Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Bezpečnosť prevádzky
Časť 2

Erik Saller, Ivan Oravec

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

VYUŽITIE TRETÍCH STRÁN PRI DODÁVKE SLUŽIEB (OUTSOURCING)

KPMG
cutting through complexity™

Využitie tretích strán pri dodávke služieb (outsourcing)

- Anglický termín „outsourcing“ znamená dodávku vývoja, implementácie, alebo podpory IKT ako služby. Rozsah „človekodní“ (anglicky MD = „man days“) ,potrebných pre realizáciu služby, resp. nápravu vzniknutého incidentu, je alokovaný v zmluvách SLA (Service Level Agreement).
- Dodávateľská firma nesie zodpovednosť za implementované zmeny tiež v rozsahu určenom v SLA.
- Preto je potrebné zmluvy revidovať a kvalitu činnosti dodávateľskej firmy pravidelne prehodnocovať aj v súvislosti so strategickým smerovaním organizácie a technologickým pokrokom.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Využitie tretích strán pri dodávke služieb (outsourcing – pokr.)

- Každá SLA zmluva by mala byť pravidelne monitorovaná a vyhodnocovaná na pravidelnej báze (v závislosti na type poskytovaných služieb, napr. raz za rok).
- V SLA by mali byť definované požadované hodnoty parametrov poskytovaných služieb (napr. reakčné doby na rôzne druhy incidentov, dostupnosť systému) ako aj penalizácie za nenaplnenie SLA.
- Dobrou praxou je zahrnúť do SLA aj „motivačné“ ustanovenia, ktoré by motivovali poskytovateľa služby proaktívne prichádzať s návrhmi na ich vylepšenie.

KPMG
cutting through complexity™

Využitie tretích strán pri dodávke služieb (outsourcing)

- Pri využívaní tretích strán môže byť problematické udržovanie kontroly nad dodávanými (a často aj u zákazníka nasadenými) produktami.
- Ako príklad poslúži úplné vlastníctvo kódu konkrétnej aplikácie a sporné možnosti jeho revízie a interného auditu.
- K takým situáciám môže dôjsť v prípade zle nastavenej SLA zmluvy.
- Pre bezpečný outsourcing je nutné vymedziť právomoci a segregovať ich (pozor tiež na konflikt záujmov).

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Riziká využitia tretích strán

- Pri využívaní tretích strán môže dôjsť k tomu, že organizácia utrpí stratu kvôli svojej závislosti na dodávateľoch, zmluvných partneroch, alebo externých konzultantoch.
- Strata môže mať za následok zníženie rozsahu kľúčových schopností, nedostatkom znalostí potrebných na prevádzku, alebo vysokými nákladmi na prevádzku vyplývajúcimi z neefektívneho poskytovania služieb tretími stranami.
- V prípade dodávky technického riešenia existuje tiež ťažko kontrolovateľné riziko zahrnutia zadných vrátok do prevádzkovaného, udržovaného a vyvíjaného riešenia (informačného systému, operačných systémov, sieťových zariadení).

KPMG
cutting through complexity™

Riziká využitia tretích strán (pokr.)

- Bezpečnostné problémy spojené so separáciou kanálov zahŕňajú tzv. nedostatočnú segregáciu právomocí, tj. vznik napr. takej situácie, v ktorej má dodávateľ plnú kontrolu nad vývojom, testovaním a nasadzovaním dodávaného riešenia a je teoreticky schopný nasadzovať do prevádzky neautorizované zmeny
- Externí dodávatelia by mali byť zaviazaní vykonať tiež nezávislý externý audit infraštruktúry na ktorej sú prevádzkované informačné systémy.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

OCHRANA PROTI ŠKODLIVÉMU KÓDU

KPMG
cutting through complexity™

Ochrana proti škodlivému kódu

- Malware (skratka z anglického malicious software) je všeobecné označenie škodlivého softvéru.
- Medzi malware patria:
  - počítačové červy, ktoré využívajú internetové pripojenie počítača na svoje vlastné šírenie a sekundárne môžu spôsobovať obmedzenie funkčnosti počítača, inštaláciu zadných vrátok (anglicky „backdoor“), alebo modifikáciu súborov na počítači. Ich rozdiel oproti vírusom je, že spravidla neinfikujú spustiteľné súbory,
  - trójske kone, ktoré môžu existovať latentné na operačnom systéme, prejaviť sa iba za určitých podmienok a spôsobiť používateľovi škodu,
  - spyware, ktorý sa bez vedomia užívateľa pokúša „vyšpehovať“ citlivé dáta (akými sú napr. heslá),

Ochrana proti škodlivému kódu (pokr.)

- Medzi malware patria (pokr.):
  - phishingové e-maily, ktoré svojím obsahom zavádzajú užívateľa a môžu ho napr. presmerovať na dôveryhodne vyzerajúcu stránku na ktorej od neho pod rôznymi zámienkami vyžadujú napr. zadanie hesla,
  - hoax, poplašné správy, ktorých tvrdenia sa nezakladajú na objektívnej pravde a vyzývajú používateľa, aby ich poslal ďalej,
  - adware, produkty znepríjemňujúce prácu s počítačom zobrazovaním reklamy,
  - exploity, škodlivé kódy, ktoré využívajú programátorskú chybu, zraniteľnosť konkrétneho produktu,
  - hackerské nástroje na zahladzovanie stôp po útoku, skenovanie sietí a predstavujú riziko,
  - nebezpečnými pre súkromie sú tiež tzv. tracking cookies, ktoré podávajú útočníkovi informáciu o činnosti užívateľa (napríklad informácie o navštívených stránkach).

Ochrana proti škodlivému kódu (pokr.)

- Riziká vyplývajúce z výskytu týchto druhov škodlivého softvéru je možné znížiť použitím rôznych typov bezpečnostných produktov v kategórii anti-malware, medzi ktoré patria:
  - Antivírusové softvéry,
  - Všeobecnejšie anti-malware softvéry,
  - Anti-intrusion riešenia,
  - End-point security riešenia vo forme softvérov na kontrolu vynášaných dát,
  - Anti-exploit nástroje – nástroje pre zvýšenie bezpečnosti systémového jadra, ktoré implementujú riadenie rolí, zabezpečujú systémový „hardening“, prevenciu spúšťania nebezpečného kódu, ochranu zásobníka a iné. Za všetky spomeňme Grsec, Sandboxy, Non-exec stack patche, AppArmor alebo priamo produkty, ktoré tieto nástroje kombinujú.

Ochrana proti škodlivému kódu (pokr.)

- Možné hrozby vyplývajúce z činnosti malware na systéme zahŕňajú:
  - získanie citlivých dokumentov (údajov) – malware môže nepozorovane odosielať útočníkom vybrané typy údajov na vzdialenú adresu,
  - získanie neautorizovaného vzdialeného prístupu pomocou zadných vrátok,
  - zničenie/modifikácia používateľských, alebo systémových dát,
  - vytvorenie platformy na ďalšie útoky (botnety)
  - vydieranie (získanými údajmi, zašifrovanie údajov, hrozba stíhania, ...)

Ochrana proti škodlivému kódu (pokr.)

- Možné kanály distribúcie škodlivého softvéru, pri ktorých treba dodržiavať prísne bezpečnostné pravidlá:
  - emailová komunikácia – neotváranie emailových príloh výrazne znižuje riziko infikovania,
  - prehliadanie internetových stránok – nenavštevovať potenciálne nebezpečné stránky, ktoré ponúkajú nelegálne sťahovanie softvéru, hudby a filmov.
  - upload dokumentov (napr. FTP, SSH, HTTP) – nesprávne nastavenie prístupových práv, alebo zraniteľná verzia démona môže vystaviť systém narušeniu,
  - fyzický prístup k PC (napr. USB, CD, HDD) – útočník, ktorý má priamy prístup k hardvéru, môže pri pripojení cudzích médií do systému aktivovať program obsahujúci malware,
  - pripojenie na sieť (napr. WiFi) – samotný prístup na neznámu bezdrôtovú sieť poskytuje útočníkovi priestor pre kompromitáciu pripojeného PC.

Ochrana proti phishingu

- Jedným z typov škodlivého obsahu, ktorý je smerovaný na organizácie a používateľov vo všeobecnosti je špeciálne skonštruovaný phishingový e-mail (anglicky „phishing email“).
- Takýto e-mail ktorý sa adresou odosielateľa a svojím obsahom pokúša uviesť používateľa do omylu, že pochádza z dôveryhodného zdroja často vyzýva používateľa k vykonaniu určitých úkonov alebo poskytnutiu informácií, ktoré následne zneužije. Hromadné zasielanie takýchto e-mailov označujeme anglickým termínom „phishing“.
- Email so škodlivým obsahom je do našej schránky doručený zo zdanlivo dôveryhodnej adresy a linka v ňom môže okrem iného navádzať na stránku s falošným autentifikačným formulárom. Tento formulár vyzýva používateľa ku zadaniu mena a hesla na niektorú zo známych webových, alebo mailových služieb.

Ochrana proti phishingu (pokr.)

- Útočník tak pri úspešnom pokuse získava možnosť tieto autentifikačné údaje zneužiť pri ďalších útokoch napr. sociálneho inžinierstva.
- Stránka môže v nemenej častých prípadoch odkazovať na stránku so škodlivým obsahom, ktorá napríklad využíva zatiaľ neopravené chyby prehliadača (tzv. „0 day“) a spôsobí viditeľnú, alebo skrytú kompromitáciu napadnutého počítača.
- Najlepšou ochranou je v tomto prípade zaškolenie personálu ohľadom používaných útočných techník a dôvodov, prečo by mali tieto emaily ignorovať.
- Problémom je, že podobné útoky pracujú s ľudskými emóciami
- Sociálne inžinierstvo sa spomedzi plejády súčasných útočných techník ešte vždy javí ako cesta najmenšieho odporu.

Ochrana proti vírusom

- Vírus je škodlivý program, ktorý sa dokáže sám šíriť bez vedomia používateľa. Aby sa mohol rozmnožovať, vkladá kópie svojho kódu do iných spustiteľných súborov a dokumentov.
- Existuje množstvo spôsobov, ako sa môžu počítače infikovať cez rôzne druhy pamäťových médií a prostredníctvom Internetu a emailovej komunikácie. Vírusy môžu spôsobiť spomalenie a nestabilitu systému, alebo poškodenie dát.
- Pri niektorých vírusoch sa škodlivý kód spúšťa až s oneskorením a pri určitých podmienkach, napr. v určitý deň, alebo po nakazení určitého počtu ostatných systémov. (napr. Timebomb)
- Okrem iného šírenie vírusov tiež spôsobuje zaťaženie sieťových liniek a iných zdrojov (procesor, pamäť, diskový priestor atď.).

Ochrana proti vírusom (pokr.)

- Moderné komplexné antivírusové riešenia, tzv. antivírusové **systémy chránia používateľov aj pred týmito a mnohými inými hrozbami poskytnutím rozšírených funkcií. Medzi tieto funkcie patrí:**
  - odstraňovanie spamu,
  - funkcia firewallu,
  - priebežné skenovanie emailov a súborového systému,
  - kontrola integrity dát,
  - plánovač akcií, ktorý v určitých termínoch vykonáva určitú činnosť,
  - karanténa, ktorá zabezpečuje izoláciu infikovaných súborov.

Ochrana proti vírusom (pokr.)

- Antivírusové systémy sú zavádzané nielen na pracovných staniciach, ale napr. aj na mailových serveroch. **Pozor, stačí to?**
- Priebežne kontrolujú nielen súbory na klientskych počítačoch, ale aj súbory preberané služobným emailom.
- Databázy signatúr antivírusového softvéru sú pravidelne aktualizované proti centrálnemu firemnému repozitáru. **Naozaj?**

Ochrana proti vírusom (pokr.)

- Antivírusové systémy samé o sebe nestačia, nevyhnutné sú tiež správne nastavenia operačného systému ohľadne kontroly prístupu k administrátorským zdrojom, ktoré by mali byť bežnému používateľovi odoprené (za všetky menujme inštaláciu nového softvéru, úprava registrov, atď.).
- Špecifické hrozby súvisiace s používaním mobilných zariadení a vzdialenou prácou a opatrenia proti nim

Ochrana proti vírusom (pokr.)

- Zariadenia, ktoré nie sú organizáciou pridelenými pracovnými stanicami, ale sú v súkromnom vlastníctve používateľa (inteligentné telefóny, súkromné laptopy, ...) sa v služobných priestoroch vyskytujú čoraz viac. Je preto nutné ich používanie a predovšetkým pripojenie k sieťovo prístupným zdrojom kontrolovať.
- Na tento účel môžu slúžiť riešenia ako MDM alebo napríklad tzv. „Antisniffer“, ktorý deteguje takéto zariadenia, klasifikuje ich ako neautorizované a nemusí im povoliť pripojenie k sieti. Stále viac zamestnancov však chce pristupovať z týchto zariadení do siete. Ich zákaz s ohľadom na technologické trendy tabletov a inteligentných telefónov nemusí byť práve strategickým a dlhodobo udržateľným riešením.
- V takýchto prípadoch je vhodné nasadenie šifrovania prenášaných dát pomocou virtuálnych privátnych sietí (VPN) a využitie šifrovania dát ukladaných na súkromný hardvér. **Pozor, politika nastavení!**

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

ZAZNAMENÁVANIE UDALOSTÍ (LOGOVANIE) A MONITORING

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zaznamenávanie udalostí a monitoring bezpečnostných incidentov

- Vo výpočtovom systéme prebieha množstvo procesov, ktorých činnosť **môže** generovať auditné záznamy.
- Tieto poskytujú kľúčové informácie, ktoré môžu byť použité na posúdenie optimálnosti nastavenia systému vzhľadom na jeho funkciu a bezpečnosť, alebo na vyšetrovanie vzniknutých incidentov.
- Dôveryhodné, relevantné a dostatočne detailné logy sú dôležité pri identifikovaní incidentov a ich príčin a tiež môžu byť kľúčovým dôkazom pri forenznej analýze v súdnom vyšetrovaní.
- Môžeme konštatovať, že auditný záznam predstavuje chronologický záznam systémových aktivít dostatočný pre rekonštrukciu, revíziu a skúmanie postupnosti stavov prostredia a aktivít, zúčastňujúcich sa na realizácii operácie, procedúry, alebo udalosti v transakcii od jej začiatku po jej konečný výsledok.

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zaznamenávanie udalostí a monitoring bezpečnostných incidentov (pokr.)

- Auditné záznamy slúžia na odhalenie infiltrácie, alebo pokusu o infiltráciu do systému, čím predstavujú veľmi dobrý základ pre činnosť interného aj externého bezpečnostného audítora. Taktiež pri forenznej analýze platí, že logy, ktoré sú samé o sebe neškodným záznamom sa môžu v kontexte s inými záznamami a nedigitálnymi dôkazmi ukázať ako zásadné pre vyvodenie záverov vyšetrovania.
- Auditné záznamy sú záznamy generované rozličnými softvérovými komponentmi bežiacimi v IT infraštruktúre. Auditné záznamy poskytujú hlavný zdroj informácií pre systémový bezpečnostný audit. **Zásady a princípy vytvárania robustných logovacích systémov sú zo zrejmých dôvodov v množstve projektov dodržiavané od začiatku vývoja.**

KPMG
cutting through complexity™

Zaznamenávanie udalostí a monitoring bezpečnostných incidentov (pokr.)

- Rozličné formy logovacích mechanizmov sú implementované prakticky vo všetkých operačných systémoch (vrátane vnorených systémov, napr. v aktívnych sieťových prvkoch), v databázových systémoch a u väčšiny špecifických softvérových aplikácií (proprietárne antivírové riešenia, apod.).
- Existuje viacero dôvodov, prečo viesť auditné záznamy:
  - vyvodenie zodpovednosti - logovacie záznamy nám pomôžu spojiť určité osoby s určitými udalosťami,
  - analýza chybových stavov
  - rekonštrukcia udalostí - auditné záznamy môžu byť zobrazené v chronologickom poradí a teda, vieme presne určiť, čo sa stalo pred incidentom a počas neho. Aby sme dosiahli absolútnu presnosť a aby sme zosynchronizovali jednotlivé zdroje logovacích záznamov, je potrebné synchronizovať systémový čas podľa centrálneho servera,
  - detekcia prieniku - neautorizovaná, alebo neobvyklá udalosť musí byť zaznamenaná, aby mohla byť spätne zobrazená. Dlhodobá archivácia logov je v tomto snažení veľmi prínosné.

Zaznamenávanie udalostí a monitoring bezpečnostných incidentov (pokr.)

- V závislosti od komplexnosti a množstva logov je potrebné zvoliť správny spôsob ich uchovávania a vyhodnocovania. Možné spôsoby analýzy logov sa delia do dvoch kategórií:
  - manuálne – tento spôsob je často neefektívny, pretože musíme hľadať čiastkové informácie po viacerých systémoch,
  - automatické (pomocou skriptov a špeciálnych softvérov) – najviac využívanie hlavne kvôli vysokej početnosti logov.
- Bezpečnostný auditný záznam musí byť bezpodmienečne chránený pred neoprávnenou zmenou, k čomu môžu byť použité princípy zaistenia kontroly prístupu. Medzi odporúčané praktiky patrí zapisovanie záznamov na médium, na ktoré je možný zápis len raz, aby nebolo možné už existujúci záznam zmeniť.

Zaznamenávanie udalostí a monitoring bezpečnostných incidentov (pokr.)

- Možné riešenie kontroly prístupu je pridelenie práv na čítanie a aktualizáciu (ale nie modifikáciu, alebo mazanie) do vyhradených častí systému na ukladanie dát. Takýto vyhradený prístup je možné zabezpečiť pridelením špecifických kľúčov.
- Systém na ukladanie dát potom vyhodnocuje pridelenie prístupu ku konkrétnej používateľskej časti na základe poskytnutého kľúča. Ak sa kľúč poskytnutý používateľom zhoduje s tým, ktorý mu je pridelený, je užívateľovi umožnený prístup.
- Prístup je pridelený aj používateľovi s tzv. „master“ kľúčom, ktorý umožňuje autorizovaný prístup do všetkých častí systému a typicky ho má k dispozícii vlastník systému.

Zaznamenávanie udalostí a monitoring bezpečnostných incidentov (pokr.)

- Dôvody prečo majú byť auditné záznamy chránené pred zásahom a čítaním nepovolanými osobami zahŕňajú zachovanie ich integrity, ale zároveň je nezanedbateľnou aj skutočnosť, že **informácie z týchto logov sú ľahko zneužiteľné útočníkom**.
- Pri uchovávaní logov je podľa dobrej praxe potrebné zabezpečiť nielen ich lokálne kópie, ale tiež ich prenášať do bezpečnej geograficky vzdialenej lokality, kvôli zachovaniu všetkých troch aspektov bezpečnosti: dôvernosti, integrity a dostupnosti.
- Dôvernosť je v tomto prípade dôležitá kvôli tomu, aby sme predišli neautorizovanému prístupu a prípadnému zneužitiu týchto dát. Zachovanie integrity zabezpečí, že nedochádza k poškodeniu uložených dát, alebo ich neautorizovanej modifikácií.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Zaznamenávanie udalostí a monitoring bezpečnostných incidentov (pokr.)

- Dostupnosť je dôležité zabezpečiť z toho dôvodu, že pri nedostatočnom zabezpečení uložených médií existuje vysoké **riziko zničenia, alebo poškodenia dát**.
- Pri prenášaní logových záznamov do geograficky vzdialenej lokality platí, že rôzne systémy a aplikácie majú rôzne formy výstupu do logovacích súborov, preto je vhodné tieto záznamy **sumarizovať a normalizovať lokálne**, aby sme predišli prenášaniu zbytočne veľkého kvanta dát po sieti do centrálneho úložiska.

KPMG
cutting through complexity™

Zaznamenávanie udalostí a monitoring bezpečnostných incidentov (pokr.)

- Definícia toho, čo sa dá považovať za **neobvyklú udalosť** sa rôzni, ale do určitej miery by sme mohli generalizovať a povedať, že neobvyklé udalosti zahŕňajú:
  - neúspešné prihlásenia,
  - prihlásenia mimo bežného pracovného času,
  - zamknutie účtov po presiahnutí povoleného počtu pokusov o prihlásenie,
  - neobvyklú sieťovú aktivitu (skenovanie siete, prenos neobvykle veľkého objemu dát apod.),
  - zmeny konfigurácie mimo bežnej údržby a bez formálneho záznamu,
  - prístupy užívateľov s následnou eskaláciou prístupových práv,
  - neautorizované použitie zdrojov,
  - neprivilegovaný prístup k súborom,
  - prístup k samotným logovacím záznamom,
  - neobvyklé čerpanie systémových prostriedkov (pamäť, CPU) atď.

Zaznamenávanie udalostí (logovanie) a monitoring bezpečnostných incidentov (pokr.)

- Systémové a aplikačné logy zaznamenávajú a uchovávajú všetky bezpečnostne relevantné incidenty. Nástroje na monitoring a logovanie bezpečnostných incidentov ponúkajú možnosť nastavenia úrovne detailnosti logov, ich konsolidáciu pri zbere **z plejády sieťových zariadení a operačných systémov** v celej sieťovej infraštruktúre.
- Citlivosť zaznamenávania udalostí a konkrétne spôsoby nastavenia zaznamenávania udalostí v operačných systémoch MS Windows, UNIX/Linux a iných sa líšia v závislosti od prostredia , v ktorom sú nasadzované a aplikácie, ktorá je na nich nasadená.

Zaznamenávanie udalostí a monitoring bezpečnostných incidentov (pokr.)

- Podstatné však je, že všetky druhy systémov, dokonca aj tie úplne základné vnorené („embedded“) systémy, majú implementované logovanie **(pozor na kapacitu pamäte na logy)**, bola to jedna z prvých vlastností operačných systémov od ich úplného začiatku (určitá forma **zaznamenávania používateľskej aktivity**, tzv. „accounting“, bola zapracovaná už do pôvodného systému Unix v 70-tych rokoch).
- Dôležité dáta, akými auditné záznamy nepochybne sú, či už z pohľadu operatívy, riešenia incidentov, hľadania príčin anomálnych udalostí, alebo forenzného vyšetrovania pri kriminálnych činoch, **musia byť chránené pred poškodením, pozmenením, alebo zničením**.

Zaznamenávanie udalostí a monitoring bezpečnostných incidentov (pokr.)

- Medzi najbežnejšie techniky na predchádzanie stratám logovacích záznamov je ich **okamžité zálohovanie do geograficky oddelenej lokality**. Pokiaľ sa dáta prenášajú po potenciálnej nebezpečnej linke, ktorá nie je dedikovaná pre zálohovanie je užitočné využiť šifrovanie prenosu (v Linuxe je možné použiť napr. nástroj rsync cez protokol ssh, alebo nástroj scp na bezpečné kopírovanie na vzdialený systém).
- Na zaznamenávanie **povolených a nepovolených eskalácií privilégií administrátorov a operátorov** na sieťových zariadeniach slúžia accounting nástroje ako napr. TACACS+, často modifikované podľa potrieb konkrétneho informačného systému na správu prístupov. TACACS+ je protokol pôvodne vyvíjaný CISCO Technologies, ktorý slúži ako sprostredkovateľ autentifikácie: sieťové zariadenia na ktoré sa používateľ snaží pristúpiť kontaktujú TACACS+ server a overia s ním, že používateľské meno a heslo súhlasí a je autorizované na prístup k danému zariadeniu.

Zaznamenávanie chýb a zlyhaní

- Súčasťou riadenia prevádzkovej bezpečnosti sú tiež monitorovacie riešenia na zaznamenávanie chýb a zlyhaní. V praxi sa **nasadzujú monitorovacie mechanizmy** pre hardvérové prvky infraštruktúry ako sú napr. diskové polia, kontroluje sa ich bezchybná prevádzka a výkon. Ďalšími dôležitými **informáciami, ktoré je vhodné monitorovať sú priebehy importu dát, výkonu databáz** apod.
- V rozsiahlych sieťových prostrediach sa tieto požiadavky realizujú integráciou mnohých monitorovacích riešení, pričom často dochádza k **nekonzistenciám a falošne pozitívnym alarmom,** resp. falošne negatívnym výsledkom a iným chybám v posúdení incidentu a vyvodení dôsledkov.

Zaznamenávanie chýb a zlyhaní (pokr.)

- Nutnou súčasťou efektívneho manažmentu bezpečnostných incidentov je aj konsolidácia časových údajov medzi systémami napr. kvôli **vyšetrovaniu ich nadväznosti a vyvodenie zodpovednosti za incident**.
- Protokol NTP slúži na synchronizáciu systémového času naprieč sieťovou infraštruktúrou, čím zabezpečuje **korektný a konzistentný časový údaj v logovacích záznamoch.**

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Otázky?

KPMG
cutting through complexity™