Az elvárt technológiai eszközök biztonsági osztályonként

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/23

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.02.26	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

1 VEZETŐI ÖSSZEFOGLALÓ

A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (Kiberbiztonsági tv.) és annak végrehajtási rendeletei, különösen a biztonsági osztályba sorolás követelményeiről szóló MK rendelet, a NIS2 irányelvvel összhangban megkövetelik az érintett szervezetektől, hogy kockázatokkal arányos védelmi intézkedéseket vezessenek be.

Az **elektronikus információs rendszereket (EIR)** „alap", „jelentős" vagy „magas" biztonsági osztályba kell sorolni, ami szigorodó védelmi előírásokkal jár.

Szervezeti szinten az alapvető követelmények (pl. kockázatmenedzsment keretrendszer, IBF kijelölése, oktatás) minden osztály esetében kötelezőek, de a magasabb osztályok esetében a technikai kontrollok megvalósításának komplexitása és szigorúsága jelentősen megnő, különösen az adatok sértetlensége és a rendszerek rendelkezésre állása vonatkozásában.

A NIS2 megfelelőség eléréséhez szükséges **technológiai intézkedések** az alapvető biztonsági követelményeken (Alap biztonsági osztály) túl a Jelentős és Magas osztályoknál speciális követelményeket írnak elő, mint például tranzakció-helyreállítás, mobil eszközök titkosítása és a Magas osztály esetében a fokozott fizikai védelem az információszivárgás ellen.

2 PROBLÉMAFELVETÉS

A NIS2 irányelv (EU 2022/2555) hazai implementációja megköveteli, hogy a szervezetek az EIR-eket a kockázatokkal arányosan osztályozzák, és ehhez illeszkedően határozzák meg és valósítsák meg a védelmi intézkedéseket. A szervezet vezetője felelős a kockázatmenedzsment keretrendszer létrehozásáért és működtetéséért. A biztonsági osztályba sorolás alapján a szervezetnek meg kell valósítania a rendeletben előírt védelmi intézkedéseket. A megfelelés érdekében nem csak adminisztratív, hanem logikai és fizikai védelem kialakítása is szükséges, beleértve a technikai és technológiai védelmi megoldásokat és intézkedéseket is.

A NIS2 megfelelés érdekében kritikus a három biztonsági osztályhoz rendelt elvárt technológiai és az azt támogató szervezeti intézkedések pontos azonosítása és differenciált bevezetése az informatikai rendszerek (EIR) védelme érdekében.

3 AZ AJÁNLOTT IRÁNYMUTATÁS RÉSZLETEZÉSE

A NIS2 irányelv (Network and Information Systems Directive 2) kiterjesztett kiberbiztonsági követelményeket ír elő kritikus infrastruktúrák számára, hangsúlyozva a kockázatkezelést, incidenskezelést és supply chain biztonságot. Az automatizáció kulcsfontosságú a fenntartható megfeleléshez, mivel csökkenti a manuális erőfeszítést és biztosítja a folyamatos nyomon követést. A szervezet kialakíthatja folyamatait dokumentációs alapokon, illetve ingyenes eszközök használatával is oly módon, hogy a későbbiekben a folyamatokat automatizálja, illetve a használt eszközöket szükség és igény szerint bővíti, illetve optimalizálja (például monitoring és naplózás funkciók felülvizsgálatával).

A tapasztalatok azt mutatják, hogy egy funkciókban gazdag, de a szervezet által nem adaptált (elavult adatokkal rendelkező, nem aktualizált) GRC rendszer használata is bukást eredményezhet az auditon. Ezzel szemben az auditotok teljes mértékben elfogadják és jó

gyakorlatként értékelik, ha egy vállalat a meglévő, integrált folyamatmenedzsment vagy hibajegykezelő (ticketing) rendszereit (például Jira, Redmine, ServiceNow) paraméterezi fel az információbiztonsági munkafolyamatok (workflow-k) lekezelésére. Ha egy egyszerű ticketing rendszer transzparensen és manipulálhatatlanul képes naplózni a jogosultság-igénylési folyamatokat, a vezetői jóváhagyási láncokat, a változáskezelési (change management) eseményeket és a biztonsági incidensek kivizsgálását, az tökéletesen megfelel a jogszabályi elvárásoknak. A siker kulcsa tehát a szervezet érettsége, a folyamati fegyelem és a technológia következetes alkalmazása, nem pedig az alkalmazott szoftver típusa.

A minimum. Ökölszabályként elmondható, hogy 70 felhasználó, illetve havi 100-150 nyitott hibajegy esetén már megéri helpdesk rendszereket használni, melyek nem csak a hibák bejelentésére, de megfelelő konfigurálás mellett jogosultságigények kezelésére, jóváhagyására, dokumentálására, incidensek dokumentálására, karbantartások nyilvántartására, változáskezelés menedzsmentjére és még sok egyéb dokumentációs és jóváhagyási folyamat kiváltására használható. Erősen javasoljuk, hogy talán elsőként specializált szoftverek helyett egy ilyen központi rendszer kerüljön bevezetésre hiszen ennek lesz a legnagyobb hatása – amennyiben a szervezet még nem rendelkezik ilyen eszközzel.

Az alábbiakban a NIS2 fő kontroll családjai szerint részletezzük a javasolt automatizációs megoldásokat.

3.1 Programmenedzsment

A kontrollcsoport kezeléséhez nem tartozik technológiai elvárás, mivel az kifejezetten a szabályozási környezet megfelelő kialakításáról szól, központi szabályozási elemként az Információbiztonsági szabályzat, illetve kapcsolódó stratégiák kialakításáról.

3.2 Hozzáférés-felügyelet

A kontrollcsoport kifejezetten a felhasználói fiókok kezelésére fókuszál erősen, így a szervezetnek meg kell tudnia válaszolni a következő kérdést: „Hogyan tudjuk kezelni a felhasználókat modern eszközökkel?”

A kérdésnek két szintje van, egyrészt a bevezetőben már felvetett központi jegykezelő rendszer segítségével magukat a kéréseket lehet jól dokumentálható módon egy nyilvántartásba csatornázni, míg egy központi címtár használatával központi nyilvántartás és hozzáférés menedzsment rendszer valósítható meg. Ne felejtsük, hogy egyetlen központi rendszer használata nem jelenti azt, hogy a beállításokat csak egyetlen ember végezheti el, hiszen egyes folyamatok és felelősök meghatározásával akár a szervezet eltérő szervezeti egységeiben dolgozó adatgazdák is kezelhetik egy rendszerben a hozzájuk tartozó rendszerek hozzáféréseit.

Alap biztonsági osztályba sorolt rendszernél a hozzáférés igénylés és kezelés folyamatát még lehetséges papíralapú "sétálópapír / kiköröző lap" (belépési/kilépési adatlap) használatával

megoldani, de a hibázási lehetőség óriási, illetve ezek általában belépés és kilépés eseteit tudják kezelni, használatuk jogosultságmódosítás esetén nehézkesebb és sokszor elhanyagolt, de ha a szervezet ezt tudja kezelni a papír alapú igénylés-jóváhagyás-végrehajtás folyamat elfogadható.

Ezen a biztonsági osztályban is segíthet ugyanakkor egy központi címtár mely SSO használata esetén a sikertelen bejelentkezési kísérletek limitálását, a rendszerhasználati jelzés megvalósítását még olyan rendszereknél is megvalósíthatja, melyeknél amúgy ez technológiailag nem lenne lehetséges.

Jelentős biztonsági szintű EIR-ek esetén már elvárás a fiókkezelés automatizálása (pl. inaktív, lejáró felhasználói fiókok automatikus tiltása, ideiglenes felhasználói hozzáférések lejáratának automatikus kezelése) és a fiókkezelés naplózása. Ezen elvárásokat manuálisan már nem lehet kezelni, kell a központi címtár (AD, LDAP) szolgáltatás vagy IAM rendszer, mely segítséget jelenthet jogosultsági szerepkörök központi kezelésére is, segítve a felelősségek szétválasztását – biztonsági funkciók, privilegizált funkciók elkülönítése - infrastruktúra elem és felhasználói alkalmazás szinteken is.

Egy központi felhasználói fiókokat kezelő rendszer képes betölteni a szerepet az elvárt eszköz és munkaszakasz lezárások megvalósítására is.

Magas biztonsági osztály esetén a fiókkezelési elvárások egy erősebb szintű fiókhasználati monitoringgal is kiegészülnek - meghatározott megszokottól eltérő használat esetén szükséges riasztást küldenie a rendszernek – ehhez a szervezet az egyébként használt naplózási, naplóvizsgálati, illetve monitoring rendszeréhez kell megfelelő szabályokat kialakítania.

Ezen osztályban már elvárás meghatározott számra korlátozni az egyidejű munkaszakaszok számát minden egyes meghatározott fiókra vagy fióktípusra vonatkozóan, mely követelmény már csak széleskörű IAM / PAM megoldásokkal megvalósítható.

Távoli hozzáférések esetén jelentős biztonsági osztálynál már elvárt a titkosított és monitorozott kapcsolat is, melyhez praktikusan valamely VPN szolgáltatás ajánlott. Fontos, hogy megfelelő – nem elavult – titkosítással rendelkező VPN alkalmazást használjunk, és nem szabad megfeledkezni a többfaktoros hitelesítésről sem. Jelentős biztonsági osztály esetén a kétfaktoros hitelesítés már minden felhasználóra elvárt (lásd.: Azonosítás és hitelesítés).

Kifejezetten privilegizált, azaz magas kockázatú hozzáférések kezeléséhez javasoltak a PAM rendszerek. Egyes PAM (Privileged Access Management) megoldások, automatikusan rotálják a jelszavakat, jóváhagyják a kiemelt hozzáféréseket és naplózzák a munkameneteket. Open-source IAM megoldás képes automatizálni az MFA és RBAC elvárások (Role-Based Access Control - szerepkör-alapú hozzáférés-vezérlés) kezelését kis hálózatokon, LDAP integrációval.

3.3 Tudatosság és képzés

LMS (Learning Management System) platformok, kötelező tréningeket futtatnak, melyek emlékeztetőt tudnak küldeni a felhasználóknak, nyomon követik a részvételt és a vizsga eredményeket, illetve e rendszerekben gamifikált modulok személyre szabott tartalommal biztosítják az éves NIS2-képzéseket, riportokkal a vezetőségnek.

Lehetséges éves NIS2 tréning videók bemutatása YouTube-on, Google Formokkal ellenőrizve, ezen követelménycsoport esetén a megvalósítás igen sokrétű lehet.

A legminimalistább megoldás is elfogadható, amely az oktatási anyag bemutatása személyes vagy online oktatás keretében, mely esetben az oktatási anyag tartalma és a résztvevők dokumentálása – aláírt jelenléti ívvel vagy képernyőképpel - elvárt.

E kontrollcsoport esetében az alap biztonsági osztály és a jelentős biztonsági osztály közötti egyetlen eltérés a szükséges oktatási tematikában rejlik, a technológiai megvalósítás ezért biztonsági osztálytól független. E témában a technológiát inkább a magas felhasználószám, illetve az eltérő oktatási igény miatt lehet egy szervezetnek mindenképpen központosított online oktatási platform (LMS) használatára. Ugyanakkor ezen platformok is igénybevehetők már felhős szolgáltatásként, ahol egy szakértő cég biztosítja az oktatások megfelelő minőségét és üzemelteti az oktatáshoz használt rendszert, nem kell egy ilyen rendszert feltétlenül a szervezeteknek házon belül kialakítani és üzemeltetni.

3.4 Naplózás és elszámoltathatóság

Általánosságban elmondható, hogy manapság már rendelkezésre állnak ingyenes naplózási funkciókat támogató rendszerek, melyek többféle naplóelemzési, naplófelügyeleti igényt megvalósítanak. Ezen rendszerek – vagy rendszer kombinációk – funkciói magas biztonsági osztályba sorolt rendszerek esetén is legalább részben megfelelő megoldást biztosíthatnak.

Amire biztosan lehetőség van e rendszerekben:

- naplózási hibák észlelése és alertek küldése,
- automata naplóelemzés, felülvizsgálat kialakítása és alerting megvalósítása,

ugyanakkor a jelentős és magas biztonsági osztályban elvárt naplóbejegyzés felülvizsgálati, csökkentési, elemzési és jelentéstételi követelményekhez már – akár ingyenes – SIEM rendszer használatára van szükség.

E rendszerek sokkal komplexebbek, mint a korábban említett szabályok vagy mintázatok alapján naplóinformációkat átvizsgáló és alertet küldő rendszerek.

A naplóinformációk integritásvédelmének és illetéktelen hozzáférések megelőzéséhez (már alap biztonsági osztálytól) két oldalról is védelmet kell kialakítani bizalmasság és integritásvédelem vonalon:

1) a naplókhoz való hozzáférést szükséges limitálni úgy, hogy a naplókat akár az élő rendszertől eltérő logikai / fizikai helyre gyűjtjük, ahol limitáljuk a hozzáférését, esetleg a hozzáféréseket kell jelentősen visszavenni azok eredeti keletkezési helyén; sajnos ezen megoldásokkal egy incidens esetén már csak jóval később derülnek ki a problémák.
2) Ennél kifinomultabb megoldások:
    a. dedikált „menedzsment” alhálózat kialakítása csak a naplók kezeléséhez;
    b. lehet a naplókat egyszerírható adathordozóra írni;

c. a naplóinformációkat hash-el ellátni időszakonként, és a hash ellenőrzésével validálni a naplóinformációk sértetlenségét;
d. digitális aláírással ellátni a naplóinformációkat;
e. fájl integritás ellenőrző rendszert lehet bevezetni a naplóinformációk ellenőrzésére (FIM rendszer).

Kiegészítés magas biztonsági osztályhoz:

Megjegyezzük, hogy kriptográfiai eszközök használata a naplóinformációk védelmére csak magas biztonsági osztály esetén elvárt, ugyanakkor bárki alkalmazhatja azokat.

Szintén a magas biztonsági osztály elvárása az egész rendszerre kiterjedő és időbeli naplózási nyomvonal biztosítása melyhez a korábban már említett SIEM rendszer használata elengedhetetlen.

3.5 Értékelés, engedélyezés és monitorozás

E kontrollcsoport esetében a hangsúly az engedélyezési folyamatok kialakításán van, melyekhez kifejezetten javasoljuk egy központi jegyzekelő / folyamatkezelő rendszer bevezetését (lásd. Hozzáférés felügyelet). Fontos kihangsúlyozni, hogy ezen rendszerek nem kizárólag a klasszikus helpdesk / hibajegykezelés folyamatokat képesek ellátni, de ha jól alakítják ki őket bármely feladatkezelésre bevethetők.

Léteznek dashboard-alapú GRC eszközök, melyek összesítik a kontrollok állapotát KPI-okkal, automatikus auditriportokkal és prediktív analitikával, folyamatos megfelelőségi szkennerek ellenőrizhetik a konfigurációkat, riasztva eltéréseknél (ezekből is vannak ingyenes verziók), mindemellett megjegyezzük, hogy a jogszabály nem vár el egyik biztonsági osztályban sem automatizációt az értékelési engedélyezési feladatok tekintetében.

3.6 Konfigurációkezelés

Alap biztonsági osztály esetén az elvárások nem kifejezetten igényelnek speciális technológiai megoldásokat, alapkonfiguráció dokumentációkat és egységes konfigurációs elvárásokat, konfigurációs dokumentációkat technikailag „papíron” is ki lehet alakítani, ugyanakkor a rendszerelemek számától és az infrastruktúra komplexitásától függően szükség lehet konfiguráció menedzsment eszközökre (CMDB).

Egy ilyen eszköz lehetővé teszi az informatikai csapatok számára, hogy több ezer szervert, virtuális gépet vagy konténert telepítsenek, frissítsenek vagy újrakonfiguráljanak percek alatt órák helyett, nyomon követi a rendszerkonfigurációk változásait az idő múlásával, egyértelmű auditnaplót biztosítva, és lehetővé téve a gyors visszaállítást, ha problémák merülnek fel.

Már jelentős biztonsági osztályba tartozó rendszernél az automatizmusok a konfigurációkezelésben már elvártak, itt mindenképpen szükséges már CMDB megoldás használata, a naprakészség és a korábbi konfigurációk megőrzésének biztosítása érdekében.

A konfigurációváltozások menedzsmentjét – ide értve a jóváhagyást, információbiztonsági hatásvizsgálatot, a végrehajtást, a kivételkezelést és ezek dokumentálását – ki lehet egészíteni a már többször említett folyamatkezelő rendszer bevezetésével, és a folyamat megfelelő kialakításával.

Az itt elvárt jogosulatlan rendszerelem észlelést hálózatmonitorozó eszközökkel oldhatjuk meg, melyekből már ingyenes verziók is biztosítják e funkcionalitást.

Magas biztonsági osztályba sorolt rendszerek esetében teljesen megkerülhetetlen CMDB megoldás használata.

3.7 Készenléti tervezés

A készenléti tervek kialakítását nagyban segítheti a korábban már említett CMDB rendszerek, melyek segítségével össze lehet rendelni a rendszerelemeket a szervezet folyamataival, így pontosan definiálni lehet, hogy mely rendszerelem kiesése mely folyamat végrehajtását akadályozza, így az egyes rendszerelemek esetében tartalékképzés, redundancia – „HA” - kialakításáról a folyamathoz kapcsolódó helyreállítási idő (RTO) és helyreállítási pont (RPO) alapján lehet dönteni.

Technológiai tanácsot leginkább a mentési követelmények tekintetében lehet adni, hiszen a mentések olvashatósága, visszatölthetősége elsődleges célja a mentések készítésének. Egyes megoldások automatizált backup és disaster recovery eszközökként, rendszeres snapshot-okat készítenek akár Google Drive-ra ingyen és tesztelik a helyreállítási időt (RTO/RPO). BCM (Business Continuity Management) szoftverek szimulálni tudják a kieséseket és generálnak riportokat a NIS2 üzletmenet-folytonossági tervekhez. Integráció felhő alapú IAM-mal (Identity Access Management) megakadályozza a jogosulatlan hozzáféréseket krízishelyzetben.

3.8 Azonosítás és hitelesítés

Azonosítók kezelése tekintetében – ugyan csak magas biztonsági osztálynál elvárt – minden szervezetnél javasolt, hogy amennyiben csoportfelhasználókat használnak, PAM rendszer segítségével egyedi hitelesítést vezessenek be a felhasználók számára mielőtt azok hozzáférnek a csoport által használt felhasználói fiókhoz. A fiókkezeléssel kapcsolatos elvárások tekintetében pedig e kontrollcsoportnál is elmondható, hogy az azonosítók kezeléséhez (pl.: státuszok kezelése) jelentős biztonsági osztály esetében egy központi címtár bevezetése lehet segítség, mellyel azon rendszereknél is lehetséges státuszok követése, melyek ezt a funkciót rendszeren belül nem biztosítják.

MFA (Többfaktoros hitelesítés):

- Alap biztonsági osztály: Kötelező a privilegizált (rendszergazda) fiókokhoz és a távoli hozzáféréshez.
- Jelentős biztonsági osztály: Kötelező minden felhasználó számára.

Javasolt megoldás: a VPN használata távoli hozzáférésnél, a VPN mögötti rendszereknél elfogadott, ha csak a VPN belépésnél van az MFA, nem kell minden egyes belső alkalmazásba külön beépíteni.

Egyéb elérések esetén, illetve webes rendszerek használata esetén másodlagos authentikátorok használata javasolt.

Jelszó alapú hitelesítés esetén – ugyan nem elvárt – rendkívüli módon segíti a szervezetek megfelelő jelszókezelését és a szabályok kikényszerítését egy központi címtár (AD, LDAP) megoldás használata, ugyanis jelenlegi tapasztalatunk alapján SSO megoldás nélkül a legtöbb rendszer még manapság sem rendelkezik megfelelően biztonságos és kikényszeríthető jelszókezelési felülettel.

Jelentős biztonsági osztály esetén egy központi címtár a tanúsítványkezelést is támogatja, hiszen akár a nyilvános kulcsú tanúsítványok (PKI) is tárolhatók ezen rendszerekben.

Jelszókezeléshez – kifejezetten az üzemeltetők és az informatikai terület más munkatársai számára, akik rengeteg privilegizált hozzáférést kezelnek de mások számára is – javasolt jelszókezelők használata melyeket javasolt szerveren vagy privát felhőben használni.

3.9 Biztonsági események kezelése

Magas szintű automatizáció megvalósításához SOAR (Security Orchestration, Automation and Response) megoldások automatizálják az incidensdetektálást, triázist és választ (pl. izolálás, értesítés). Ezek feldolgozzák a SIEM riasztásokat, playbook-okat futtatnak, és automatikusan jelentést generálhatnak a hatóságoknak. Loggyűjtő és -elemző eszközök biztosítják a 24 órás bejelentési kötelezettség betartását auditálható időpecsétes lenyomatokkal.

Mindezek mellett a legegyszerűbb megoldást itt – is – egy központi helpdesk rendszer tudja jelenteni, melybe a hibákat és az incidenseket bárki bejelentheti, illetve egyes monitoring eszközök is tudnak bele automatikus leveleket küldeni melyek hibajegyeket generálnak. Ezen dokumentált bejelentésekből lehet továbblépni incidenskezelésbe, és az incidensek részleteit, kivizsgálását és egy helyreállítás lépéseit e rendszerben egyben lehet rögzíteni, mely később tökéletes dokumentációként szolgálhat.

3.10 Karbantartás

A karbantartások kezelésre CMMS (Computerized Maintenance Management System) rendszerek adhatnak megoldást, melyek automatizálják a karbantartási ütemezést, munkalapokat generálnak és kezelik a dokumentációt.

Mindezek mellett a legegyszerűbb megoldást itt – is – egy központi helpdesk rendszer tudja jelenteni, melybe a karbantartásokat akár rendszeres feladatként lehet rögzíteni, a karbantartásokat, karbantartókat, karbantartási eszközöket lehet nyilvántartani, mely később tökéletes dokumentációként szolgálhat.

A távoli karbantartások megfelelő kezeléséhez a megfelelő távoli elérés (VPN), MFA, a távolról indított munkamenet naplózása és monitoringja szükséges, melyeket korábbi kontrollcsoportoknál már említettünk.

3.11 Adathordozók védelme

Adathordozók védelmére léteznek olyan megoldások melyek segíthetnek a cserélhető adathordozók kezelésében, megakadályozva az USB-meghajtókra, CD-kre és más tárolóeszközökre történő jogosulatlan adatátvitelt, közvetlenül kezelve az adatszivárgás kockázatát.

Amikor a szervezet az adathordozók titkosítására gondol, soha nem szabad elfelejteni a mobil eszközöket, mint laptopokat, telefonokat melyek elvesztése esetén MDM (Mobile Device Management) szoftver segítheti a távoli törlést.

Az adathordozók megfelelő törlésére több lehetséges szoftver is létezik, egyes szoftverek NIST, GDPR vagy egyéb megfelelőségi tanúsítvánnyal is rendelkeznek, így használatuk az egyes standardok szerint elfogadott.

3.12 Fizikai és környezeti védelem

A megfelelő fizikai védelem kialakításához minden biztonsági osztály esetén fontos megfelelő erre kiképzett szakember bevonása. Belépések naplózása, tűzvédelem, vízbetörésvédelem, mozgásérzékelős megfigyelés mind olyan elemek melyek megoldása több eszközzel is lehetséges.

A környezeti kontrollok megvalósításához EMS (environmental monitoring systems) és / vagy BMS (building management systems) rendszerek használhatók amennyiben tényleg precíz, azonnali visszajelzést szeretnénk.

3.13 Tervezés

A kontrollcsoport kezeléséhez nem tartozik technológiai elvárás, mivel az kifejezetten a biztonságtervezésről és a tervezett, valamint a megvalósított biztonság dokumentálásáról szól, központi szabályozási elemként a Rendszerbiztonsági terv (alap biztonsági osztály) illetve a kapcsolódó Információbiztonsági architektúra leírás (jelentős biztonsági osztály) elkészítéséről.

3.14 Személyi biztonság

A személybiztonság területén a technológiák helyett a központi szerepet a felhasználók háttérellenőrzése, és a dokumentációk megismertetése kapta. Ugyanakkor megjegyezzük, hogy e kontrollcsoportnál is megjelenik a felhasználók áthelyezésének, távozásának kezelése, mely esetekben a hozzáférés felügyeleti pontokat a Hozzáférés-felügyelet alfejezetben leírtak szerint javasoljuk kezelni. (Központi címtár használatával, folyamatkezelő rendszeren keresztül)

3.15 Kockázatkezelés

A **jelentős** biztonsági osztályú EIR-eknél elvárt automatizált sérülékenységvizsgálatot végző eszközök (melyekből létezik ingyenes verzió is, az NKI, illetve az MKIK is biztosít ilyen szolgáltatást a kapcsolódó szervezeteknek), valós idejű sebezhetőség-szkennelést végeznek hálózati eszközökön és alkalmazásokon, automatizálják a kockázati felméréseket és nyomon követést sablonokkal. Ezek integrálhatók SIEM rendszerekkel (melyből egyszerűbb funkciójú rendszerek szintén elérhetők ingyenesen) a fenyegetések prioritizálásához és kockázati pontszámok kiszámításához. Jegykezelő rendszerek, automatikus munkafolyamatokat indíthatnak kockázatcsökkentő akciókra, nyomon követve a javításokat időbélyegzővel.

A szervezeti szintű kockázatelemzés mely az alkalmazások / hálózatok sérülékenységein túlmutató fizikai és szervezeti kockázatokat is tartalmaz könnyen karbantartható excel fájl(ok)ban, a vezetők számára pedig egy összefoglaló jelentés elfogadása javasolt, melynek ki kell elégítenie ugyan a jogszabályi követelményeket ugyan, de nem ír elő menedzselhetetlen komplexitást.

A kockázatok elemzésére és a kockázatok kezelésének tervezésére természetesen erre kialakított speciális szoftverek is használhatók, ugyanakkor az adatbevitel ezekbe is manuálisan kell, hogy megtörténjen.

3.16 Rendszer- és szolgáltatásbeszerzés

A rendszerek és szolgáltatások beszerzése alapvetően egy adminisztratív folyamat. Amit kiemelnénk e témakörből az a fejlesztői tesztelések, változáskövetés megfelelő kialakítása. Ugyan ezen kontrollok kifejezetten a jelentős biztonsági osztálynál jelennek meg, de javasoljuk minden fejlesztés esetén alkalmazni ezeket.

Fejlesztői változáskövetéshez a folyamatmenedzsment vagy CMDB rendszerek ugyanúgy használhatók, mint az éles környezethez.

Fejlesztői biztonsági tesztelésekhez már elérhetők APPSEC eszközök (Application Security) melyek használatával a fejlesztői kódok már korán tesztelhetők az információbiztonság szempontjából

SAST eszközök (Static Application Security Testing)

Ezek az eszközök a program futtatása nélkül keresik a forráskódot, a futtatható kódot vagy a bináris fájlokat sebezhetőségek után kutatva. Ezek a legalkalmasabbak a szerkezeti hibák korai felismerésére.

SCA eszközök (Software Composition Analysis)

Az SCA eszközök harmadik féltől származó könyvtárakat és függőségeket vizsgálnak az ismert sebezhetőségek (CVE-k) és licenckockázatok észlelése érdekében.

DAST eszközök (Dynamic Application Security Testing)

A DAST eszközök kívülről tesztelik a futó alkalmazásokat, támadásokat szimulálva (mint például az SQL injekció vagy az XSS) a sebezhetőségek felkutatására.

És természetesen olyan eszközök is rendelkezésre állnak, melyek ezen elemeket vegyítve több szempontból is képesek tesztelni a fejlesztett rendszereket.

3.17 Rendszer- és kommunikációvédelem

Alap biztonsági osztályba vagy feljebb sorolt rendszerek védelmére elvárt a Ddos védelem kialakítása. A megvalósítása többrétegű megközelítést igényel, amely ötvözi a hálózati infrastruktúrát, a forgalomtisztítást és a viselkedéselemzést. A kulcsfontosságú lépések közé tartozik az erre specializálódott szolgáltatások használata – többnyire a megbízott internetszolgálató által biztosított -, a sebességkorlátozás megvalósítása, a webalkalmazás-tűzfalak (WAF) telepítése, valamint a CDN (Content Delivery Network) vagy Load Balancer szolgáltatások használata a forgalom elosztására és a volumetrikus támadások elnyelésére, gyakran mesterséges intelligencia által vezérelt mérséklést alkalmazva a valós idejű észleléshez.

Kriptográfiai kulcsok előállításához léteznek ingyenes szoftverek melyeket megfelelő konfigurációval – kulcs hossz, használt kulcs típusa - bárki használat (például GPG).

Határok védelme

Tűzfal megoldásként mind dedikált eszköz, illetve szoftveres megoldás is elfogadható amennyiben azt a jogszabály elvárásainak megfelelően konfigurálják.

Menedzselt interfészek kialakításához például BGP (Border Gateway Protocol), illetve DNS (Domain Name System) és egyéb felügyeleti protokollok használatók a hozzáféréseket kontrolláló (ACL) listák mellett

Forgalomáramlási szabályokat azon intelligens hálózati eszközökön kell beállítani, amelyek a forgalom útvonalát, biztonságát és sebességét kezelik.

A legfontosabb helyszínek és eszközök:

- Tűzfalak: A bejövő és kimenő forgalom szűrésére, engedélyezésére vagy tiltására.
- Routerek: Az adatcsomagok útvonalának meghatározására, forgalomirányításra.
- Switchek: Főleg a rétegzett (VLAN) forgalom kezelésére és a forgalom korlátozására (QoS).

A legtöbb speciális elvárás a jelentős biztonsági osztályba sorolt rendszerek esetében jelentkezik, e kontrollcsoportnál az alap és a jelentős biztonsági osztály esetén elég nagy technológiai ugrás történik.

Míg a tűzfal megakadályozza az illetéktelen hozzáférést a hálózathoz, a proxy szerver növeli az anonimitást, szűri a tartalmat és javítja a hálózati teljesítményt. Proxy szerverek használat esetén – jelentős biztonsági osztálytól - A webtartalom-szűrő az egyik leggyakoribb proxy szerver.

Megosztott csatornahasználat kivédésére megfelelően konfigurált VPN (biztosítva, hogy minden távoli forgalom áthalad a szervezet biztonsági rendszerein), illetve a hozzáférés kontroll (mely biztosítja, hogy a felhasználók nem módosíthatnak a hálózati beállításokon). A megosztott csatornahasználat detektálása megfelelő monitoring eszközökkel lehetséges, melyek figyelik a távoli forgalmat.

Az adatátvitel bizalmasságát és sértetlenségét olyan hálózati mechanizmusok által védhetjük, mint a TLS, HTTPS, és VPN.

Mobilkód használat blokkolására használható az automatikus indítás/automatikus lejátszás funkciók letiltása az operációs rendszer összetevőin, USB-meghajtókon, valamint az e-mail kliensek konfigurálása a mellékletek automatikus megnyitásának blokkolására.

A kommunikációs munkaszakaszok hitelességét a kijelentkezéskor érvénytelenített munkamenet-azonosítókkal lehet védeni, mely korlátozza egy támadók azon képességét, hogy később is használja a korábban érvényes munkamenet-azonosítókat.

Magas biztonsági osztályban már elvárt a biztonságos állapot fenntartása a rendszereknél, amelyet a forgalom blokkolásával, hálózati szegmensek elkülönítésével vagy a hálózati kapcsolatok megszakításával lehet elérni, melyek védik a rendszer a nyílt hozzáférés engedélyezése helyett.

3.18 Rendszer- és információsértetlenség

A rendszerek monitoringjának megoldására közepes és nagy rendszereknél is SIEM megoldások használhatók, melyek segítségével a szükséges megfelelési szintet el lehet érni.

Magas biztonsági osztályban, ahol a titkosított kommunikációs forgalom monitoringja és elemzése is elvárt, minimum megvalósítandó, hogy a releváns monitoring rendszer képes legyen mintázatok felismerésére és metaadatok értelmezésére, és használja ezeket a titkosított kommunikáció elemzésére. A teljes elemzéshez proxyszerver használata, illetve az adatok végcélnál történő elemzése segít.

3.19 Ellátási lánc kockázatkezelése

A kockázatelemzés és kockázatkezelés kivitelezése önmagában nem tér el a Kockázatkezelés alfejezetben leírtaktól.

Kifejezetten ellátási lánchoz kapcsolódóan ugyanakkor SBOM (Software Bill of Materials) eszközök használhatók, melyek automatikusan nyilvántartják a harmadik féltől származó komponenseket sebezhetőségekkel együtt. GRC szoftverben kezelt szerződésmenedzsment figyeli az automatikus auditigényeket. Értelemszerűen ezen eszközök fizikai elemekből álló rendszerelemekre használhatók (ahol a szoftver fizikai részeként a kódrészletet modult tekinthetjük).

Egyes szoftverek hitelességét termék kulcs, aktiválási kód vagy a szállító elektronikus aláírása, tanúsítványa segítségével ellenőrizhetjük, ugyanakkor jelenleg sajnos ilyen hitelesség ellenőrzésre adó elektronikus bizonyíték nem mindig van, ilyenkor a forrás megfelelő biztosításával van lehetőség egy termék hitelességének ellenőrzésére.