Kritické bezpečnostné opatrenia

CSIRT.SK na základe materiálu vypracovaného inštitútom SANS
26.11.2012

Obsah

Zoznam použitých skratiek a cudzích slov

ACL (Access Control Lists) – zoznamy, ktoré určujú, kto alebo čo má povolenie pristupovať k objektu a aké operácie s ním môže vykonávať

AES (Advanced Encryption Standard) - je symetrická bloková šifra (pre šifrovanie a dešifrovanie využíva rovnaký kľúč na dáta s pevne danou dĺžkou bloku)

APT (Advanced Persistent Threat) - pokročilá pretrvávajúca hrozba – sieťový útok, pri ktorom neautorizovaná osoba získa prístup do siete a dlhodobo v nej pretrváva nedetegovaná s cieľom krádeže dát

buffer overflow (pretečenie vyrovnávacej pamäte) - chyba v programe, ktorá vedie k zápisu mimo vyhradeného priestoru v pamäti a k chybnému behu, prípadne aj k pádu programu

CCE (Common Configuration Enumeration) – poskytuje jedinečné identifikátory pre problémy spojené s konfiguráciou systémov na rýchlu a presnú koreláciu konfiguračných dát z viacerých zdrojov a nástrojov

clickjacking - spôsob útoku na používateľov webových stránok, pri ktorom používateľ nejakou činnosťou na zdanlivo neškodnej stránke (napr. kliknutím na tlačidlo či obrázok) spustí akciu, ktorú nepredpokladal

command injection – cieľom tohto útoku je vsunúť a vykonať útočníkom určený príkaz v zraniteľnej aplikácií

CPE (Common Platform Enumeration) – štandardizovaná metóda popisovania a identifikácie druhov aplikácií, operačných systémov a hardvérových zariadení zahrnutých do aktív organizácie

Cross-site Request Forgery - jedna z metód útoku na internetové aplikácie (typicky implementované skriptovacími jazykmi alebo cgi) pracujúca na báze neočakávanej resp. nezamýšľanej požiadavky pre vykonanie určitej akcie v tejto aplikácií, ktorý ale pochádza z nelegitímneho zdroja

cross-site scripting - metóda narušenia WWW stránok využitím bezpečnostných chýb v skriptoch (predovšetkým neošetrené vstupy)

CSIRT/CERT – Computer Security Incident Response Team/Computer Emergency Response Team – tím pre riešenie bezpečnostných počítačových incidentov

CVE (Common Vulnerabilities and Exposures) – zoznam verejne známych zraniteľností a odhalení informačnej bezpečnosti

CVSS (Common Vulnerability Scoring System) – štandard na posudzovanie závažnosti bezpečnostných zraniteľností počítačových systémov

CWE (Common Weakness Enumeration) – zoznam bezpečnostných zraniteľností softvéru, ktorý slúži ako jazyk na ich popísanie, poskytuje možnosť hodnotenia nástrojov zameraných na tieto zraniteľnosti a predstavuje štandard na identifikáciu, zmierňovanie a prevenciu zraniteľností

časová pečiatka (time stamp) – identifikátor, ktorý jednoznačne definuje čas s rôznou granularitou

červený tím – nezávislá skupina, ktorú si organizácia najíma na zvýšenie efektívnosti, pokúša sa o škodlivé prieniky (fyzické, virtuálne), aby odhalila slabé miesta v systémoch

DEP (Data Execution Prevention) - funkcionalita OS, ktorá má za cieľ predchádzať spusteniu kódu z oblasti pamäte označenej ako non-executable memory region, tj. oblasti, v ktorej nie je možné spúšťať akýkoľvek kód.

directory traversal attack (útok prechádzania do adresárov) – spočíva v zneužití nedostatočnej bezpečnostnej validácie používateľom vložených názvov súborov

DLP (Data loss prevention) – systém, ktorý je navrhnutý tak, aby detegoval a predchádzal potenciálnym incidentom súvisiacim s narušením dát na koncových staniciach, v sieťovej prevádzke a ukladaných dát

DMZ (demilitarizovaná zóna) – časť siete (oddelenej od zvyšku siete) ktorá sa používa na oddelenie LAN od Internetu

DNS (domain name system) - systém, ktorý ukladá prístup k informácii o názve stroja (hostname) a názve domény v istej distribuovanej databáze v počítačových sieťach ako internet, poskytuje mechanizmus získania IP adresy pre každé meno stroja (lookup) a naopak (reverse)

EAP-TLS (Extensible Authetication Protocol-Transport Layer Security) – autentifikačný protokol pre bezdrôtové siete
ENISA (European Network and Information Security Agency) - Európska agentúra pre bezpečnosť sietí a informácií
FDCC (Federal Desktop Core Configuration) – zoznam bezpečnostných nastavení odporúčaný NIST (National Institute of Standards and Technology) pre počítače, ktoré sú priamo napojené do siete vládnej agentúry Spojených Štátov
FTP (File Transfer Protocol) - TCP/IP protokol určený na prenos súborov medzi počítačmi, či už na internete alebo lokálnej sieti
halda – druh jednoduchej stromovej dátovej štruktúry
hardening – proces zvyšovania bezpečnosti systému a odstraňovania zraniteľností pomocou odobratia nepotrebného softvéru, používateľských účtov, služieb, aplikáciou záplat, zatváraním nepotrebných portov, nasadením IDS, IPS a špecifických nastavení aplikácií
honeypot – nastražená pasca (izolovaný počítačový systém) na detekciu a marenie neoprávnených aktivít útočníkov
honeytoken – honeypot, ktorý nie je počítačovým systémom
HTTP (Hypertext transfer protocol) - protokol na prenos html dokumentov medzi servermi a klientmi služby WWW
IDS (Intrusion Detection System) – systém na detekciu prieniku
IP – internet protokol
IPS (Intrusion Prevention System) – systém na prevenciu prieniku
IPsec (Internet Protocol Security) - bezpečnostné rozšírenie IP protokolu založené na autentifikácií a šifrovaní každého IP datagramu
IPv6 -verzia 6 Internet protokolu
IS – informačný systém – v tomto dokumente chápané širšie ako súhrn HW, operačného, aplikačného a ďalšieho SW, sieťovej infraštruktúry a jej prvkov
Keylogger (Keystroke Logger) je software alebo hardware, ktorý zaznamenáva stlačenia jednotlivých kláves
LANMAN haš (LAN Manager hash) – bol primárny haš, ktorý Microsoft LAN Manager a Microsoft Windows (pred Windows NT) používali na ukladanie hesiel
MAC (Media Access Control) - riadenie prístupu k médiu
Middleware - počítačový softvér, ktorý prepája softvérové komponenty alebo osoby a ich aplikácie
NTP (Network Time Protocol) - protokol pre synchronizáciu vnútorných hodín počítačov po paketovej sieti s premenlivým oneskorením, zaisťuje, aby všetky počítače v sieti mali rovnaký a presný čas
OS – operačný systém
OVAL (Open Vulnerability and Assessment Language) – snaha o štandardizáciu posudzovania a nahlasovania stavu strojov v počítačových systémoch
PEAP (Protected EAP) – protokol, ktorý enkapsuluje EAP v rámci šifrovaného a autentifikovaného TLS tunela
ping (Packet InterNet Groper) - umožňuje preveriť funkčnosť spojenia medzi dvoma sieťovými rozhraniami (počítača, sieťového zariadenia) v počítačovej sieti
proxy server - server počítačovej siete, ktorý umožňuje klientom nepriame pripojenie k inému serveru
RDP (Remote Desktop Protocol) - sieťový protokol, ktorý umožňuje používateľovi ovládať vzdialený počítač prostredníctvom pripojenia k jeho desktopovému prostrediu
SANS Institute - System Administration, Networking And Security Institute
SIEM (Security Information and Event Management) - manažment bezpečnostných informácií a udalostí
sniffer - počítačový program alebo hardvér, ktorý dokáže zachytiť a logovať prevádzku prechádzajúcu cez sieť alebo jej časť
SPF (Sender Policy Framework) – systém na overovanie e-mailov navrhnutý tak, aby sa zabránilo spamu pomocou detegovania e-mail spoofingu (overovaním IP adries)

spoofing - je typ útoku, pri ktorom osoba, alebo program maskuje svoju totožnosť a tvári sa ako druhá osoba
SQL injection - technika napadnutia databázovej vrstvy programu vsunutím (odtiaľ „injection“) kódu cez neošetrený vstup a vykonanie vlastnej, pozmenenej, SQL požiadavky
SSH (Secure shell) - počítačový program ako aj súvisiaci sieťový protokol určený na prihlasovanie a vykonávanie príkazov na vzdialenom počítači v počítačovej sieti
SSID (Service Set Identifier) - je jedinečný identifikátor každej bezdrôtovej (WiFi) počítačovej siete
SSL (Secure Sockets Layer) – protokol, ktorý slúži na šifrovanie dát a bezpečnú komunikáciu cez internet (hlavne prehliadanie webu, odosielanie e-mailov, výmenu správ a iné prenosy dát)
SSL offloading – zbavuje webový server záťaže spôsobenej šifrovaním a dešifrovaním prevádzky posielanej cez SSL
SYN/ACK (Synchronize Acknowledge) – pri nadväzovaní spojenia pošle klient úvodný SYN segment serveru. Server by mal odpovedať platnou požiadavkou SYN so SYN/ACK. Nakoniec by mal klient odpovedať ACK a fáza nadviazania spojenia sa ukončí.
tarpit – technika čo možno najdlhšieho oneskorovania prichádzajúcich spojení ako obrana proti počítačovým červom
TCP (Transmission Control Protocol) – Vďaka TCP môžu programy na počítačoch v sieti vytvárať medzi sebou *spojenia* (*connections*), ktorými je možné posielať dáta
URL (Uniform Resource Locator) - univerzálny formát mien používaný na označenie zdroja na internete
UTM – zariadenie, ktoré má v sebe integrované mnohé bezpečnostné funkcie: firewall, IPS, antivírus, antispam, VPN, filtrovanie obsahu, vyvažovanie záťaže, DLP a reporting
VLAN (Virtual Local Area Network) - virtuálna lokálna sieť
VNC (Virtual Network Computing) - grafický program, ktorý umožňuje vzdialené pripojenie ku grafickému používateľskému rozhraniu pomocou počítačovej siete
VoIP (Voice over Internet Protocol) – je prenos komunikácie uskutočňovanej ľudským hlasom cez Internet alebo inú sieť založenú na protokole IP
VPN (Virtual Private Network) - počítačová sieť na prepojenie počítačov na rôznych miestach internetu do jednej virtuálnej počítačovej siete. Aj keď počítače môžu byť vo fyzicky nezávislých sieťach na rôznych miestach sveta, prostredníctvom virtuálnej privátnej siete medzi sebou môžu komunikovať, ako keby boli na jednom sieťovom segmente
wardriving - mapovanie nezabezpečených bezdrôtových prístupových bodov
WIDS (Wireless Intrusion Detection Systems) – systém na detekciu bezdrôtového prieniku, sleduje rádiové spektrum na prítomnosť neautorizovaných/podvodných prístupových bodov a použitia bezdrôtových útočných nástrojov
WPA2 (Wi-Fi Protected Access 2) – poskytuje ochranu dát a riadenie prístupu k sieti v súvislosti s WI-Fi, zabezpečuje, že len oprávnení používatelia majú prístup k bezdrôtovým sieťam
XCCDF (The Extensible Configuration Checklist Description Format) – špecifikačný jazyk pre písanie bezpečnostných kontrolných zoznamov (checklists), testov (benchmarks) a súvisiacich dokumentov

20 kritických bezpečnostných opatrení

Úvod

Zaistenie ochrany pred útokmi na informačné systémy verejnej správy by malo byť jednou z najvyšších priorít SR. Na dosiahnutie tohto cieľa je potrebné, aby počítačové siete a systémy dokázali odolať širokému spektru interných a externých hrozieb. V prípade úspešného útoku musia byť pripravené obranné mechanizmy, ktoré umožnia detegovať a zmariť prebiehajúce útoky. Kritickou súčasťou takýchto mechanizmov je neustály monitoring, čiže schopnosť automatizovaným spôsobom testovať a overovať, či sú súčasné bezpečnostné opatrenia funkčné a proaktívne a včas ošetrovať zraniteľnosti.

Hlavnou zásadou kybernetickej obrany je: *„Útok má poskytovať informácie obrane“*. Inými slovami povedané, znalosť prebiehajúcich útokov ohrozujúcich informačné systémy poskytuje nevyhnutný základ informácií, na ktorom možno postaviť efektívnu obranu. Obranné mechanizmy musia brať do úvahy moderné trendy útokov, reagovať na ne a prispôsobovať sa im.

Pretože verejná správa má na zabezpečenie ochrany a efektívnej obrany svojich informačných systémov obmedzené prostriedky, je potrebné tieto zdroje využiť efektívne a sústrediť sa predovšetkým na ochranu kritických systémov.

Americký SANS Institute vytvoril dokument “20 Critical Security Controls“, čo je 20 prioritizovaných oblastí opatrení, ktoré sú aplikovateľné na rôzne typy organizácií a ktoré sú efektívne na blokovanie v súčasnosti známych útokov s vysokou prioritou a útokov očakávaných v blízkej budúcnosti. Je vhodné upozorniť, že ide o opatrenia technického charakteru. Na dosiahnutie komplexnej ochrany informačných systémov je potrebné vziať do úvahy aj ostatné aspekty informačnej bezpečnosti, ako napríklad bezpečnostné politiky, organizačná štruktúra, personálna, fyzická bezpečnosť a iné.

Navrhované opatrenia sú navrhnuté tak, aby mohli podporiť organizácie s rôznymi úrovňami informačnej bezpečnej bezpečnosti. V každej z 20 oblastí sú opatrenia zaradené do štyroch kategórií:

- *Rýchle výhry (Quick wins)* – ide o základné aspekty informačnej bezpečnosti, ktoré umožnia rapídne zvýšiť bezpečnosť bez významnejších procesných, technických alebo zásahov do architektúry. Tieto opatrenia však neposkytujú rozsiahlejšiu ochranu voči najkritickejším útokom.
- *Lepšia prehľadnosť a priraďovanie (Improved visibility and attribution)* – opatrenia z tejto kategórie sú zamerané na zlepšenie procesov, architektúry a technických možností pre lepší monitoring sietí, počítačových systémov a sprehľadnenie IT procesov. Pod priraďovaním je myslené určovanie počítačových systémov, prípadne používateľov a ich spájanie so špecifickými udalosťami. Lepšia prehľadnosť a priraďovanie pomôže organizácii detegovať pokusy o útok, lokalizovať miesta vstupu úspešných útokov, identifikovať kompromitované systémy, prerušiť aktivity infiltrovaných útočníkov a získať informácie o zdrojoch útokov.
- *Spevnená konfigurácia a lepšia očista (Hardened configuration and improved information security hygiene)* – opatrenia navrhnuté pre zvýšenie informačnej bezpečnosti znížením počtu a rozsahu potenciálnych zraniteľností a zlepšením procesov prepojených počítačových

systémov. Opatrenia v tejto kategórii sú navrhnuté so zreteľom na fakt, že dobre udržiavaná a riadená sieť je väčšinou ťažším cieľom pre potenciálnych útočníkov.

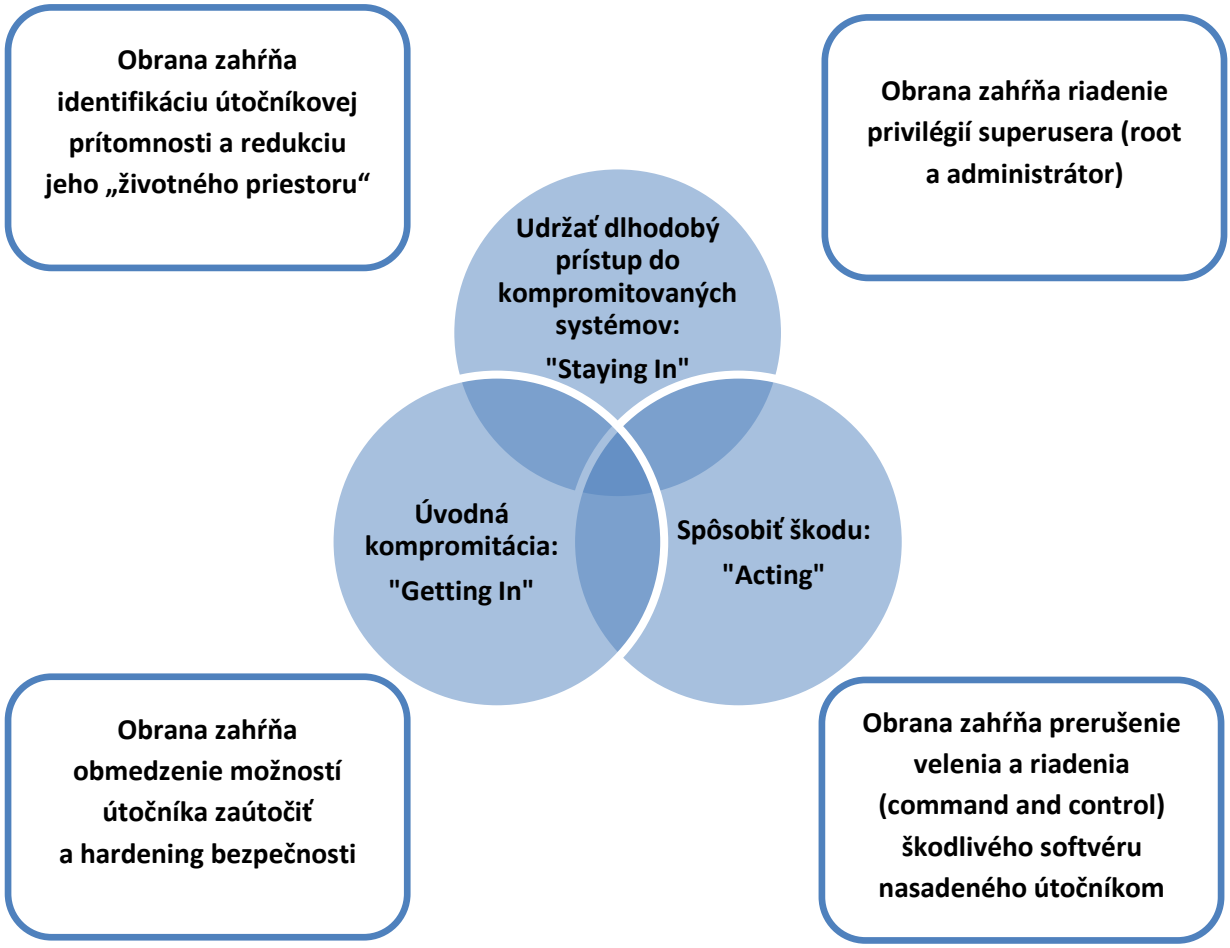
- *Pokročilé (Advanced)* – opatrenia v tejto kategórii ponúkajú zlepšenie bezpečnosti organizácie nad rámec ostatných kategórií a sú určené pre tých, ktorí už zaviedli všetky opatrenia z predchádzajúcich kategórií. Tieto opatrenia sú určené najmä ako súčasť obrany pred APT.

Organizácie by mali porovnať opatrenia zo všetkých 20 oblastí a ich kategórií s aktuálnym stavom zabezpečenia a vytvoriť plán zavádzania týchto opatrení ako kritickú súčasť celkovej ochrany IS organizácie. Organizácie s nižšou úrovňou bezpečnosti IS by mali začať s implementáciou opatrení z kategórie „Rýchle výhry" pre dosiahnutie rýchleho zlepšenia. Následne je potrebné aplikovať všetky kategórie oblastí opatrení. Každá oblasť opatrení tiež obsahuje sekciu metrík a testovaciu sekciu.

20 kritických opatrení

Tento zoznam obsahuje opatrenia, ktoré je možné priebežne monitorovať a overovať aspoň z časti automatizovaným spôsobom a opatrenia, ktoré musia byť overované manuálne.

1. Inventár autorizovaných a neautorizovaných zariadení.
2. Inventár autorizovaného a neautorizovaného softvéru.
3. Bezpečné konfigurácie hardvéru a softvéru na notebookoch, pracovných staniciach a serveroch.
4. Priebežné posúdenie zraniteľností a ich odstránenie.
5. Ochrana pred škodlivým softvérom.
6. Bezpečnosť aplikačného softvéru.
7. Opatrenia pre bezdrôtové zariadenia.
8. Schopnosť obnovy dát (overované manuálne).
9. Posúdenia bezpečnostných schopností a vhodné školenia (overované manuálne).
10. Bezpečná konfigurácia sieťových zariadení ako firewally, routery a switche.
11. Obmedzenia a opatrenia pre sieťové porty, protokoly a služby.
12. Riadenie administratívnych privilégií.
13. Ochrana perimetra.
14. Údržba, monitoring a analýza bezpečnostných auditných log záznamov.
15. Kontrola prístupu založená na princípe „need to know".
16. Monitoring a riadenie používateľských účtov.
17. Predchádzanie strate dát (Data Loss Prevention).
18. Schopnosť reakcie na incidenty (overované manuálne).
19. Bezpečné sieťové inžinierstvo.
20. Penetračné testy



Obrázok 1 Aktivity počítačových útočníkov a súvisiaca obrana voči nim

Krúžky na *Obrázku 1* znázorňujú činnosti, ktoré vykonávajú útočníci na cieľové zariadenia. Patrí sem úvodné napadnutie stroja využitím jednej, alebo viacerých zraniteľností. Útočníci potom môžu udržať dlhodobý prístup do systému vytvorením používateľských účtov, narušením existujúcich účtov, alebo pozmenením softvéru na strojoch – vložením zadných vrátok (back door) a root kitov (slúži na utajenie škodlivých aktivít). Útočníci s prístupom na stroje môžu spôsobiť škody krádežou, pozmenením alebo zničením informácií, oslabením funkcionality systému s cieľom ohroziť efektivitu procesov alebo plnenia úloh, alebo využívaním napadnutých strojov ako vstupného bodu na kompromitáciu ostatných systémov. Na mieste, kde sa krúžky prekrývajú, existuje vyššia šanca a schopnosť kompromitácie citlivých informácií a spôsobenia škody. V rámikoch okolo krúžkov sú uvedené rôzne stratégie obrany proti týmto činnostiam, ktoré sú pokryté opatreniami opísanými v tomto článku.

Kritické opatrenie 1: Inventár autorizovaných a neautorizovaných zariadení

Ako útočníci zneužívajú absenciu tohto opatrenia?

Mnohé kriminálne skupiny a národné štáty nasadzujú systémy, ktoré neustále skenujú adresný priestor cieľových organizácií a vyčkávajú na pripojenie nových a ešte nezabezpečených systémov do siete. Taktiež vyhľadávajú napr. notebooky, ktoré nemajú aktualizovaný operačný systém, pretože nie sú pravidelne pripojené do siete. Útočníci, ktorí už získali prístup do siete potom hľadajú ďalšie nedostatočne zabezpečené systémy. Tiež často hľadajú aj experimentálne systémy a systémy v testovacej prevádzke. Napriek tomu, že väčšinou neobsahujú citlivé dáta, často poskytujú útočníkovi vstupnú bránu do siete organizácie.

Ako implementovať, automatizovať a merať účinnosť tohto opatrenia

Vhodný a aktuálny inventár s aktívnym monitoringom a konfiguračným manažmentom môže znížiť šance útočníkov nájsť neautorizované a nezabezpečené systémy, ktoré sú potenciálne zneužiteľné.

1. *Rýchle výhry*: Nasadiť nástroj na automatizované zisťovanie aktív na vytvorenie predbežného inventáru systémov pripojených do siete organizácie. Nasadené by mali byť aktívne nástroje skenujúce adresný priestor aj pasívne nástroje identifikujúce hostiteľov (hosts) analýzou prevádzky.
2. *Prehľadnosť a priraďovanie*: Udržiavať inventár aktív všetkých systémov pripojených do siete, ako aj samotných sieťových zariadení spolu s ich sieťovou adresou, názvom, účelom, vlastníkom a oddelením organizácie. Takýto inventár by mal obsahovať každé zariadenie s IP adresou, ktoré je zapojené do siete (počítače, notebooky, servery, sieťové zariadenia, tlačiarne, úložné priestory a VoIP telefóny.
3. *Prehľadnosť a priraďovanie*: Inventár aktív musí obsahovať informáciu o tom, či je dané aktívum prenosné. Zariadenia ako mobilné telefóny, tablety, notebooky a i. musia byť identifikované bez ohľadu na to, či sú pripojené do siete, alebo nie.
4. *Prehľadnosť a priraďovanie*: Uistiť sa, že nástroje na monitorovanie inventáru sú funkčné a priebežne monitorujú. Ďalej udržiavať inventár aktív aktuálny v reálnom čase, hľadať odchýlky od predpokladaného inventáru aktív v sieti a v prípade objavenia odchýlky upozorňovať bezpečnostných zamestnancov.
5. *Konfigurácia a očista*: Zabezpečiť databázu inventáru aktív a s ňou súvisiacich systémov, ubezpečiť sa, že je na nich pravidelne vykonávané skenovanie zraniteľností a že informácie o aktívach sú šifrované. Obmedziť prístup do týchto systémov len autorizovaným zamestnancom a ukladať log záznamy prístupov. Doplnkovým opatrením môže byť zálohovanie inventáru na offline systéme oddelenom od produkčného systému.
6. *Konfigurácia a očista*: Okrem inventáru hardvéru by mala organizácia viesť inventár informačných aktív, ktorý obsahuje kritické informácie organizácie a mapuje tieto informácie k ich hardvérovým aktívam, na ktorých sa nachádzajú.
7. *Konfigurácia a očista*: Nasadiť autentifikáciu na úrovni siete (Network Level Authentication) prostredníctvom protokolu 802.1x pre obmedzenie a kontrolu zariadení, ktoré môžu byť pripojené do siete.

8. *Pokročilé*: Je možné použiť kontrolu prístupu do siete na monitorovanie autorizovaných systémov, aby bolo možné v prípade útoku znížiť dôsledky daného útoku presunutím dotknutého systému do VLAN, ktorá má minimálny prístup.

Postupy a nástroje na implementáciu a automatizáciu týchto opatrení

Organizácia musí v prvom rade určiť vlastníkov aktív a informácií, následne určiť a zdokumentovať zodpovednosti za každý komponent informačného systému. Pri zavádzaní nových systémov do organizácie je vhodné zaznamenať vlastníka a funkcie každého aktíva spolu s MAC adresou a unikátnym identifikátorom, ktorý je napevno vložený do väčšiny sieťových zariadení a kariet.

Keď je vytvorený inventár aktív, mnoho organizácií získava informácie o jednotlivých strojoch zo sieťových zariadení ako switche a routery. Tieto informácie (obsahujúce MAC adresy a iné) sú potom zlučované s inventárom aktív organizácie. Je možné zaviesť periodické skenovanie siete na identifikáciu pripojených zariadení prostredníctvom komerčných, alebo voľne dostupných nástrojov (posielanie ping, TCP, SYN, alebo ACK paketov). Ako prídavok k aktívnym nástrojom je možné zaviesť aj pasívne nástroje na identifikáciu zariadení, ktoré sledujú sieťovú prevádzku a na jej základe identifikujú zariadenia, ktoré ju vytvárajú).

Rovnako ako pevne pripojené zariadenia, by mali byť zahrnuté do inventáru aktív aj zariadenia, ktoré sa na sieť pripájajú zriedkavo. Ide prevažne o pripojenia pomocou WiFi (bezdrôtové pripojenie), VPN (virtuálna privátna sieť), či virtuálne stroje.

Kritické opatrenie 2: Inventár autorizovaného a neautorizovaného softvéru

Ako útočníci zneužívajú absenciu tohto opatrenia?

Útočníci nasadzujú systémy, ktoré priebežne skenujú adresný priestor cieľových organizácií a hľadajú zraniteľné verzie softvéru, ktoré je možné zneužiť. Niektorí útočníci tiež rozširujú škodlivé web stránky, súbory, súbory médií a iný obsah prostredníctvom vlastných web stránok alebo iných (dôveryhodných) stránok tretích strán. Pokiaľ nepodozrievavé obete pristúpia k takémuto obsahu pomocou zraniteľného prehliadača alebo iného klientskeho programu, útočníci kompromitujú ich počítače inštalovaním zadných vrátok (back door) a botov, ktorí umožnia útočníkovi dlhodobú kontrolu nad systémom. Sofistikovaní útočníci môžu využiť tzv. útok nultého dňa (zero-day exploit), ktorý spočíva v zneužití neznámej zraniteľnosti, na ktorú ešte výrobca nevydal žiadnu záplatu (patch). Bez dostatočnej znalosti a kontroly softvéru používaného v organizácií je možné sa voči takýmto útokom len ťažko brániť.

Bez inventáru a kontroly softvéru, ktorý je nainštalovaný a povolený spúšťať, sú systémy viac zraniteľné. Takéto stroje umožnia, aby na nich bežal softvér, ktorý nie je potrebný pre biznis procesy a môže obsahovať zraniteľnosti, alebo umožnia útočníkovi nasadenie škodlivého softvéru na kompromitované stroje. Akonáhle je kompromitovaný jeden stroj, útočníci ho môžu využiť ako štartovací bod na zbieranie citlivých informácií, alebo na vstup ďalej do siete. Organizácie,

ktoré nemajú kompletné a aktuálne inventáre softvéru nie sú schopné zistiť, ktoré systémy obsahujúce zraniteľnosti sú v prevádzke, alebo zisťovať prítomnosť škodlivého softvéru.

Ako implementovať, automatizovať a merať účinnosť tohto opatrenia

1. *Rýchle výhry*: Vytvoriť zoznam autorizovaného softvéru, ktorý je nevyhnutný pre chod systémov (vrátane serverov, pracovných staníc a notebookov).
2. *Prehľadnosť a priraďovanie*: Zaviesť nástroje na inventarizáciu softvéru, ktoré budú schopné stopovať typy a verzie operačných systémov a aplikácií, ktoré sú na ňom spúšťané.
3. *Prehľadnosť a priraďovanie*: Nástroj na inventarizáciu softvéru by mal byť schopný sledovať neautorizovaný softvér, ktorý je nainštalovaný v systéme. K neautorizovanému softvéru patrí (aj inak legitímny) softvér, ktorý je nasadený tam, kde to nie je potrebné.
4. *Konfigurácia a očista*: Nasadiť technológiu, ktorá umožní na strojoch spúšťať iba schválený softvér a zabráni spúšťaniu všetkých ostatných aplikácií (white listing). Takéto nástroje na white listing musia byť založené na (prijateľných) hašovacích algoritmoch, ktoré určia autorizované binárne súbory vykonateľné na systéme.
5. *Pokročilé*: Je vhodné použiť virtuálne stroje a/alebo izolované systémy (air-gapped systems) na inštaláciu softvéru, ktorý predstavuje vyššie riziko a nie je možné ho inštalovať na stroji, ktorý je pripojený do siete.
6. *Pokročilé*: Klientske pracovné stanice vybaviť virtuálnym operačným systémom, ktorý je možné pravidelne, rýchlo a ľahko uviesť do dôveryhodného stavu (trusted snapshot).

Postupy a nástroje na implementáciu a automatizáciu týchto opatrení

Je dostupných mnoho nástrojov na inventarizáciu softvéru a aktív. Najlepšie z nich poskytnú kontrolu stoviek aplikácií, zistia stupeň zaplátania zraniteľností (patch level) na uistenie sa, že sú v poslednej verzii a používajú štandardizované názvy a CPE (common platform enumeration) špecifikácie.

Funkcionality, ktoré používajú white, či black listing softvéru (povoľovanie, či blokovanie spúšťania), sú súčasťou mnohých balíkov na ochranu koncových staníc. Mnoho komerčných riešení v sebe spája antivírus, antispyware, osobný firewall, IDS, či IPS spolu s white, či black listingom aplikácií. Dokážu vyhľadať názov, umiestnenie v systéme, kryptografický haš daného spustiteľného súboru na určenie, či je možné povoliť jeho spúšťanie.

Kritické opatrenie 3: Bezpečné konfigurácie hardvéru a softvéru na notebookoch, pracovných staniciach a serveroch.

Ako útočníci zneužívajú absenciu tohto opatrenia?

Na sieti Internet, ale aj na interných sieťach, ktoré už boli kompromitované, útočníci neustále hľadajú systémy, ktoré sú nakonfigurované so zraniteľným softvérom priamo od výrobcov, resp. predajcov. Pôvodné konfigurácie sú väčšinou zamerané na jednoduchosť nasadenia a používania, nie však na bezpečnosť. Preto sú ľahko zneužiteľné. Obrana proti takýmto útokom zahŕňa bezpečnú konfiguráciu všetkých zariadení v sieti, hardening, pravidelné aktualizácie a ich zaznamenávanie do systému riadenia konfigurácií.

Ako implementovať, automatizovať a merať účinnosť tohto opatrenia

1. *Rýchle výhry:* Je potrebné dodržiavať riadenie konfigurácií, vytvoriť bezpečný obraz (image), ktorý sa používa na vytvorenie všetkých systémov nasadzovaných v organizácií. Tento obraz je potrebné vytvoriť pre každý typ zariadenia. Pravidelné aktualizácie tohto obrazu je potrebné zahrnúť do manažmentu zmien organizácie.
2. *Rýchle výhry:* Pre obrazy systému musia existovať zdokumentované bezpečnostné nastavenia, ktoré sú pred nasadením otestované, schválené a zaradené do knižnice obrazov. Tieto obrazy by mali byť vyhodnocované a pravidelne aktualizované (napr. každých 6 mesiacov), aby sa zvýšila ich odolnosť voči nedávnym zraniteľnostiam a vektorom útokov.
3. *Rýchle výhry:* Štandardizované obrazy by mali byť hardenovanými verziami operačných systémov a aplikácií na nich nainštalovaných. Hardening spravidla zahŕňa odstránenie nepotrebných používateľských účtov, vypnutie, alebo odstránenie nepotrebných služieb, konfigurácia nevykonateľných zásobníkov a háld využitím funkcionality operačného systému, ako napr. data execution prevention (DEP). Hardening tiež zahŕňa aplikáciu záplat, uzatvorenie otvorených a nepoužívaných portov, nasadenie IDS, IPS, nástroje proti škodlivému softvéru a použitie firewallov (host – based).
4. *Rýchle výhry:* Akékoľvek odchýlky, alebo aktualizácie štandardizovaných obrazov musia byť zdokumentované a schválené manažmentom zmien.
5. *Rýchle výhry:* Organizácia by mala vyjednať také zmluvy s dodávateľmi, aby systémy boli dodané s bezpečnou konfiguráciou na zníženie možností útokov a náchylnosti na zraniteľnosti.
6. *Rýchle výhry:* Samotné hlavné obrazy musia byť uložené na bezpečne nakonfigurovanom serveri, s nástrojmi na kontrolu integrity a riadením zmien na zaistenie len povolených zmien. Tieto obrazy je tiež možné ukladať na offline strojoch, oddelených od produkčnej siete.
7. *Rýchle výhry:* Spúšťať len posledné verzie softvéru so zaplátanými zraniteľnosťami. Starší softvér odstrániť zo systému.
8. *Konfigurácia/očista:* Vzdialenú administráciu serverov, pracovných staníc, sieťových zariadení a podobného vybavenia je možné vykonávať len prostredníctvom zabezpečených kanálov. Protokoly ako telnet, virtual network computing (VNC), remote desktop protocol (RDP) alebo iné protokoly, ktoré nepodporujú silné šifrovanie je možné použiť, len prostredníctvom sekundárneho šifrovaného kanálu, ako napr. secure sockets layer (SSL), alebo Internet protocol securty (IPSEC).
9. *Konfigurácia/očista:* Aspoň raz mesačne spustiť program na vyhodnotenie súladu konfigurácie systémov s pravidlami na bezpečnú konfiguráciu.
10. *Konfigurácia/očista:* Aspoň raz týždenne použiť nástroje na kontrolu integrity súborov, na uistenie sa, či kritické systémy neboli pozmenené. Všetky zmeny musia byť automaticky nahlasované bezpečnostným zamestnancom.
11. *Konfigurácia/očista:* Zaviesť a testovať automatizovaný systém na monitorovanie konfigurácií, ktorý bude schopný vyhodnocovať všetky súčasti systému, ktoré sú merateľné na diaľku. Tieto testy by mali analyzovať zmeny hardvéru, softvéru, zmeny sieťovej konfigurácie a ostatné zmeny, ktoré vplývajú na bezpečnosť systému.
12. *Konfigurácia/očista:* Vedeniu poskytnúť tabuľky a grafy, ktoré ilustrujú množstvo systémov, ktoré spĺňajú požiadavky na konfiguráciu a tých, ktoré ich nespĺňajú.

Postupy a nástroje na implementáciu a automatizáciu týchto opatrení

Organizácia môže implementovať tieto opatrenia vytvorením série obrazov a bezpečných serverov na ukladanie týchto štandardných obrazov. Je možné zaviesť komerčné, alebo voľne dostupné nástroje na riadenie konfigurácií, ktoré budú hľadať odchýlky od štandardizovaných obrazov v organizácii.

Kritické opatrenie 4: Priebežné posúdenie zraniteľností a ich odstránenie.

Ako útočníci zneužívajú absenciu tohto opatrenia?

Hneď ako sú objavené a nahlásené nové zraniteľnosti bezpečnostnými výskumníkmi či výrobcami, útočníci vytvárajú škodlivý kód na zneužitie danej zraniteľnosti a spúšťajú tento kód proti objektom svojho záujmu. Akékoľvek závažnejšie zdržanie pri hľadaní a opravách softvéru s nebezpečnými zraniteľnosťami poskytuje silnú príležitosť pre útočníkov na pretrvávajúce útoky proti zraniteľným strojom s cieľom získania kontroly a prístupu k citlivým dátam. Organizácie, ktoré pravidelne neskenujú zraniteľnosti a proaktívne neriešia objavené nedostatky čelia zvýšenému riziku kompromitácie ich počítačových systémov.

Ako implementovať, automatizovať a merať účinnosť tohto opatrenia

1. *Rýchle výhry:* Organizácia by mala aspoň raz polročne spúšťať nástroje na skenovanie zraniteľností všetkých systémov v sieti. Tam, kde je to možné, je potrebné skenovať denne. Každá zistená zraniteľnosť by mala byť včas odstránená a kritické zraniteľnosti by mali byť odstránené do 72 hodín.
2. *Rýchle výhry:* Logy z udalostí by mali byť korelované s informáciami zo skenov zraniteľností na dosiahnutie dvoch cieľov. Je potrebné overiť, že sa loguje aktivita samotných skenovacích nástrojov. Zamestnanci by mali byť schopní korelovať detekciu útokov s predošlými výsledkami skenu zraniteľností, aby bolo možné určiť, či bola využitá známa zraniteľnosť.
3. *Prehľadnosť a priraďovanie*: Organizácia by mala zaviesť automatizované nástroje na plátanie zraniteľností a nástroje na aktualizáciu softvéru a operačných systémov na všetkých systémoch, na ktoré sú takéto nástroje dostupné a bezpečné.
4. *Konfigurácia/očista:* Na prekonanie obmedzení neautentifikovaného skenovania zraniteľností, organizácia musí zabezpečiť, aby všetko skenovanie bolo vykonané lokálne na kontrolovanom stroji, alebo pomocou diaľkových skenerov, ktorým sú pridelené administratívne práva na testovanom systéme.
5. *Konfigurácia/očista:* Organizácie by mali porovnávať minulé výsledky skenov zraniteľností, aby boli schopné overiť, že zraniteľnosti boli riešené buď prostredníctvom záplat, zavedením opatrenia alebo akceptáciou a zdokumentovaním rizika. Akceptácia rizika by mala byť pravidelne preverovaná, aby sa určilo, či nie sú k dispozícii novšie opatrenia na ošetrenie v minulosti akceptovanej zraniteľnosti.
6. *Konfigurácia/očista:* Nástroje na skenovanie zraniteľností musia byť schopné porovnať služby, ktoré počúvajú na každom stroji so zoznamom autorizovaných služieb. Tiež by mali byť schopné identifikácie zmien systémov v autorizovaných i neautorizovaných službách.

7. *Konfigurácia/očista:* Bezpečnostní zamestnanci by mali vytvárať rebríček neošetrených, kritických zraniteľností pre každé oddelenie.
8. *Konfigurácia/očista:* Bezpečnostní zamestnanci by mali zdieľať správy o zraniteľnostiach s vedením, aby mali prehľad o kritických problémoch a motiváciu na ich odstránenie.
9. *Konfigurácia/očista:* Organizácia by mala merať časové oneskorenia v zaplátaní nových zraniteľností a uistiť sa, že oneskorenie je menšie alebo rovné normálu, ktorý si ustanovila organizácia.
10. *Konfigurácia/očista:* Kritické záplaty musia byť vyhodnotené v testovacom prostredí ešte pred tým, ako budú nasadené do produkčného systému. Ak tieto záplaty narušia kritické aplikácie na testovacích strojoch, je potrebné nájsť iné opatrenia na ošetrenie zraniteľností, ktoré znemožnia ich zneužitie a nenarušia funkcionalitu kritických procesov a aplikácií.

Postupy a nástroje na implementáciu a automatizáciu týchto opatrení

Na vyhodnocovanie bezpečnej konfigurácie systémov je dostupných mnoho nástrojov na skenovanie zraniteľností. Najznámejšie nástroje na skenovanie používajú schémy a jazyky na klasifikáciu zraniteľností kompatibilné s CVE, CCE, OVAL, CPE, CVSS, a XCCDF. Pokročilejšie nástroje sú schopné pripojiť sa do systému pomocou používateľského konta a vykonať tak oveľa vyčerpávajúcejšie skenovanie (do skenu zahrnúť aj zraniteľnosti týkajúce sa konfigurácie operačného systému a aplikácií pre vektor útoku autentifikovaného používateľa). Okrem nástrojov, ktoré hľadajú zraniteľnosti a nesprávne konfigurácie, existuje množstvo nástrojov, ktoré dokážu overiť bezpečnostné nastavenia a konfigurácie lokálnych strojov, na ktorých sú nainštalované. Takéto nástroje môžu poskytnúť náhľad na neautorizované zmeny v konfigurácii a neúmyselné chyby administrátorov. Efektívne organizácie mapujú svoje skenery zraniteľností s tiketovacími systémami, ktoré automaticky monitorujú a hlásia vývoj riešenia problémov a tak zviditeľňujú kritické zraniteľnosti aj pre vyššie vedenie. Najefektívnejšie nástroje porovnávajú aktuálne výsledky skenov s minulými a tak umožňujú sledovať trendy a zmeny v čase.

Kritické opatrenie 5: Ochrana pred škodlivým softvérom.

Ako útočníci zneužívajú absenciu tohto opatrenia?

Škodlivý softvér je jednou z najvýznamnejších internetových hrozieb, ktorá sa zameriava na koncových používateľov aj na organizácie prostredníctvom prehliadania internetu, príloh e-mailov, mobilných zariadení a inými vektormi. Škodlivý softvér je schopný manipulovať s obsahom systému, zachytávať citlivé dáta a šíriť sa do ďalších systémov. Moderný škodlivý softvér sa snaží vyhnúť detekcii na základe správania a typických znakov, prípadne dokáže vyradiť antivírusový softvér na cieľovom systéme.

Ako implementovať, automatizovať a merať účinnosť tohto opatrenia

1. *Rýchle výhry:* Nasadiť automatizované nástroje na neustále monitorovanie pracovných staníc, serverov, mobilných zariadení na aktívnu ochranu pred škodlivým softvérom pomocou antivírusu, antispywaru, osobného firewallu a IPS (host based). Všetky udalosti detekcie

škodlivého softvéru majú byť logované a odosielané do systému na administráciu škodlivého softvéru.

2. *Rýchle výhry:* Organizácia by mala nasadiť automatické aktualizácie softvéru na ochranu pred škodlivým softvérom a vírusovej databázy, prípadne ich nechať denne manuálne aktualizovať administrátormi.
3. *Rýchle výhry:* Organizácie by mali nakonfigurovať notebooky, pracovné stanice a servery tak, aby neumožňovali automatické spúšťanie obsahu z USB kľúčov, tokenov, CD/DVD, zariadení s Firewire alebo iných médií.
4. *Rýchle výhry:* Organizácia by mala nakonfigurovať systémy tak, aby umožnila automatický sken škodlivého softvéru na vymeniteľných médiách okamžite po ich vložení.
5. *Rýchle výhry:* Všetky prílohy e-mailov by mali byť skenované a v prípade, že obsahujú škodlivý kód, alebo typy súborov, ktoré sú pre organizáciu nepotrebné, by mali byť blokované ešte pred príchodom do e-mailovej schránky používateľa.
6. *Prehľadnosť a priraďovanie*: Automatizované nástroje na monitorovanie by mali využívať detekciu anomálií správania na doplnenie a zlepšenie tradičnej detekcie na základe znakov (signature based detection).
7. *Prehľadnosť a priraďovanie*: Nástroje proti škodlivému kódu by mali obsahovať centrálnu konzolu, prostredníctvom ktorej administrátori dokážu identifikovať infikované zariadenia a zariadenia, na ktorých neprebehol sken alebo neprebehla aktualizácia signatúr.
8. *Konfigurácia/očista:* Organizácie by mali nasadiť nástroje na kontrolu prístupu do siete na overenie bezpečnej konfigurácie pred povolením prístupu do siete.
9. *Pokročilé*: Malo by byť nasadené nepretržité monitorovanie odchádzajúcej prevádzky. Akékoľvek väčšie toky dát, alebo neautorizovaná šifrovaná prevádzka by mala byť označená. Pokiaľ bude vyhodnotená ako škodlivá, je potrebné daný počítač presunúť do izolovanej VLAN.
10. *Pokročilé*: Organizácia by mala implementovať procesy na riešenie incidentov, ktoré umožnia organizácii získať vzorky škodlivého softvéru zo systémov organizácie a v prípade potreby ich poskytnúť výrobcovi antivírusového produktu nasadeného v organizácií.

Postupy a nástroje na implementáciu a automatizáciu týchto opatrení

Ako ukázala prax v otázke udržania aktuálnosti nástrojov na ochranu pred škodlivým softvérom, nie je možné spoliehať sa na používateľov a bezpečnostné politiky. Je potrebné používať automatické aktualizácie antivírusových signatúr, využívať administratívne funkcionality balíkov na ochranu koncových staníc na overenie, či všetky antivírusy, anti-spyware a IDS sú aktívne na všetkých riadených systémoch. Je potrebné denne vyhodnocovať, či na nejakých systémoch nie sú tieto prvky ochrany vypnuté a či na nejakých systémoch nie sú zastarané definície škodlivého softvéru. Niektoré organizácie používajú na identifikáciu svojich útočníkov rôzne honeypoty a tarpity. Je potrebné ich monitorovať s cieľom určenia prevádzky, ktorá je na ne smerovaná a ktoré používateľské účty sú skúšané.

Kritické opatrenie 6: Bezpečnosť aplikačného softvéru.

Ako útočníci zneužívajú absenciu tohto opatrenia?

V posledných rokoch sa jednou z najvyšších priorít počítačových kriminálnikov stali útoky na webové aplikácie a iný aplikačný softvér. Predovšetkým softvér, ktorý správne nekontroluje veľkosť vstupov, ktoré vložia používatelia, zlyháva pri ich čistení od nepotrebných a potenciálne škodlivých znakových sekvencií, alebo nesprávne inicializuje a čistí premenné, môže byť zraniteľný na vzdialené zneužitie. Útočníci používajú špecifické útoky ako napr. pretečenie pamäti (buffer overflow), SQL injection, cross-site scripting, cross-site request forgery, alebo click jacking na získanie kontroly nad zraniteľnými strojmi.

Ako implementovať, automatizovať a merať účinnosť tohto opatrenia

1. *Rýchle výhry:* Organizácie by mali chrániť webové aplikácie nasadením web aplikačného firewallu, ktorý preveruje do neho smerujúcu prevádzku na bežné útoky ako cross-site scripting, SQL injection, command injection, a útoky založené na prehľadávaní adresárov (directory traversal attacks). Pokiaľ sú dostupné aj aplikačné firewally pre nie webové aplikácie, je vhodné ich nasadiť. Pokiaľ je premávka šifrovaná, je potrebné nasadiť firewall tak, aby bol schopný túto premávku analyzovať (SSL – offloading).
2. *Prehľadnosť a priraďovanie*: Vykonávať kontrolu chýb pre všetky vstupy. Vždy keď je v zdrojovom kóde vytvorená premenná, je potrebné určiť jej veľkosť a typ. Vždy keď vstup vkladá používateľ, tak je potrebné overiť, či vstup nepresahuje veľkosť alebo typ pamäte, do ktorej bude tento vstup premiestnený.
3. *Konfigurácia/očista:* Organizácia by mala testovať vlastnými silami vytvorený softvér a softvér tretích strán, aby bolo možné nájsť chyby v kóde alebo vložený škodlivý softvér, vrátane zadných vrátok ešte skôr, ako bude nasadený automatizovaný softvér na analýzu kódu. V prípade, že nie je dostupný zdrojový kód, je možné testovať kompilovaný kód použitím nástrojov na statickú binárnu analýzu (static binary analysis tools). Validácia vstupov a bežné kódovanie výstupov aplikačného softvéru by mali byť obzvlášť preverované a testované.
4. *Konfigurácia/očista:* Organizácia by mala testovať vlastnými silami vytvorený softvér a softvér tretích strán na bezpečnostné zraniteľnosti použitím vzdialených web aplikačných skenerov ešte pred ich nasadením, po každej aktualizácii a potom v pravidelných intervaloch.
5. *Konfigurácia/očista:* V prípade aplikácií, ktoré využívajú databázy, je potrebné preverovať konfiguráciu operačného systému, ktorý ju zastrešuje a samotného databázového softvéru. Je potrebné preveriť nastavenia a to, či bol databázový systém hardenovaný.
6. *Konfigurácia/očista:* Organizácia by mala verifikovať, či sú do požiadaviek, návrhu, implementácie, testovania a ostatných fáz životného cyklu vývoja softvéru zohľadnené bezpečnostné aspekty.
7. *Konfigurácia/očista:* Organizácia musí zabezpečiť, aby zamestnanci, ktorí sa podieľajú na vývoji softvéru dostali školenia o písaní bezpečného kódu pre ich špecifické vývojové prostredie.
8. *Konfigurácia/očista:* Organizácia musí vyžadovať, aby všetok softvér vyvíjaný v rámci organizácie obsahoval filtrovanie na základe white listingu pre všetky dátové vstupy

a výstupy spojené so systémom. Filtrovanie musí byť nastavené tak, aby dovnútra aj von vpustilo iba typy dát, ktoré sú potrebné.

9. *Konfigurácia/očista:* Vzorkové skripty, knižnice, komponenty, kompilátory alebo iný nepotrebný kód, ktorý nie je aplikáciou využívaný musí byť odinštalovaný, alebo odstránený zo systému.

Postupy a nástroje na implementáciu a automatizáciu týchto opatrení

Nástroje na testovanie zdrojového kódu, nástroje na skenovane bezpečnosti web aplikácií a nástroje na testovanie objektového kódu sú veľmi užitočné pri zabezpečovaní bezpečnosti aplikačného softvéru spolu s manuálnym penetračným testovaním aplikácií skúsenými testermi s rozsiahlym vzdelaním v oblasti programovania. Iniciatíva Common Weakness Enumeration (CWE) je používaná mnohými nástrojmi na identifikáciu nájdených zraniteľností. Takisto ju používajú organizácie, ktoré chcú určiť typy zraniteľností, na ktoré je potrebné sa prioritne zamerať a odstrániť ich. Pri vývoji aplikačného softvéru je možné využiť bezplatnú online publikáciu „Top 25 Most Dangerous Programming Errors“.

Kritické opatrenie 7: Opatrenia pre bezdrôtové zariadenia.

Ako útočníci zneužívajú absenciu tohto opatrenia?

Mnoho veľkých krádeží dát bolo spustených útočníkmi, ktorí získali prístup do siete organizácie z neďalekých parkovísk pomocou bezdrôtového pripojenia V prípade používania notebookov s bezdrôtovým pripojením v hoteloch a kaviarňach počas pracovných ciest je veľmi častým javom infekcia notebooku, alebo umiestnenie zadných vrátok a pri najbližšom pripojení notebooku do internej siete organizácie ďalšie šírenie infekcie do siete. Niektoré organizácie nahlásili aj objavenie neautorizovaných bezdrôtových prístupových bodov v organizácii, často skrytým spôsobom, čo umožňuje útočníkom dlhodobejší prístup do cieľového prostredia.

Ako implementovať, automatizovať a merať účinnosť tohto opatrenia

1. *Rýchle výhry:* Zabezpečiť, že každé bezdrôtové zariadenie pripojené do siete spĺňa požiadavky na autorizovanú konfiguráciu a bezpečnostný profil spolu s dokumentovaným vlastníkom a dôvodom. Zariadeniam, ktoré toto nespĺňajú je potrebné zamietnuť prístup.
2. *Rýchle výhry:* Zabezpečiť, že všetky bezdrôtové zariadenia sú manažovateľné použitím podnikových nástrojov na riadenie. Prístupové body na domáce použitie často nemajú tieto funkcionality, je preto potrebné sa im v podnikovom prostredí vyhnúť.
3. *Rýchle výhry:* Nástroje na skenovanie zraniteľností siete musia byť nakonfigurované tak, aby boli schopné detekcie bezdrôtových prístupových bodov do drôtovej siete. Identifikované zariadenia musia byť v súlade so zoznamom autorizovaných bezdrôtových zariadení. Neautorizované prístupové body musia byť deaktivované.
4. *Prehľadnosť a priraďovanie*: Organizácia by mala používať systémy na detekciu bezdrôtového prieniku (Wireless Intrusion Detection Systems - WIDS) na identifikáciu podvodných bezdrôtových zariadení a detekciu pokusov o prienik a úspešných útokov. Celá bezdrôtová

prevádzka by mala byť monitorovaná drôtovým IDS v mieste, kde prevádzka vchádza do drôtovej siete.

5. *Prehľadnosť a priraďovanie*: Použiť 802.1x na kontrolu toho, ktoré zariadenia majú povolenie pripájať sa do bezdrôtovej siete.
6. *Prehľadnosť a priraďovanie*: Vykonávať prehliadky priestorov a určiť, ktoré časti v rámci organizácie je potrebné pokryť. Po strategickom rozmiestnení bezdrôtových prístupových bodov je potrebné nastaviť silu signálu tak, aby boli pokryté len potrebné časti priestorov organizácie.
7. *Konfigurácia/očista:* V prípade, že je potrebný bezdrôtový prístup, organizácia musí zabezpečiť, aby mali klientske stroje prístup iba do autorizovaných bezdrôtových sietí.
8. *Konfigurácia/očista:* V zariadeniach, ktoré nevyhnutne nepotrebujú bezdrôtový prístup je potrebné vypnúť túto možnosť hardvérovo a túto konfiguráciu zabezpečiť heslom.
9. *Konfigurácia/očista:* Organizácia musí robiť pravidelné skeny na vyhľadanie neautorizovaných a zle nakonfigurovaných bezdrôtových zariadení použitím techník ako napr. „war driving“ na identifikáciu prístupových bodov a klientov, ktorí akceptujú peer-to-peer spojenia. Takéto zariadenia musia byť odstránené zo siete, alebo prekonfigurované tak, aby spĺňali bezpečnostné požiadavky organizácie.
10. *Konfigurácia/očista:* Zabezpečiť, že celá bezdrôtová premávka dosahuje pokročilý šifrovací štandard (AES) využitím ochrany WPA2.
11. *Konfigurácia/očista:* Zabezpečiť, že bezdrôtové siete používajú autentifikačné protokoly ako EAP/TLS alebo PEAP, ktoré poskytujú ochranu oprávnení a vzájomnú autentifikáciu.
12. *Konfigurácia/očista:* Zabezpečiť, že bezdrôtoví klienti používajú silné, multifaktorové prístupové dáta na autentifikáciu.
13. *Konfigurácia/očista:* Vypnúť možnosť peer-to-peer bezdrôtovej komunikácie na bezdrôtových klientoch, okrem prípadov zdokumentovanej potreby pre takúto komunikáciu.
14. *Konfigurácia/očista:* Vypnúť bezdrôtový periférny prístup zariadení, ako napr. bluetooth, okrem prípadov zdokumentovanej potreby pre takúto komunikáciu.
15. *Konfigurácia/očista:* Bezdrôtové prístupové body nikdy nesmú byť pripojené priamo do internej siete. Je potrebné ich umiestniť za firewall, alebo na separátnu VLAN tak, aby celá premávka mohla byť preskúmavaná a filtrovaná.
16. *Pokročilé*: Nakonfigurovať všetkých bezdrôtových klientov, ktorí pristupujú do siete organizácie alebo spracovávajú dáta organizácie tak, aby nebolo možné pripojiť ich do verejných bezdrôtových sietí alebo iných sietí, ktoré nie sú organizáciou povolené.

Postupy a nástroje na implementáciu a automatizáciu týchto opatrení

Mnoho organizácií používa komerčné nástroje na skenovanie, detekciu a vyhľadávanie bezdrôtových sietí a zariadení, ako aj komerčné WIDS. Je potrebné pravidelne zachytávať bezdrôtovú prevádzku v rámci organizácie a uistiť sa, či nie sú používané slabšie protokoly a šifrovanie ako tie, ktoré požaduje organizácia. Pokiaľ sú identifikované zariadenia so slabou ochranou bezdrôtovej komunikácie, je potrebné ich prekonfigurovať alebo im zamietnuť prístup.

Kritické opatrenie 8: Schopnosť obnovy dát.

Ako útočníci zneužívajú absenciu tohto opatrenia?

Keď útočníci kompromitujú stroje, väčšinou vykonajú závažné zmeny v konfigurácii a softvéri. Niekedy vykonajú drobné zmeny v dátach uložených v kompromitovaných strojoch potenciálne ohrozujúc efektívnosť organizácie podvrhnutými dátami. Aj keď sú útočníci odhalení, v prípade ak organizácia nemá schopnosť obnovy týchto dát, môže byť skutočne ťažké identifikovať a odstrániť všetky napáchané škody.

Ako implementovať, automatizovať a merať účinnosť tohto opatrenia

1. *Rýchle výhry:* Zabezpečiť, aby boli všetky systémy zálohované aspoň raz týždenne a systémy s citlivými dátami častejšie. Aby bolo možné rýchlo zo zálohy obnoviť operačný systém, aplikačný softvér a dáta, je potrebné, aby ich obnova bola zahrnutá a popísaná v celkovom postupe zálohovania.
2. *Rýchle výhry:* Dáta na zálohovom médiu musia byť pravidelné testované vykonaním testovacej obnovy.
3. *Rýchle výhry:* Kľúčoví zamestnanci musia byť vyškolení na proces zálohovania a aj proces obnovy. Vyškolení musia byť aj zastupujúci zamestnanci pre prípad nedostupnosti kľúčových zamestnancov.
4. *Konfigurácia/očista:* Zabezpečiť, že zálohy sú dostatočne chránené fyzickou bezpečnosťou, resp. sú šifrované na ich lokálnom umiestnení ako aj pri presune po sieti.
5. *Konfigurácia/očista:* Zálohové média ako pevné disky alebo pásky musia byť uložené na bezpečnom uzamknutom mieste.

Postupy a nástroje na implementáciu a automatizáciu týchto opatrení

Je potrebné vykonávať testovacie obnovy náhodnej vzorky záloh aspoň raz za kvartál. Obnovené systémy musia byť otestované, aby sa preverila neporušenosť a funkčnosť operačného systému, aplikácií a dát.

Kritické opatrenie 9: Posúdenia bezpečnostných schopností a vhodné školenia.

Schopnosti piatich skupín ľudí, ktoré sú neustále preverované útočníkmi

1. Koncoví používatelia sú obalamutení prostredníctvom sociálneho inžinierstva a útočníkovi poskytnú heslá, otvárajú prílohy e-mailov, inštalujú softvér z nedôveryhodných zdrojov alebo navštevujú škodlivé stránky.
2. Systémoví administrátori sú balamutení rovnako ako používatelia, ale útočníci navyše od nich často požadujú, aby vytvorili neautorizované používateľské účty.
3. Bezpečnostní operátori a analytici sú každodenne preverovaní stále novými a inovatívnymi útokmi.
4. Programátori sú testovaní kriminálnikmi, ktorí nájdu a zneužijú zraniteľnosti v kóde.

5. Vlastníci systémov sú skúšaní v prípadoch, keď je potrebné investovať do informačnej bezpečnosti, a to hlavne vtedy, ak nie sú dostatočné znalí problematiky a nedokážu reálne posúdiť, aký dopad môže mať na organizáciu kompromitácia, únik, alebo modifikácia dát.

Každá organizácia, ktorá má záujem efektívne reagovať na útoky, potrebuje zistiť nedostatky v znalostiach zamestnancov a dodávateľov a tieto nedostatky zaplniť prostredníctvom vhodných školení. Dobrý program na vyhodnotenie bezpečnostných zručností zamestnancov poskytne základ pre rozhodovanie o povedomí, ktoré je potrebné rozšíriť a o bezpečnostných praktikách, ktoré je potrebné vylepšiť. Školenia sú úzko previazané s politikami, pretože tie hovoria zamestnancom čo je potrebné robiť a školenia im k tomu poskytnú zručnosti.

Ako implementovať, automatizovať a merať účinnosť tohto opatrenia

1. *Rýchle výhry:* Vyvinúť školenia bezpečnostného povedomia pre rôzne typy zamestnancov. Školenia by mali zahŕňať špecifické scenáre incidentov na ilustráciu hrozieb, ktorým musí organizácia čeliť a možností obrany pred útokmi.
2. *Rýchle výhry:* Povedomie by malo byť podložené politikami a školeniami. Politiky hovoria čo je potrebné robiť, školenia poskytujú zručnosti na vykonanie tých činností a povedomie umožní zmeniť chovanie zamestnancov, aby porozumeli dôležitosti dodržiavania politík.
3. *Prehľadnosť a priraďovanie*: Vytvoriť metriky pre všetky politiky a vykonávať pravidelné merania. Školenia povedomia je potrebné orientovať na tie s najhoršími výsledkami.
4. *Konfigurácia/očista:* Zaviesť periodické dotazníky na vyhodnotenie bezpečnostného povedomia zamestnancov a dodávateľov. Aspoň raz ročne overiť ich porozumenie politikám informačnej bezpečnosti a postupov, ako aj ich rolu v týchto postupoch.
5. *Konfigurácia/očista:* Vykonávať pravidelné cvičenia na overenie, či si zamestnanci a dodávatelia plnia svoje povinnosti v oblasti informačnej bezpečnosti napr. overenie, či zamestnanci kliknú na odkaz v podozrivom e-maile, alebo či poskytnú citlivé informácie cez telefón bez dostatočnej autentifikácie volajúceho.
6. *Pokročilé*: Poskytnúť sedenia na zvýšenie povedomia pre zamestnancov, ktorí aj napriek školeniam nedodržiavajú politiky.

Postupy a nástroje na implementáciu a automatizáciu týchto opatrení

Kľúčom na zlepšenie zručností je meranie, ktoré ukáže aj zamestnancovi aj zamestnávateľovi oblasti, v ktorých sú znalosti dostatočné a v ktorých je čo dobiehať. Keď sa podarí identifikovať tieto medzery v znalostiach, je možné povolať skúsenejších a znalejších zamestnancov, aby pomohli tým menej skúseným.

Kritické opatrenie 10: Bezpečná konfigurácia sieťových zariadení ako firewally, routery a switche.

Ako útočníci zneužívajú absenciu tohto opatrenia?

Útočníci využívajú fakt, že konfigurácia sieťových zariadení môže byť po nejakom čase menej bezpečná. Používatelia požadujú od administrátorov rôzne výnimky v konfigurácii pre účely dočasných biznis potrieb a tieto výnimky v konfigurácii často ostávajú aj po zániku daných dočasných potrieb. Niekedy dokonca nie sú udeľované výnimky dôkladne analyzované a bezpečnostné riziko z nich vyplývajúce nie je známe. Útočníci následne hľadajú bezpečnostné diery vo firewalloch, UTM bránach, routeroch a switchoch a zneužívajú ich na prienik cez obranné prvky. Keď sa im podarí dostať sa do cieľovej siete, môžu presmerovať premávku alebo zachytiť, prípadne pozmeniť informácie.

Ako implementovať, automatizovať a merať účinnosť tohto opatrenia

1. *Rýchle výhry:* Porovnať konfigurácie firewallov, routerov, UTM brán a switchov so štandardnými bezpečnými konfiguráciami v organizácii. Takáto bezpečná konfigurácia by mala byť zdokumentovaná, prehodnotená a schválená vedením. Akékoľvek zmeny v štandardnej konfigurácii musia byť zdokumentované a schválené.
2. *Rýchle výhry:* V sieťových prepojovacích bodoch, ako napr. Internetová brána (gateway), medzi podnikové prepojenia alebo segmenty internej siete, implementovať filtrovanie vchádzajúcej a odchádzajúcej premávky a povoliť len tie porty a protokoly, pre ktoré existuje odôvodnená a zdokumentovaná potreba. Všetky ostatné protokoly a porty majú byť blokované pravidlami na routeroch, firewalloch a IPS.
3. *Rýchle výhry:* Sieťové zariadenia, ktoré filtrujú nepotrebné služby a blokujú útoky, musia byť testované v laboratórnych podmienkach. Je potrebné otestovať všetky konfigurácie používané v organizácii, aby bolo možné uistiť sa, že dané zariadenia aj pod značnou záťažou pracujú správne.
4. *Konfigurácia/očista:* Všetky nové konfiguračné pravidlá nad rámec základnej hardenovanej konfigurácie, ktoré povoľujú prevádzku cez bezpečnostné sieťové zariadenia (firewally, IPS) musia byť zdokumentované a zaznamenané v systéme na riadenie konfigurácií. Zaznamenané musia byť špecifické potreby pre tieto zmeny, osoby zodpovedajúce za tieto potreby a očakávaná doba trvania tejto potreby.
5. *Konfigurácia/očista:* Technológie na sieťové filtrovanie nasadené medzi sieťami s rôznymi úrovňami bezpečnosti musia byť schopné filtrovať IPv6 prevádzku.
6. *Konfigurácia/očista:* Sieťové zariadenia musia byť manažované použitím autentifikácie s použitím silných hesiel a šifrovaných relácií. V prípade, že je to možné je vhodné použiť dvojfaktorovú autentifikáciu. Dvojfaktorová autentifikácia môže byť napr. použitie hesla a hardvérového tokenu, alebo hesla a biometrického údaju. Použite dvoch rôznych hesiel nie je dvojfaktorová autentifikácia.
7. *Konfigurácia/očista:* Najnovšia stabilná verzia operačných systémov sieťových zariadení (IOS, resp. OS od iných výrobcov) musí byť otestovaná a nainštalovaná do 3 mesiacov od jej vydania výrobcom.

8. *Pokročilé*: Sieťová infraštruktúra musí byť manažovaná prostredníctvom spojení, ktoré sú oddelené od produkčnej časti na separátnej VLAN, resp. na úplne odlišnom fyzickom pripojení pre manažment sieťových zariadení.

Postupy a nástroje na implementáciu a automatizáciu týchto opatrení

Niektoré organizácie používajú komerčné nástroje na vyhodnotenie sady pravidiel pre zariadenia na sieťovú filtráciu, aby bolo možné určiť, či sú konzistentné a nie sú v konflikte. Poskytujú tiež automatickú kontrolu logickosti sieťových filtrov a hľadajú chyby v sadách pravidiel a zoznamoch riadenia prístupu (Access Control Lists – ACL), ktoré by mohli do siete prepustiť nechcené služby. Takéto nástroje by mali byť použité po každej zásadnej zmene v konfigurácii.

Kritické opatrenie 11: Obmedzenia a opatrenia pre sieťové porty, protokoly a služby.

Ako útočníci zneužívajú absenciu tohto opatrenia?

Útočníci hľadajú diaľkovo prístupné sieťové služby, ktoré sú zraniteľné a je ich možné zneužiť. Môže ísť o slabo nakonfigurované web servery, mail servery alebo DNS servery. Mnoho softvérových balíkov automaticky inštaluje a zapína služby, ktoré nie sú potrebné a to bez toho, aby na to upozornili používateľa alebo administrátora. Útočníci takéto služby vyhľadávajú a snažia sa ich zneužiť použitím základných používateľských ID a hesiel, alebo široko dostupným kódom na zneužitie (exploitation code, exploit).

Ako implementovať, automatizovať a merať účinnosť tohto opatrenia

1. *Rýchle výhry:* Použiť host-based firewally alebo nástroje na filtrovanie portov na koncové systémy, ktoré povolia len špecificky určené služby a porty na špecifikovaných zariadeniach.
2. *Rýchle výhry:* Pravidelne vykonávať automatizované skeny portov všetkých kľúčových serverov a porovnávať ich s efektívnym a známym základom (baseline). V prípade otvorenia nového portu je potrebné zasielať upozornenia a preverovať.
3. *Prehľadnosť a priraďovanie*: Preveriť každý server, ktorý je viditeľný alebo dostupný z internetu (v DMZ) a pokiaľ to nie je potrebné, presunúť ho na internú VLAN.
4. *Konfigurácia/očista:* Služby, ktoré sú potrebné na biznis účely cez internú sieť je potrebné preverovať štvrťročne a zamestnanci zodpovední za tieto služby ich musia zdôvodniť. Stáva sa, že služby bývajú zapnuté na účely časovo obmedzeného projektu a ostávajú zapnuté aj po uplynutí ich potreby.
5. *Konfigurácia/očista:* Kritické služby umiestňovať na separátne fyzické stroje (DNS, file, mail, web a databázové servery).
6. *Pokročilé*: Pre kritické servery je potrebné umiestniť aplikačný firewall na preverovanie a schvaľovanie prevádzky. Neautorizované služby a prevádzku je potrebné blokovať a zasielať upozornenia.

Postupy a nástroje na implementáciu a automatizáciu týchto opatrení

Na určenie toho, ktoré porty sú otvorené je možné použiť port skenery. Je možné ich nakonfigurovať tak, aby dokázali identifikovať verziu protokolu a služby, ktoré počúvajú na danom otvorenom porte. Takýto zoznam služieb a ich verzií sa porovnáva s inventárom služieb , ktoré organizácia požaduje pre každý server a pracovnú stanicu.

Kritické opatrenie 12: Riadenie administratívnych privilégií.

Ako útočníci zneužívajú absenciu tohto opatrenia?

Zneužitie administrátorských práv je primárnou metódou útočníkov na ich postupovanie po sieti cieľovej organizácie. Používatelia pracovných staníc, ktorí fungujú s administratívnymi právami, sú oklamaní, aby otvorili škodlivú prílohu e-mailu, stiahli a otvorili súbor zo škodlivej stránky, alebo len jednoducho surfujú a natrafia na stránku, ktorá obsahuje útočníkov kód, ktorý automaticky zneužije prehliadač a spustí sa na počítači obete. V prípade, že má používateľ administrátorské práva, útočník môže získať úplnú kontrolu nad počítačom a môže nainštalovať keyloggery, sniffery a na diaľku ovládaný softvér na nájdenie administrátorských hesiel a iných citlivých dát. Inou technikou je napr. získanie privilégií uhádnutím alebo zlomením hesla administrátora a následné získanie prístupu do cieľového stroja. V prípade, ak sú administratívne privilégia neuvážene distribuované, útočník ma omnoho ľahšiu prácu pri získavaní úplnej kontroly nad systémami.

Ako implementovať, automatizovať a merať účinnosť tohto opatrenia

1. *Rýchle výhry:* Používať automatizované nástroje na inventarizáciu všetkých administratívnych účtov a preverovať, že každý takýto účet je schválený vedením, a že každé administratívne heslo má minimálne 12 pseudonáhodných znakov a spĺňa FDCC štandard.
2. *Rýchle výhry:* Pred nasadením akýchkoľvek nových zariadení v sieťovom prostredí je potrebné zmeniť všetky pôvodné heslá pre aplikácie, operačné systémy, routery, firewally, bezdrôtové prístupové body a iné systémy na heslá, ktoré sú ťažko uhádnuteľné.
3. *Rýchle výhry:* Nakonfigurovať všetky účty na administratívnej úrovni tak, aby vyžadovali pravidelné zmeny hesiel v intervaloch nie dlhších ako 60-90 dní.
4. *Rýchle výhry:* Uistiť sa, že všetky servisné účty majú dlhé a ťažko uhádnuteľné heslá, ktoré sú pravidelne menené (tak ako aj pri administratívnych a používateľských účtoch) v intervaloch nie dlhších ako 90 dní.
5. *Rýchle výhry:* Heslá do všetkých systémov musia byť uložené v dobre hašovanom alebo šifrovanom formáte, slabšie formáty ako napr. Windows LANMAN haš treba odstrániť z prostredia.
6. *Rýchle výhry:* Používať automatizované skripty na uistenie sa, že sa administratívne účty využívajú len k administratívnym úkonom a nie na čítanie e-mailov, vytváranie dokumentov alebo surfovanie po internete. Internetové prehliadače a e-mailoví klienti musia byť nakonfigurované tak, aby ich nebolo možné spustiť pod administratívnym účtom.
7. *Rýchle výhry:* Pomocou politík a zvyšovaním povedomia používateľov vyžadovať, aby administrátori zaviedli jedinečné a rôzne heslá do ich administratívnych a neadministratívnych účtov. Každá osoba, ktorá potrebuje administratívny prístup, musí mať

samostatný účet. Administratívne účty sa nesmú nikdy zdieľať medzi používateľmi. Účty ako „administrator“ vo Windows alebo „root“ v Unixe sa môžu použiť len v krajných prípadoch.

8. *Rýchle výhry:* Nakonfigurovať operačné systémy tak, aby staré heslá nebolo možné istú dobu (napr. 6 mesiacov) opätovne použiť.
9. *Prehľadnosť a priraďovanie*: Implementovať dôsledné auditovanie používania administratívnych účtov a funkcií a monitorovať podozrivé správanie (napr. rekonfigurácie počas noci).
10. *Prehľadnosť a priraďovanie*: Nakonfigurovať systémy tak, aby vytvorili log záznam a upozornenie, keď je pridaný alebo odobraný účet zo skupiny doménových administrátorov.
11. *Konfigurácia/očista:* Používať dvojstupňovú autentifikáciu pri všetkých administratívnych prístupoch, vrátane administratívneho prístupu do domény.
12. *Konfigurácia/očista:* Blokovať prístup (vzdialený aj lokálny) do strojov pre účty s administratívnymi oprávneniami. Namiesto toho by sa administrátori mali prihlasovať pomocou neadministratívnych účtov a po prihlásení (bez admin. práv) získať administratívne privilégia pomocou nástrojov ako „sudo“ v Linux/Unix alebo „runas“ vo Windows.
13. *Konfigurácia/očista:* Ak sú služby outsource-ované tretím stranám, je potrebné do zmlúv zakotviť spôsob náležitej ochrany a riadenia administratívneho prístupu. Malo by byť overené, že nie sú zdieľané heslá a ďalej, že administrátori sú zodpovední za svoju činnosť.
14. *Pokročilé:* Diferencovať administrátorské účty na základe definovaných rol v rámci organizácie. Napr. administrátor pracovnej stanice môže mať prístup len do pracovných staníc, notebookov atď.

Postupy a nástroje na implementáciu a automatizáciu týchto opatrení

Je potrebné overiť, že používatelia s vysokými privilégiami nevyužívajú svoje účty pri surfovaní po internete, čítaní e-mailov a pod. prostredníctvom priebežného zbierania zoznamov prebiehajúcich procesov. Zber takýchto informácií môže byť skriptovaný a môže prehľadávať desiatky prehliadačov či e-mailových klientov na strojoch. Tiež je možné nakonfigurovať administrátorské účty tak, aby na prístup do internetu používali webové proxy 127.0.0.1 a neobsahovali e-mailového klienta. Je potrebné vyžadovať dĺžku a komplexnosť všetkých hesiel s administrátorskými oprávneniami. Dĺžku, zložitosť a interval zmeny hesla je potrebné vynucovať konfiguráciou operačného systému a/alebo aplikácie.

Kritické opatrenie 13: Ochrana perimetra.

Ako útočníci zneužívajú absenciu tohto opatrenia?

Útočníci sa zameriavajú na zneužívanie systémov, ktoré sú dosiahnuteľné z internetu. Nejedná sa iba o systémy z DMZ, ale aj pracovné stanice a notebooky, ktoré sťahujú obsah z Internetu z perimetra siete. Hrozby ako napr. organizovaný zločin alebo národné štáty zneužívajú zraniteľnosti v konfigurácii a architektúre systémov v perimetri, sieťových zariadení či klientskych staníc, ktoré pristupujú na internet, aby získali prístup do organizácie. Následne sa pomocou operácií na týchto strojoch snažia dostať hlbšie do organizácie s cieľom kradnúť alebo pozmeniť informácie, prípadne si pripraviť prostredie na dlhšie zotrvanie a neskoršie útoky na interné systémy. Hranice medzi

internými a externými sieťami sa zužujú, pretože rastie interkonektivita v rámci a medzi organizáciami a tak isto sa zvyšuje aj používanie bezdrôtových sietí. Tieto „vyblednuté“ hranice často umožnia útočníkovi získať prístup do siete obídením hraničných systémov.

Ako implementovať, automatizovať a merať účinnosť tohto opatrenia

Obranné mechanizmy popísané v tejto sade opatrení sú založené na kritických opatreniach 10 z tohto dokumentu. Sú zamerané na zlepšenie celkovej architektúry a implementácie hraničných bodov s Internetom a internou sieťou. Segmentácia internej siete je pre tieto opatrenia kľúčová, pretože ako náhle je útočník vnútri siete, snaží sa dostať k najcitlivejším strojom. Ochrana internej siete väčšinou nie je dostatočne účinná pred útokmi z vnútra. Zlepšiť ju je možné nastavením aspoň základnej segmentácie siete a každý segment chrániť pomocou proxy a firewallu.

1. *Rýchle výhry:* Zakázať komunikáciu so známymi škodlivými IP adresami (black listy), resp. obmedziť prístup na dôveryhodné stránky (white listy). Je možné robiť periodické testy posielaním paketov z falošných zdrojových IP adries (neroutovateľné, nevyužité IP adresy) na overenie toho, že tieto pakety neprejdú cez perimeter siete.
2. *Rýchle výhry:* Nasadiť network-based IDS senzory do DMZ na hľadanie nezvyčajných útočných mechanizmov a detekciu kompromitácie týchto systémov. Senzory detegujú útoky pomocou signatúr, analýzy správania sa siete a iných mechanizmov na analýzu prevádzky.
3. *Rýchle výhry:* Nasadiť network-based IPS zariadenia na doplnenie IDS blokovaním známych signatúr a spôsobov útokov. Ako sa útoky automatizujú, metódy ako IDS oneskorujú dobu reakcie na útok. Správnou konfiguráciou IPS je možné dosiahnuť automatizáciu blokovania škodlivej prevádzky.
4. *Rýchle výhry:* Na sieťach v DMZ je potrebné nastaviť monitorovacie systémy tak, aby boli schopné zaznamenávať aspoň informácie z hlavičky paketu, ideálne celú hlavičku a obsah paketu, ktoré smerujú do/alebo cez perimeter siete. Táto premávka by mala byť zasielaná do správne nakonfigurovaného SIEM systému, aby udalosti zo všetkých zariadení mohli byť korelované.
5. *Rýchle výhry:* Na zníženie pravdepodobnosti spoofovaných e-mailových správ je potrebné implementovať SPF (Sender Policy Framework). Ide o verifikáciu odosielateľa pomocou SPF záznamov v DNS na predchádzanie SPAMu.
6. *Prehľadnosť a priraďovanie*: Formulovať sieťovú architektúru s jasne oddelenými internými sieťami od DMZ a systémov v extranete. Stroje v DMZ potrebujú komunikovať s internými systémami ako aj s internetom, systémy extranetu komunikujú predovšetkým so systémami biznis partnerov. Systémy v DMZ nesmú obsahovať citlivé informácie a interné systémy nesmú byť priamo dosiahnuteľné z internetu.
7. *Prehľadnosť a priraďovanie*: Navrhnúť a implementovať sieťové perimetre tak, aby celá odchádzajúca prevádzka (web, FTP, SSH) išla v DMZ cez aspoň jednu proxy. Proxy musí podporovať logovanie individuálnych TCP relácií, blokovanie špecifických URL, domén a IP adries (black list) a používanie white listov povolených stránok, ktoré môžu byť dosiahnuté počas blokovania všetkých ostatných stránok.
8. *Prehľadnosť a priraďovanie*: Vyžadovať dvojfaktorovú autentifikáciu pri všetkých prístupoch na diaľku.

9. *Konfigurácia/očista:* Všetky zariadenia, ktoré sú na diaľku pripájané do internej siete musia byť riadené organizáciou, spolu s diaľkovým ovládaním ich konfigurácie, inštalovaného softvéru a úrovní záplat.
10. *Konfigurácia/očista:* Pravidelne skenovať pre spojenia do internetu, ktoré obchádzajú DMZ, vrátane neautorizovaných VPN, zariadení pripojených do siete organizácie a zároveň do iných sieti pomocou WI-FI, modemu alebo iným spôsobom.
11. *Konfigurácia/očista:* Na obmedzenie možnosti šírenia sa škodlivého softvéru alebo vnútorného útočníka po sieti je potrebné zaviesť internú segmentáciu siete, aby bol umožnený prístup len k tým službám, ktoré sú potrebné.
12. *Konfigurácia/očista:* Vyvinúť plány na rýchle nasadenie filtrov na interných sieťach na zabránenie šíreniu škodlivého softvéru.
13. *Pokročilé:* Na zníženie dôsledkov útočníkovho pohybu medzi kompromitovanými systémami je potrebné, aby systémy z DMZ mohli komunikovať so systémami z privátnych sietí cez aplikačné proxy, alebo firewally schválenými a kontrolovanými kanálmi.
14. *Pokročilé:* Na identifikáciu skrytých kanálov získavajúcich dáta cez firewall je potrebné nakonfigurovať mechanizmy na stopovanie firewall relácií (zahrnuté do mnohých komerčných firewallov), aby bolo možné identifikovať TCP relácie, ktoré trvajú nezvyčajne dlho pre danú organizáciu a zariadenie firewall. Tiež je potrebné upozorňovať zodpovedných zamestnancov na zdrojové a cieľové adresy spojené s takýmito reláciami.

Postupy a nástroje na implementáciu a automatizáciu týchto opatrení

Jednu časť tejto sady opatrení je možné implementovať použitím voľne dostupných alebo komerčných IDS a snifferov, ktoré hľadajú útoky z externého prostredia smerujúce do DMZ a interných systémov a tiež z interného prostredia do DMZ a internetu. Je potrebné pravidelne testovať tieto senzory pomocou nástrojov na skenovanie zraniteľností, aby bolo možné overiť, že skener (sniffer) spúšťa správne upozornenia. Ďalej je treba nasadiť paketový sniffer do DMZ na sledovanie toho, či HTTP prevádzka neobchádza HTTP proxy. Firewally na perimetri siete nesmú povoliť spojenie do Internetu z klientskeho segmentu, ale iba z definovaných a schválených proxy serverov.

Kritické opatrenie 14: Údržba, monitoring a analýza bezpečnostných auditných log záznamov.

Ako útočníci zneužívajú absenciu tohto opatrenia?

Nedostatky v bezpečnostnom logovaní a analýze umožňujú útočníkom skryť sa, utajiť použitý škodlivý softvér na získanie vzdialeného prístupu a aktivitu na stroji obete. Aj keď obete vedia, že ich systém je kompromitovaný, bez chráneného a kompletného logovania nie je možné vidieť detaily útoku a následné akcie útočníka. Log záznamy sú niekedy jediným dôkazom úspešného útoku. Mnoho organizácií uchováva auditné log záznamy kvôli tomu, aby spĺňali požiadavky noriem, zákonov či obchodných zmlúv. Útočníci sa spoliehajú na fakt, že organizácie tieto log záznamy vyhodnocujú len výnimočne a tak nevedia, že ich systémy boli kompromitované. Kvôli tomu útočníci dokážu v niektorých prípadoch bez povšimnutia organizácie kontrolovať ich stroje dlhé mesiace.

Ako implementovať, automatizovať a merať účinnosť tohto opatrenia

1. *Rýchle výhry:* Overiť nastavenia auditných log záznamov pre každé zariadenie a softvér na ňom nainštalovaný. Uistiť sa, že logy obsahujú dátum, čas (timestamp), zdrojovú a cieľovú adresu a ostatné užitočné časti paketu. Systémy majú uchovávať logy v štandardizovanom formáte (ak nie, je potrebné ich normalizovať).
2. *Rýchle výhry:* Uistiť sa, že všetky systémy, ktoré ukladajú logy majú dostatočný úložný priestor pre pravidelne generované logy. Logy musia byť pravidelne archivované a digitálne podpísané.
3. *Rýchle výhry:* Detailne logovať všetky vzdialené prístupy do DMZ alebo internej siete.
4. *Rýchle výhry:* Nakonfigurovať operačné systémy tak, aby logovali udalosti spojené s prístupom (používateľa k súborom a zložkám) bez oprávnenia. Neúspešné pokusy o prihlásenie musia byť tiež logované.
5. *Rýchle výhry:* Bezpečnostní zamestnanci a/alebo administrátori majú raz za dva týždne urobiť zápisy anomálií logov, preveriť ich a zdokumentovať.
6. *Prehľadnosť a priraďovanie*: Organizácia by mala do systému zahrnúť aspoň dva časové zdroje (NTP) z ktorých všetky servery a ostatné zariadenia získavajú údaje o čase, aby časové údaje v logoch boli konzistentné.
7. *Prehľadnosť a priraďovanie*: Hraničné sieťové zariadenia ako firewally, IPS a proxy musia byť nastavené tak, aby logovali celú prichádzajúcu (povolenú aj blokovanú) prevádzku.
8. *Prehľadnosť a priraďovanie*: Pre všetky servery je potrebné zabezpečiť, aby boli logy ukladané iba na write-only zariadenia alebo dedikované logovacie servery oddelené od zariadení generujúcich logy. Znižuje sa tak možnosť útočníka manipulovať s nimi.
9. *Prehľadnosť a priraďovanie*: Nasadiť SIEM systém na agregáciu a konsolidáciu logov z rôznych strojov a ich koreláciu a analýzu. Jeho používaním je možné získať profily bežných udalosti pre dané systémy a umožniť tak detekciu nezvyčajnej aktivity, vyhnúť sa planým poplachom, rýchlejšie identifikovať anomálie a predchádzať zaťažovaniu analytikov nepodstatnými udalosťami.

Postupy a nástroje na implementáciu a automatizáciu týchto opatrení

Väčšina zdarma dostupných a komerčných operačných systémov, sieťových zariadení a firewallov ponúka možnosť logovania. To je potrebné využiť a logy zasielať na centralizovaný logovací server. Firewally, proxy a systémy prístupné na diaľku musia byť nakonfigurované tak, aby ukladali všetky dostupné informácie o udalostiach. Operačné systémy, najmä serverov, musia logovať prístupy k zdrojom bez dostatočných privilégií. Organizácia by mala pravidelne skenovať svoje logy a porovnávať ich s inventárom aktív, aby bolo možné posúdiť, či každé riadené zariadenie generuje logy. Je potrebné používať nástroje na koreláciu logov, pretože manuálne vyhodnocovanie logov je veľmi náročné. Užitočné môžu byť aj analytické nástroje ako SIEM, avšak ľudské posúdenie a logika sú najdôležitejšie pre identifikáciu a porozumenie útokom.

Kritické opatrenie 15: Kontrola prístupu založená na princípe „need to know“.

Ako útočníci zneužívajú absenciu tohto opatrenia?

Niektoré organizácie neidentifikujú a neoddeľujú dostatočne starostlivo najcitlivejšie dáta od menej citlivých, verejne dostupných informácií na svojich interných sieťach. V mnohých prípadoch majú zamestnanci prístup ku všetkým alebo k väčšine informácií na sieti. Potom útočník, v prípade úspešného prieniku do siete, nemá problém nájsť a získať citlivé informácie.

Ako implementovať, automatizovať a merať účinnosť tohto opatrenia

1. *Rýchle výhry:* Zaviesť viacúrovňovú schému identifikácie a klasifikácie informácii.
2. *Rýchle výhry:* Uistiť sa, že zdieľané súbory sú chránené pred prístupom neautorizovaných zamestnancov pomocou ACL (Access Control Lists).
3. *Prehľadnosť a priraďovanie*: Organizácia musí vynucovať detailné logovanie prístupu k interným dátam a mimoriadnu autentifikáciu na prístup k citlivým dátam.
4. *Konfigurácia/očista:* Segmentovať sieť na základe klasifikačného stupňa informácií na ňom uchovávaných. Vždy, keď dáta tečú smerom do siete s nižším klasifikačným stupňom, je potrebné použiť šifrovanie.
5. *Konfigurácia/očista:* Obmedziť používanie USB kľúčov alebo automaticky šifrovať dáta na ne zapisované.
6. *Pokročilé:* Použiť host-based data loss prevention (DLP) na vynútenie ACL aj v prípade, že dáta sú kopírované zo servera. Predchádza sa tým obídeniu ACL pri ďalšom šírení dát (napr. z pracovnej stanice), ktoré boli predtým skopírované zo servera.
7. *Pokročilé:* Nasadiť honeytokeny na kľúčové servery pre identifikáciu používateľov, ktorí sa snažia dostať k dátam, ku ktorým by sa nemali dostať.

Postupy a nástroje na implementáciu a automatizáciu týchto opatrení

Je potrebné, aby organizácia pochopila, ktoré sú jej citlivé dáta, kde sa nachádzajú a kto k nim potrebuje mať prístup. Je potrebné zaviesť politiku klasifikácie informácií (verejné/interné/chránené) a informácie následne rozčleniť do ďalších skupín. Následne je potrebné informácie namapovať k svojim informačným systémom a aplikovať segmentáciu siete podľa citlivosti dát v nej uchovávaných. Ak je to možné, je nevyhnutné nasadiť firewally na kontrolu prístupu do každého segmentu. Ďalej je potrebné identifikovať požiadavky pre prístup jednotlivých používateľov (princíp need-to-know) k skupinám informácii a na ich základe definovať ACL. Zapnúť detailné logovanie na všetkých serveroch, aby bolo možné vystopovať situácie kedy niekto pristupoval k dátam, ku ktorým by nemal pristupovať.

Kritické opatrenie 16: Monitoring a riadenie používateľských kont.

Ako útočníci zneužívajú absenciu tohto opatrenia?

Útočníci často objavia a zneužijú legitímne, ale neaktívne používateľské kontá (dodávateľské, bývalých zamestnancov) a takto sťažujú možnosti svojho objavenia pre tých, ktorí sieť sledujú. Dokonca niektorí zamestnanci s nekalými úmyslami, prípadne bývalí zamestnanci, mali prístup do organizácie dlho po vypršaní pracovnej zmluvy a takto mohli dáta zneužiť.

Ako implementovať, automatizovať a merať účinnosť tohto opatrenia

1. *Rýchle výhry:* Preveriť všetky používateľské kontá a vymazať/vypnúť tie, ktoré nie sú spojené s procesom alebo vlastníkom.
2. *Rýchle výhry:* Systém musí denne vytvárať správu, ktorá obsahuje zoznam zamknutých účtov, vypnutých účtov, účty so starými heslami a účty s heslami, ktorých platnosť nikdy nevyprší. Tento zoznam potom bezpečným spôsobom zasielať administrátorovi.
3. *Rýchle výhry:* Zriadiť a dodržiavať proces na zrušenie prístupu vypnutím účtov okamžite po ukončení pracovného pomeru so zamestnancom alebo dodávateľom.
4. *Rýchle výhry:* Pravidelne monitorovať používanie účtov a automaticky odhlasovať používateľov po štandardnej dobe nečinnosti.
5. *Rýchle výhry:* Monitorovať používanie účtov na odhalenie „spiacich“ účtov, ktoré neboli použité istú dobu (napr. 30 dní) a upozorniť na to používateľa a jeho nadriadeného. Po dlhšej dobe (napr. 60 dní) je potrebné účet zrušiť alebo vypnúť.
6. *Rýchle výhry:* Po zrušení účtu je potrebné zašifrovať a presunúť s ním spojené súbory na bezpečný server na analýzu.
7. *Rýchle výhry:* Pri všetkých neadministrátorských účtoch vyžadovať minimálne 12-znakové heslá obsahujúce písmená, čísla a špeciálne znaky. Heslá sa musia meniť aspoň každých 90 dní a nesmie byť povolené použitie heslá z posledných 15 použitých hesiel.
8. *Rýchle výhry:* Po ôsmich neúspešných pokusoch o prihlásenia v rozmedzí 45 minút je potrebné účet zamknúť na 120 minút.
9. *Prehľadnosť/priraďovanie:* Pravidelne (štvrťročne alebo aspoň ročne) vyžadovať, aby manažéri porovnali aktívnych zamestnancov a dodávateľov s existujúcimi používateľskými účtami. Účty, ktoré nie sú k nim priradené, je potrebné vymazať.
10. *Prehľadnosť/priraďovanie:* Prostredníctvom auditného logovania monitorovať pokusy o prístup k vypnutým účtom.
11. *Konfigurácia/očista:* Pre každého používateľa vytvoriť profil typického používania účtu na základe bežného času a dĺžky prístupu. Generovať denné správy, ktoré poukazujú na používateľov prihlásených počas nezvyčajného času alebo s nezvyčajne dlhou dobou prihlásenia (o 150 percent).

Postupy a nástroje na implementáciu a automatizáciu týchto opatrení

Napriek tomu, že väčšina operačných systémov obsahuje možnosť logovania používaných účtov, niekedy je táto možnosť defaultne vypnutá. Aj keď je táto možnosť zapnutá a aktívna, často neposkytuje detaily o prístupe do systému s dostatočnou granularitou. Bezpečnostní zamestnanci môžu nakonfigurovať systémy tak, aby zaznamenávali detailnejšie informácie

o prístupe k účtom a používať vlastné skripty alebo nástroje na analýzu logov tretích strán. Používateľské účty je potrebné pozorne sledovať, všetky „spiace“ účty musia byť zrušené a následne odstránené zo systému. Všetky aktívne účty musia byť priradené k autorizovaným používateľom a je potrebné uistiť sa, že ich heslá sú dostatočne silné a pravidelne menené. Používatelia musia byť po istej dobe nečinnosti automaticky odhlásení zo systému, aby sa znížili možnosti útočníka zneužiť ich systém na získanie informácií organizácie.

Kritické opatrenie 17: Prevencia straty dát

Ako útočníci zneužívajú absenciu týchto opatrení?

V posledných rokoch útočníci exfiltrovali viac ako 20 TB často citlivých dát z obranných zložiek, ich dodávateľov a podobných organizácií. Ku mnohým útokom došlo na sieti, v iných prípadoch došlo k odcudzeniu notebookov a iného zariadenia obsahujúcich citlivé informácie. Kvôli tomu, že mnoho používateľov nemonitoruje odchádzajúcu prevádzku zo svojich systémov, v mnohých prípadoch ani nevedeli, že ich systémy opúšťa značné množstvo citlivých dát. Toky dát, ktoré prekračujú hranice siete elektronicky alebo fyzicky, musia byť dôkladne sledované na minimalizáciu ich vystavenia útočníkom. Strata kontroly nad chránenými alebo citlivými dátami je vážnou hrozbou pre biznis operácie a potenciálne ohrozenie národnej bezpečnosti. Kým niektoré dáta uniknú z dôvodu krádeže alebo špionáže, drvivá väčšina týchto problémov pochádza zo zle pochopených postupov, chýbajúcich efektívnych politík a chýb používateľov. Prevencia straty dát (DLP) predstavuje komplexný prístup zahŕňajúci zamestnancov, procesy a systémy, ktoré identifikujú, monitorujú a ochraňujú dáta pri používaní (koncové stanice), dáta pri presune (sieť) a uložené dáta prostredníctvom kontroly obsahu a centralizovaným riadením.

Ako implementovať, automatizovať a merať efektívnosť týchto opatrení

1. *Rýchle výhry:* Nasadiť šifrovanie pevných diskov na mobilných strojoch obsahujúcich citlivé dáta.
2. *Prehľadnosť/priraďovanie:* Pomocou nástrojov na monitorovanie siete analyzovať odchádzajúcu prevádzku a hľadať rôzne anomálie ako sú napríklad presuny veľkých súborov, dlho pretrvávajúce spojenia, spojenia obnovované v pravidelných intervaloch, používanie nezvyčajných protokolov a portov a prítomnosť určitých kľúčových slov v dátach prekračujúci perimeter siete.
3. *Prehľadnosť/priraďovanie:* Na perimetre siete nasadiť automatizované nástroje na monitorovanie citlivých informácií, kľúčových slov a iných charakteristík na objavenie neautorizovaných pokusov o exfiltráciu dát cez hranicu siete a blokovať takéto presuny dát a zasielať upozornenie zodpovedným zamestnancom.
4. *Prehľadnosť/priraďovanie:* Použitím automatizovaných nástrojov pravidelne skenovať serverové stroje na určenie toho, či sa na nich nachádzajú citlivé dáta vo forme otvoreného textu. Tieto nástroje hľadajúce vzorce indikujúce prítomnosť citlivých informácií a pomáhajú určiť, či nejaký proces určitým spôsobom neprepúšťa citlivé informácie.
5. *Prehľadnosť/priraďovanie:* Používať proxy odchádzajúcej prevádzky na monitorovanie a riadenie informácií opúšťajúcich organizáciu.

6. *Konfigurácia/očista:* Používať bezpečné, autentifikované a šifrované mechanizmy pri presune dát medzi sieťami.
7. *Konfigurácia/očista:* Šifrovať dáta uložené na vymeniteľných a ľahko transportovateľných úložných médiách (USB,CD,DVD).
8. *Konfigurácia/očista:* V prípade, že nie je požiadavka na používanie takýchto zariadení, je potrebné nakonfigurovať systémy tak, aby neumožňovali zápis dát na USB média. Ak je používanie takýchto zariadení nevyhnuté, treba nakonfigurovať systémy tak, aby umožnili používanie iba špecifických USB zariadení (na základe sériového čísla a i.) a automatické šifrovanie dát, ktoré sú na ne ukladané. Je potrebné udržiavať inventár všetkých autorizovaných zariadení.
9. *Konfigurácia/očista:* Používať sieťové DLP riešenia na monitorovanie a riadenie toku dát v rámci siete. Všetky anomálie, ktoré presahujú normálne vzorce prevádzky, musia byť zaznamenané a je potrebné podniknúť vhodné kroky na ich riešenie.
10. *Pokročilé:* Monitorovať všetku odchádzajúcu prevádzku z organizácie a detegovať neautorizované použitie šifrovania. Útočníci často používajú šifrované kanály na obídenie bezpečnostných sieťových zariadení. Preto je dôležité, aby bola organizácia schopná detegovať podvodné spojenia, ukončiť tieto spojenia a napraviť infikovaný systém.

Postupy a nástroje na implementáciu a automatizáciu týchto opatrení

Sú dostupné komerčné DLP riešenia, ktoré hľadajú pokusy o exfiltráciu a detegujú ostatné podozrivé aktivity spojené s chránenou sieťou, ktorá obsahuje citlivé informácie. Organizácia nasadzujúca takéto nástroje, musí pozorne preveriť logy a ísť po všetkých objavených pokusoch (aj keď úspešné blokovaných) o prenos citlivých informácií von z organizácie bez autorizácie.

Kritické opatrenie 18: Schopnosť reakcie na incidenty

Ako útočníci zneužívajú absenciu týchto opatrení

Organizácie, ktoré nemajú efektívne plány na riešenie incidentov, utrpeli mnoho škôd na reputácii a strate informácií. Bez plánov na riešenie incidentov organizácia nemá ako zistiť, že prebieha útok, resp. ak je útok detegovaný, organizácia nemá ako podniknúť adekvátne kroky na minimalizáciu škôd, objavenie a odstránenie útočníkovej prítomnosti zo systému a bezpečne obnoviť systém. Čiže útočník môže mať oveľa väčší vplyv na spôsobenie škôd, infikovanie ďalších systémov a exfiltráciu väčšieho množstva citlivých dát, ako pri existencii efektívnych plánov riešenia incidentov v organizácii.

Ako implementovať, automatizovať a merať efektívnosť týchto opatrení

1. *Rýchle výhry:* Uistiť sa, že v organizácii existujú postupy na riešenie incidentov zahŕňajúce definíciu rol zamestnancov pri riešení incidentov. Postupy by mali definovať fázy riešenia incidentov v súlade so smernicami NIST, ktoré inšpirovali aj odporúčania agentúry ENISA.
2. *Rýchle výhry:* Organizácie musia priradiť pracovné zaradenia a povinnosti pre riešenie počítačových a sieťových incidentov.
3. *Rýchle výhry:* Definovať manažérskych zamestnancov, ktorí budú podporovať proces riešenia incidentov pri kľúčových rozhodnutiach.

4. *Rýchle výhry:* Zaviesť štandardy na časové rámce pre systémových administrátorov a ostatných zamestnancov na hlásenie nezvyčajných udalostí tímu na riešenie incidentov, mechanizmov na hlásenie a druh informácií, ktorý musí byť zahrnutý v notifikácii o incidente. Je vhodné informovať národný CERT/CSIRT tím, interný CSIRT/CERT tím, alebo tím CSIRT/CERT, do ktorého konštituencie daná organizácia patrí (v prípade štátnych inštitúcií je to vládny CSIRT/CERT tím).
5. *Rýchle výhry:* Publikovať informácie pre všetkých zamestnancov (vrátane dodávateľov) ohľadom hlásenia počítačových anomálií a incidentov tímu na riešenie incidentov. Tieto informácie je vhodné zahrnúť do pravidelných školení na zvýšenie bezpečnostného povedomia.
6. *Konfigurácia/očista:* Organizovať pravidelné sedenia pre zamestnancov poverených riešením incidentov ohľadom možných scenárov priebehu incidentov na zaistenie toho, že rozumejú súčasným hrozbám a rizikám, ako aj ich zodpovednostiam pri riešení incidentov.

Postupy a nástroje na implementáciu a automatizáciu týchto riešení

Po definovaní detailných postupov na riešenie incidentov je potrebné organizovať pravidelný tréning a cvičenia pre tím na riešenie incidentov. Je vhodné pracovať so sériami pravdepodobných útokov, ktoré sú nastavené tak, aby zodpovedali aktuálnym hrozbám a zraniteľnostiam, ktorým organizácia čelí. Tieto scenáre pomôžu pri uistení sa, že členovia tímu rozumejú svojim roliam a sú pripravení riešiť počítačové incidenty.

Kritické opatrenie 19: Bezpečné sieťové inžinierstvo.

Ako útočníci zneužívajú absenciu týchto opatrení

Mnohé opatrenia v tomto dokumente sú efektívne, ale je možné ich obísť v zle navrhnutých sieťach. Bez starostlivo naplánovanej a vhodne implementovanej sieťovej architektúry útočníci dokážu obísť bezpečnostné opatrenia na istých systémoch a z nich potom podniknúť útok na cieľové stroje. Útočníci často mapujú siete hľadajúc nepotrebné spojenia medzi systémami, chabé filtrovanie a chýbajúcu separáciu sietí. Preto je potrebné nasadiť účinný proces bezpečného sieťového inžinierstva na doplnenie opatrení v ostatných častiach tohto dokumentu.

Ako implementovať, automatizovať a merať efektívnosť týchto opatrení

1. *Rýchle výhry:* Sieť musí byť navrhnutá s použitím aspoň trojvrstvovej architektúry (DMZ, middleware a interná sieť). Všetky systémy dostupné z internetu musia byť v DMZ, ale DMZ nesmie nikdy obsahovať citlivé dáta. Všetky systémy obsahujúce citlivé dáta musia byť obsiahnuté na internej sieti a nikdy nesmú byť priamo dostupné z internetu. DMZ systémy môžu s internou sieťou komunikovať len cez aplikačné proxy, ktoré sa nachádza na vrstve middleware.
2. *Konfigurácia/očista:* Na podporu rýchlej reakcie na detegované útoky musí byť sieťová architektúra a systémy, ktoré to zabezpečujú navrhnuté tak, aby bolo možné rýchle nasadenie nových ACL pravidiel signatúr blokovania čiernych dier a ostatných obranných opatrení.

3. *Prehľadnosť/priraďovanie:* DNS majú byť nasadené hierarchickým a štruktúrovaným spôsobom tak, že všetky klientske stroje z internej siete sú nakonfigurované tak, aby posielali požiadavky na DNS servery v intranete, nie na DNS servery v internete. Tieto interné DNS servery musia byť nakonfigurované tak, aby preposielali požiadavky, ktoré nevedia vyriešiť na DNS servery umiestnené v chránenej DMZ. Tieto DMZ servery musia byť jedinými DNS servermi, ktoré majú povolené posielať požiadavky do internetu.
4. *Prehľadnosť/priraďovanie:* Bezpečnosť musí byť zakomponovaná do všetkých fáz životného cyklu vývoja softvéru, aby bolo zabezpečené, že všetky bezpečnostné problémy sú včas riešené.
5. *Konfigurácia/očista:* Segmentovať sieť organizácie do viacerých oddelených dôveryhodných zón na poskytnutie lepšej kontroly prístupu do systému a ochrany hraníc intranetu.

Postupy a nástroje na implementáciu a automatizáciu týchto opatrení

Na zaistenie konzistentnej a obranyschopnej siete musí byť jej architektúra založená na šablóne, ktorá popisuje celkovú schému siete a služby, ktoré poskytuje. Organizácia musí pripraviť diagramy každej jej siete, ktorá znázorňuje sieťové komponenty ako routery, firewally a switche, spolu s dôležitými servermi a skupinami klientskych strojov.

Kritické opatrenie 20: Penetračné testovanie

Ako útočníci využívajú absenciu týchto opatrení

Útočníci prenikajú do sietí a systémov pomocou sociálneho inžinierstva a zneužitím zraniteľného softvéru a hardvéru. Ako náhle získajú prístup, často sa zahrabú hlboko do cieľových systémov a zvýšia množstvo strojov, nad ktorými majú kontrolu. Väčšina organizácií neprecvičuje svoje obranné mechanizmy, takže nemajú prehľad o ich možnostiach a sú nepripravení na identifikáciu a riešenie útoku. Penetračné testovanie zahŕňa napodobňovanie činnosti počítačového útočníka na identifikáciu zraniteľnosti cieľovej organizácie a ich zneužitie na určenie toho, akého prístupu je útočník schopný. Penetračné testy poskytujú dôslednejšiu analýzu bezpečnostných chýb než posúdenie zraniteľnosti. Posúdenie zraniteľnosti sa zameriava na identifikáciu potenciálnej zraniteľnosti, kým penetračné testovanie riadenými pokusmi o zneužitie zraniteľnosti napodobňuje útočníkovu činnosť. Výsledkom je hlbšia znalosť bezpečnostných rizík, pretože ukazuje či a ako vie útočník zneužiť stroje, presúvať sa do ostatných systémov vo vnútri cieľovej organizácie a získať prístup k citlivým informáciám.

Cvičenia červených tímov (tím, ktorý sa snaží exploitovať aj zraniteľnosti v rámci fyzickej bezpečnosti) idú ešte viac do hĺbky ako penetračné testovanie. Tie cvičenia majú za cieľ zvýšenie pripravenosti organizácie, lepšie tréningy pre zamestnancov, ktorí sa starajú o obranu systémov a preverenie súčasnej úrovne. Nezávislé červené tímy môžu poskytnúť cenné a objektívne poradenstvo o existencii zraniteľností a o účinnosti už nasadených či plánovaných obranných mechanizmov a opatrení.

Ako implementovať, automatizovať a merať efektívnosť týchto opatrení

1. *Rýchle výhry:* Pravidelne vykonávať externé a interné penetračné testovanie na odhalenie zraniteľností a vektorov útokov, ktoré môžu byť použité na úspešné zneužitie systémov organizácie. Penetračné testovanie má byť vykonávané z vonku siete (napr. internet, bezdrôtové siete), ako aj z vnútra siete (interná sieť), aby boli simulované útoky vonkajšieho útočníka ako aj vnútorného.
2. *Prehľadnosť/priraďovanie:* Pravidelne vykonávať cvičenia červených tímov na preverenie pripravenosti organizácie identifikovať a zastaviť útoky a rýchlo a efektívne na ne reagovať.
3. *Prehľadnosť/priraďovanie:* Uistiť sa, že systémové problémy preukázané počas penetračného testovania a cvičení červených tímov sú úplne ošetrené.
4. *Prehľadnosť/priraďovanie:* Merať, či organizácia dostatočne zmiernila chyby, ktoré môžu umožniť útoky, pomocou zavedenia automatizovaných procesov na:
    - E-maily vo forme cleartextu a dokumenty s výrazom „password“ v názve súboru alebo v tele.
    - Diagramy kritickej siete uložené online alebo vo forme cleartextu.
    - Kritické konfiguračné súbory uložené online alebo vo forme cleartextu.
    - Záznamy z posúdenia zraniteľností penetračných testov a zistenia červených tímov uložené online alebo vo forme cleartextu.
    - Ostatné citlivé informácie, ktoré boli manažmentom označené ako kritické pre fungovanie organizácie počas určovania rozsahu penetračných testov a cvičení červených tímov.
5. *Prehľadnosť/priraďovanie:* Do penetračného testovania zahrnúť sociálne inžinierstvo. Ľudský prvok je často najslabším článkom v organizácii a častým cieľom útočníkov.
6. *Pokročilé:* Vyvinúť metódu ohodnocovania výsledkov cvičení červených tímov, a aby ich bolo možné postupom času porovnávať.
7. *Pokročilé:* Vytvoriť pokusné prostredie, ktoré imituje produkčné prostredie pre špecifické penetračné testy a útoky červených tímov proti prvkom, ktoré nie sú bežne testované počas prevádzky, ako napr. útoky proti hlavným kontrolným systémom a systémom na zber dát.

Postupy a nástroje na implementáciu a automatizáciu týchto opatrení

Každá organizácia by mala definovať jasný rozsah a pravidlá pri zapojení penetračného testovania a analýz červených tímov. Rozsah takýchto projektov by mal zahŕňať minimálne systémy s najcennejšími informáciami a s najdôležitejšou produkčnou funkcionalitou v organizácii. Ostatné menej hodnotné systémy môžu byť tiež testované, aby sa preverilo, či môžu byť použité ako odrazové body na kompromitáciu hodnotnejších cieľov. Pravidlá pre penetračné testovanie a analýzy červených tímov musia minimálne uvádzať čas testovania, trvanie testovania a celkový prístup k testovaniu.