A GDPR FELKÉSZÜLÉS INFORMATIKAI KÉRDÉSEI

{ Az audit gyakorlati szempontjai

Sipos Győző *CISA* – IT biztonságtechnikai auditor

Mobil: +36 20 916 3541
E-mail: sipos.gyozo@nador.hu

Nádor RENDSZERHÁZ

SZÁMSZERŰSÍTETT KOCKÁZATOK

63%	Az adatlopások, támadások 63%-át a default, gyenge, vagy ellopott jelszavak tették lehetővé.
89 %	A visszaélések 89%-ának pénzügyi vagy adatszerzési motívuma van
72%	Az alkalmazottak közel háromnegyede tulajdonított már el adatot a munkahelyéről.
86%	A biztonsági visszaélések 86 %-át nem veszi észre az érintett szervezet, hanem harmadik fél figyelmezteti rá.
96%	Az esetek 96 százalékában megfelelő kontrollok alkalmazásával egyszerűen megelőzhető lett volna a visszaélés.

hvg.hu

2017. december. 11. 00:03 – Utolsó frissítés: 2017. december. 11. 13:38 TECH

Százezreket érinthet: mikrofonnal lehallgatták a vásárlókat és a kasszásokat a hazai OMV-kutakon

szerző:
hvg.hu

838
Ajánlom

Sokan felkapták fejüket a hírre, miszerint a maximális 20 millió forinthoz közeli bírságot szabta ki az adatvédelmi hatóság az OMV-re az elektronikus megfigyelőrendszereivel kapcsolatos adatvédelmi jogszabálysértések miatt.

Állampolgári panasz alapján indult az eljárás annak kapcsán, hogy OMV "a kockázatok elkerülése és a helyi lakosok biztonságának, valamint kárenyhítés biztosítása" érdekében az egyik töltőállomás kasszájánál a kamera mellé mikrofont is szereltetett. A Nemzeti Adatvédelmi és Információszabadsági

IT AUDIT SZABÁLYOZÁSI TÁMOGATÁSA

Milyen szabványi támogatás használható az informatikai biztonság értékeléséhez?

- MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonság irányítási rendszerek. Követelmények.
- NIST SP 800-53 Revision 4
- Ibtv. végrehajtási rendelete, 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

A GDPR RENDELET IT VONATKOZÁSAI

2. szakasz
Adatbiztonság
32. cikk
Az adatkezelés biztonsága

(1) Az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

Mi a kockázat?

Definíciós problémák! Milyen kockázatokról van szó?

- Mi az adott kockázat valószínűsége és súlya?
- Mi a kockázat mértékének megfelelő adatbiztonság?
- Hogyan vehetők figyelembe a megvalósítás költségei?

(83) …Az adatbiztonsági kockázat felmérése során a személyes adatok kezelése jelentette olyan kockázatokat – mint például a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés –mérlegelni kell, amelyek fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek.

A GDPR RENDELET IT VONATKOZÁSAI

A GDPR előírja:

a) a személyes adatok álnevesítését és titkosítását;

b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;

c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;

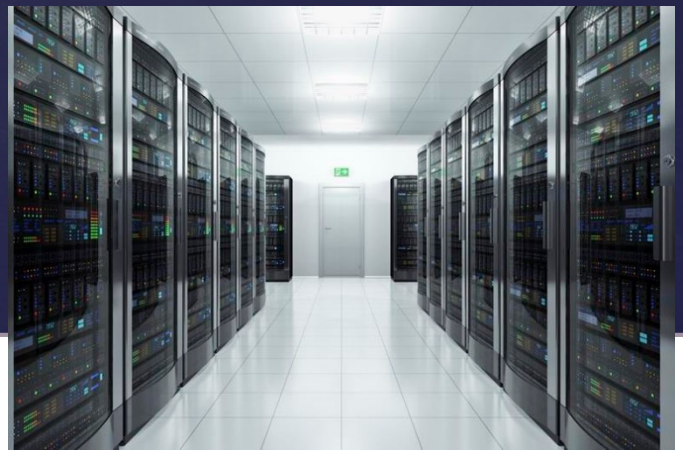
d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

ADATFELDOLGOZÓK

(81) …ha az adatkezelő adatfeldolgozót bíz meg az adatkezelési tevékenységek elvégzésével, csakis olyan adatfeldolgozókat vehet igénybe, amelyek megfelelő garanciákat nyújtanak – különösen a szakértelem, a megbízhatóság és az erőforrások tekintetében – arra vonatkozóan, hogy az e rendelet követelményeinek teljesülését biztosító technikai és szervezési intézkedéseket végrehajtják, ideértve az adatkezelés biztonságát is.

Az adatkezelő kötelezettségeit és felelősségét minden esetben részletekbe menően, szerződésben kell rögzíteni!

- Magatartási kódex (40. cikk)
- Jóváhagyott tanúsítás (42. cikk)



GYAKORLATI MEGKÖZELÍTÉS

SANS Institute: kutatási és oktatási szervezet.

- SANS Top 20 kritikus biztonsági kontroll

OWASP – webalkalmazások biztonsága

- OWASP Top 10

20 KRITIKUS BIZTONSÁGI KONTROLL

kibev
Önkéntes kibervédelmi összefogás
voluntary cyber defence collaboration

A 20 kritikus kontroll költséghatékony számítógépes és hálózati védelmet tesz lehetővé, mérhetővé, skálázhatóvá és megbízhatóvá téve a folyamatokat a teljes (USA) kormányzaton belül, a védelmi iparágban és egyéb olyan szervezeteknél, amelyeknek védendő információi és rendszerei vannak. A kontrollok az aktuális fenyegetések alapján készültek. A kiválasztás a nagy kormányzati szervezetek konszenzusa alapján történt, mely szervezetek aszerint védekeznek a kibertámadások ellen, hogy mely kontrollok a legkritikusabbak az ismert támadások elleni védekezésben.

Az anyag meghivatkozza az Ausztrál védelmi hivatal hasonló tartalmú dokumentumát, a NIST 800-53 anyagát, vagy éppen a brit Nemzeti Infrastruktúra Védelmi Központ (CPNI) kapcsolódó tanácsait.

A poszter célja, hogy összefoglalva felvillantsa azokat a kontrollokat, melyek a leghatékonyabban járulhatnak hozzá a szervezet védelméhez. Egyben rangsorolja is a potenciális támadásokat, és a támadáshoz szükséges tudást, ill. sikeres támadás esetén a támadás hatását. Ezek alkalmazása, ill. a saját szervezetre történő átültetése megkerülhetetlen, jelen anyag csak segítség abban, hogy a fontos dolgokra felhívja a figyelmet.

Ez a poszter a '20 Critical Security Controls' című, a www.sans.org/critical-security-controls oldalon elérhető SANS publikáció esetenként módosított változata, amelyet az Önkéntes Kibervédelmi Összefogás (KIBEV) tagjai fordították magyar nyelvre.

A 20 kritikus kontroll automatizálásában rejlő értékek bizonyítékai

[illegible]

Domestic Sites
Foreign Sites
Google - Aurora Attack

20 kritikus biztonsági kontroll			Az amerikai Nemzetbiztonsági hivatal értékelése a 20 kritikus biztonsági kontrollról				Kapcsolódó NIST speciális publikáció 800-53, Revision 3, Priority 1 Kontrollok
	A kritikus biztonsági kontroll megnevezése	A kritikus biztonsági kontroll leírása	Fontosság	Hatása egy támadás sikerességére	Függőségek	Technológiai érettség	
1	Jogosult és jogosulatlan eszközök leltára	[illegible]	1	Nagyon magas	Alapvető	Magas	CM-8 (a, c, d, 2, 3, 4) PM-5, PM-6
2	Jogosult és jogosulatlan szoftverek leltára	[illegible]	1	Nagyon magas	Alapvető	Magas	CM-1, CM-2 (2, 4, 5), CM-3, CM-5 (2, 7), CM-7 (1, 2), CM-8 (1, 2, 3, 4, 6), CM-9 PM-6, SA-6, SA-7
3	Biztonságos beállítások hardvereken és szoftverekben laptopokra, munkaállomásokra és szerverekre	[illegible]	1a	Nagyon magas	Adottság	Magas	CM-1, CM-2 (1, 2), CM-3 (b, c, d, e, 2, 3), CM-5 (2), CM-6 (1, 2, 4), CM-7 (1), SA-1 (a), SA-4 (5), SI-7 (3), PM-6
4	Folyamatos sebezhetőségi felmérés és felszámolás	[illegible]	1a	Nagyon magas	Adottság	Magas	RA-3 (a, b, c, d), RA-5 (a, b, 1, 2, 5, 6)
5	Rosszindulatú kód elleni védekezés	[illegible]	1a	Magas / közepes	Adottság	Magas / közepes	SC-18, SC-26, SI-3 (a, b, 1, 2, 5, 6)
6	Alkalmazói szoftverek biztonsága	[illegible]	2	Magas	Adottság	Közepes	CM-7, RA-5 (a, 1), SA-3, SA-4 (3), SA-8, SI-3, SI-10
7	Vezetéknélküli eszközök felügyelete	[illegible]	2	Magas	Adottság	Közepes	AC-17, AC-18 (1, 2, 3, 4), SC-9 (1), SC-24, SI-4 (14, 15)
8	Adatvisszaállítási képesség	[illegible]	2	Közepes	Adottság	Közepes	CP-9 (a, b, d, 1, 3), CP-10 (6)
9	Biztonsági ismeretek felmérése és megfelelő képzés a hiányosságok pótlására	[illegible]	2	Közepes	Adottság	Közepes	AT-1, AT-2 (1), AT-3 (1)
10	Biztonságossá kell tenni a hálózati eszközök, tűzfalak, router-ek és switch-ek konfigurációját	[illegible]	3	Magas / közepes	Adottság / Függő	Közepes / alacsony	AC-4 (7, 10, 11, 16), CM-1, CM-2 (1), CM-3 (2), CM-5 (1, 2, 5), CM-6 (4), CM-7 (1, 3), RA-5, IA-2 (1, 6), IA-5, IA-8, SC-7, SC-7 (2, 4, 5, 6, 8, 11, 13, 14, 18)
11	Korlátozott és ellenőrzött hálózati portok, protokollok és szolgáltatások	[illegible]	3	Magas / közepes	Adottság / Függő	Közepes / alacsony	CM-6 (a, b, d, 2, 3), CM-7 (1), SC-7 (4, 5, 11, 12)
12	Rendszergazdai jogosultságok ellenőrzött használata	[illegible]	4	Magas / közepes	Függő	Közepes	AC-6 (2, 5), AC-17 (3), AC-19, AU-2 (4)
13	Határvédelem	[illegible]	4	Magas / közepes	Függő	Közepes	AC-17 (1), AC-20, CA-3, IA-2 (1, 2), IA-8, RA-5, SC-7 (1, 2, 3, 8, 10, 11, 14), SC-18, SI-4 (c, 1, 4, 5, 11), PM-7
14	Karbantartás, ellenőrzés és a biztonsági naplók elemzése	[illegible]	4	Közepes	Függő	Közepes	AC-17 (1), AC-19, AU-2 (4), AU-3 (1, 2), AU-4, AU-5, AU-6 (a, 1, 5), AU-8, AU-9 (1, 2), AU-12 (2), SI-4 (8)
15	Hozzáférés-kezelés a „szükséges és elégséges" elv alapján	[illegible]	4	Közepes	Függő	Közepes / alacsony	AC-1, AC-2 (b, c), AC-3 (4), AC-4, AC-6 MP-3, RA-2 (a)

Nádor RENDSZERHÁZ

www.nador.hu I Tel.: + 36 1 470-5000 I info@nador.hu

A kritikus biztonsági kontroll megnevezése	A kritikus biztonsági kontroll leírása
1 Jogosult és jogosulatlan eszközök leltára	**Csökkenteni kell a támadók lehetőségét, hogy jogosulatlan vagy védtelen rendszereket találhassanak és használhassanak ki:** Aktív feltérképező és beállításkezelő rendszert kell alkalmazni, hogy naprakész leltárral rendelkezzünk a vállalati hálózathoz csatlakozó eszközökről, beleértve a szervereket, az asztali gépeket, a hordozható számítógépeket és a távoli eszközöket.
2 Jogosult és jogosulatlan szoftverek leltára	**Azonosítani kell a sebezhető vagy rosszindulatú szoftvereket, hogy csökkentsük vagy kizárjuk a támadásokat:** Készíteni kell minden rendszer esetében egy engedélyezett szoftvereket tartalmazó listát, és ki kell alakítani egy eszközparkot a telepített szoftverek nyomon követésére (beleértve a típusát, verziószámát és a kiegészítő frissítéseket), és figyelni kell a jogosulatlan vagy szükségtelen szoftvereket.
3 Biztonságos beállítások hardvereken és szoftverekben laptopokra, munkaállomásokra és szerverekre	**Meg kell előzni, hogy a támadók hálózatokon vagy böngészőkön keresztül könnyű elérést biztosító szolgáltatásokat vagy beállításokat használjanak ki:** Biztonságos telepítőkészletet kell létrehozni, melyet az újonnan telepítendő rendszerekre lehet alkalmazni, ezt biztonságos tárhelyen kell elérhetővé tenni, időnkénti ellenőrzéssel és frissítéssel, és egy beállítás-kezelő rendszerbeni nyomon követéssel.
4 Folyamatos sebezhetőségi felmérés és felszámolás	**Kezdeményező módon kell azonosítani és javítani a biztonsági kutatók vagy szállítók által jelentett szoftver sebezhetőségeket:** Rendszeres időközönként automatikus sebezhetőség-vizsgáló alkalmazásokat kell futtatni minden rendszerrel szemben, és gyorsan fel kell számolni minden sebezhetőséget, a kritikusakat 48 órán belül.
5 Rosszindulatú kód elleni védekezés	**Meg kell akadályozni, hogy rosszindulatú kódok befolyásoljanak rendszerbeállításokat és tartalmakat, érzékeny adatokat szerezzenek meg, vagy terjedjenek:** Vírus és kémprogramok elleni automatikus védelmet kell alkalmazni a munkaállomások, szerverek és mobil eszközök folyamatos figyelése és védelme érdekében.
6 Alkalmazói szoftverek biztonsága	**Semlegesíteni kell a Web-alapú és egyéb szoftver termékek sebezhetőségeit:** Gondosan tesztelni kell a belső fejlesztések és a harmadik fél által fejlesztett alkalmazások biztonságát, beleértve a fejlesztői hibákat és a rosszindulatú kódokat is. Olyan Web-alkalmazás tűzfalat kell telepíteni, amely minden forgalmat vizsgál és minden felhasználói adatot hibaellenőrzésnek vet alá (az adat megfelelő méretét és típusát egyaránt vizsgálva).
7 Vezetéknélküli eszközök felügyelete	**Védeni kell a biztonsági határvonalat a jogosulatlan vezeték nélküli hozzáférésektől:** Csak akkor szabad engedélyezni a vezeték nélküli csatornán kapcsolódni szándékozó eszközöket, ha azok engedélyezett beállítással és biztonsági profillal rendelkeznek, és dokumentált tulajdonoshoz rendelve valamilyen üzleti igényt elégítenek ki.
8 Adatvisszaállítási képesség	**A támadásból származó károk minimalizálása:** Megbízható terv megvalósítása, ami alapján egy támadás informatikai rendszerekre gyakorolt hatásait meg lehet szüntetni. Automatikusan menteni kell minden információt, amire az egyes rendszerek teljes helyreállítása során szükség lehet, beleértve az operációs rendszert, az alkalmazást és az adatokat. Minden rendszerről készüljön legalább heti mentés, az érzékeny rendszerekről ennél gyakrabban. Rendszeresen tesztelni kell a visszaállítási eljárásokat.
Biztonsági ismeretek	

KIEMELT KOCKÁZATOK

Ami nem maradhat ki az auditból:

- Távmunka, mobil eszközök
- Privilegizált hozzáférések
- Rosszindulatú programok elleni védelem (vírus és malware)
- Adatszivárgás, távozó munkatársak jogosultságai
- Adathozzáférések naplózása

Kérdése van? Tegye fel!