AmCham Slovakia

#FUTUREREADY

AKO CHRÁNIŤ FIRMU S MINIMÁLNYM ROZPOČTOM?

ZÁKLADY KYBERNETICKEJ BEZPEČNOSTI PRE MALÉ A STREDNÉ PODNIKY

S PODPOROU

U.S. Embassy Bratislava

ODBORNÍ PARTNERI

accenture

SIEMENS Healthineers

Void

OBSAHOVÝ PARTNER

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

PARTNERI

SBA SLOVAK | BUSINESS | AGENCY

Slovenská obchodná a priemyselná komora

American Center Košice

American Center Žilina

American Center Banská Bystrica

UVP TECHNICOM

RIADENIE RIZÍK

Na zabezpečenie vašich údajov a systémov si osvojte prístup založený na riziku.

V kontexte kybernetickej bezpečnosti je riadenie rizík (anglicky „risk management“) proces identifikácie, posúdenia a riadenia potenciálnych hrozieb, ktoré by mohli ohroziť dáta a IT systémy organizácie. Ide o systematický prístup, ktorý má za cieľ minimalizovať negatívny dopad možných útokov na kritické obchodné operácie.

KĽÚČOVÉ FÁZY RIADENIA RIZÍK

Riadenie rizík je nepretržitý cyklus, ktorý sa opakuje a prispôsobuje sa novým hrozbám a zmenám v IT prostredí. Jeho hlavné fázy sú:

IDENTIFIKÁCIA RIZÍK

V tejto fáze organizácia hľadá potenciálne hrozby a zraniteľnosti. Identifikujú sa všetky dôležité aktíva (dáta, servery, aplikácie, siete) a možné hrozby, ktoré by ich mohli poškodiť (napr. malvér, phishing, prírodné katastrofy, zlyhanie hardvéru). Pýtate sa: “Čo môžeme stratiť?” a “Ako to môžeme stratiť?”.

ANALÝZA A HODNOTENIE RIZÍK

Tu sa posudzuje pravdepodobnosť, že sa riziko naplní, a potenciálny dopad, ak k tomu dôjde. Hodnotí sa finančná strata, poškodenie reputácie, narušenie prevádzky alebo právne následky. Riziká sa často kategorizujú na nízke, stredné a vysoké, čo pomáha určiť prioritu. Vzorec pre výpočet rizika môže byť napr.: *Riziko=Pravdepodobnosť×Dopad*

OŠETRENIE RIZÍK

V tejto fáze sa rozhoduje, ako s identifikovanými rizikami naložiť. existujú štyri hlavné stratégie:

- **Zníženie rizika:** Implementácia kontrolných opatrení na zníženie pravdepodobnosti alebo dopadu rizika. Napríklad inštalácia antivírusového softvéru, pravidelné zálohovanie alebo školenie zamestnancov.
- **Akceptovanie rizika:** Rozhodnutie, že riziko je dostatočne nízke a nie je ekonomicky výhodné ho riešiť. Organizácia sa rozhodne, že prípadné škody sú menšie ako náklady na ich prevenciu.
- **Prenesenie rizika:** Presunutie zodpovednosti za riziko na tretiu stranu, napríklad prostredníctvom poistenia proti kybernetickým útokom.
- **Vyhnutie sa riziku:** Zastavenie činnosti, ktorá vytvára riziko. Napríklad zrušenie projektu, ktorý by mohol ohroziť kritické dáta.

MONITOROVANIE A KONTROLA

Riadenie rizík sa nekončí implementáciou opatrení. Je potrebné ich neustále monitorovať a vyhodnocovať ich účinnosť. Hrozby sa neustále menia, preto je nevyhnutné pravidelne prehodnocovať a aktualizovať rizikové plány.

PREČO JE RIADENIE RIZÍK DÔLEŽITÉ?

Riadenie rizík nie je len o technológiách, ale o strategickom rozhodovaní. Umožňuje organizáciám:

- Identifikovať a prioritizovať investície do bezpečnosti, aby sa peniaze použili na ochranu najdôležitejších aktív.
- Zlepšiť odolnosť voči útokom a znížiť finančné a reputačné škody.
- Splniť regulačné požiadavky, ktoré vyžadujú od organizácií zabezpečenie dát (napr. GDPR).
- Získať dôveru zákazníkov a partnerov.

TRÉNUJTE A VZDELÁVAJTE

Spoločne budujte bezpečnosť uplatniteľnú pre všetkých zamestnancov vo vašej organizácii.

Vzdelávanie a tréningy v oblasti kybernetickej bezpečnosti už nie sú len pre IT profesionálov, ale sú nevyhnutné pre každého, kto používa internet. Digitálne útoky sú čoraz sofistikovanejšie a častejšie, a preto je dôležité vedieť sa im brániť. Pravidelné tréningy sú efektívnym spôsobom, ako sa naučiť rozpoznať hrozby a správne reagovať na incidenty.

DÔVODY VZDELÁVANIA

- **Ochrana vlastných údajov:** Naučíte sa, ako chrániť svoje osobné údaje, finančné informácie a online identitu. Získate znalosti o tom, ako vytvoriť silné heslá, rozpoznať phishingové útoky a zabezpečiť svoje domáce siete a zariadenia.
- **Zodpovednosť a dôvera:** Získate zručnosti, ktoré vám pomôžu chrániť nielen seba, ale aj svojich blízkych. Môžete im poradiť, ako sa bezpečne pohybovať v online prostredí a vyhnúť sa digitálnym hrozbám.
- **Kritické myslenie:** Kybernetická bezpečnosť podporuje analytické a kritické myslenie. Budete sa učiť, ako identifikovať zraniteľné miesta, predvídať útoky a nachádzať kreatívne riešenia na ich prevenciu.

TYPY VZDELÁVANIA V KYBERNETICKEJ BEZPEČNOSTI

Školenia sa môžu deliť na viacero kategórií, zameraných na rôzne úrovne znalostí a profesionálne ciele. Základné delenie:

- **Základné školenia pre zamestnancov:** Tieto tréningy sú určené pre všetkých v organizácii, od administratívnych pracovníkov po manažérov. Zameriavajú sa na základné koncepty, ako je rozoznanie phishingu, bezpečné používanie hesiel, ochrana pred sociálnym inžinierstvom a bezpečné používanie firemných zariadení. Tieto kurzy zvyšujú kolektívne povedomie a znižujú riziko, že sa stane obeťou útoku.
- **Technické školenia:** Tieto kurzy sú pre profesionálov z IT sektora. Sú zamerané na špecializované oblasti ako penetračný testing (testovanie slabých miest v systéme), digitálna forenzia (vyšetrovanie kybernetických zločinov), alebo správa bezpečnostných systémov. Technické školenia poskytujú praktické zručnosti na ochranu a správu IT infraštruktúry.

SPRÁVA AKTÍV

Identifikujte dáta a ostatné informačné aktíva a namapujte procesy, ktoré sú nimi podporované.

Aktíva predstavujú všetko, čo má pre organizáciu hodnotu a vyžaduje ochranu. Ich strata, poškodenie alebo neoprávnený prístup by mohol mať negatívny vplyv na firmu, jej operácie alebo jej reputáciu. Správa aktív je systematický proces riadenia a optimalizácie hodnoty aktív počas celého ich životného cyklu. Správa aktív je kľúčovým prvkom pre znižovanie alebo elimináciu rizík.

Správne riadenie aktív je základom akejkoľvek účinnej stratégie ochrany. Bez poznania toho čo vlastníte a čo potrebujete chrániť, nie je možné reálne zabezpečiť ochranu aktív.

ZÁKLADNÉ DELENIE AKTÍV

- **Primárne aktíva:** zahŕňajú údaje, citlivé údaje, ako sú osobné údaje zákazníkov, finančné záznamy, duševné vlastníctvo (patenty, obchodné tajomstvá), databázy a e-mailová komunikácia, ...
- **Podporné aktíva:** všetky hmatateľné veci, ako sú servery, počítače, telefóny, pevné disky, sieťové zariadenia a dokonca aj budovy, softvérové vybavenie, ľudia, ...

HLAVNÉ KROKY

- **Identifikácia a kategorizácia:** základným krokom je vytvorenie inventára všetkých aktív, ich lokalizácia a priradenie zodpovednosti.
- **Analýza rizík:** nasleduje posúdenie rizík, ktoré im hrozia.
- **Aplikácia bezpečnostných kontrol:** rozhodnutie, ktoré bezpečnostné opatrenia sú potrebné pre jednotlivé aktíva. Je potrebné zamerať sa na najdôležitejšie aktíva s najvyšším rizikom.
- **Súlad s predpismi:** takýto postup zabezpečuje aj dodržanie súladu s medzinárodnými aj lokálnymi predpismi.

ARCHITEKTÚRA A KONFIGURÁCIA

Navrhujte, implementujte, udržiavajte a spravujte systémy bezpečným spôsobom.

Bezpečnostná architektúra je viac menej strategický plán o tom, ako je celá IT infraštruktúra navrhnutá a chránená. Architektúra integruje riešenie bezpečnosti všetkých systémov a procesov s cieľom vytvorenia komplexného, viacvrstvového obranného systému, ktorý dokáže identifikovať, predchádzať a reagovať na kybernetické hrozby.

DÔLEŽITÉ PRINCÍPY BEZPEČNOSTNEJ ARCHITEKTÚRY

- **Viacvrstvová obrana:** Podstatou je, že žiadne jediné bezpečnostné opatrenie nie je stopercentne spoľahlivé. Preto sa vytvára viacero vrstiev ochrany. Po prelomení jednej vrstvy (napríklad firewall), narazí útočník na ďalšiu (napríklad systém na detekciu hrozieb).
- **Princíp najnižších oprávnení:** Každému používateľovi, systému alebo aplikácii je poskytnutý prístup len k tým zdrojom, ktoré nevyhnutne potrebuje na vykonanie svojich úloh.
- **Zabezpečenie na úrovni aplikácií a údajov:** Ochrana na úrovni softvéru a šifrovanie samotných dát, dokáže zabezpečiť, že ak sa útočník dostane údajom, nebudú pre neho čitateľné.
- **Kontinuálne monitorovanie a audit:** Bezpečnostná architektúra zahŕňa nástroje na nepretržité sledovanie systémov, ktoré umožňujú včasné odhalenie anomálií a ich reakciu.
- **Segmentácia siete:** Oddelenie kritických častí siete od ostatných zabezpečí, že sa útočník po prelomení perimetra nedostane do iných častí siete, kde sa môžu nachádzať citlivé údaje.

Bezpečnostná konfigurácia predstavuje súbor nastavení a parametrov hardvérových a softvérových komponentov s cieľom minimalizovať bezpečnostné riziká.

KĽÚČOVÉ ASPEKTY BEZPEČNOSTNEJ KONFIGURÁCIE

Bezpečnostná konfigurácia sa uplatňuje na všetkých úrovniach, od operačných systémov cez aplikácie až po sieťové zariadenia.

- **Odstránenie zbytočných služieb:** Každá spustená služba alebo aplikácia, ktorá nie je nevyhnutná, predstavuje potenciálne riziko. Ak je služba zraniteľná, útočník ju môže zneužiť na prístup k systému. Príkladom je vypnutie vzdialeného prístupu alebo starých verzií softvéru, ktoré už nie sú podporované.
- **Používanie silných hesiel a riadenie prístupu**: Jednoduché heslá sú jedným z najčastejších dôvodov kompromitácie. Bezpečnostná konfigurácia vyžaduje zavedenie komplexných hesiel a viacfaktorovej autentifikácie (MFA). Taktiež sa uplatňuje princíp najmenších oprávnení, kedy majú používatelia prístup iba k tomu, čo je pre ich prácu absolútne nevyhnutné.
- **Implementácia bezpečnostných záplat:** Pravidelné aktualizácie (patch management) sú nevyhnutné. Výrobcovia softvéru vydávajú záplaty na opravu zraniteľností, ktoré boli objavené. Ignorovanie týchto aktualizácií je ako nechať otvorené dvere pre útočníkov.
- **Zabezpečenie siete:** To zahŕňa konfiguráciu firewallov, segmentáciu siete a šifrovanie dát, ktoré prechádzajú sieťou. Je dôležité mať jasne definované pravidlá, ktorá prevádzka je povolená a ktorá nie.
- **Audit a monitorovanie:** Bezpečnostná konfigurácia nie je jednorazová úloha. Je potrebné ju pravidelne kontrolovať a monitorovať, aby sa odhalili akékoľvek neoprávnené zmeny. Automatizované nástroje na správu konfigurácie môžu pomôcť zabezpečiť konzistentnosť a súlad s internými pravidlami.

SPRÁVA ZRANITEĽNOSTÍ

Chráňte systémy počas celého ich životného cyklu.

Riadenie zraniteľností je systematický proces, ktorého cieľom je identifikovať, analyzovať a opraviť slabé miesta v systémoch a sieti. Tieto slabé miesta môžu byť softvérové chyby, nesprávna konfigurácia alebo zraniteľnosti v hardvéri. Zanedbanie tohto procesu môže mať závažné následky.

HLAVNÉ DÔVODY PRE SPRÁVU ZRANITEĽNOSTÍ

Najdôležitejším dôvodom je prevencia. Väčšina kybernetických útokov, vrátane ransomvéru a únikov dát, využíva známe a neopravené zraniteľnosti. Pravidelným riadením zraniteľností eliminujete hlavné slabiny, ktoré by mohli útočníci zneužiť.

- **Ochrana citlivých dát:** Mnoho zraniteľností umožňuje útočníkom získať prístup k citlivým informáciám, ako sú osobné údaje zákazníkov, finančné záznamy alebo duševné vlastníctvo. Systematické riadenie zraniteľností chráni tieto dáta a znižuje riziko finančných strát a poškodenia reputácie.
- **Dodržiavanie predpisov:** Mnoho regulačných štandardov (napríklad GDPR, PCI DSS a iné) vyžaduje, aby firmy aktívne spravovali svoje zraniteľnosti a preukázali, že podnikli primerané kroky na ochranu dát. Nesplnenie týchto požiadaviek môže viesť k vysokým pokutám a právnym problémom.
- **Optimalizácia nákladov:** Aj keď sa to na prvý pohľad nezdá, riadenie zraniteľností je nákladovo efektívnejšie ako riešenie dôsledkov úspešného kybernetického útoku. Náklady spojené s obnovou systémov, právnymi poplatkami, pokutami a stratou dôvery zákazníkov sú oveľa vyššie ako investícia do preventívnych opatrení.
- **Zlepšenie celkovej bezpečnosti:** Riadenie zraniteľností nie je len o zaplátaní softvéru. Je to komplexný proces, ktorý pomáha organizácii pochopiť, kde sa nachádzajú jej najväčšie slabiny. Vďaka tomu môžete prijímať lepšie rozhodnutia o investíciách do bezpečnosti a neustále zvyšovať úroveň ochrany.

HLAVNÉ FÁZY SPRÁVY ZRANITEĽNOSTÍ

IDENTIFIKÁCIA

V tejto prvej fáze je cieľom nájsť všetky potenciálne slabé miesta v systémoch a sieti.

- **Skenovanie zraniteľností:** Využívajú sa špeciálne nástroje (napr. Nessus, Qualys), ktoré automaticky skenujú sieť a systémy, hľadajú známe chyby v softvéri, nesprávne konfigurácie a otvorené porty.
- **Penetračný testing:** Etickí hackeri simulujú reálny útok na systém, aby odhalili zraniteľnosti, ktoré by automatizované skenery nemuseli nájsť.
- **Audit konfigurácií:** Kontroluje sa, či sú systémy nastavené bezpečne a či spĺňajú interné štandardy.

HODNOTENIE

Po identifikácii slabých miest je potrebné určiť ich závažnosť.

- **Analýza rizík:** Každá zraniteľnosť sa posudzuje na základe dvoch faktorov: pravdepodobnosť zneužitia a potenciálny dopad na spoločnosť (napr. finančné straty, strata dát, poškodenie reputácie).
- **Štandardy hodnotenia:** Závažnosť zraniteľností sa často hodnotí pomocou štandardov, ako je napríklad CVSS (Common Vulnerability Scoring System), ktorý prideľuje skóre od 0 do 10.

PRIORITIZÁCIA

Keďže nie je možné opraviť všetky zraniteľnosti naraz, je dôležité určiť, ktoré sú najkritickejšie.

- **Zameranie na kritické aktíva:** Najvyššiu prioritu majú zraniteľnosti, ktoré ohrozujú kľúčové aktíva (napr. databázy s citlivými údajmi alebo systémy, ktoré sú nevyhnutné pre prevádzku firmy).
- **Rýchlosť nápravy:** Niektoré zraniteľnosti majú už verejne dostupný exploit, čo znamená, že ich útočníci môžu zneužiť veľmi rýchlo. Tieto zraniteľnosti vyžadujú okamžitú pozornosť.

NÁPRAVA

Táto fáza sa zameriava na odstránenie zraniteľností.

- **Aplikácia záplat:** Inštalácia bezpečnostných aktualizácií, ktoré vydávajú výrobcovia softvéru, je najčastejším spôsobom nápravy.
- **Zmena konfigurácie:** Vypnutie zbytočných služieb, zmena hesiel alebo úprava nastavení, ktoré znižujú riziko.
- **Dočasné riešenia:** V prípadoch, keď nie je možné okamžite aplikovať záplatu, sa môžu použiť dočasné opatrenia (napr. zmena pravidiel na firewalle), aby sa zraniteľnosť zmiernila, kým sa problém nevyrieši.

VERIFIKÁCIA

Posledným krokom je overenie, či bola náprava úspešná.

- **Opätovné skenovanie:** Použijú sa rovnaké nástroje ako v prvej fáze, aby sa potvrdilo, že zraniteľnosť bola skutočne opravená a systém je bezpečný.
- **Dokumentácia:** Celý proces, vrátane všetkých krokov, rozhodnutí a výsledkov, sa zaznamenáva pre auditné účely.

SPRÁVA IDENTITY A RIADENIE PRÍSTUPU

Riaďte kto a čo môže pristupovať k vašim dátam a informačným aktívam.

Správa identity a riadenie prístupu (Identity and Access Management - IAM) je bezpečnostný rámec, ktorý zabezpečuje, že správne osoby a zariadenia majú správny prístup k správnym zdrojom v správnom čase a z správneho dôvodu. Rieši tri zásadné otázky:
Kto sa pokúša o prístup? K akým zdrojom sa pokúša o prístup? Čo môže s týmito zdrojmi robiť?

SPRÁVA IDENTITY (IDENTITY MANAGEMENT)

Tento proces sa zameriava na vytvorenie, správu a údržbu digitálnej identity pre každého používateľa (či už je to zamestnanec, zákazník alebo dodávateľ) a každé zariadenie.

- **Autentifikácia:** Overenie, že používateľ je skutočne ten, za koho sa vydáva. Bežné metódy zahŕňajú heslá, biometriu (odtlačky prstov) alebo viacfaktorovú autentifikáciu (MFA).
- **Autorizácia:** Proces nasledujúci po autentifikácii. Jedná sa o udeľovanie povolenia k prístupu k zdrojom, údajom alebo funkciám.
- **Správa používateľských účtov:** Vytváranie, prideľovanie a odoberanie účtov, keď sa zmení rola používateľa alebo opustí organizáciu.
- **Synchronizácia:** Udržiavanie konzistentnosti identít v rôznych systémoch a aplikáciách.

RIADENIE PRÍSTUPU (ACCESS MANAGEMENT)

Tento proces sa zameriava na autorizáciu, čiže rozhodnutie, čo môže používateľ robiť po úspešnej autentifikácii.

- **Princíp najmenších oprávnení (Principle of Least Privilege):** Používateľom sa udeľuje iba minimálny prístup, ktorý potrebujú na splnenie svojich úloh. Ak napríklad zamestnanec v marketingu nepotrebuje prístup k finančným záznamom, jeho prístup k nim je zamietnutý.
- **Riadenie prístupu na základe rolí (Role-Based Access Control - RBAC):** Používatelia sú priradení k rolám (napr. „manažér“, „účtovník“, „IT podpora“), a každá rola má preddefinované oprávnenia. To zjednodušuje správu prístupu, pretože namiesto individuálneho nastavenia sa prístup prideľuje celým skupinám.
- **Podmienený prístup (Conditional Access):** Prístup sa udeľuje na základe ďalších podmienok, ako je poloha používateľa, typ zariadenia, ktoré používa, alebo čas prístupu. Napríklad prístup k citlivým dátam môže byť povolený len z firemného zariadenia a z internej siete.

BEZPEČNOSŤ DÁT

Kontrolujte funkčnosť zálohovacieho procesu a overujte proces obnovy.

Bezpečnosť dát je súbor postupov a opatrení, ktoré chránia informácie pred neoprávneným prístupom, zneužitím, poškodením alebo zničením.

TRI ZÁKLADNÉ PRINCÍPY BEZPEČNOSTI DÁT

Bezpečnosť dát sa opiera o tri základné princípy, často označované skratkou CIA:

- **Dôvernosť (Confidentiality):** Tento princíp zaisťuje, že k dátam majú prístup len oprávnené osoby. To sa dosahuje použitím šifrovania, silných hesiel a riadenia prístupu. Bez dôvernosti by citlivé údaje, ako sú osobné informácie alebo obchodné tajomstvá, mohli ľahko uniknúť.
- **Integrita (Integrity):** Ide o zabezpečenie, že dáta sú presné a kompletné a neboli neoprávnene zmenené. Používajú sa rôzne mechanizmy, ako sú digitálne podpisy a kontrolné súčty, ktoré odhalia akúkoľvek manipuláciu s dátami.
- **Dostupnosť (Availability):** Tento princíp zaručuje, že oprávnení používatelia majú prístup k dátam vždy, keď to potrebujú. Opatrenia ako zálohovanie dát, plány obnovy po havárii a ochrana pred DDoS útokmi sú kľúčové pre zabezpečenie dostupnosti.

AKO OCHRÁNIŤ DÁTA

Efektívna stratégia bezpečnosti dát zahŕňa kombináciu technických a organizačných opatrení.

- **Šifrovanie dát:** Dáta by mali byť šifrované v pokoji (napríklad na pevných diskoch) aj počas prenosu (cez sieť).
- **Silné riadenie prístupu:** Používajte viacfaktorovú autentifikáciu (MFA) a udeľujte prístup len na základe princípu najmenších oprávnení.
- **Kontroly nastavení:** Kontrolujte nastavenia jednotlivých systémov pre zabezpečenie správneho fungovania a bezpečnosti.
- **Pravidelné zálohovanie a plány obnovy:** Pravidelne zálohujte kritické dáta a pripravte si plán, ako ich rýchlo obnoviť v prípade útoku alebo havárie.
- **Ochrana pred malvérom a phishingom:** Inštalujte kvalitný antivírusový softvér a pravidelne vzdelávajte svojich zamestnancov, ako rozoznať hrozby ako phishing.

LOGOVANIE A MONITOROVANIE

Navrhnite svoje systémy tak, aby ste boli schopní detegovať a vyšetrovať incidenty.

Logovanie je proces zaznamenávania udalostí v systéme, sieti alebo aplikácii. Tieto záznamy (logy) zachytávajú všetky aktivity, od prihlásenia sa používateľov a zmien v konfigurácii až po možné pokusy o útoky.

HLAVNÉ DÔVODY LOGOVANIA

- **Detekcia hrozieb:** Logy slúžia ako prvá línia obrany, pretože umožňujú včasnú detekciu podozrivých aktivít.
- **Overenie funkčnosti:** Overenie či systém, softvér, zariadenie alebo služba funguje presne tak, ako bolo navrhnuté a očakávané.
- **Forenzná analýza po incidente:** Logy sú základným zdrojom informácií pre vyšetrovanie. Pomáhajú rekonštruovať sled udalostí, ktoré viedli k útoku. Vďaka logom je možné určiť, ako sa útočník dostal do systému, aké dáta ukradol a aký bol rozsah útoku.
- **Dodržiavanie predpisov:** Mnoho regulačných a priemyselných štandardov vyžaduje, aby organizácie viedli podrobné záznamy o prístupoch k citlivým dátam. Logovanie je nevyhnutné na preukázanie súladu s týmito predpismi, čo môže predísť pokutám alebo právnym problémom.
- **Optimalizácia výkonu a riešenie problémov:** Logy sú neoceniteľné aj pri bežnej správe IT systémov. Ak nejaká aplikácia zlyhá alebo systém nefunguje, logy môžu poskytnúť informácie o príčine problému, čím sa skracuje čas potrebný na jeho vyriešenie.

- **Audit a sledovanie zmien:** Logy poskytujú záznam o tom, kto, kedy a kde vykonal zmeny v systéme. To je dôležité nielen z bezpečnostného hľadiska, ale aj z pohľadu interného auditu. Pomáha to zabezpečiť, že zamestnanci dodržiavajú pravidlá a že neoprávnené zmeny sú okamžite odhalené.

Monitorovanie je proaktívny proces, ktorý neustále sleduje a analyzuje aktivity v sieti, systémoch a aplikáciách. Hlavným cieľom je včas odhaliť anomálie a podozrivé správanie, ktoré by mohlo signalizovať kybernetický útok alebo iný bezpečnostný incident. Na rozdiel od pasívneho logovania (ktoré iba zaznamenáva udalosti), monitorovanie je aktívny a dynamický proces. Využíva nástroje, ako sú systémy SIEM (Security Information and Event Management), ktoré zbierajú dáta z rôznych zdrojov (serverové logy, sieťová prevádzka, udalosti z firewallu) a analyzujú ich v reálnom čase, aby našli súvislosti a vzory, ktoré sú často prehliadané.

SPÔSOBY MONITOROVANIA

MONITOROVANIE SIETE

Tento typ monitorovania sa zameriava na sledovanie všetkej komunikácie, ktorá prebieha v sieti.

- **Detekcia hrozieb:** Systémy IDS (Intrusion Detection System) a IPS (Intrusion Prevention System) analyzujú sieťovú prevádzku a porovnávajú ju so známymi vzormi útokov. IDS vás upozorní na podozrivé aktivity, zatiaľ čo IPS ich dokáže automaticky zablokovať.
- **Analýza sieťového toku:** Monitorujú sa dáta o sieťovej prevádzke, ako sú zdroje, ciele, protokoly a porty. Aj keď neanalyzujú obsah dát, dokážu odhaliť anomálie, napríklad náhly a neobvyklý nárast dátového toku.

MONITOROVANIE SPRÁVANIA POUŽÍVATEĽOV

Systémy UEBA (User and Entity Behavior Analytics) sledujú, ako sa používatelia a zariadenia správajú v sieti. Vytvárajú si vzory bežného správania a akékoľvek odchýlky od tohto normálu vyhodnotia ako potenciálnu hrozbu.

- **Identifikácia anomálií:** Ak sa zamestnanec zvyčajne prihlasuje z Bratislavy, ale zrazu sa prihlási z inej krajiny a začne sťahovať citlivé dáta, UEBA to vyhodnotí ako podozrivú aktivitu, ktorá môže znamenať, že bol jeho účet kompromitovaný.
- **Detekcia interných hrozieb:** Táto metóda je účinná aj pri odhaľovaní rizík, ktoré prichádzajú zvnútra organizácie (napríklad nespokojný zamestnanec, ktorý sa snaží ukradnúť dáta).

LOGOVANIE A KORELAČNÁ ANALÝZA

SIEM (Security Information and Event Management) systémy zbierajú logy (záznamy o udalostiach) z rôznych zdrojov, ako sú servery, firewally, antivírusový softvér a aplikácie.

- **Centralizácia dát:** SIEM vytvára centralizované úložisko všetkých logov, čo zjednodušuje ich správu.
- **Korelácia udalostí:** Najväčšou silou SIEM je schopnosť korelovať udalosti z rôznych zdrojov. Napríklad, neúspešné prihlásenie na jednom serveri nemusí byť hrozbou. Ak však nasledujú pokusy o prístup k viacerým serverom, SIEM to vyhodnotí ako pokus o útok a upozorní vás na to.

MONITOROVANIE INTEGRITY SÚBOROV

FIM (File Integrity Monitoring) monitoruje zmeny kritických súborov a priečinkov v systéme.

- **Ochrana pred neoprávnenými zmenami:** FIM vás okamžite upozorní, ak sa zmení konfigurácia dôležitých súborov alebo ak sa pridá, zmení či vymaže nejaký súbor. Toto je kľúčové pri detekcii malvéru alebo neoprávnených zmien, ktoré by mohli oslabiť bezpečnosť.

RIEŠENIE INCIDENTOV

Vopred si naplánujte reakcie na kybernetické incidenty.

Riadenie incidentov (Incident Management) je systematický proces, ktorý pomáha efektívne reagovať na bezpečnostné incidenty a kybernetické útoky. Hlavným cieľom je minimalizovať škody, skrátiť čas obnovy a učiť sa z každého incidentu, aby sa v budúcnosti predišlo podobným udalostiam.

FÁZY RIADENIA INCIDENTOV

PRÍPRAVA
Táto fáza sa deje ešte pred incidentom a je kľúčová pre úspešnú reakciu.

- **Vytvorenie tímu:** Zostavenie tímu na riešenie incidentov (Computer Security Incident Response Team - CSIRT), ktorý je jasne definovaný, trénovaný a vie, aké sú jeho úlohy a zodpovednosti.
- **Vytvorenie plánu:** Vypracovanie detailného plánu, ktorý definuje kroky pre rôzne typy incidentov (napríklad únik dát, ransomvér alebo DDoS útok).
- **Školenia a testovanie:** Pravidelné tréningy a simulácie incidentov pomáhajú uistiť sa, že tím je pripravený reagovať pod tlakom.

DETEKCIA A ANALÝZA
Táto fáza sa zameriava na odhalenie incidentu a získanie informácií.

- **Detekcia:** Používajú sa nástroje ako SIEM systémy, antivírusový softvér a systémy na detekciu hrozieb, ktoré monitorujú sieť a systémy, aby odhalili neobvyklé správanie.
- **Analýza:** Po odhalení incidentu sa zhromažďujú a analyzujú dáta (napríklad logy), aby sa potvrdila hrozba a pochopil sa jej rozsah a typ.

REAKCIA A OBNOVA
Táto fáza je o akcii. Ide o okamžité kroky na minimalizáciu škôd a obnovu systémov.

- **Zadržanie (Containment):** Cieľom je zabrániť šíreniu útoku. To môže zahŕňať odpojenie infikovaných systémov od siete, zablokovanie prístupov alebo vypnutie určitých služieb.
- **Odstránenie (Eradication):** Po izolovaní incidentu sa odstraňuje jeho príčina, napríklad malvér, a opravujú sa zraniteľnosti, ktoré umožnili útok.
- **Obnova (Recovery):** Po odstránení hrozby sa systémy obnovujú zo záloh, a to v bezpečnom a čistom stave.

POST-INCIDENTNÁ AKTIVITA
Táto fáza je o učení sa. Je rovnako dôležitá ako samotná reakcia.

- **Hodnotenie:** Tím analyzuje, čo sa stalo, aké kroky boli podniknuté a čo sa dalo urobiť lepšie.
- **Správa:** Vytvorí sa záverečná správa o incidente, ktorá dokumentuje jeho príčiny, následky a prijaté opatrenia.
- **Zlepšenie:** Na základe získaných poznatkov sa posilní bezpečnostná stratégia, aby sa predišlo podobným incidentom v budúcnosti.

ZABEZPEČENIE DODÁVATEĽSKÉHO REŤAZCA

Spolupracujte so svojimi dodávateľmi a obchodnými partnermi.

Zabezpečenie dodávateľského reťazca predovšetkým znamená ochranu dodávaných produktov a služieb pred možnými kybernetickými hrozbami.

HLAVNÉ KROKY

Účinné zabezpečenie dodávateľského reťazca si vyžaduje komplexný a viacvrstvový prístup.

DÔKLADNÁ KONTROLA DODÁVATEĽOV
Pred začiatkom spolupráce s novým dodávateľom, je nevyhnutné preveriť jeho bezpečnostné postupy.

- **Prieskum:** Preverte, aké bezpečnostné certifikácie má dodávateľ (napríklad ISO 27001), aké má interné bezpečnostné politiky a aké má skúsenosti s riadením kybernetických incidentov.
- **Audit:** Vykonajte vlastný bezpečnostný audit dodávateľa, aby ste sa uistili, že spĺňajú vaše bezpečnostné štandardy.
- **Zmluvné podmienky:** V zmluve musíte jasne definovať bezpečnostné požiadavky a zodpovednosti.

MONITOROVANIE A TESTOVANIE
Kontrola bezpečnosti sa nekončí uzavretím zmluvy.

- **Pravidelné audity:** Audity vykonávajte pravidelne. Takto sa uistite, že dodávateľ stále dodržiava dohodnuté bezpečnostné opatrenia.

- **Testovanie:** Vykonávajte napr. penetračné testy u dodávateľa. Takto viete identifikovať a prípadne dosiahnuť nápravu potenciálnych zraniteľností.
- **Monitorovanie:** Monitorujte zmeny v systémoch dodávateľa na včasné odhalenie bezpečnostných hrozieb.

RIADENIE PRÍSTUPU A SEGMENTÁCIA SIETE

Vždy obmedzte prístup tretích strán k vašim systémom len na to, čo je absolútne nevyhnutné.

- **Princíp najnižších oprávnení:** Dodávateľom poskytnite prístup iba k tým dátam a systémom, ktoré sú nevyhnutné na plnenie ich úloh.
- **Segmentácia siete:** Izolujte dodávateľské systémy v samostatných sieťových segmentoch, aby sa potenciálny útok nemohol rozšíriť na dôležitej časti vašej siete.

VZDELÁVANIE A KOMUNIKÁCIA

Nezabudnite, že požadované zabezpečenie dodávateľského reťazca nie je zodpovednosťou len IT oddelenia, ale všetkých.

- **Interné školenie:** Školťe svojich zamestnancov, ako bezpečne komunikovať s dodávateľmi a ako rozoznať potenciálne riziká, napríklad phishingové e-maily, ktoré sa tvária, že pochádzajú od dodávateľa.
- **Plán komunikácie:** Zadefinujte jasný plán, ako sa bude komunikovať s dodávateľmi nie len pri bežnom plnení úloh, ale napr. aj v prípade kybernetického incidentu, aby ste mohli rýchlo a koordinovane reagovať.

UŽITOČNÉ LINKY

Indikatívna pomôcka na určenie subjektu ako poskytovateľa základnej služby (PZS) – dotazník
https://nis2.nbu.gov.sk/indikativna-pomocka-na-urcenie-subjektu-ako-poskytovatela-zakladnej-sluzby/?csrt=4819364572552175553

Metodické usmernenia k zákonu č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov účinného od 01.01.2025
https://www.nbu.gov.sk/metodiky/
Vyhlášky a EÚ materiály na stiahnutie: https://www.nbu.gov.sk/1620-sk/kyberneticka-bezpecnost/

Link na materiál Metodiku analýzy rizík
https://www.nbu.gov.sk/metodika-analyzy-rizik/

Link na Vyhlášku NBÚ č. 226/2025 Z. z. o hláseniach
https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2025/226/20250901

Link na Vyhlášku NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach
https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2025/227/20250901

Praktické bezplatné webináre zamerané na vysvetlenie povinností, vyplývajúcich z novely Zákona č.69/2018 Z.z. o kybernetickej bezpečnosti a informáciami k implementácii organizačných opatrení
https://cybercompetence.sk/webinare-nis2/

CIS Inventory Tracking Spreadsheets
https://www.cisecurity.org/insights/white-papers/cis-controls-inventory-tracking-spreadsheets

Kompletný metodický postup na správu IT aktív (príklad)
https://csrc.nist.gov/pubs/sp/1800/5/final

Viete, čo všetko máte na vašej firemnej sieti?
https://nmap.org/

Databázy zraniteľností pri hodnotení rizík (príklady)
CVE, NVD, OpenVAS Skener

Top hrozby pre kybernetickú bezpečnosť
ENISA Threat Landscape 2024, Foresight Cybersecurity Threats For 2030

Dopad útokov
IBM report: Cost of a data breach 2025

Nástroje na hodnotenie rizík
NIST vzorová tabuľka na správu rizík a Príručka alebo Eramba Community

10 essential insights from the Microsoft Digital Defense Report 2024
https://www.microsoft.com/en-us/security/security-insider/threat-landscape/10-essential-insights-from-the-microsoft-digital-defense-report-2024

Metodika vzdelávania (príklad)
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50r1.pdf

Metodika vzdelávania (príklad)
https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content

Tipy pre pokročilých: Ako zabezpečiť a správne nastaviť Wi-Fi sieť
https://zive.aktuality.sk/clanok/150175/tipy-pre-pokrocilych-ako-zabezpecit-a-spravne-nastavit-wi-fi-siet/

Plán reakcie na kybernetický incident (príklad)
https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

Plán reakcia na kybernetický incident (príklad)
https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Cyber%20Incident%20Response%20Plan%20Guidance_A4.pdf

Návod na zastavenie šírenia ramsonware (príklad)
https://www.cisa.gov/resources-tools/resources/stopransomware-guide

Záloha a obnova (príklad technológie)
https://www.bareos.com/

Záloha a obnova (príklad technológie)
https://www.bacula.org/

10 KROKOV KU KYBERNETICKEJ BEZPEČNOSTI

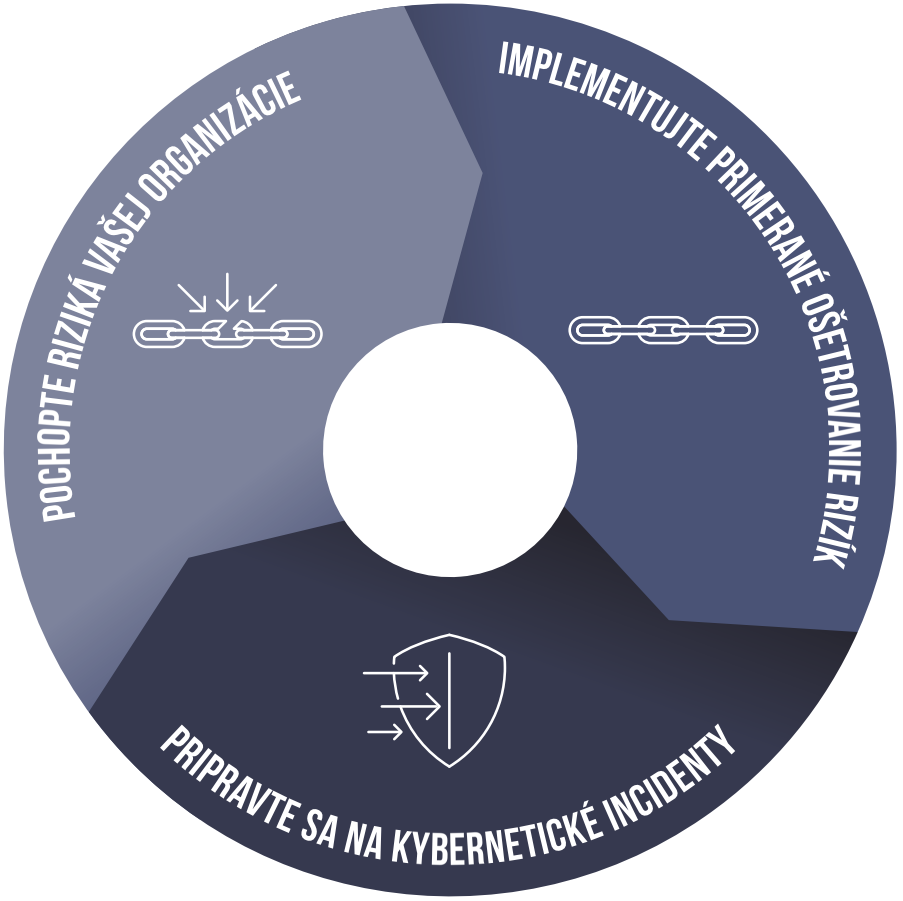
1 **Riadenie rizík**
Na zabezpečenie vašich údajov a systémov si osvojte prístup založený na riziku

2 **Trénujte a vzdelávajte**
Spoločne budujte bezpečnosť uplatniteľnú pre všetkých zamestnancov vo vašej organizácii

3 **Správa aktív**
Identifikujte dáta a ostatné informačné aktíva a namapujte procesy, ktoré sú nimi podporované

4 **Architektúra a konfigurácia**
Navrhujte, implementujte, udržiavajte a spravujte systémy bezpečným spôsobom

5 **Správa zraniteľností**
Chráňte systémy počas celého ich životného cyklu



6 **Správa identity a riadenie prístupu**
Riaďte kto a čo môže pristupovať k vašim dátam a informačným aktívam

7 **Bezpečnosť dát**
Kontrolujte funkčnosť zálohovacieho procesu a overujte proces obnovy

8 **Logovanie a monitorovanie**
Navrhnite svoje systémy tak, aby ste boli schopní detegovať a vyšetrovať incidenty

9 **Riešenie incidentov**
Vopred si naplánujte reakcie na kybernetické incidenty

10 **Zabezpečenie dodávateľského reťazca**
Spolupracujte so svojimi dodávateľmi a obchodnými partnermi

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

www.cybercompetence.sk