Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Bezpečnosť prevádzky
Časť 3

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

- 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.)

- Ďalšie metódy zachovania dôvernosti, integrity a dostupnosti logových záznamov:
  - **šifrovanie citlivých dát** – v prípade, ak sú dáta prenášané po sieti a predovšetkým v prípade, že sa jedná o prenos dát po bezdrôtovej sieti,
  - **evidencia médií** – je dôležité mať prehľad o tom, kde sú dáta uložené a kto má k nim prístup,
  - **označovanie médií –** označenie interných aj externých médií, zapísanie dátumu vytvorenia média, dátumu zničenia, mená prenášaných súborov, verzia a stupeň klasifikácie,
  - **použitie fyzickej ochrany prenášaných informácií** – zabezpečenie toho, že lokalita, v ktorej sú dáta fyzicky umiestnené je v súlade so štandardami fyzickej a objektovej bezpečnosti,
  - **vyškolený personál** – organizovanie školení, ktoré zvýšia povedomie zamestnancov o správnom zaobchádzaní s dátami.

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 udalostí a monitoring bezpečnostných incidentov (pokr.)

- Funkciami TACACS+ sú teda autentifikácia, autorizácia a accounting (AAA). Zaznamenáva prístupy ku zdrojom vrátane neoprávnených pokusov.
- Tento AAA (**autentifikácia, autorizácia, accounting**) protokol pôvodne vyvíjaný americkým ministerstvom obrany a neskôr spoločnosťou Cisco Systems je dnes už voľne šíriteľný a v IT priemysle sa stal štandardom. V produkčných prostrediach je často nasadzovaný a modifikovaný podľa individuálnych potrieb.
- Jeho tri hlavné funkcie sú „AAA“:
  - Autentifikácia – určuje kto, resp. ktorý počítačový program môže pristupovať,
  - Autorizácia – určuje k čomu môže pristupovať,
  - Accounting – vedenie záznamov o vyššie uvedených operáciách.

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

Systémy pre automatizované vyhodnocovanie bezpečnostných udalostí (SIEM) – pokr.

- Predpoklad **správneho monitoringu a skonsolidovaných časových informácií naprieč celou IT infraštruktúrou** je významnou pomocou, ale stále neposkytuje ochranu pred množstvom sofistikovaných útokov, ktoré by mohli ohroziť operatívu a spôsobiť významné materiálne straty a straty renomé.
- Systémy SIEM (Security Incident and Event Management) sú nástrojom, ktorý preberá z pliec bezpečnostného analytika úlohu konsolidácie a kontroly rôznych typov logových záznamov zo serverov, IDS/IPS zariadení, klientských staníc, sieťových zariadení, databáz, zariadení na kontrolu prístupu atď.

KPMG
cutting through complexity™

Systémy pre automatizované vyhodnocovanie bezpečnostných udalostí (SIEM) – pokr.

- Takýchto logových záznamov sú obrovské kvantá, SIEM zabezpečuje ich triedenie, vyhodnocovanie, ich združovanie do vlákien a ich vizualizáciu v reálnom čase. Tieto kroky prispievajú k včasnému varovaniu a promptnej eliminácii potenciálnych hrozieb.
- Riešenie pre SIEM typicky ukladá, triedi, konsoliduje a vyhodnocuje logovacie záznamy. Hľadá vzťahy medzi udalosťami, prioritizuje, štatisticky spracováva a vizualizuje bezpečnostné incidenty kvôli ich posúdeniu bezpečnostným analytikom.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

BEZPEČNOSTNÉ INCIDENTY, ZODPOVEDNOSŤ ZA ICH NAHLASOVANIE A RIEŠENIE

KPMG
cutting through complexity™

Bezpečnostné incidenty, zodpovednosť za ich nahlasovanie a riešenie

- Bezpečnostným incidentom rozumieme udalosť, ktorá má potenciálne negatívny dopad na prevádzku a chránené aktíva. Je zodpovednosťou organizácie kategorizovať udalosti, ktoré by mali byť posudzované ako incidenty a kategorizovať ich. Ich výskyt by mal spúšťať proces eskalácie a v súvislosti s ním by mali byť podniknuté systematické kroky pre bezprostredné zabránenie incidentu.
- Incidentom môže byť napríklad:
  - preniknutie útočníka do systému,
  - odopretie služby (anglicky Denial of service, DoS), prípadne špeciálny typ distribuovaného odopretia služby, kedy je útok realizovaný z mnohých IP adries (Distributed DoS, DDoS), takže je ťažšia jeho prevencia,
  - prítomnosť škodlivého kódu,
  - poškodenie/krádež komponentov IKT.

Bezpečnostné incidenty, zodpovednosť za ich nahlasovanie a riešenie (pokr.)

- Spôsoby použité pri realizácii útokov zahŕňajú:
  - napadnutie samotnej aplikácie a zneužitie jej zraniteľností,
  - použitie techník sociálneho inžinierstva, alebo nainštalovania škodlivého kódu na konkrétne pracovné stanice (odchytávanie stlačených kláves, odpočúvanie, snímanie obrazu) kvôli získaniu cenných informácií,
  - priame zneužitie privilegovaného prístupu iných používateľov systému, operátorov, alebo administrátorov,
  - použitie slovníkových útokov na slabé heslá v informačnom systéme a následná eskalácia privilégií,
  - násilné činy vlámania, vydierania a krádeže pre získanie prístupu k inkriminovanému systému, alebo jeho dátam.

Bezpečnostné incidenty, zodpovednosť za ich nahlasovanie a riešenie (pokr.)

- Incident sa môže v IKT prostredí prejavovať:
  - úplnou nefunkčnosťou systému – hardvérový komponent, alebo informačný systém nereaguje, alebo nie je prístupný,
  - zmeneným obsahom webovej stránky – pôvodný obsah webovej stránky bol zmenený kvôli chybe v systéme, alebo úmyselne prepísaný útočníkom,
  - neobvyklou sieťovou aktivitou – dajú sa pozorovať určité anomálie oproti štandardnej prevádzke, nezodpovedajúca frekvencia činností používateľov, alebo podozrivé druhy činností,
  - neobvyklou záťažou systému - veľké preťaženia systému, ktoré vedú k odopretiu dostupnosti služby,
  - podozrivými záznamami v logoch – ak auditné záznamy nie sú konzistentné so skutočným správaním systému, nedá sa vylúčiť riziko, že systém je skompromitovaný a útočník tieto auditné záznamy pozmenil.

Bezpečnostné incidenty, zodpovednosť za ich nahlasovanie a riešenie (pokr.)

- Fázy riešenia bezpečnostných incidentov:
  - kategorizácia vzniknutých udalostí (eventov) - pri riešení bezpečnostných incidentov sa bez ohľadu na použitú metodológiu začína triedením vzniknutých incidentov podľa ich dôležitosti posúdením ich dopadu na IKT infraštruktúru. Zatriedenie býva v praxi realizované automatizovanými nástrojmi manažmentu bezpečnostných udalostí a incidentov (Security incident and event management, SIEM),
  - detekcia potenciálnych incidentov – použitím skúseností a vedomostí z predchádzajúcej fázy sa v tomto kroku zisťuje, nakoľko pravdepodobné je, že konkrétna udalosť by mohla mať dopad na komponenty IKT,

Bezpečnostné incidenty, zodpovednosť za ich nahlasovanie a riešenie (pokr.)

- obnova bežnej prevádzky – po vyriešení incidentu obvykle dochádza ku fáze obnovy prevádzky (ale nie nutne). Návrhy opatrení na obnovu štandardnej prevádzky sú formalizované v rámci plánovania kontinuity činností (Business Continuity Managment - BCM) a plánu obnovy po havárii (Disaster Recovery Planning - DRP). Plán obnovy po havárii v písomnej forme definuje procedúry, ktoré má organizácia podniknúť pred, počas a po vzniku havárie na obnovu štandardného stavu. Táto havária môže mať prírodný charakter (prírodná katastrofa), alebo to môže byť dôsledok ľudskej činnosti (úmyselnej, alebo neúmyselnej). Plány zahŕňajú podrobnosti postupov obnovy dôležitých dát, informačných aktív a prevádzky ako celku.
- zhodnotenie úspešnosti metodiky riešenia incidentov, úspešnosti obnovy pôvodnej kvality služieb a prípadná úprava metodológie riešenia bezpečnostných incidentov s ohľadom na zmenu podmienok a situácie. Cieľom zhodnotenia úspešnosti je určiť vhodné prístupy ku riešeniu vzniknutých incidentov. Táto fáza môže zahŕňať interný, alebo externý audit a s ním súvisiacu optimalizáciu procesov v organizácii pomocou štúdia dostupnej dokumentácie, rozhovorov s personálom a ohodnotením kvality použitej technológie.

Bezpečnostné incidenty, zodpovednosť za ich nahlasovanie a riešenie (pokr.)

- Interná dokumentácia by mala byť adekvátne aktualizovaná a mala by obsahovať údaje o tom, aké nápravné opatrenia boli podniknuté a kto ich vykonal.
- Na doplnenie dokumentácie je možné využiť nástroje správy riadenia zmien, tzv. „service desk“, alebo „helpdesk“ nástroje (konkrétnym takým riešením je napr. HP ITSM).

Bezpečnostné incidenty, zodpovednosť za ich nahlasovanie a riešenie (pokr.)

- Dokumentácia existujúcej infraštruktúry by mala zahŕňať:
  - topológiu siete,
  - podrobnosti o konfigurácii serverov a sieťových zariadení vrátane bezpečnostných nastavení,
  - nastavenia pracovných staníc,
  - kontakty na zodpovedné osoby.
- Ľudia, ktorí spravujú IKT by mali mať dostatočnú technickú spôsobilosť a mali by byť v prípade incidentu schopní citlivo zasiahnuť v krátkom časovom intervale. Zodpovednosť za riešenie bezpečnostných incidentov je obvykle pridelená bezpečnostnému manažérovi (anglicky „security officer“), alebo zamestnancovi oddelenia IT v príslušnej roli.

Bezpečnostné incidenty, zodpovednosť za ich nahlasovanie a riešenie (pokr.)

- Typicky sa opakovanie rovnakých incidentov dá eliminovať alebo aspoň zmierniť:
  - Zmenou politík,
  - Zmenou procedúr
  - Ráznejším vynucovaním dodržiavania pravidiel
  - zmenou konfigurácie operačného systému, resp. aktualizáciou relevantného softvéru.
  - aktualizáciou antivírusovej databázy, alebo databázy IDS/IPS charakteristík (anglicky nazývaných „signatures“, ktoré sú detekovateľnými vzormi útokov, na základe nich je možné identifikovať a zabrániť útoku),
  - eliminációu chýb aplikačného softvéru - na tieto činnosti je nutné pracovať s odborne zdatnými vývojármi a administrátormi (či už z interných zdrojov, alebo zdrojov dodávateľa), ktorí sú schopní chybu nielen zachytiť, ale aj urýchlene riešiť.

Bezpečnostné incidenty, zodpovednosť za ich nahlasovanie a riešenie (pokr.)

- V procese aktualizácie musí byť pre prípad jej neúspechu umožnená obnova do predošlej funkčnej verzie, tzv. „rollback“. Medzi najdôležitejšie vlastnosti riešení centrálneho riadenia údržby operačných systémov patrí centrálna správa aktualizácií, selektívna distribúcia balíčkov, ktoré sa majú nainštalovať na konkrétny systém, zálohovanie a monitorovanie „zdravia“ serverov.

Bezpečnostné incidenty, zodpovednosť za ich nahlasovanie a riešenie (pokr.)

- Nahlasovanie incidentov
  - Formálne nahlasovanie incidentu môže byť iniciované:
    - zistením z priebežným monitorovaním auditných záznamov,
    - automatizovaným vyhodnotením incidentu z IDS/IPS,
    - alarmom z monitoringu, alebo z antivírusového systému,
    - signalizáciou iného incidentu postúpeného zo systému manažmentu bezpečnostných udalostí a incidentov (SIEM),
    - spozorovaniu neštandardného správania na používateľskej úrovni,
    - spozorovanie porušenia bezpečnostnej politiky organizácie alebo len pokusu o jej porušenie
- Kto a ako musí nahlásiť incident?
  - Sú potrebné štruktúrované a systematicky aktualizované postupy pre nahlasovanie incidentov s jasne vyhradenými právami, povinnosťami a zodpovednosťami za ich riešenie.

Ministerstvo financií Slovenskej republiky

EFQM Recognised for excellence 5 star - 2012

Automatizácia detekcie a riešenia bezpečnostných incidentov

- Nahlasovanie bezpečnostných incidentov je často automatizované vďaka riešeniam monitoringu prevádzky a manažmentu bezpečnostne relevantných incidentov (SIEM).
- Manažment bezpečnostných udalostí a incidentov funguje na princípe zbierania auditných záznamov do centrálneho servera na analýzu prevádzky danej sieťovej infraštruktúry.
- Tieto dáta sú neskôr interpretované v reportoch a poskytnuté koncovému používateľovi systému (spravidla sa jedná o bezpečnostného manažéra), aby mu uľahčili prácu pri identifikovaní rizík.

KPMG cutting through complexity™

Automatizácia detekcie a riešenia bezpečnostných incidentov

- Proces činnosti systémov SIEM by sa dal schematicky znázorniť v nasledovných krokoch:
  - zbieranie - prijímanie logov cez protokoly na to určené ako je SNMP (aktívne) a Syslog (pasívne),
  - normalizácia - normalizácia logovacích záznamov z rozličných systémov (rôznych výrobcov, rôznych produktov, systémov, zariadení, apod.), normalizácia formátu časových údajov apod.,
  - obohatenie - pridanie verejne známeho údaju o použitom exploite, súvisiacich informácii o aktuálnom stave siete, vlastných výsledkoch penetračného testu (známe zraniteľnosti nášho systému) atď.,
  - korelácia - zoskupovanie podobných udalostí, priradenie príslušnej dôležitosti, označenie obzvlášť zaujímavých udalostí apod.

Ministerstvo financií Slovenskej republiky

EFQM Recognised for excellence 5 star - 2012

Automatizácia detekcie a riešenia bezpečnostných incidentov

- Systém SIEM redukuje množstvo informácii, ktoré by bezpečnostný analytik musel ručne spracovávať, zvýrazňuje abnormálne správanie v IT infraštruktúre a tiež redukuje falošne pozitívne, alebo falošne negatívne výsledky.
- Oddeľovanie bežnej aktivity od nebezpečnej sa deje tiež formou konsolidácie logovacích riadkov do vlákien (angl. „threadov“) a užitočnou funkciou je tiež ich zapúzdrenie do udalostí (angl. „eventov“).
- Jednou z mnohých výhod zavedenia SIEM je teda úspora nákladov pri prevádzke rutinnej bezpečnostnej analýzy a tiež zníženie vplyvu zlyhania ľudského faktoru v tomto procese.

KPMG cutting through complexity™

Forenzná analýza a honeypot/honeynet systémy

- Pokiaľ dôjde k závažnému napadnutiu systému a je nutné ho podrobiť forenznej analýze, často býva pravidlom zabezpečiť jeho odpojenie od prevádzky kvôli forenznej analýze.
- Takýto postup je však možný iba vtedy, ak má systém redundantnú náhradu. Úžitok z analýzy príčin incidentu na odpojenom systéme by mal byť väčší ako škody spôsobené jeho odpojením.

Forenzná analýza a honeypot/honeynet systémy (pokr.)

- Oddelenie napadnutého systému od ostatných systémov v prevádzke pomáha predísť ďalšiemu rozširovaniu následkov incidentu, ale v prípade, že má útočník na systéme implementovaný škodlivý mechanizmus, ktorý takú izoláciu deteguje a pri takýchto snahách napríklad poškodí súborový systém, je možné, že odpojením spôsobíme ešte väčšiu škodu.
- Z tohto dôvodu je vhodnejšie citlivo izolovať ostatné systémy v prevádzke a tým ich ochrániť pred následkami kritických incidentov. V praxi sa často používajú nastrčené tzv. „honeypot“ systémy, ktoré môžu byť spojené do sietí („honeynet“).

Forenzná analýza a honeypot/honeynet systémy (pokr.)

- Tieto simulujú reálne produkčné systémy kvôli získavaniu informácii o útočníkoch. Môžu byť neaktualizované a zraniteľné voči útokom, prípadne nakonfigurované ako ľahká korisť pre útočníka.
- Pri uskutočnení útoku však zaznamenávajú a zachytávajú všetku útočníkovu činnosť a poskytnú svojmu vlastníkovi informácie o používaných technikách, použitom škodlivom kóde a nástrojoch.
- Problémom sú ťažko detekovateľné riziká, akými sú zadné dvierka („backdoory“), alebo prekompilované systémové, alebo aplikačné binárne súbory. Pri sofistikovaných útokoch nemusí ani podrobná analýza odhaliť takéto zmeny v systéme.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Otázky?

KPMG
cutting through complexity™