Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Bezpečnosť prevádzky
Časť 1

Erik Saller, Ivan Oravec

2013

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, auditových 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

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

Manažment informačnej bezpečnosti

- Vyhotovovanie analýzy dopadov (BIA)
- Vývoj a implementácia politík, procedúr a štandardov
- Pravidelné interné/externé audity
- Implementácia formálneho manažmentu zraniteľností

Manažment prevádzky

- alokácia prostriedkov
- tvorba štandardov a procedúr
- monitorovanie prevádzkových procesov

Prevádzková dokumentácia

- Dokumentácia systémov a aplikácií
- Dokumentácia používateľských incidentov (od momentu iniciácie riešenia)
- Súvisí s knowledge managementom

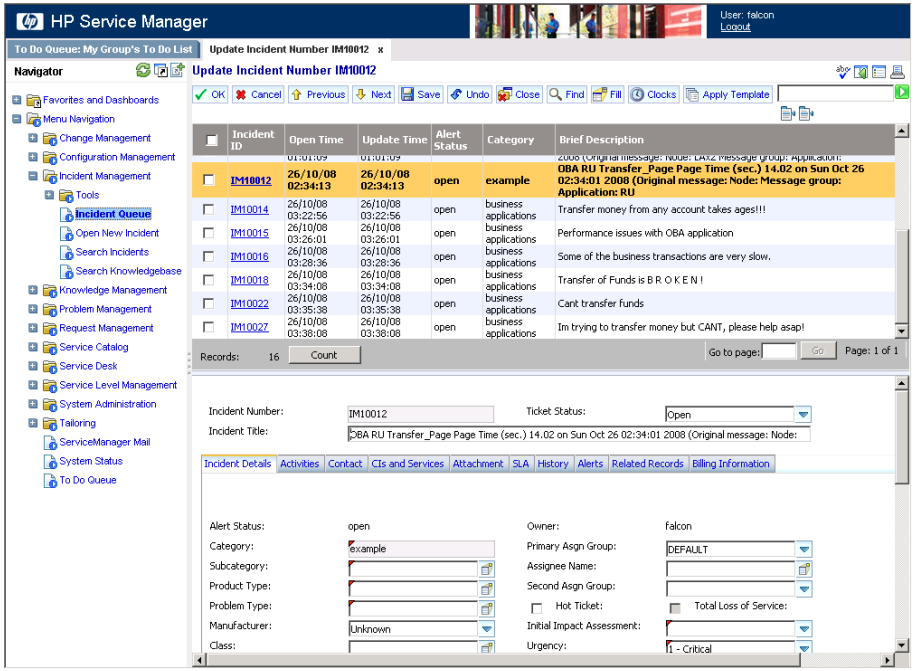
Procesy riadenia zmien

- 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



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

Prenos a výmena informácií

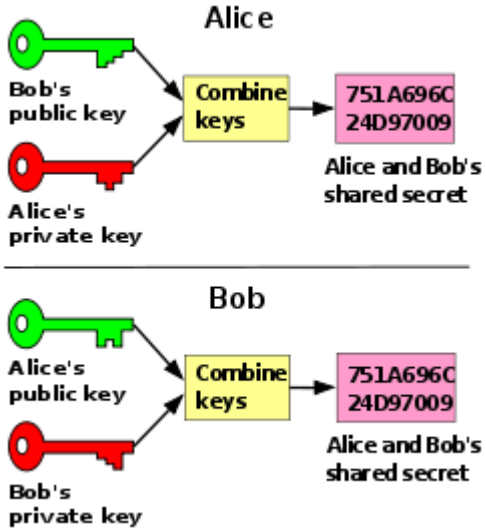
Politiky a postupy pre prenos a výmenu informácií

- 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

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.)

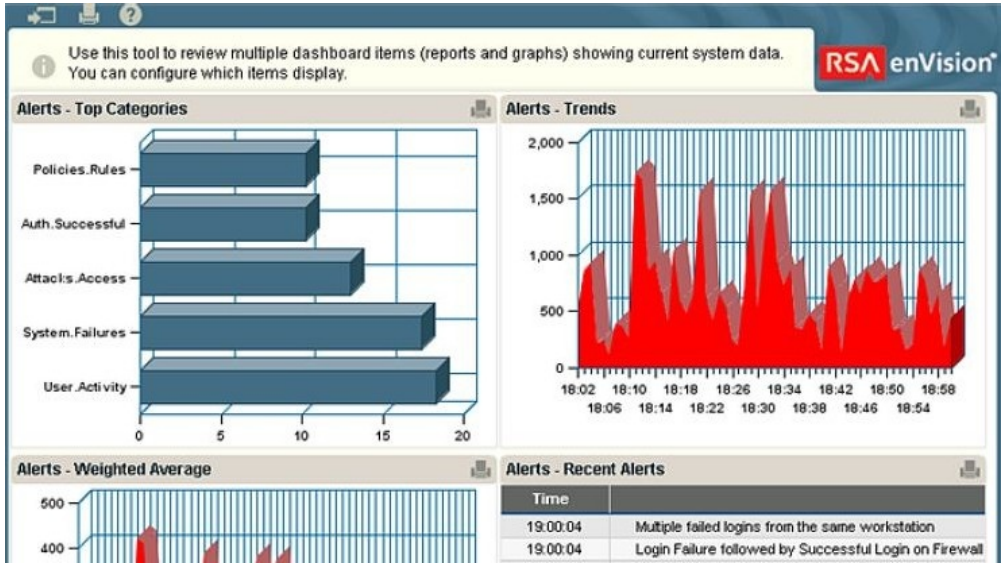
SIEM riešenia

- 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
- 2012

Kontrola nad privilegovaným prístupom

- Privilegovaný používateľ je používateľ, ktorému je kvôli jeho funkcii, dôveryhodnosti a/alebo znalostiam pridelené oprávnenie pristupovať k zdrojom IKT na úrovni administrátora, teda vo významne širšom rozsahu ako má väčšina ostatných používateľov toho istého systému.
- Kontrola nad privilegovaným prístupom sa v praxi realizuje na rôznych úrovniach, môže sa jednať o obmedzenie používateľského prístupu na úrovni fyzického vstupu do budovy, operačného systému, informačného systému apod.

KPMG
cutting through complexity™

Kontrola nad privilegovaným prístupom (pokr.)

- Každý systém má systémové súbory, ktoré sú pre beh systému dôležité.
- Pri neautorizovanej modifikácii týchto súborov môže dôjsť ku kompromitácii systému, narušeniu behu operačného systému alebo dôležitej služby, prípadne znemožneniu riešenia denných povinností používateľmi.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
2012

Kontrola nad privilegovaným prístupom (pokr.)

- Privilegovaný prístup administrátora poskytuje možnosť využívať pri plnení povinností súvisiacich s údržbou tie časti informačného systému, ktoré nie sú bežným používateľom prístupné.
- Vyžadovanie prihlásenia administrátora do privilegovaných častí systému je prínosné, pretože znižuje riziko úmyselného, alebo neúmyselného poškodeniu systému záškodným, alebo neskúseným administrátorom.

KPMG
cutting through complexity™

Kontrola nad privilegovaným prístupom (pokr.)

- Oprávnenia na privilegovaný prístup by mali byť pridelené iba na limitovanému okruhu používateľov. Používateľ s privilegovaným prístupom k operačnému systému (administrátor, v linuxových systémoch nazývaný „root“) má práva inštalovať nový softvér, odinštalovať softvér, meniť nastavenia systému , ...

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 Star 2012

Kontrola nad privilegovaným prístupom (pokr.)

- Administrátor operačného systému má zväčša takisto možnosť modifikovať nastavenie kontroly prístupu tak, aby umožnil prístup neautorizovaným používateľom.
- Ak dôjde ku kompromitácii mechanizmov riadenia prístupu, útočníkovi je spravidla umožnený prístup ku všetkým zdrojom, ku ktorým má prístup samotný systém.

KPMG
cutting through complexity™

Kontrola nad privilegovaným prístupom (pokr.)

- Administrátor je obvykle oprávnený pozmeniť auditné záznamy operačného systému a (napr. pri súčasnej kompromitácii systému IDS/IPS) ovplyvňovať nastavenia detekcie incidentov tak, aby jeho potenciálne nebezpečné aktivity zostali nezachytené.
- Takto napadnutý systém môže byť často pozmenený a môže byť negatívne ovplyvnená funkcia detekcie a zneškodnenia škodlivého kódu („malware“).

Kontrola nad privilegovaným prístupom (pokr.)

- Eventuálne na ňom môže dôjsť tiež k nasadeniu tzv. zadných vrátok („backdoorov“), ktoré umožňujú útočníkovi spätné prihlásenie a prístup ku kompromitovanému systému. Detekcia takto pozmenených používateľských staníc a serverov je problematická a často neefektívna.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 Star 2012

Kontrola nad privilegovaným prístupom (pokr.)

- Nasadenie systému na odhalenie a prevenciu prieniku (Intrusion Detection/Prevention System - IDS/IPS) na detekciu odchýlky od korektného fungovania používateľských staníc a detekciu indikátorov narušenia sieťovej prevádzky infraštruktúry organizácie útočníkom má priaznivý vplyv na prevenciu súvisiacich incidentov.
- Často však ani metódy použité IDS/IPS systémami akými sú napr. detekcia neobvyklých vzorov správania v sieťovej prevádzke, alebo hĺbková kontrola prenášaných paketov (anglicky „deep packet inspection“) nezaručujú úplnú ochranu voči existujúcim hrozbám.

KPMG
cutting through complexity™

Kontrola nad privilegovaným prístupom (pokr.)

- Administrátorské práva, ktoré by za normálnych okolností mali byť pridelené len úzkej skupine administrátorov, môžu byť nevyhnutné aj pre zamestnancov na pozíciách vývojárov, operatívy, alebo systémového monitorovania.
- Dobrou praxou je v takom prípade model riadenia prístupu, v ktorom sú používatelia zaradení do skupín (anglicky „groups“), ktoré majú špecifické úrovne prístupu a práva.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 Star 2012

Kontrola nad privilegovaným prístupom (pokr.)

- Toto definovanie privilegovaných prístupov pre skupiny používateľov a s ním súvisiace prideľovanie a odnímanie prístupových práv sa deje kontrolovaným spôsobom podľa druhu činnosti vykonávanej používateľmi.
- Správne odstupňovaným riadením prístupu používateľov k zdrojom je systém vystavený nižšiemu riziku incidentov spojených s neautorizovaným prístupom a pozmenením dôležitých nastavení.

KPMG
cutting through complexity™

Kontrola nad privilegovaným prístupom (pokr.)

- Implementácia obmedzenia neautorizovaných aktivít administrátorských používateľov nie je jednoduchá a preto **je vhodné zaviesť monitoring systémových zmien** pomocou ktorého je možné aktivity administrátorov posudzovať v kontexte ostatných bezpečnostne relevantných udalostí a to „zvonka“ systému (teda tak, **aby ich útočník nemohol zmeniť na napadnutom lokálnom systéme**).

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 Star 2012

Kontrola nad privilegovaným prístupom (pokr.)

- Medzi takéto upresňujúce udalosti patrí napríklad informácia:
  - z ktorého účtu bežného používateľa došlo k eskalácii privilégií - pokiaľ nešlo o priame prihlásenie administrátorského užívateľa,
  - či ku eskalácii privilégií došlo po prvej výzve na zadanie administrátorského hesla,
  - či k privilegovanému prístupu došlo v čase, alebo mimo času bežnej prevádzky,
  - aké príkazy boli spustené a ktoré systémové súbory boli zmenené.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 Star 2012

Kontrola nad privilegovaným prístupom (pokr.)

- Na to, aby sme mali dôveryhodný záznam o všetkých týchto podrobnostiach činností administrátorov, je nutné práve splnenie predpokladu zachovania integrity a autentickosti auditných záznamov.
- Dobrou praxou je okamžite (resp. v stanovených intervaloch) prenášať záznamy o bezpečnostne relevantných udalostiach na iný systém v sieťovej infraštruktúre, ktorý sa stará o ich vyhodnocovanie, ukladanie, triedenie a prípadné vyvodzovanie vhodných protiopatrení.

KPMG
cutting through complexity™

Separácia kanálov pre administráciu od kanálov pre bežnú prevádzku

- Používanie spoločných účtov pre viacero používateľov nie je v súlade so štandardami bezpečnostných politík a predovšetkým pri administrátorskom prístupe predstavuje veľké riziko zneužitia.
- Ideálne je preto zabezpečiť separáciu účtov pre administráciu od účtov pre bežnú prevádzku.

Separácia kanálov pre administráciu od kanálov pre bežnú prevádzku (pokr.)

- Získanie prístupu do privilegovaného účtu z účtu bežného používateľa sa v ideálnom prípade deje až pri splnení vopred stanovených podmienok (autentifikácia) a je nevyhnutné zabezpečiť riadne zaznamenávanie (auditovanie) takejto činnosti, tak aby bolo jasné, kto a kedy vyžiadal administrátorské práva.

Separácia kanálov pre administráciu od kanálov pre bežnú prevádzku (pokr.)

- Zaznamenávanie operácií vykonaných používateľmi a administrátormi sa nazýva „accounting“. Jeho implementáciou v prístupe k sieťovým zariadeniam je napr. TACACS+.
- Tento nástroj však neplní iba funkciu accountingu, ale okrem nej vykonáva ešte autentifikáciu (anglicky „authentication“) a autorizáciu (anglicky „authorization“).

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Kontrola integrity

- V praxi sa hlavne pri snahe vyhovieť prísnejším štandardom (napr. v bankovej sfére) nasadzujú nástroje na overovanie integrity systémových a aplikačných komponentov a ich aktualizácií pred inštaláciou pomocou hašovania súborov a ich porovnávania s „etalónovými“ hašmi.
- Etalónovými hašmi máme na mysli také, ktoré sú v databáze softvérového nástroja na kontrolu integrity vedené ako vzorové a boli správne overené. Tento postup má význam pri kontrolovaní konfigurácií a logov a prevencii neautorizovaného zásahu.

KPMG
cutting through complexity™

Kontrola integrity (pokr.)

- Nástroje používané pri kontrole integrity (napríklad Tripwire) detegujú pozmenenie dát neoprávnenou osobou a v prípade ak je to vhodné a možné vykonajú aj nápravné opatrenia (napr. korekciu vlastníctva a prístupových práv súborového systému).
- Môžu byť súčasťou kontrolných mechanizmov slúžiacich na priebežné vyhodnocovanie dodržiavania bezpečnostných politík organizácie.
- Poskytujú možnosti korelácie logov a vyvodenia záverov o súvislostiach incidentu. Ich výstup je možné využiť pri zbieraní digitálnych dôkazov, napr. podľa štandardu stanovenom v dokumente ISO 27037 (Guidelines for identification, collection, acquisition and preservation of digital evidence).

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 Star - 2012

Zmena počiatočnej konfigurácie po inštalácii

- V praxi často dochádza k tomu, že i pri implementácii kvalitného a drahého informačného systému s pokročilými bezpečnostnými funkciami sa **pozabudne na zmenu prednastavených hesiel**, prípadne sa v systéme ponechá menej bezpečné nastavenie komunikačnej metódy, ktoré umožní útočníkovi prienik do systému, alebo poslúži ako medzi krok k úspešnému prieniku.

KPMG
cutting through complexity™

Zmena počiatočnej konfigurácie po inštalácii (pokr.)

- Typickými príkladmi sú nastavenia slabých hesiel pre administrátorského používateľa ako napr. „admin“, „administrator“, „root“, „toor“ , alebo iné triviálne uhádnuteľné znenia.
- Pokiaľ ide o konfiguračné nedostatky, môže sa stať, že je aj pokročilé VPN riešenie pri nasadzovaní a nastavení dodávateľom ponechané s **nevhodným protokolom na výmenu kľúčov, ktorý má slúžiť iba ako dočasné riešenie.**

Zmena počiatočnej konfigurácie po inštalácii (pokr.)

- Za všetky problematické nastavenia spomeňme agresívny mód VPN sietí, anglicky „aggresive mode“, pri ktorom má útočník možnosť relatívne triviálnym útokom odchytiť autentifikačný hash založený na tzv. preshared key - zdieľanom kľúči, použitom na nie veľmi bezpečnú komunikáciu dvoch koncových uzlov VPN siete.
- V prípade VPN riešení je neporovnateľne jednoduchšie útočiť na takto nedostatočne nastavené úrovne zabezpečenia, ako sa napr. púšťať do kryptografickej analýzy prenášaných dát.

Zmena počiatočnej konfigurácie po inštalácii (pokr.)

- Predovšetkým pri proprietárnych systémoch tiež existuje riziko, že systém bude obsahovať predprogramované používateľské mená a heslá („hard-coded credentials“), ktoré môžu potenciálnemu útočníkovi poslúžiť ako zadné vrátka a predstavovať veľké bezpečnostné riziko neautorizovaného prístupu.
- Pri aktualizácii dôležitých systémových a aplikačných softvérových komponentov (napr. v exponovaných prevádzkach) sa musí postupovať v súlade so štandardami, ktorých dobré praktiky odporúčajú pravidelné „rozbaľovanie“ nových verzií informačných systémov, operačných systémov a softvérových balíkov vo všeobecnosti najprv do testovacieho prostredia.

Zmena počiatočnej konfigurácie po inštalácii (pokr.)

- Až po ich dôkladnom otestovaní dochádza k ich nasadeniu do tzv. produkčnej prevádzky, ktorá pracuje s reálnymi dátami v „ostrej“ prevádzke.
- Zo skúseností je možno konštatovať, že proprietárne systémy sú spravidla väčšmi náchylné na výskyt chýb pri vývoji, hlavne pokiaľ používajú neštandardné protokoly na výmenu dát, alebo neštandardné metódy na ukladanie dát.
- Tieto chyby poskytujú priestor pre zraniteľnosti, ktorých zneužitie útočníkom predstavuje potenciálne riziko narušenia dôvernosti spracovávaných dát, ich vymazanie, alebo neautorizovanú modifikáciu, nestabilitu softvéru a nedostupnosť produkčného systému na ktorom je tento softvér nasadený.

Zmena počiatočnej konfigurácie po inštalácii (pokr.)

- Iniciatívy vývoja softvérových produktov s otvoreným zdrojovým kódom („open source“) a štandardizácia metód vývoja softvéru pomáha zmierňovať výskyt incidentov zapríčinených softvérovými chybami.
- Tým, že sú softvérové produkty s otvoreným zdrojovým kódom masovo využívané a ich testovanie je vykonávané veľkou komunitou výskumných pracovníkov v oblasti bezpečnosti aj „masou“ používateľov na celom svete, je zabezpečená včasná eliminácia veľkej väčšiny softvérových chýb.

Zmena počiatočnej konfigurácie po inštalácii (pokr.)

- Príkladom komunitného softvéru, ktorý má široké uplatnenie na produkčných platformách je webový server Apache.
- Pri ochrane systémového a aplikačného kódu a údajov proti neoprávnenej manipulácii počas prevádzky pomáha kontrola integrity pomocou hašovania dôležitých súborov a archivácia výstupov hašovacích algoritmov, kvôli neskoršiemu porovnaniu.
- Implementáciou tohto prístupu je napríklad už spomínaný nástroj Tripwire a v praxi sa využíva jeho nasadzovanie naprieč všetkými produkčnými serverovými systémami v produkcii.

Zmena počiatočnej konfigurácie po inštalácii (pokr.)

- V prípade nasadzovania nových komponentov do existujúcej infraštruktúry je nutné, aby nový hardvér a softvér zapadol do aktuálnej „mozaiky“ IKT prostredia a podľa možností nespĺňal úlohy, ktoré už za neho pokrýva iný systém (pokiaľ to nie je explicitne vyžadované).
- Niekedy dochádza k zbytočným kolíziám technológií kvôli nesprávnemu plánovaniu, napr. pri použití viacerých VPN riešení naraz.

Zmena počiatočnej konfigurácie po inštalácii (pokr.)

- Pripojenie na VPN, ktorá sprístupňuje sieťové zdroje (dátové úložiská, informačné systémy, webové lokality, atď.), z nej následné pripojenie na inú VPN, kvôli prístupu k iným zdrojom nemusí vždy fungovať práve kvôli tomu, že dochádza ku kolíziám s ktorými sa nerátalo pri pôvodnom plánovaní.
- Príkladom môže byť problém v prístupe k lokálnym, alebo naopak vzdialeným sieťovým zdrojom (kolízia adresného priestoru podsietí v lokálnej sieti s rovnakým adresným priestorom vo vzdialenej sieti, napr. obe siete by nemali používať rozsah 192.168.1.x).

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Aktualizácia softvéru

- Centralizovaná správa aktualizácií informačných systémov v prostrediach so zložitejšou infraštruktúrou sa typicky rieši vyhradenými repozitármi aktualizácií v rámci konkrétnej organizácie, ktoré sú v danom prostredí (na konkrétnych platformách, napr. hardvérových) riadne odskúšané a pri ich následnom nasadeni na koncových staniciach a serveroch nedochádza k nepredvídateľným chybám.
- Aktualizácia používaných systémov je dôležitá, pretože aktualizácie systémov alebo aplikácií sú dodávateľmi vytvárané s cieľom dostránenia známej bezpečnostnej alebo inej chyby v ich produkte.

KPMG
cutting through complexity™

Aktualizácia softvéru (pokr.)

- Pri nasadzovaní aktualizácií je potrebné myslieť aj na riziká z tohto procesu vyplývajúce. S každou novu nasadenou aktualizáciou sa totiž systém vystavuje napr. riziku nestability. Paradoxne sú po aplikovaní záplaty niekedy do systému vnášané zraniteľnosti.
- Typickým príkladom takéhoto nežiadúceho dôsledku bolo, keď v máji 2008 vývojový tím linuxovej distribúcie Debian vydal novú „stabilnú“ verziu balíka OpenSSH s výrazne zmenšeným priestorom generovaných SSH kľúčov, čím vystavil produkčné servery na celom svete riziku úspešného útoku hrubou silou.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Kontrola nad hardvérom

- Dokonca aj pri korektne nastavených pravidlách riadenia prístupu, správnom manažmente používateľských účtov a hesiel na sieťových zariadeniach, dobrej politiky konfiguračného manažmentu a aktualizácií softvéru môže útočník využiť niektorú z metód neautorizovaného pripojenia na hardvér za účelom získania a zneužitia citlivých informácií.
- Používané techniky zahrňujú pripojenie sledovacieho nástroja na „trunk“ port sieťového zariadenia kvôli monitorovaniu a eventuálnej modifikácii sieťovej prevádzky, priamy prístup k administrátorskému rozhraniu komponentu IKT/informačného systému, alebo v špecifických prípadoch o použitie sondy, ktorá aktívne, alebo pasívne narúša dôvernosť a/alebo integritu prenosu dát po zbernici počítača, alebo sieťovej, resp. telekomunikačnej linke.

Kontrola nad hardvérom (pokr.)

- Prístup k systémovým zdrojom je kontrolovaný operačným systémom/firmvérom, ale treba mať na pamäti, že zariadenia pripojené k tomuto systému môžu tiež poskytnúť útočníkovi informáciu, ktorej vyzradenie pre nás môže predstavovať riziko.
- Z týchto dôvodov je potrebné dodržiavať režimové opatrenia a riadiť prístup tiež na úrovni fyzickej bezpečnosti, v rámci ktorých povolíme prístup do serverovní a kancelárií, kde sú umiestnené prvky IKT iba obmedzenému okruhu osôb, ktoré sú dostatočne dôveryhodné a poučené o zásadách bezpečnej manipulácie s dátami a citlivými dokumentmi.

Kontrola nad hardvérom (pokr.)

- V prípade ak je potrebné, aby cudzia osoba pristupovala k týmto priestorom, je nutné aby sa tak vždy dialo v sprievode kvalifikovaného a poučeného personálu.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Otázky?

KPMG
cutting through complexity™