Információbiztonsági oktatás

Üzemeltetők részére

2025

Tartalom

1. IT biztonsági alapismeretek

1.1. Az információbiztonság alapjai

Mi a biztonság?

A köznyelvben gyakran keveredő fogalmak, mint adatvédelem és adatbiztonság nem szinonimák. Az adatvédelem a személyes adatok védelme, míg az adatbiztonság az információs rendszereken tárolt, továbbított vagy feldolgozott adatok biztonságát jelenti.

Az informatikai biztonság az informatikai rendszerek azon kedvező állapota, amelyben a kezelt adatok bizalmassága (confidentiality), sértetlensége (integrity) és rendelkezésre állása (availability) a rendszer elemeinek szempontjából zárt, és folyamatosan biztosított (ez az úgynevezett „CIA elv”):

- *bizalmasság:* az információhoz csak az arra jogosultak férhetnek hozzá;
- *sértetlenség:* az információ formája és tartalma az elvárttal megegyező, és egyértelműen azonosítható az információval kapcsolatos műveletek végzője;
- *rendelkezésre állás:* az az állapot, mikor egy informatikai rendszer szolgáltatásai az arra jogosultak számára egy meghatározott időben elérhetőek, és a rendszer elvárt működése sem átmentileg, sem tartósan nem akadályoztatott;

Az információbiztonság jóval tágabb fogalom, mint az IT biztonság, hiszen beletartozik az információ minden megjelenési formája (nem csak elektronikus), valamint a szolgáltatások biztonsága is.

1.2. Jogszabályi alapok

DORA rendelet

A Digital Operational Resilience Act (DORA) egy EU-s rendelet, amely 2023. január 16-án lépett hatályba, és 2025. január 17-től alkalmazandó. Célja a pénzügyi szektor informatikai biztonságának megerősítése, hogy a pénzügyi intézmények ellenállóak maradjanak súlyos működési zavarok esetén.

Az alábbi pillérek biztosítják a pénzügyi szektor digitális operatív ellenálló képességének növelését:

1. **ICT kockázatkezelés:** A pénzügyi intézményeknek átfogó keretrendszert kell kialakítaniuk az informatikai kockázatok azonosítására, értékelésére, kezelésére és mérséklésére.
2. **Incidensjelentés**: Mechanizmusokat kell létrehozni a jelentős informatikai incidensek időben történő jelentésére a szabályozó hatóságok felé, beleértve az incidensek részletes dokumentálását és elemzését.
3. **Digitális operatív ellenálló képesség tesztelése**: Rendszeres tesztelést kell végezni a digitális operatív ellenálló képesség biztosítása érdekében, beleértve az alap- és haladó teszteket is.
4. **Harmadik fél kockázatkezelése**: A pénzügyi intézményeknek kezelniük kell a harmadik fél szolgáltatókkal kapcsolatos kockázatokat, beleértve a kulcsfontosságú szerződéses rendelkezéseket is.
5. **Információmegosztás**: A kiberveszélyekkel kapcsolatos információk és hírszerzés cseréje a pénzügyi szektor szereplői között.

MNB 8/2020 ajánlás az informatikai rendszer védelméről

Az ajánlás célja, hogy a pénzügyi közvetítőrendszer tagjai számára gyakorlati útmutatást adjon informatikai rendszerük védelmének kockázatokkal arányos kialakításban, valamint azok védelmére vonatkozó jogszabályi rendelkezések alkalmazásának egységes értelmezésében. Az ajánlás a közösségi és publikus felhőszolgáltatás igénybevételéről szóló 4/2019. (IV. 1.) MNB ajánlásban foglaltakkal, valamint az elektronikus úton megkötött írásbeli szerződésekről, megtett írásbeli jognyilatkozatokról szóló vezetői körlevéllel, a belső védelmi vonalak kialakításáról és működtetéséről, a pénzügyi szervezetek irányítási és kontroll funkcióiról szóló 12/2022. (VIII.11.) MNB ajánlással, valamint a külső szolgáltatók igénybevételéről szóló MNB ajánlással együtt alkalmazandó.

1.3. Kockázatkezelés

A működésből fakadó információbiztonsági kockázatok és veszélyek feltérképezhetőek. Ezeket ismerve, és figyelembe véve a felsővezetés által felvállalt kockázati szinteket a biztonsági szakemberek állítják fel a szervezet számára elfogadható védelmi mechanizmusok kombinációját.

Az információs rendszer szempontjából fenyegetésnek minősül minden olyan körülmény vagy esemény, amely az adatok vagy az információs rendszerek biztonságát veszélyeztetik. Ide tartoznak a külső behatások (pl. természeti katasztrófa), vagy a személyektől eredő támadások (számítógépes betörés).

Fenyegetés modellezés

A kockázatelemzés során fontos tisztában lenni azzal, hogy milyen fenyegetések vonatkoznak az információs rendszerek biztonságára. A fenyegetési modell strukturális ábrázolása mindazon információknak, melyek a környezet biztonságára hatással lehetnek.

Egy fenyegetési modell tipikusan az alábbi elemekből áll:

- a modellezni kívánt rendszer leírása,
- ellenőrizhető, illetve a jövőben változtatható feltételezések a rendszerről,
- a rendszert érintő potenciális fenyegetések,
- akcióterv a lehetséges fenyegetések csökkentésére,
- a modell validálása.

Ezen elemek begyűjtése, rendszerezése és elemzése a fenyegetési modellezés. Többféle modellezési eljárás létezik, az egyik a Microsoft által adoptált STRIDE, mely a rendszert érintő potenciális fenyegetéseket hat csoportra bontja.

Fenyegetés	Fenyegetés természete	Definíció
Identitás hamisítás	Azonosítás	Identitás hamisítása
Adatok módosítása	Integritás	Valamilyen információ módosítása
Letagadhatóság	Ellenőrizhetőség	Cselekmény letagadása
Információfelfedés	Bizalmasság	Jogosulatlan hozzáférés adatokhoz
Szolgáltatás megtagadás	Rendelkezésre állás	Szolgáltatás megtagadás, vagy visszavonása a felhasználótól

Jogosultsági szint emelése	Jogosultság	Képességek szerzése megfelelő felhatalmazás nélkül

1.4. Információbiztonsági incidensek kezelése

A biztonsági esemény, olyan nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő. Az ilyen esemény hatására a rendszerben kezelt információk bizalmassága, sértetlensége, hitelessége, funkcionalitása és rendelkezése állása sérülhet, vagy a sérülésük kockázata megnő.

A szervezetet érő károk csökkentése érdekében meg kell tervezni, meg kell valósítani és menedzselni kell az információbiztonsági események azonosításának, kivizsgálásának, rájuk való reagálásnak és a helyreállításnak a képességét.

- Az információbiztonsági incidensekre való reagálás akciótervét ki kell alakítani, és naprakészen kell tartani azért, hogy minden eseményre eredményesen, és időben legyen képes reagálni a szervezet.
- Ki kell alakítani, és fenn kell tartani az információbiztonsági események kivizsgálásának és jegyzőkönyvezésének folyamatát.
- Ki kell alakítani és naprakészen kell tartani az eseményekről való tájékoztatás rendszerét és azok eszkalálásának a folyamatát azért, hogy a biztonsági eseményekre adott válaszok meghatározásába és végrehajtásába az érintetteket a szervezet be tudja vonni.
- Meg kell szervezni, ki kell képezni a rendkívüli információbiztonsági eseményekre időben és eredményesen reagálni képes csapatot.
- Időszakonként tesztelni kell, és felül kell vizsgálni az eseménykezelési tervet azért, hogy az információbiztonsági incidensekre a szervezet eredményesen reagáljon.
- Ki kell dolgozni naprakészen kell tartani a kommunikációs tervet és folyamatot azért, hogy a belső és külső érintettekkel való kommunikációt kézben lehessen tartani.
- A rendkívüli események elhárítását követően felülvizsgálatot kell tartani. Meg kell határozni az információbiztonsági események okát. Felül kell vizsgálni a javító intézkedéseket, illetve újra fel kell mérni a kockázatokat. Újra kell értékelni az elhárítás eredményességét is, és amennyiben szükséges, megfelelő javító intézkedéseket kell hozni.
- Ki kell alakítani, és naprakészen kell tartani az eseménykezelési tervek, a katasztrófa elhárítási tervek, és az üzletfolytonossági tervek integrációját.

Biztonsági napló menedzsment

Számos elnevezése van a kiberbiztonsági incidensek kezelését végző csapatnak, például CIRT (Computer Incident Response Team), SOC (Security Operations Center) vagy CDC (Cyber Defense Center).

A kiberbiztonsági incidenskezelés a releváns humánerőforrások, folyamatok és technológiai szintek megfelelő összehangolásával valósítható meg. A technológia szintnek integráltnak kell lennie a kiberbiztonsági architektúra egyéb elemeivel, az alapvető incidenskezelési folyamatoknak definiáltnak, valamint a kapcsolódó IT, illetve nem IT folyamatokhoz igazítottnak kell lenniük, emellett a kiberbiztonsági incidensek kezelését végző csapatnak megfelelően képzettnek kell lennie a folyamatok elvégzéséhez.

Ahhoz, hogy a kártékony tevékenységek felismerhetőek legyenek, folyamatosan felügyelni (continuous monitoring) kell a szervezet rendszereit. A cél valós idejű „rálátás” megteremtése a védett

adatvagyonra. Ennek szükséges előfeltétele, hogy a kiberbiztonsági relevanciával rendelkező események megfelelően naplózásra kerüljenek minden egyes végponton. A rálátás a biztonsági naplók, végponti naplók és hálózati forgalom feldolgozásával valósítható meg. Ha a szükséges adat begyűjtésre került, akkor azt aggregálni, értelmezni, indexelni és elemezni kell kártékony minták, viselkedés azonosítása érdekében. Általában ezt a feladatot a SIEM (Security Incident and Event Management) termékek biztosítják a technológiai szinten.

Ha egy potenciális kiberbiztonsági incidens észlelésre kerül (detection), akkor első lépésként meg kell róla bizonyosodni, hogy valós incidensről van-e szó, vagy téves riasztás történt. Ha igazolásra kerül, hogy az esemény valós kiberbiztonsági incidens, akkor a következő lépés a kategorizálás, illetve a súlyosság felmérése, amelyek a válaszlépéseket és azok elvégzésének határidejét fogják meghatározni (ezeket a feladatok összefoglalóan triage lépésként nevezik).

A következő lépések célja a válaszlépések meghatározása és elvégzése annak érdekében, hogy az incidens üzletmenetre gyakorolt hatását minimalizálni lehessen.

A következő két lépés, elemzés (analysis) és elhatárolás (containment) általában egymással párhuzamosan, több iterációban kerülnek elvégzésére. Az elemzés célja az incidens részleteinek megértése, amely alapján egy meglévő, vagy egyedileg definiált választerv elvégezhető. Az elhatárolás célja az incidens elszigetelése, hogy időt lehessen nyerni az elemzés elvégzésére. A forensics és kártékony kód elemzések általában szignifikáns időt vesznek igénybe, ezért a megfelelő elhatárolási stratégia alkalmazása elengedhetetlen a további üzleti károk megelőzése érdekében.

Ha a megfelelő válaszlépések már definiálásra kerültek az elemzés eredményei alapján, az incidens felszámolását (eradication) és a rendszerek helyreállítását (remediation) kell elvégezni, mielőtt az incidens lezárásra kerülhet.

A fent bemutatott lépések sorozatára (continuous monitoring, detection, triage, containment, analysis, eradication, és remedation) általában „incidens válaszlánc” -ként (incident response chain) hivatkoznak.

SOAR

Napjainkban az incidensek kezelését végző csapatok hasonló kihívásokkal szembesülnek:

- a kiberbiztonsági támadások száma és azok kifinomultsága folyamatosan növekszik,
- védendő környezet komplexitása nő (a tradicionális IT rendszerek mellett új környezetek is megjelennek, mint például az IoT, vagy a Felhő).

Ennek eredményeként a SOC csapatoknak nagy számú riasztást kell feldolgozniuk, amelyek során az incidens válasz lánc lépéseit kell minden esetben elvégezniük. A feladataik során számos, egymástól eltérő rendszert kell használniuk. Mivel az egyes részfeladatokat különböző eszközökkel végzik, nehéz hatékonyan nyomon követni egy adott incidenshez tartozó valamennyi információt egy központi helyen.

Ezek következménye az úgynevezett „riasztási kiégés” (alert fatigue) fogalma, amely miatt adott incidensek kezeletlenül maradhatnak és megnő az incidensek kezelésének ideje.

Elméletileg ezek a kihívások könnyen kezelhetőek lehetnének az operáció megfelelő felskálázásával. Azonban a kívánt szintre történő felskálázás nem valósítható meg a gyakorlatban még végtelen büdzsé rendelkezésre állásával sem, elég csak arra gondolni, mekkora hiány van megfelelően képzett kiberbiztonsági elemzőkből.

A technológia szintjén a SOAR (Security Orchestration, Automation and Response) termék az, amelynek a célja a fent említett kihívások megoldása. A SOAR termékek fő funkciói a harmonizáció (orchestration) és az automatizálás (automation). A harmonizáció integrációt biztosít a SOAR, és az egyéb termékek között, míg az automatizálás lehetővé teszi incidenskezelési feladatok lépéseinek elvégzését humán erőforrás bevonása nélkül (például egy adathalász incidens során az érintett felhasználók azonosítását, annak ellenőrzését, hogy valaki megadott-e hitelesítési információkat, kompromittált felhasználói fiókok letiltását, stb.)

A SOAR egy egységes felületet biztosít az elemzők részére, amelyen keresztül az incidenskezelés valamennyi lépését el tudják végezni. Az észlelés és válasz lépései, valamint a sérülékenységmenedzsment (vulnerability management) és fenyegetettségi információk (threat intelligence) kezelése a SOAR platformon belül lehetséges, nem kell folyamatosan váltogatni az egyes rendszerek között a feladatok elvégzése során. A gyakorlatban ez azt jelenti, hogy a SOAR rendszer „elhozza" a SIEM rendszerben keletkező riasztásokat, összegyűjti a triázshoz szükséges információkat és automatizált lépésekkel támogatja az elhatárolást, vagy akár a felszámolás és helyreállítás lépéseit. Mivel az incidens válasz lánc valamennyi lépése ezen belül kerül nyomon követésre, a SOAR válik az incidenskezelő csapatok fő eszközévé. A műszak elején az elemzők ebbe a rendszerbe lépnek be és legtöbb idejüket ebben töltik. Ideális esetben, ha a megfelelő integrációk rendelkezésre állnak, az elemzők megtalálnak az incidens elemzéséhez szükséges valamennyi információt a SOAR-ban, valamint a válaszlépések végrehajtását is tudják onnan indítani (például egyéb logok begyűjtését, izolációt, társ IT osztályokkal való együttműködést hibajegyek nyitásán keresztül, stb.)

1.5. NIST kibervédelmi keretrendszer

A NIST keretrendszer minden informatikai biztonsági képességet, folyamatot és napi tevékenységet az alábbi 5 fő funkcióba sorol:

- *Azonosítás*: milyen folyamatok és eszközök igényelnek védelmet.
- *Védelem*: megfelelő biztonsági intézkedések alkalmazása a szervezet eszközeinek megóvása érdekében.
- *Felderítés*: megfelelő mechanizmusok alkalmazása az informatikai biztonsági események azonosítására.
- *Reagálás*: megfelelő technikák alkalmazása az informatikai biztonsági események kezelésére.
- *Helyreállítás*: az informatikai biztonsági esemény során keletkezett károk kijavítására megfelelő folyamatok alkalmazása.

Mindegyik fő funkció további alkategóriát tartalmaz a megfelelő ajánlásokkal.

A NIST SP-800-53 ajánlás tartalmazza azokat az ellenőrző lépéseket, melyekkel a biztonsági keretrendszer sikeresen bevezethető.

Kategória	Példák kontrollokra
Hozzáférés-szabályozás	Fiókbiztonság és felügyelet; legkisebb kiváltság; a feladatok szétválasztása
Tudatosság és képzés	Felhasználói képzés a biztonsági fenyegetésekről; műszaki képzés kiemelt felhasználók számára
Ellenőrzés és elszámoltathatóság	Az ellenőrzési jegyzőkönyvek tartalma; elemzés és jelentéskészítés; rekordmegőrzés

Értékelés, engedélyezés és felügyelet	Csatlakozás nyilvános hálózatokhoz és külső rendszerekhez; penetrációs vizsgálat
Konfiguráció-menedzsment	Engedélyezett szoftver házirendek, konfiguráció módosítások ellenőrzése
Vészhelyzeti intézkedési tervek	Alternatív feldolgozási és tárolási helyek; üzletmenet-folytonossági stratégiák; tesztelés
Azonosítás és hitelesítés	A felhasználók, eszközök és szolgáltatások hitelesítési szabályzatai; hitelesítő adatok kezelése
Egyéni részvétel	Hozzájárulás és adatvédelmi felhatalmazás
Incidensre adott válasz	Esemény-elhárítási képzés, megfigyelés és jelentés
Karbantartás	Rendszer-, személyzet- és eszközkarbantartás

2. Általános támadási technikák

Az információbiztonsági támadások anatómiájának, illetve egy kiberbiztonsági támadás során alkalmazott támadási technikák megismeréséhez jó kiindulási pont a MITRE ATT&CK keretrendszer.

A keretrendszer a támadók által használt taktikákat, technikákat és eljárásokat (TTP-tactics, techniques and procedures) dokumentálja valós rendszerek ellen irányult támadások alapján, ezáltal lehetőséget ad támadói viselkedések megismerésére.

A MITRE ATT&CK egy viselkedési modellt állít, amely a következő elemekből épül fel:

- Taktikák, amelyek a támadó rövid távú, taktikai céljait jelentik a támadás során.
- Technikák, melyek az eszközöket, eljárásokat jellemzik, amelyeket a támadó a célja elérésére használ.
- Altechnikák, melyek még specifikusabban, részleteiben jellemzik a cél elérésére használt technikát.
- Metaadatok: amelyek a támadó által használt technikák, eljárások dokumentációja, illetve egyéb kapcsolódó információ.

2.1. Támadási taktikák és technikák

A taktikai szint a hatását jellemzi egy alkalmazott ATT&CK technikának vagy altechnikának. Ez a támadó taktikai célja, amiért az adott cselekvést végzi. Például, egy támadó felhasználói hozzáférést akar szerezni egy adott rendszerhez.

Taktika neve	Leírás
Felderítés (Reconnaissance)	A támadó információkat gyűjt, amiket a jövőbeni műveletei során tud felhasználni
Erőforrások megteremtése (Resource Development)	A támadó megteremti az erőforrásokat a műveletei támogatásához

Kezdő belépés (Initial Access)	A támadó próbál bejutni a hálózatba
Kivitelezés (Execution)	A támadó kártékony kódot próbál futtatni
Folyamatos jelenlét (Persistence)	A támadó próbál a hálózaton belül maradni
Jogosultság kiterjesztés (Privilege Escalation)	A támadó magasabb szintű hozzáférést próbál szerezni
Védelem kikerülése (Defense Evasion)	A támadó próbálja elkerülni, hogy felfedezzék jelenlétét
Felhasználói hozzáférés (Credential Access)	A támadó próbál felhasználói adatokat és jelszavakat szerezni
Felfedezés (Discovery)	A támadó próbálja minél jobban megismerni a műveleti környezetet
Oldalirányú haladás (Lateral Movement)	A támadó próbál minél tovább jutni a hálózatban, rendszerekben
Begyűjtés (Collection)	A támadó próbálja begyűjteni azokat az adatokat, amik a célját szolgálják
Vezérlés (Command and Control)	A támadó próbál kommunikálni a kompromittált rendszerrel, és irányítása alá vonni azt
Kiszivárogtatás (Exfiltration)	A támadó megpróbálja ellopni az adatokat
Behatás (Impact)	A támadó megpróbálja manipulálni, megzavarni, vagy megsemmisíteni a rendszereket vagy adatokat.

A technikák azt mutatják be, hogy egy támadó hogyan éri el a taktikai céljait egy bizonyos cselekvés által. Például, a támadó kigyűjthet belépési adatokat, hogy hozzáférést szerezzen bizonyos rendszerekhez.

2.2. Hálózati támadás során használt technikák példája

A következő ábra egy hálózati hozzáférésen keresztül végrehajtott támadás lépéseihez tartozó technikákat foglalja össze.

Hozzáférés megszerzése (Initial Access)

Alkalmazott technika: Exploit Public-Facing Application (Internetre publikált alkalmazások exploitálása)

A támadó kihasználja egy az Internet felé publikált eszköz gyenge pontjait, amely lehet működési, vagy biztonsági hiba, vagy akár architektúra dizájnból fakadó sérülékenység.

Kártékony kód futtatása (Execution)

Alkalmazott technika: Command and Scripting Interpreter (parancs és szkript értelmező kihasználása)

A támadó parancsot, szkriptet, vagy bináris állományt futtat az Internetről hozzáférhető parancs- és szkript értelmezőn keresztül. A kártékony kód eljuthat az előző lépés során használt payloadba ágyazva, vagy számos egyéb módon a célrendszer sérülékeny parancsértelmezőjéhez.

Hozzáférés fenntartásának kiépítése (Persistence)

Alkalmazott technika: Modify Authentication Process (azonosítási folyamat hibájának kihasználása)

Az azonosítási folyamatokat kezelő szolgáltatások, mint például a Local Security Authentication Server (LSASS) és Security Accounts Manager (SAM) Windows környezetben felelősek a belépési adatok begyűjtéséért, tárolásáért és jóváhagyásáért. A támadó kihasználja ezek sérülékenységeit, így hozzáférve hitelesítési információkhoz, ezáltal megoldva hosszútávú bejutásukat a célrendszerekbe.

Alkalmazott technika: Pre-OS Boot (boot folyamatok során kivitelezett visszaélések)

A támadó módosítja a boot folyamatot, a megszerzett hozzáféréssel annak érdekében, hogy a továbbiakban is távolról hozzáférést tartson fenn az eszközön. Ennek felderítése különösen nehéz, mivel a szoftveres védelmi technológiák nem képesek ezek észlelésére.

Alkalmazott technika Traffic Signaling (jelzés forgalmon keresztül)

A támadó elhelyez olyan szolgáltatásokat, amelyeken keresztül távolról parancsokat küldhet a kompromittált eszközre. Ez történhet például olyan formában, hogy a támadó sorozatosan, meghatározott karakterisztikákkal rendelkező hálózati csomagokat küld az eszköznek.

Védelem megkerülése (Defense Evasion)

Alkalmazott technika: Impair Defenses (védelem megbénítása)

A támadó kikapcsolja a preventív (mint például a tűzfal, vagy antivírus szoftver) és detektív (mint például a naplózás) védelmi kontrollokat az eszközön annak érdekében, hogy minél kevésbe legyen észlelhető a jelenléte, illetve egy ezután következő támadási technika.

Alkalmazott technika: Modify System Image (rendszerképek megváltoztatása)

A támadó megváltoztatja az eszköz operációs rendszereinek beállításait, hogy gyengítse a védelmet és akár ezeken keresztül új képességekre tegyen szert.

Alkalmazott technika: Network Boundary Bridging (hálózati határokon való átjutás)

A támadó átjárhatóságot épít ki a szeparált hálózatok között például kompromittált hálózati, vagy határvédelmi eszköz beállításainak módosításával, vagy több hálózati interfésszel rendelkező végponti eszköz beállításainak megváltoztatásával. Ezáltal lehetőséget teremt további, belső hálózati szegmensek eléréséhez.

Alkalmazott technika: Weaken Encryption (gyengített titkosítás)

A támadó módosítja, vagy kikapcsolja a hálózati kapcsolatok titkosításának követelményét a kompromittált eszközön. Emellett hozzáférést szerez a titkosításoknál használt kulcsokhoz, amelyek segítségével az érintett kulccsal titkosítva tárolt, vagy hálózaton továbbított adatokhoz is hozzáférhet.

Hitelesítési adatok megszerzése (Credential Access)

Alkalmazott technika: Input Capture (Beviteli adatok rögzítése)

A támadó rögzíti a felhasználók hitelesítési adatait tartalmazó bevitt adatfolyamokat, amiből később kinyerheti és visszafejtheti a hitelesítési adatokat.

Felderítés (Discovery)

Alkalmazott technika: Network Sniffing (hálózati forgalom lehallgatása)

A támadó rögzíti a hálózati forgalmat, amelyből további sérülékeny, célpontként használható eszközöket azonosít, vagy adatokat szerez meg.

Információgyűjtés (Collection)

Alkalmazott technika: Data from Configuration Repository (konfigurációs adattárakból nyert információ)

A támadó adatokat gyűjt a különböző konfigurációs adattárakból (configuration repository), amely segíti távoli, vagy akár adminisztrátori hozzáférés megszerzését.

Vezérlés (Command and Control)

Alkalmazott technika: Non-Application Layer Protocol (alkalmazás szint alatti protokoll használata)

A támadó hálózati kapcsolat szintű kommunikációs protokollokat használ a kompromittált eszköz távoli vezérlésére.

Alkalmazott technika: Proxy

A támadók proxy használatával irányítja a hálózati forgalmat az egyes rendszerek között, vagy köztes rétegként használja a megtámadott eszköz és a támadó által fenntartott parancsokat küldő szerver közötti kommunikációhoz.

Adatkinyerés (Exfiltration)

Alkalmazott technika: Automated Exfiltration (Automatizált adatkinyerés)

A támadó a megszerzett adatokat, érzékeny információkat a korábban kialakított kommunikációs csatornán keresztül kiszivárogtatja a kompromittált rendszerből.

3. Hacker támadások megelőzése

A hacker támadások megelőzésére számos folyamat és technológia szintű kontrollt alkalmaznak a szervezetek. Ebben a fejezetben ezek közül a legfontosabbak kerülnek bemutatásra.

Hozzáférés management

A hozzáférés-vezérlés olyan biztonsági mechanizmusok gyűjteménye, mely meghatározza, hogy a felhasználók mit tehetnek a rendszerben, azaz milyen erőforrásokhoz férhetnek hozzá és milyen műveleteket hajthatnak végre. Azok a védelmi intézkedések tartoznak ide, melyek szabályozzák, hogy egy felhasználó:

- milyen felhatalmazással férhet a rendszerhez,
- milyen alkalmazásokat futtathat,
- milyen információkat olvashat, hozhat létre, adhat hozzá és törölhet.

Általánosságban magába foglalja az azonosítás (identification), a hitelesítés (authentication), a hozzáférés-engedélyezés (access approval) és az audit (hozzáférés-ellenőrzés) lépéseit, de bizonyos esetekben a hozzáférés-vezérlés részének tekintik az elszámoltathatóságot (accountability) is.

A hozzáférés-vezérlés során alkalmazott fő elvek:

- Feladatok szétválasztása (Separation of Duties)

Célja, hogy egy folyamat lépéseit különböző személyek végezzék el. Ehhez a folyamatot meg kell tervezni, meg kell akadályozni, hogy egy személy a teljes folyamatot ellenőrizze és manipulálja. (például egy könyvelési osztályon nem fogadhatja be ugyanaz a személy a számlákat, és nem kezdeményezheti ezek kifizetését).

- Legkevesebb jogosultság (Least Privilege)

Az elv betartásával a rendszer a felhasználók és az alkalmazások erőforrásokhoz való hozzáférését csak a legszükségesebbekre korlátozza. Ehhez meg kell határozni a felhasználók munkájához szükséges jogosultságok minimális halmazát.

A hozzáférés vezérlés azért is fontos, mert ha egy támadás során egy felhasználói fiókhoz hozzáfértek a támadók, akkor minimalizálható az általuk okozható kár (amennyiben nem privilegizált fiókról van szó). Az incidensek megelőzése érdekében javasolt a megfelelő erősségű jelszavak beállítása a felhasználói fiókokhoz, illetve ezek rendszeres cseréje.

Hálózati szeparáció

A hálózatot úgy kell megtervezni, hogy az egyes eszközök csak azokkal az eszközökkel tudjanak kommunikálni, amelyek feltétlenül szükségesek ahhoz, hogy a funkciójukat ellássák. A szeparáció megvalósításának egyik technológiai módja a tűzfalak alkalmazása.

3.1. Sérülékenység-kezelés alapjai

A sérülékenységkezelés célja a szervezetet érintő sérülékenységek azonosítása, és az azok által hordozott kockázatok csökkentése a sérülékenység megszűntetésével, vagy kompenzációs kontroll alkalmazásával.

3.2. Sérülékenység elemzés

A szervezetet érintő sérülékenységeket ismerni kell, hogy megfelelő intézkedésekkel csökkenteni lehessen az általuk hordozott kockázatokat. A folyamatos sérülékenység elemzés (vulnerability assessment) az egyik első lépés a sérülékenységkezelési folyamatban, mert ez felelős összevetni az új sérülékenységekről érkező információkat a belső eszközökről rendelkezésre álló információkkal annak érdekében, hogy azonosítani lehessen az érintett eszközöket.

A sérülékenység elemzés során az elemzők összegyűjtik az érintett eszközöket és értesítik az eszköz felelősöket, vagy üzemeltetési csapatokat a sérülékenységről. A sérülékenység elemzés hatékonysága nagyban függ attól, hogy mennyire naprakész, pontos a szervezeti eszközinformációs adatbázisa.

Egy nagyvállalati környezetben a sérülékenység vizsgálat számos nehézségbe ütközhet, többek között:

- mielőtt megtörténne maga a vizsgálat, megfontolt tervezésre van szükséges a vizsgálat megfelelő idejének meghatározására, hogy az esetleges üzleti hatásokat minimalizálni lehessen, mert akár még passzív vizsgálatok is negatívan befolyásolhatják a rendszerek működését;
- egy nagyvállalati környezetben egy vizsgálat teljes lefutása hosszú időt (heteket, vagy akár hónapokat) is igénybe vehet az infrastruktúra nagy mérete miatt. Ha a sérülékenység vizsgálatot nem egészíti ki sérülékenység elemzés is, akkor két vizsgálati ciklus között számos sérülékenység hosszú ideig nem szerez tudomást a szervezet;

- nagymértékben, vagy akár teljesen elszigetelt környezetekben a hálózaton keresztüli vizsgálat bonyolulttá válhat, a helyileg telepített szkennerek használata viszont megnöveli a vizsgálat idő és erőforrásigényét;
- néhány kritikus, vagy egyedi technológiákat használó környezetben a tervezés és megvalósítás további körültekintést kíván.

3.3. Sérülékenységek priorizálása és osztályozása

Ha egy sérülékenységről megállapításra kerül, hogy érinti a szervezet valamely információs eszközét, meg kell határozni, hogy milyen kockázatokat képvisel, hogy ezek alapján a válaszlépéseket, vagy a kompenzációs kontrollok megvalósítását priorizálni lehessen.

A priorizálás nem alapulhat kizárólag a sérülékenység súlyosságán, figyelembe kell venni az érintett eszköz szervezeten belüli kritikusságát is. Ezért a sérülékenység priorizálásának módja, amit a szervezet alkalmaz, mindkettőt figyelembe kell vegye.

Az úgynevezett 0-day sérülékenységek, amelyekre még nem létezik javítás, de már létezik már az adott sérülékenységet kihasználó kártékony kód (exploit), kiemelt körültekintést igényelnek a priorizálás során, mert néha túlzott figyelmet kapnak valós hatásuk és kockázati kitettségükhöz képest. Alap esetben a legmagasabb súlyossággal kezelendők a 0-day sérülékenységek, de kiemelten fontos a megszokott priorizálási folyamat követése, hogy a valós kockázattal arányos módon legyenek kezelve.

A sérülékenységek osztályozásának (vulnerability triage) célja a válaszlépések elvégzése határidejének meghatározása.

Ha egy sérülékenység azonosításra kerül a sérülékenység elemzés, vagy vizsgálat során, akkor a sérülékenység osztályzás biztosítja azt, hogy a sérülékenységhez rendelt prioritás ellenőrzésre, illetve szükség esetén finomhangolásra kerüljön annak függvényében, hogy az adott sérülékenységet tartalmazó rendszerkomponens milyen módon van használva a szervezeten belül.

3.4. Sérülékenységek hatásának csökkentése

Ha egy információs eszközről megerősítésre kerül, hogy sérülékeny és az adott sérülékenység ki is használható, akkor meg kell határozni milyen módon csökkenthető az adott sérülékenység hatása.

Ha rendelkezésre áll biztonsági frissítés, akkor a megállapított prioritással összhangban el kell végezni a patch kezelését. Ellenkező esetben valamilyen kompenzációs kontroll definiálásra van szükség. Ha létezik a sérülékenység hatásának csökkentéséről nyilvánosan elérhető információ (például a sérülékeny rendszer gyártójától), ez alapul szolgálhat, de minden esetben ellenőrizni kell annak szervezeten belüli alkalmazhatóságát.

Ha bármilyen okból nem lehetséges a frissítés, vagy kompenzációs kontroll alkalmazása, akkor a kapcsolódó kockázatot nyomon kell követni a szervezet általános kockázatmenedzsment folyamatait követve.

4. Patch menedzsment

A patch menedzsmenttel kapcsolatban az alábbi fogalmak merülnek fel leggyakrabban:

patch	A *patch* (javítás) egy kis programkód, amit azért adnak ki, hogy egy vagy több, a program publikálása után felfedezett hibát javítsanak vele.

hotfix	A *Hotfix* a patch-ek egy fajtája, amely, ahogy a neve is mutatja, olyan, általában sürgős és létfontosságú javítás a programfolyamban, amelyet a lehető leghamarabb telepíteni kell.
hivatalos patch	A hivatalos javításokat és frissítéseket a termék gyártója adja ki. A gyártóknak különböző támogatási irányelvei vannak, de a biztonsági patch-eket, amelyekkel sérülékenységeket javítanak, általában a sztenderd támogatási időszak végéig biztosítják.
nemhivatalos patch	Amikor egy szoftver életciklusa végére ér, és a gyártó már nem ad támogatást rá, vagy megszünteti a terméket, nem adnak ki több hivatalos javítást. Vannak azonban olyan esetek, amikor néhány lelkes fejlesztő a szoftver életben tartása érdekében a saját idejét és erőforrásait felhasználva maga fejleszt és publikál javításokat. Az ilyen javításokat nevezik nemhivatalos patch-nek.

A kiberbiztonsági incidensek jelentős része olyan sérülékenység kihasználásának eredménye, amelyekre a támadás időpontjában már hetek, hónapok óta létezik javítás (patch).

Az egyik leghíresebb zsarolóvírus (ransomware), a WannaCry, olyan sérülékenységet használt ki, amelyre már két hónappal az első sikeres támadás előtt kiadták a javítást, a támadás mégis több mint 150 országban, több mint 200 000 számítógépet érintett, és zavart vagy kiesést okozott olyan kritikus szolgáltatásokban, mint az egészségügy Nagy-Britanniában, önkormányzatokban Svédországban vagy a vasúti közlekedésben Németországban. A zsarolóvírusokkal operáló támadók az idők során, mivel valószínűleg elégedetlenek voltak az áldozatok fizetési hajlandóságával, változtattak a támadási módszerükön. Manapság a zsarolóvírus támadások egy része már nemcsak az adatok túszul ejtéséről szól, hanem a megszerzésükről is. Sok esetben először ellopják az adatokat, csak utána következik a titkosítás. A zsarolás így már nem kizárólag arról szól, hogy visszaállítják-e az adatokat, hanem arról is, hogy ha az áldozat nem fizet, akkor nyilvánosságra hoznak olyan információt, amelyeknek a közzététele hátrányosan érintheti az áldozatot, legyen az szellemitulajdon vagy kellemetlen e-mailek, mint a Sony hackelés esetében, sőt, ha személyes adatokat lopnak el a támadók, akkor még jelentős hatósági bírságot is kaphat a cég.

A fentiekből látható, hogy a sérülékenységek javításának kiemelt jelentősége van a kiesésmentes működés és a veszteségek elkerülése szempontjából. A sérülékenységek javítása az esetek többségében javító kód (patch) telepítésével történik. Patch-ek nemcsak biztonsági, hanem működési hibákat is javíthatnak, emellett jelennek meg olyanok is, amelyek új funkciókat hoznak a rendszerekbe.

A fenti kihívások megoldása mellett azzal tehetjük jobbá, egyúttal hatékonyabbá a patch menedzsment folyamatunkat, ha nem próbáljuk meg az összes patch telepítését az összes eszközünkre, hanem átgondoljuk, hogy melyiket kell telepíteni, és melyik javít olyan problémát, ami csak vállalható kockázatot jelent, így telepítésük várhat, vagy nem is feltétlenül szükséges.

A gyakorlatban természetesen az ütemezés, a tesztelés és a telepítés is tartogat kihívásokat.

A patchek telepítésének utolsó lépése sok esetben az újraindítás, ami az eszköz átmeneti kiesésével jár. Ez egy munkaállomás esetében, ha a felhasználó elmentette az összes megnyitott fájlját, akkor az újraindítás csak apró kényelmetlenség. Egy szerver, egy hálózati eszköz vagy egy hasonlóan fontos, 24/7-ben működő infrastruktúra elem újraindítása azonban szolgáltatáskieséssel járhat, ami rosszul időzítve nemcsak a belső felhasználók munkáját hátráltatja, hanem például egy internetes bank esetén, az ügyfelek elégedettségére és az üzletre is hatással lehet. Éppen ezért az időzítés során figyelembe kell venni az üzlet igényeit is, és lehetőleg olyan időpontban kell végrehajtani a telepítést, amikor a legkisebb negatív hatása van.

A patch menedzsmentet megkönnyítheti az eszközök egységesítése is. Célszerű az IT környezetben használt eszköztípusok számát a lehetőségekhez mérten minimalizálni, mert ezzel nemcsak a folyamat bonyolultságát tudjuk csökkenteni, hanem a teszteléshez szükséges időt is. A teszteléshez, amennyire csak lehetséges, az éles rendszerekkel megegyező konfigurációjú, azoktól különálló teszt rendszereket kell használni. A patch menedzsment folyamatnak fontos eleme a kivételkezelés. Előfordulhat, hogy egy javítást nem lehet telepíteni, például kompatibilitási problémák miatt, például előfordulhat, hogy egy patch telepítése a rendszer összeomlását eredményezi, vagy egy harmadik fél által gyártott eszköz esetén a gyártó jóváhagyása nélkül nem változtatható meg a konfiguráció. A folyamatban ezeknek a kivételeknek a kezelésére is ki kell térni, és a gyakorlatban ennek megfelelően kell kezelni őket, nem megfeledkezve a kivételek jóváhagyásáról, követéséről és rendszeres felülvizsgálatáról.

5. Felhős biztonság

A felhőalapú számítástechnika az NIST definíciója szerint egy olyan modell, amely lehetővé teszi a hozzáférést konfigurálható számítási eszközök közös tárházához (például hálózatok, szerverek, adattárolók, alkalmazások és szolgáltatások) igény szerint, bárhonnan, kényelmesen. Ezeknek gyorsan kiépíthetőnek, skálázhatónak és megszüntethetőnek kell lenniük minimális felhasználói erőforrással, illetve szolgáltató interakcióval.

5.1. Felhőalkalmazások biztonsága

Felhőalkalmazások biztonságának megteremtése olyan szabályok, eszközök és kontrollok (ellenőrzések) használatát jelenti, melyek a felhőben futtatott szoftvert védik.

Felhőalkalmazások különböző kiberfenyegetéseknek vannak kitéve, például:

- jogosulatlan hozzáférés alkalmazásfunkciókhoz vagy adatokhoz,
- helytelen konfigurációk által fenyegetéseknek kitett alkalmazásszolgáltatások,
- felhasználói fiókok 'eltérítése' (account hijacking) gyenge titkosítás és identitáskezelés miatt ,
- adatszivárgás nem biztonságos API-k vagy infrastrukturális végpontok miatt,
- Distributed Denial of Service (DDos) támadások rosszul kezelt erőforrások miatt.

Az 5 legjobb gyakorlat (best practice) felhőalkalmazások hatékony biztonsági lépéseinek implementálására:

- *Identitás és hozzáférés kezelés (Identity Access Management)*
  Az IAM biztosítja, hogy minden felhasználó csak hitelesítés után férhessen hozzá a jogosultságokat igénylő adatokhoz és alkalmazás funkciókhoz.

- *Titkosítás (Encryption)*
  Titkosítás implementálása az alkalmazás megfelelő részein optimalizálja az alkalmazás teljesítményét miközben megvédi a szenzitív adatokat. Általánosságban meg kell oldani az adatok tárolás, átvitel és használat közbeni titkosítását.

- *Fenyegetés figyelés/monitorozás (Threat monitoring)*
  Miután egy alkalmazást implementálnak a felhőben, elengedhetetlen a fenyegetések valós idejű folyamatos monitorozása.

- *Adatvédelem és Megfelelőség (Data privacy & compliance)*
  Az alkalmazások biztonsága mellett az adatvédelem és a megfelelőség is elengedhetetlen a felhőalkalmazások végfelhasználóinak védelméhez.

- *Automatizált biztonsági tesztelés*

A felhőalkalmazások biztonsága megteremtésének egyik kulcsfontosságú része az automatizált biztonsági tesztelés integrálása közvetlenül a fejlesztési folyamatba. A minél korábbi tesztelés (shifting left testing) csökkenti a sebezhetőségek észlelésének és kijavításának költségeit, miközben biztosítja a fejlesztők számára, hogy továbbra is gyorsan kiadják a kódot.

5.2. Felhős infrastruktúra és platform biztonság

Az IaaS és Paas szolgáltatók úgy kezelik a felhasználók virtuális példányán (instance) belüli alkalmazásokat, mint fekete dobozokat, mivel a felhasználók alkalmazásainak üzemeltetése és kezelése nem az ő feladatuk. Ezért fontos megjegyezni, hogy a felhasználó felelőssége biztonságossá tenni az ilyen felhőben futtatott alkalmazásokat, a következő lépések szerint:

- A felhőben futtatott alkalmazások tervezése során az alkalmazás fenyegetettségi modellezését is el kell végezni, és az eredményeket vissza kell csatolni a tervezési folyamatba.
- A kármentesítési (remediation) folyamatokat definiálni kell, és végre kell hajtani a webes sebezhetőségek hatásainak csökkentése érdekében.
- A felhasználó felelőssége naprakészen tartani az alkalmazásait, és javasolt olyan biztonsági hibákat javító (patch) stratégiát biztosítani, amely védelmet nyújt az ismert sebezhetőségeket kihasználó kártékony programok és exploitok ellen. Ezzel is biztosíthatják az adataik bizalmasságát, sérthetetlenségét és integritását.

6. System hardening legjobb gyakorlatok

A hardening eljárások célja a rendszerbiztonsági minimum szintek megteremtése a támadási felület és ezáltal az információbiztonsági kockázatok csökkentése érdekében.

6.1. CIS referenciaértékek (CIS Benchmarks)

A CIS különböző referencia beállításokat dolgozott ki megadott rendszerekhez, például Microsoft és Linux termékekhez. A szabványok a konfiguráció két szintjére terjednek ki:

- Az első szint a támadási felület csökkentésére (attack surface reduction) összpontosít.
- A második szint a mélységi védelem (defense-in-depth) megteremtését célozza.

A CIS által definiált referenciaérték kategóriák:

- Asztali és webböngészők
- Mobil eszközök
- Hálózati eszközök
- Virtualizációs platformok
- Felhős környezetek

6.2. Rendszer hardening legjobb gyakorlatok

Egységesített operációs környezetek (Standard Operating Environment - SOE) alkalmazása

A SOE az operációs rendszer és alkalmazások szabványosított telepítése és beállítása, amelynek célja a következetes és biztonságos alapbeállítások- és értékek megteremtése.

Amikor harmadik féltől vagy szolgáltatóktól származik a SOE, további ellátási lánc jellegű kockázatokat kell figyelembe venni, például a kártékony tartalom vagy konfigurációk véletlen vagy szándékos átadását. Az ilyen események valószínűségének csökkentése érdekében a szervezeteknek nemcsak

megbízható forrásokból kell beszerezniük az operációs környezeteket, hanem használatuk előtt sérülékenységi – és konfigurációs szkennelést is végre kell hajtani, hogy biztosítsák integritásukat.

Operációs rendszer kiadások és verziók (Operating system releases and versions) használata

Az operációs rendszerek újabb kiadásai gyakran a biztonsági funkciók javulását eredményezik a régebbi kiadásokhoz képest. Ez megnehezítheti a támadó számára, hogy az általuk felfedezett sérülékenységekre működő exploitot (sérülékenységet kihasználó kód vagy technika) hozzanak létre.

Ajánlott biztonsági kontrollok:

- Az operációs rendszerek legújabb kiadásainak, frissített verzióinak használata munkaállomásokhoz, szerverekhez és hálózati eszközökhöz.

Operációs rendszer konfiguráció (Operating system configuration)

Ha az operációs rendszerek alapértelmezett állapotban kerülnek telepítésre, az könnyen nem biztonságos működési környezethez vezethet, amely lehetővé teszi a támadók számára, hogy kezdő belépési pontként használják azt a hálózaton.

Ajánlott biztonsági kontrollok:

- A gyártóknak az adott operációs rendszer biztonságos konfigurációjához készített hardening útmutatásainak betartása.
- Az operációs rendszer alapértelmezett fiókjainak letiltása, átnevezése, vagy a jelszavak módosítása.
- A szükségtelen operációsrendszer-fiókok, szoftverek, összetevők, szolgáltatások és funkciók letiltása, vagy eltávolítása.
- Az operációs rendszerek biztonsági funkcióinak megváltoztatását, letiltását, vagy megkerülését ellehetetlenítő eljárások engedélyezése.
- A nem kiemelt felhasználók számára szkript futtató motorok és alkalmazások használatának tiltása Microsoft Windows környezetben.

Helyi rendszergazdai fiókok (Local administrator accounts) kezelése

Ha a helyi rendszergazdai fiókokokat közös fióknevekkel és jelszavakkal használják, az lehetővé teheti, hogy az egyik munkaállomást vagy szervert kompromittáló támadó könnyen átvihesse a hitelesítési adatokat a hálózaton keresztül más munkaállomásokra vagy kiszolgálókra.

Ajánlott biztonsági kontrollok:

- A helyi rendszergazdai fiókok letiltása; alternatív megoldásként véletlenszerű és egyedi jelszavakat használata az egyes eszközök helyi rendszergazdai fiókjához
- Munkaállomások és a szerverek esetén egyedi helyi rendszergazdai fiókok használata, tartományi rendszergazdai jogosultságok nélkül

Alkalmazás kezelés (Application management)

Alkalmazások telepítésének jogosultsága valós üzleti igény lehet a felhasználók számára, ezt azonban kihasználhatja egy támadó.

Ajánlott biztonsági kontrollok:

- A felhasználók nem jóváhagyott szoftver telepítési jogosultságainak megvonása.
- A felhasználók jóváhagyott szoftver eltávolítási jogosultságainak megvonása.

Alkalmazás ellenőrzés (Application control)

Az alkalmazás ellenőrzés rendkívül hatékony mechanizmus lehet nemcsak a rosszindulatú kódok futtatásának megakadályozásában, hanem annak biztosításában is, hogy csak jóváhagyott alkalmazások legyenek telepíthetők.

Ajánlott biztonsági kontrollok:

- Az alkalmazás ellenőrzés (application control) implementálása végponti eszközökre

Exploit védelem (Exploit protection)

Egy támadó hatékonyan ki tudja használni az operációs rendszerek sérülékenységeit célzott exploit létrehozásával és alkalmazásával, amennyiben az operációs rendszer ezt megakadályozó funkciói nincsenek aktiválva.

Ajánlott biztonsági kontroll:

- Exploit védelmi funkciók bevezetése a munkaállomásokon és a szervereken

PowerShell

A PowerShell könnyen használható a Microsoft Windows környezetek teljes felügyeletéhez, akár támadó részéről is.

Ajánlott biztonsági kontrollok:

- Windows PowerShell 2.0 tiltása, vagy eltávolítása.
- A PowerShell nyelv használatának korlátozása (Constrained Language Mode).
- A PowerShell-eseménynaplók központi védett tárolása, folyamatosan monitorozása, és kompromittálásra utaló riasztás esetén incidens kezelési lépések elvégzése.

SSH

Az SSH biztonságos, titkosított helyettesítője az olyan gyakori bejelentkezési szolgáltatásoknak, mint a telnet, ftp, rlogin, rsh és rcp. Erősen ajánlott, hogy az egyes környezetekben elhagyják a régebbi, tisztán szöveges bejelentkezési protokollokat.

Ajánlott biztonsági kontrollok:

- Az /etc/ssh/sshd_config engedélyeinek megfelelő beállítása.
- Az SSH privát és publikus kulcsok engedélyeinek megfelelő beállítása.
- Az SSH Protocol 2-es használata.
- Az SSH HostbasedAuthentication tiltása.
- Az SSH root login tiltása.

Az SSH LogLevel megfelelő szintre állítása. **Hoszt-oldali behatolásmegelőző rendszer (Host-based Intrusion Prevention System - HIPS)** Számos végpontbiztonsági megoldás szignatúrákra támaszkodik a kártékony kódok észlelésében. Ez a megközelítés csak akkor hatékony, ha egy adott kártékony kódot már profiloztak, és a szignatúra adatbázisok naprakészek. A hoszt-oldali behatolásmegelőzési rendszer viselkedésalapú észlelési sémákat használ a rendellenes viselkedés azonosításához és blokkolásához, mint például kártékony folyamat injektálás (process injection), billentyűleütés naplózók (keylogger), valamint a víruskereső gyártók által még azonosítandó (unknown) rosszindulatú kódok észleléséhez.

Ajánlott biztonsági kontrollok:

- HIPS telepítése és futtatása munkaállomásokon.

- HIPS telepítése és futtatása kritikus szervereken, például hitelesítési szervereken, DNS-kiszolgálókon, webszervereken, fájlszervereken és e-mail szervereken.

Szoftveres tűzfal

A hagyományos hálózati tűzfalak gyakran nem akadályozzák meg a kártékony kódok terjedését a hálózaton, vagy a támadót érzékeny adatok kiszivárogtatásában, mivel általában csak azt szabályozzák, hogy mely portok vagy protokollok használhatók a különböző hálózati szegmensek között. A szoftveres tűzfalak abban hatékonyabbak, mint a hálózati tűzfalak, hogy szabályozhatják, hogy mely alkalmazások és szolgáltatások kommunikálhatnak a munkaállomásokkal és szerverekkel.

Ajánlott biztonsági kontrollok:

- Szoftveres tűzfal telepítése és futtatása a munkaállomásokon és szervereken, a bejövő és kimenő alkalmazás szintű hálózati kapcsolatok és kommunikáció szabályzására

Végpontvédelmi szoftver (Endpoint protection software)

A támadók gyakran jelentős időt és erőfeszítést tesznek a jól működő és megbízható exploitok fejlesztésébe. Bár az ismert exploitokat a víruskereső gyártók profilozhatják, továbbra is hatékony behatolási módszer maradhat azokban a szervezetekben, amelyek nem rendelkeznek az észlelésükre szolgáló technológiákkal, folyamatokkal.

Ajánlott biztonsági kontrollok:

- Végpontvédelmi szoftver bevezetése és futtatása a munkaállomásokon és szervereken.
- Szignatúra alapú észlelés beállítása, magas észlelési szintre állítva.
- Heurisztikus alapú észlelés beállítása, magas észlelési szintre állítva.
- Ransomware elleni intézkedések beállítása.
- Szignatúra adatbázisok legalább napi szintű frissítése.
- Automatikus és rendszeres szkennelés beállítása az összes rögzített - és cserélhető adathordozóhoz.

Eszközhozzáférést felügyelő szoftver (Device access control software - DAC)

Az eszközhozzáférést felügyelő szoftver használata a nem engedélyezett eszközök (pl. nem jóváhagyott okostelefonok, táblagépek, Bluetooth-eszközök, vezeték nélküli eszközök, 4G/5G hardverkulcsok) munkaállomásokhoz és szerverekhez való csatlakoztatásának megakadályozását teszi lehetővé külső interfészeken, például USB-portokon keresztül, hozzájárulva a munkaállomások és szerverek mélységi védelméhez.

Ajánlott biztonsági kontrollok:

- Eszközhozzáférést vezérlő szoftver telepítése és futtatása munkaállomásokon és szervereken a célból, hogy megakadályozzák a jogosulatlan eszközök csatlakoztatását.
- A DMA-t engedélyező munkaállomások és szerverek külső interfészeinek letiltása.

7. SWIFT biztonsági alapok, biztonsági követelmények

A Society for Worldwide Interbank Financial Telecommunication (SWIFT) egy olyan hálózatot biztosít, amely lehetővé teszi pénzügyi intézményeknek világszerte, hogy egy biztonságos, szabványosított és megbízható környezetben küldjenek és fogadjanak pénzügyi tranzakciókkal kapcsolatos információkat.

A SWIFT's Customer Security Programme (CSP) segít ezeknek az intézményeknek biztosítani a védelmük naprakészségét és hatékonyságát a kibertámadásokkal szemben, ezzel védve a szélesebb pénzügyi hálózat integritását is.

A kötelező biztonsági kontrollok egy biztonsági alapot határoznak meg a teljes SWIFT-et használó szervezet számára. Ezeket minden SWIFT felhasználónak alkalmaznia kell a helyi SWIFT infrastruktúrán. A SWIFT azért priorizálja ezeket a kötelező kontrollokat, hogy reális rövidtávú célt tűzzön ki kézzelfogható biztonsági előrelépésekhez és kockázatcsökkentéshez.

Változtatások 2021-ben

A 2021-es CSCF verzió két jelentős változtatást vezetett be. Ezek célja a framework fejlesztése, változó fenyegetésekhez való igazítása, és a biztonsági kontrollok szigorúbb implementálása. Egy korábban csak ajánlott kontroll kötelezővé vált, és növelték egy másik korábbi kontroll hatályát:

- Új Kötelező Control: a 1.4-es Control, Restriction of Internet Access (Internethozzáférés korlátozása) kötelezővé vált. Ez a kontrol arra koncentrál, hogy az internethozzáférés az üzleti funkciók elvégzéséhez szükséges minimális mennyiségre korlátozódjon mind a biztonsági zónában, mind az operátor PC-kben, melyeknek van interfésze a SWIFT-tel.
- Scope változás: A 4.2-es Control, Multi-factor Authentication (Többfaktoros azonosítás), hatálya kibővült. Mostantól hozzáférés előtt megköveteli többfaktoros azonosítás használatát, olyan third-party szolgáltatók által üzemeltetett, SWIFT-tel kapcsolatos applikációkhoz vagy komponensekhez, melyek tranzakciók feldolgozását végzik.

8. CIS és NIST ajánlások biztonsági iránymutatásai üzemeltetőknek

8.1. CIS

A CIS (Center for Information Security) keretrendszert 2008-ban fejlesztették a szervezetek komplex informatikaibiztonsági igényeinek megfelelően.

A prioritások meghatározása a CIS-kontrollok egyik fő előnye. Arra tervezték őket, hogy segítsenek a szervezeteknek gyorsan meghatározni védekezésük kiindulópontját, szűkös erőforrásaikat azonnali és nagy értékű megtérülést hozó tevékenységekre irányítani. A CIS 8.1 változata 18 kontrollt különböztet meg.

Vállalati eszközök leltározása és ellenőrzése	Auditnapló kezelése	Beszállítók, szolgáltató kezelése
Szoftvereszközök nyilvántartása és felügyelete	E-mail és webböngésző védelme	Szoftver-biztonság
Adatvédelem	Kártevő elleni védelem	Incidensek kezelése
Vállalati eszközök és szoftverek biztonságos konfigurálása	Adat-helyreállítás	Behatolási tesztelés (Pentest)
Fiókkezelés	Hálózati infrastruktúra kezelése	
Hozzáférési jogosultság kezelés	Hálózatfigyelés és védelem	

Folytonos sebezhetőség-kezelés	Biztonsági tudatosság és készségek képzése	

8.2. NIST

Mi az a NIST 800-53?

A NIST 800-53 egy biztonsági megfelelőségi szabvány, amelyet az Egyesült Államok Kereskedelmi Minisztériuma és a National Institute of Standards in Technology (NIST) hozott létre válaszul a nemzeti ellenfelek gyorsan növekvő technológiai fejlődésére. Összefoglalja az Informatikai Laboratórium (ITL) által javasolt kontrollokat.

A szabványt úgy fejlesztették ki, hogy integrálja az adatvédelmi és biztonsági ellenőrzéseket, és elősegítse az integrációt más IT biztonsági és kockázatkezelési megközelítésekkel.

Mi a NIST 800-53 célja?

A biztonsági és adatvédelmi szabvány célja háromféle:

- Olyan átfogó és rugalmas kontrollok biztosítása, melyek a jelen és jövő IT biztonságát szavatolják a technológia és a fenyegetések állandóan változó világában.
- Olyan módszertani alapok kidolgozása, melyek növelik a folyamatok és technikák ellenőrzésének hatékonyságát.
- Olyan közös alapokon nyugvó kommunikációs séma kidolgozása, mely javítja a szervezetek közötti kockázatviselés koncepciók megvitatását.

NIST 800-53 biztonsági kontrollok

A NIST keretrendszer minden informatikai biztonsági képességet, folyamatot és napi tevékenységet az alábbi 5 fő funkcióba sorolja:

- *Azonosítás:* milyen folyamatok és eszközök igényelnek védelmet.
- *Védelem:* Megfelelő biztonsági intézkedések alkalmazása a szervezet eszközeinek megóvása érdekében.
- *Észlelés:* Megfelelő mechanizmusok alkalmazása az informatikai biztonsági események azonosítására.
- *Reagálás:* Megfelelő technikák alkalmazása az informatikai biztonsági események kezelésére.
- *Helyreállítás:* Az informatikai biztonsági esemény során keletkezett károk kijavítására megfelelő folyamatok alkalmazása.

A NIST 800-53 biztonsági és adatvédelmi kontrollokat és útmutatást kínál. Ezek az alábbi 20 témakörhöz vannak hozzárendelve, melyek az előbb említett 5 kategória valamelyikének felelnek meg.

Azonosítás	Védelem	Észlelés	Reagálás	Helyreállítás
Vagyonkezelés	Jogosultságkezelés	Anomáliák és események	Reagálási ütemterv	Helyreállítási ütemterv
Üzleti környezet	Tudatosság és oktatás	Folyamatos biztonsági monitorozás	Kommunikáció	Folyamatok fejlesztése

Irányítás gyakorlatok	Adatbiztonság	Felderítési folyamatok	Elemzés	Kommunikáció
Kockázatelemzés	Információ biztonsági protokoll és folyamatok		Kármentés	
Kockázatkezelési startégiák	Védelmi rendszerek karbantartása		Folyamatok fejlesztése	
Beszállítói kockázatelemzés	Védelmi technológiák kezelése			

9. Tananyag elsajátítására vonatkozó nyilatkozat

A jelen tananyag elsajátítására vonatkozó nyilatkozatot az alábbi szöveggel kérjük a dora_oktatas@otpbank.hu e-mail címre eljuttatni:

„Az OTP Bank Nyrt. által az IKT szolgáltatónak minősülő Szerződő Partnerek számára a DORA rendelet előírásainak megfelelően kialakított oktatási anyagot a [Partner cég neve] által az OTP Bank Nyrt-nek nyújtott szolgáltatásban résztvevő valamennyi személy elolvasta, az abban foglaltakat megértette és magára nézve kötelezőként ismeri el. A [Partner cég neve] vállalja, hogy a szolgáltatás teljes életciklusa alatt biztosítja a szolgáltatás nyújtásába bevont munkavállalói és alvállalkozói részére az oktatási anyag megismertetését és elvárja munkavállalóitól és alvállalkozóitól az azokban foglaltak betartását."

10. Tananyag elsajátítására vonatkozó nyilatkozat egyéni vállalkozók részére

Amennyiben Ön egyéni vállalkozó, kérjük, hogy az alábbi tartalmú nyilatkozatot szíveskedjék kitölteni, és a dora_oktatas@otpbank.hu e-mail címre elküldeni: „A nyilatkozat kitöltésével kijelentem, hogy az OTP Nyrt. Általános Adatkezelési tájékoztatójában (https://www.otpbank.hu/portal/hu/adatvedelem) foglaltakat megismertem és annak tartalmát elfogadom.”

Tájékoztatjuk továbbá, hogy az OTP Bank, mint adatkezelő a nyilatkozattétellel összefüggésben a DORA rendelet szerinti elvárásoknak való megfelelés érdekében az Általános Adatvédelmi Rendelet 6. cikk (1) bekezdés f) pontja szerinti jogos érdek jogalapján kezeli az egyéni vállalkozó nevét, e-mail címét, továbbá az oktatás elvégzésének tényét.