis aplikácií
- Akejkoľvek veľkosti, od najväčšieho sálového počítača, cez inštalácie stredného rozsahu až po skupiny osobných počítačov
- Bežiace v špecializovaných prostrediach (dátové centrum), alebo v bežných pracovných prostrediach (kancelárie, fabriky, sklady)
- Používajú ľubovoľný operačný systém, IBM MVS, Digital VMS, Windowsový, alebo Unixový

Prevádzka informačných systémov

Pokrytie biznis procesov operáciami IS:

- Manažment operatívy
- Manažment služieb IT
- Podpora infraštruktúry
- Monitoring používania zdrojov
- Technická podpora/Helpdesk
- Procesy zmenového manažmentu

Prevádzka informačných systémov (pokr.)

Pokrytie biznis procesov operáciami IS (pokr.)

- Systémy manažmentu programových knižníc
- Softvér na kontrolu knižníc – integrita spustiteľných súborov a zdrojových kódov
- Manažment verzií
- Overenie kvality
- Riadenie bezpečnosti informácií uložených na médiách

Monitorovanie a plánovanie kapacít systémových zdrojov

- Procesy riadenia incidentov
- Manažment problémov
- Detekcia, dokumentácia, kontrola, riešenie a reportovanie abnormálnych udalostí

Oddelenie vývojového, testovacieho a produkčného prostredia

- Kontrola nad používanými IKT a spôsobom spracovania dát
- Riziko neautorizovaných úprav softvéru
- Udržovanie IKT v konzistentnom stave
- Segregácia rolí - každú z týchto funkcií by mali realizovať iné entity/roly

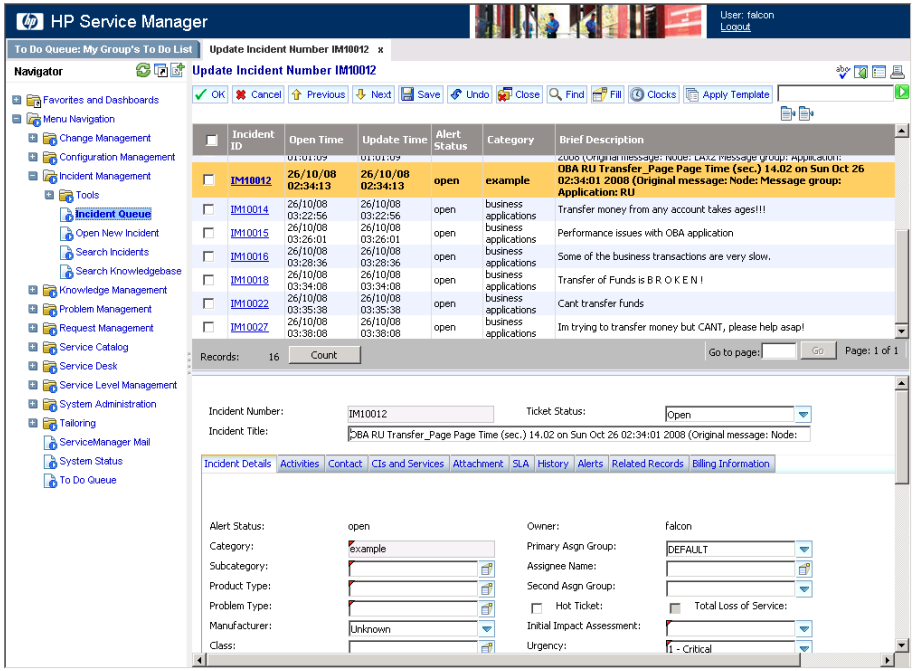
Procesy riadenia zmien

- Vedenie záznamov o systémoch, prevádzke a zmenách
- Zadávanie žiadostí
- Posudzovanie žiadostí
- Aktualizácia dokumentácie
- Príprava prác, načasovanie a operačné inštrukcie
- Konverzia dátových formátov (centrálne úložisko dát)
- Konverzia systémov

Príklady konkrétnych riešení a technológií

Nástroje automatizácie manažmentu služieb (HP ITSM)

- Integruje a automatizuje manažment služieb a kontrolu kvality
- Podporuje používateľský self-support (bez toho, aby používateľ musel kontaktovať prvú líniu podpory vie si vyriešiť rôzne problémy sám)
- Reportovacie funkcie efektivity služieb



Komponenty IKT

Back-endové zariadenia

- Print server
- File server
- Aplikačné servery
- Web servery
- Proxy servery
- Databázové servery
- Špecializované zariadenia (appliances), ktoré môžu existovať nepovšimnuté (wifi smerovače ...)

Komponenty IKT (pokr.)

Prenosné zariadenia

- USB zariadenia
- Pamäťové karty/dátové nosiče
- RFID čipy pre prístup do priestorov

Význam a základy ochrany proti škodlivému kódu

Antivírusové systémy

- Zavádzané naprieč celou organizáciou
- Spoľahlivosť a kvalita detekcie - pravidelne aktualizované databázy signatúr
- Samé o sebe nestačia, nevyhnutné sú tiež systémy riadenia prístupu

Správanie používateľov pri používaní bežných služieb – web, mail

- Ochrana proti vyzradeniu citlivých informácií (proti phishingu)
- Sociálne inžinierstvo ako cesta najmenšieho odporu

Význam a základy ochrany proti škodlivému kódu (pokr.)

Význam zálohovania, zálohovanie a obnova vlastných súborov pre používateľov

- Zálohovanie kritických dát
- Re-inštalácia systému

Význam redundancie kritických komponentov

- Záleží od kritickosti biznis procesu, ktorý tento prvok IKT pokrýva

Narábanie s pamäťovými médiami

Používanie prenosných pamäťových médií

- Riziká použitia pamäťových kariet/dátových nosičov – vírusy, škodlivý softvér, dátové úniky a straty, poškodenia dát
- Obrana: Šifrovanie, vzdelávanie personálu, zamkýnanie obrazovky, bezpečné mazanie, vedenie protokolu o vrátení aktív

Likvidácia pamäťových médií

- Keď bezpečné zmazanie nestačí pri klasifikovaných/kritických dátach
- Skartovacie stroje podľa stupňa klasifikácie utajovaných skutočností

Narábanie s pamäťovými médiami (pokr.)

Transport pamäťových médií a dát vo všeobecnosti

- Berieme do úvahy stupeň utajenia/množstvo prenášaných dát/ časovú aktuálnosť
- Nezabúdajme na papierové dokumenty/mikrofilmy/magnetické médiá/ CD a DVD/ pásky
- Ide o neautorizované použitie tlačív, krádež identity

Špecifické hrozby používania mobilných zariadení a vzdialenej práce

- „Cudzie“ zariadenia (inteligentné telefóny, súkromné laptopy, ...) sa vyskytujú stále viac
- Detekcia neautorizovaných zariadení, blokovanie pripojenia k sieti
- Stále viac zamestnancov chce pristupovať z týchto zariadení do siete => **zákaz nie je riešenie**
- Šifrovanie prenášaných a ukladaných dát (VPN riešenia)

Potreba a význam aktualizácie IKT

Aktualizácia softvéru

- Pravidelná publikácia informácií o nových zraniteľnostiach IKT
- Neaktualizovaný softvér -> ľahko získateľný neautorizovaný prístup
- Dôveryhodné zdroje softvéru a aktualizácií
- Obmedzenia práv na inštalovanie nového softvéru
- Testovanie aktualizácií

Potreba a význam aktualizácie IKT (pokr.)

- Zraniteľnosti v softvéri často využívajú aj vírusy a malware vo všeobecnosti
- Detekcia backdoorov a malware je problematická
- IDS/IPS na detekciu vzorov správania

Centrálna správa a politiky antivírusovej ochrany

- Najnovšie digitálne signatúry vírusov
- Kontrola mailových príloh a sťahovaných súborov
- Antivírusové riešenia sa dopĺňajú s politikou obmedzení v prístupe k systémovým zdrojom a kontrolou médií

Zálohovanie a obnova

Typy záloh

- Základné otázky pri voľbe: ako **často**, aký **obsah** a **kam** chceme zálohovať?
- Časový ohľad na dáta
- Čas potrebný na zálohovanie („backup window“) a obnovu („data horizon“)

Zálohovanie a obnova (pokr.)

Plné zálohy

- Celý disk
- Systémové aj dátové časti
- Vyžaduje priestor
- Poskytuje najviac redundancie a najrýchlejšiu obnovu
- Dobrý spôsob ako alternatíva k zrkadleniu (mirroring)

Zálohovanie a obnova (pokr.)

Inkrementálne zálohy

- Všetky také súbory, ktoré sa zmenili od poslednej **inkrementálnej** zálohy
- Na obnovu z inkrementálnych záloh je potrebná posledná plná + reťaz inkrementálnych
- Inkrementálna != diferenčná záloha , pretože nezálohuje všetko, čo sa zmenilo od poslednej **plnej** zálohy
- Snapshotovanie výrazne urýchľuje obnovu (napr. Acronis True Image na klientských, rsyncové zálohy pomocou rsnapshot na linuxových systémoch)

Zálohovanie a obnova (pokr.)

Diferenčné zálohy

- Všetky dáta, ktoré sa zmenili od poslednej **plnej** zálohy
- Na ich obnovu je potrebná posledná **plná** záloha **a** stačí posledná **diferenčná**

Zálohovanie a obnova (pokr.)

Frekvencia zálohovania

- Menia sa podľa prostredia a druhu dát
- Napr. kompletná záloha raz za týždeň a potom inkrementálna záloha raz za noc pre každý produkčný systém

Špecifické požiadavky na zálohovanie rôznych systémov (aplikačných, databázových)

- Kontinuálne zálohy = databáza všetkých zálohovaných súborov a ich lokalizácia na médiu

Zálohovanie a obnova (pokr.)

Problematika získania konzistentného obrazu zálohovaného systému

- Záleží od použitého druhu zálohovania
- Snapshotovanie nezálohuje nič, pokiaľ sa v systéme nič nezmení

Testovanie záložných médií

- Testovanie súborového systému záložného média

Zálohovanie a obnova (pokr.)

Ukladanie a ochrana záložných médií

- Lokalita úložiska záložných médií ovplyvňuje rýchlosť obnovy

- Lokálne zálohy rýchle na obnovu, ale je tam riziko problematického zotavenia po havárii (požiar, záplavy, zemetrasenia, ...)

Zálohovanie a obnova (pokr.)

Ukladanie a ochrana záložných médií (Pokr.)

- Preto: zálohovanie do vysunutých lokalít
- Napojenie na pult centralizovanej ochrany
- Prijateľné podmienky (teplota, vlhkosť, ...)
- Požiarna a vodná ochrana (požiaru-vzdorná konštrukcia, detekcia požiaru, alarm, požiarne sprchy: sprinklery, napojenie na lokálnu požiarnu stanicu)
- Vysunutá lokalita musí byť dostatočne vzdialená (aby nedošlo k tej istej havárii ako má lokalita z ktorej zálohujeme)
- Poučený personál pripravený zasiahnuť

Zálohovanie a obnova (pokr.)

Testovanie postupov obnovy zo zálohy

- Pravidelná obnova do testovacieho prostredia

Redundancia diskového priestoru

Redundancia diskového priestoru

- Duplicitné kópie (produkčných) dát
- Chyba na disku teda (pri použití správnej konfigurácie) nespôsobí poškodenie kritických dát ani ich nedostupnosť

Diskové polia

- Softvérové RAID-ové polia – pomalé vstupno-výstupné operácie
- Hardvérové RAID-ové polia – využívajú vlastný kontrolér, ktorý riadi ukladanie dát

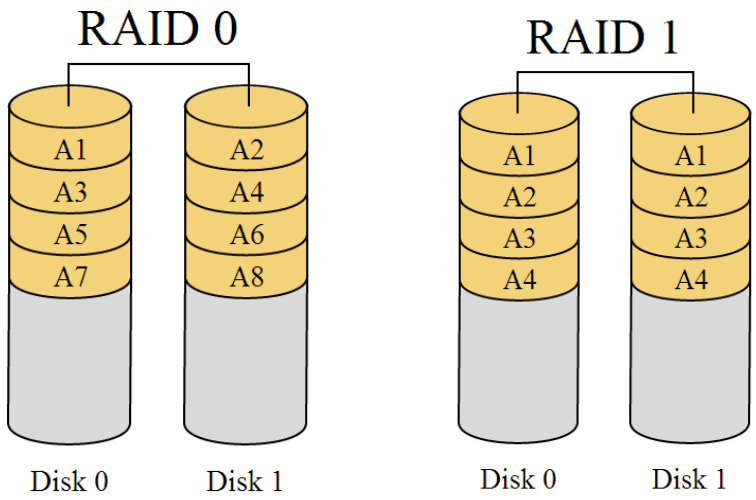
Redundancia diskového priestoru (pokr.)

RAID 0

- „just a bunch of disks“
- RAID 0 = žiadna redundancia, iba zdieľanie spoločného dátového priestoru
- **Lineárne zreťazenie** – jeden disk sa postupne zaplní, potom sa pokračuje na druhom
- Alebo **striping** („prekladanie“ dát) – cyklicky sa dáta ukladajú a potom čítajú z rôznych diskov

RAID 1

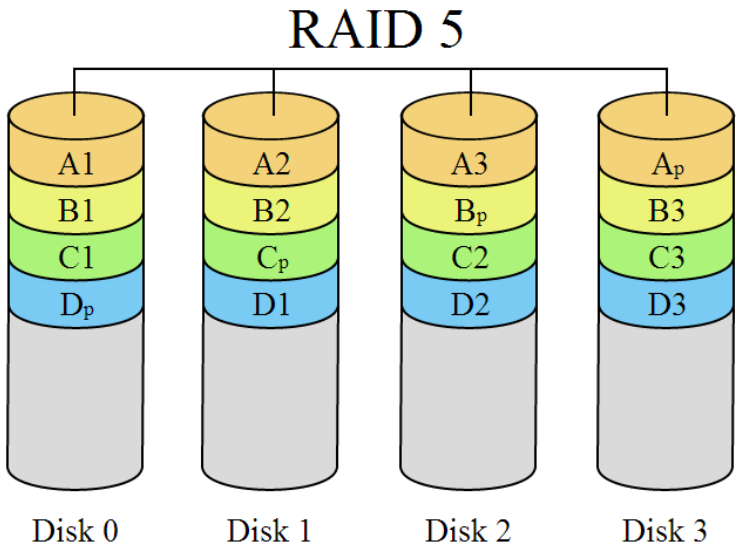
- Zrkadlenie
- V prípade výpadku okamžité použitie druhého disku



Redundancia diskového priestoru (pokr.)

RAID 5

- Vyžaduje najmenej tri disky
- Použitie samoopravných kódov
- Striedavo sú na všetkých diskoch uložené samoopravné kódy (zaberajú kapacitu jedného disku)



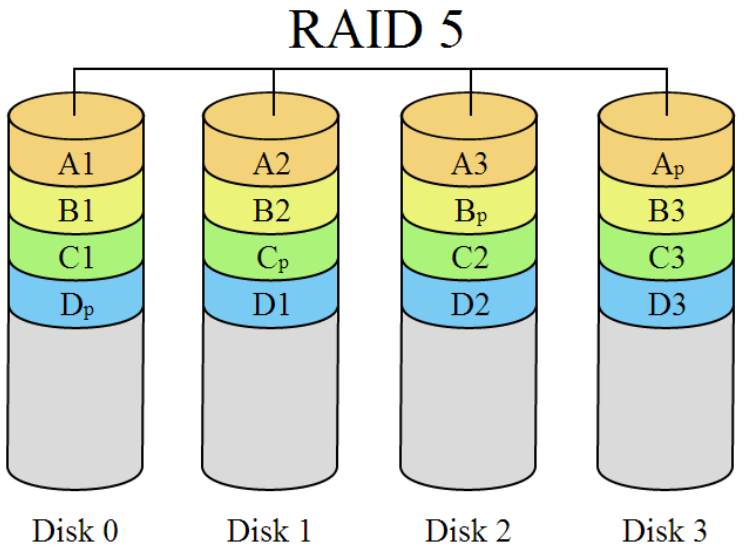
Redundancia diskového priestoru (pokr.)

RAID 5 (pokr.)

- Pri zlyhaní jedného z diskov ho stačí nahradiť novým a dáta na ňom sa „zregenerujú“

- Výhoda: paralelný prístup k dátam, rýchlejšie čítanie

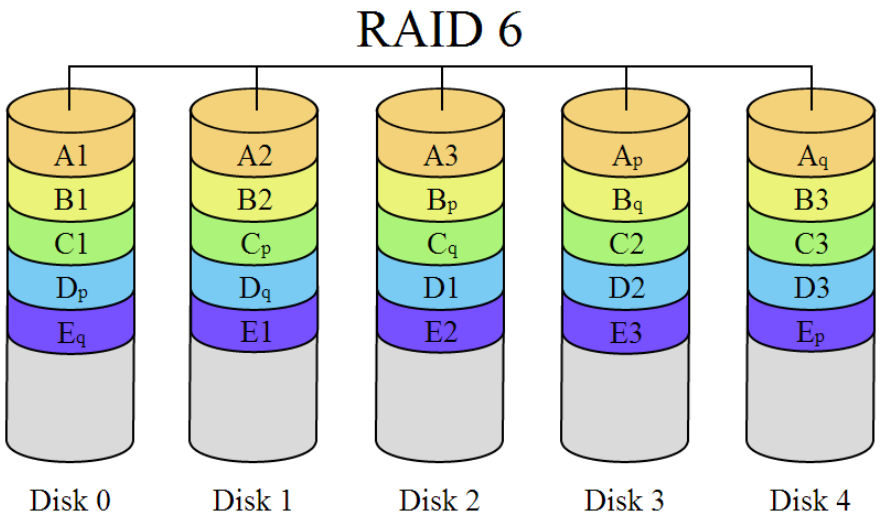
- Nevýhoda: pomalý zápis, kvôli výpočtu samoopravného kódu



Redundancia diskového priestoru (pokr.)

RAID 6

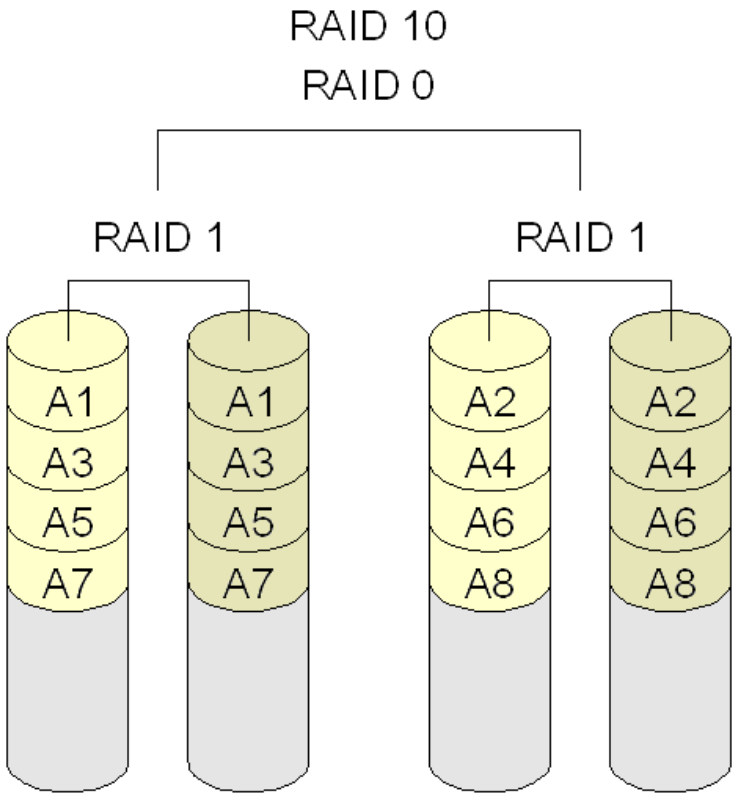
- Je odolný proti výpadku dvoch diskov
- Používa dva paritné disky
- Paritné dáta sú uložené na všetkých diskoch
- Oplatí sa ho použiť až pri použití 5tich diskov (inak je kapacita poľa „polovičná“ a oplatí sa skôr zrkadlenie v RAID 1. Okrem toho pri zrkadlení netreba taký vysoký výpočtový výkon.)



Redundancia diskového priestoru (pokr.)

RAID 10 (1+0)

- Najprv sa dáta zrkadlia a potom sú prístupné v poli RAID 0
- Kvôli väčšej rýchlosti prenášania sa používa pre veľmi vyťažené databázy
- Nie je potrebné nič počítať
- Môže zlyhať jeden disk z každej dvojice



Prenos a výmena informácií

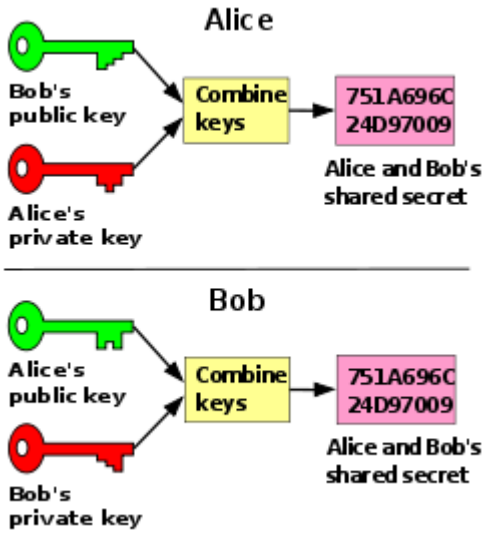
Politiky a postupy pre prenos a výmenu informácií

- Šifrovanie citlivých dát
- Vedenie záznamov o aktívach s citlivými informáciami
- Označovanie médií – dátum vytvorenia média, dátum zničenia, mená prenášaných súborov, verzia a stupeň klasifikácie
- Použitie fyzickej ochrany prenášaných informácií
- Vyškolený personál

Prenos a výmena informácií (pokr.)

Dohody o výmene informácií

- **algoritmy zdieľaného tajomstva** – pre prístup k utajovanej skutočnosti je potrebný kľúč od viacerých dôveryhodných osôb (nie nutne tých istých)
- **Asymetrická kryptografia**: napr. výmena kľúčov pomocou algoritmu Diffie-Hellmann



Prenos a výmena informácií

Ochrana informácií pri výmene elektronickými prostriedkami prenosu

- Kontrola integrity pomocou hašovacích funkcií
- Možnosť využiť viacero rozdielnych hašovacích funkcií pre rôzne typy dát
- Testovanie správnosti sekvencie dát
- Dôležité zaznamenávať sekvenčné číslo kvôli overeniu prijímaných a spracovaných dát

Prenos a výmena informácií (pokr.)

Ochrana informácií pri výmene elektronickými prostriedkami prenosu (pokr.)

- Vedenie záznamov o prijatých dátach
- „Čo bolo prenášané, dátum a čas kedy to bolo prenášané, pôvod, typ/formát dát“
- Kontrola a oprava chýb vďaka kódovaniu
- Logovanie chýb v prenose a ich klasifikácia podľa chybového kódu
- Vynútenie opakovaného prenosu

Zaznamenávanie udalostí a monitoring bezpečnostných incidentov

Zhrnutie aktivít riešenia incidentov IB

- **Detekcia a identifikácia** – sledovanie výskytu a aktívne vyhľadávanie incidentov IB;
- **Izolácia** – inicializácia reakcie na incident IB a zabránenie ich šíreniu;
- **Odstránenie príčiny a obnova** – odstránenie príčiny vzniku incidentov IB a obnova dotknutých systémov a služieb;
- **Post mortem** – identifikácia príčin a návrh systematickej nápravy;
- **Reporting** – informovanie relevantných zainteresovaných strán.

Zaznamenávanie udalostí a monitoring bezpečnostných incidentov

Zaznamenávanie udalostí a nastavenia v OS Windows, UNIX/Linux

- Systémové a aplikačné logy
- Možnosť nastavenia úrovne detailnosti logov

Ochrana záznamov udalostí – logov

- Zálohovanie do geograficky oddelenej lokality
- Šifrovanie prenosu (rsync cez ssh, scp, ...)

Zaznamenávanie udalostí a monitoring bezpečnostných incidentov

Zaznamenávanie činnosti administrátorov a operátorov – accounting

- Zaznamenávanie povolených a nepovolených eskalácií privilégií (napr. TACACS+)
- Zaznamenávanie prístupu ku zdrojom a pokusov o neoprávnený prístup k zdrojom

Zaznamenávanie chýb a zlyhaní

- Dohľadové mechanizmy pre hardvérové prvky infraštruktúry, importy dát, operatívu databáz

Zaznamenávanie udalostí a monitoring bezpečnostných incidentov (pokr.)

Potreba a spôsoby synchronizácie času, protokol NTP

- „Timestamping“ (aj keď nie v kryptografickom zmysle) logových záznamov
- Nutná konsolidácia časových údajov naprieč infraštruktúrou napr. kvôli vyšetrovaniu incidentov

Zaznamenávanie udalostí a monitoring bezpečnostných incidentov (pokr.)

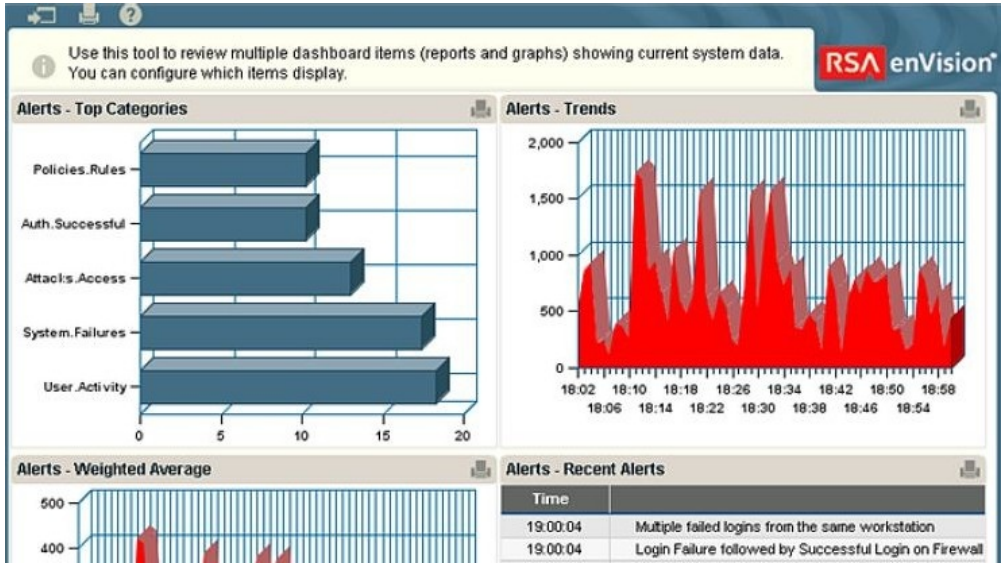
SIEM riešenia

- Kontrola nad konsolidáciou **obrovského množstva** logov z rôznych systémov, sieťových zariadení, databáz, zariadení na kontrolu prístupu, atď.
- Monitorovanie nadväznosti logovaných udalostí a detekcia incidentov
- Ich triedenie do vlákien a vizualizácia v reálnom čase
- Príkladom takéhoto riešenia je RSA ENvision

Príklady konkrétnych riešení a technológií

RSA Envision

- SIEM riešenie od RSA – bezpečnostnej divízie firmy EMC
- Ukladá, triedi, konsoliduje, vyhodnocuje logové záznamy
- Koreluje, prioritizuje, štatisticky spracováva a vizualizuje bezpečnostné incidenty



Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Ďakujem Vám za pozornosť

Otázky?

- Priestor pre publikum
- Aké sú Vaše skúsenosti s bezpečnosťou prevádzky?

KPMG
cutting through complexity™