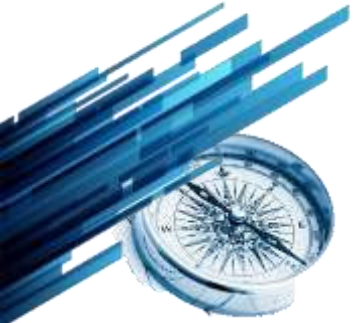
NIS2 kihívásai az auditor szemével – Tippek, Trükkök, Biztonsági csemegék

SIPOS GYŐZŐ
IT Biztonsági tanácsadó, CISA, CDPSE, ISO27LA
Adatvédelmi és adatbiztonsági jogi szakokleveles szaken
sipos.gyozo@nador.hu

Nádor 30 éve RENDSZERHÁZ

KIBERTAN TV. – ÜTEMEZÉS

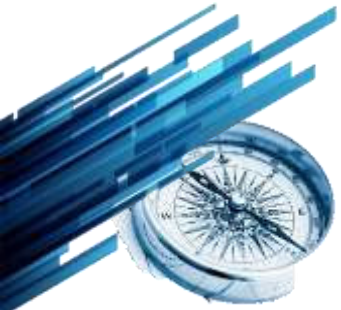


Nádor RENDSZERHÁZ 30 éve

INFORMÁCIÓK, HATÓSÁGI TÁJÉKOZTATÓK

- A **Szabályozott Tevékenységek Felügyeleti Hatósága** (a továbbiakban: SZTFH) honlapja
  - Felsorolva a Kibertan. tv., a kiadott két SZTFH rendelet a tanúsításról, továbbá megemlítve az Ibtv. és végrehajtási rendelete, a 41/2015. BM rendelet, továbbá az IBF képzésről szóló 26/2013 KIM rendelet. Ez utóbbi kettő még változatlan, nincsenek NIS2-es vonatkozásai;

- **Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet** (NBSZ NKI)
  - „A NIS irányelv implementációja által érintett jogszabályok”, 14 elemű felsorolás. Kiemelendő a létfontosságú rendszerelemekre (kritikus infrastruktúra) vonatkozó jogszabályok és az eseménykezelő központra és a sérülékenység vizsgálatokra vonatkozó szabályozások. Ezen jogszabályok módosításra várnak.



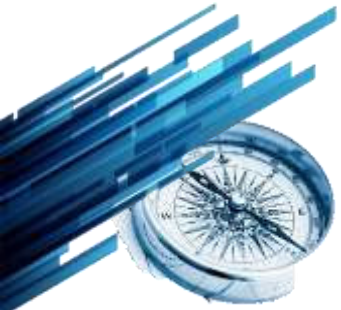
JELENLEGI HAZAI JOGSZABÁLYOK

- A kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény (Kibertan. tv.)
- A nemzeti kiberbiztonsági tanúsító hatóság eljárásával összefüggő kiberbiztonsági tanúsítás keretében fizetendő igazgatási szolgáltatási díjról szóló 30/2022. (II. 14.) SZTFH rendelet
- Információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló 10/2023. (V. 15.) SZTFH rendelet

- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) (Már számos változás történt a NIS2 miatt)
- 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 szóló 41/2015. (VII. 15.) BM rendelet (Ibtv. vhr.)

KÉSLEKEDŐ SZABÁLYOZÁS

- A vonatkozó jogszabályok egy részét még ebben az évben ki kell adni, mivel a kibertan. tv. előírja a hatósági regisztrációt, az IBF kinevezését vagy megbízását, a biztonsági osztályba sorolást, 2024 január 1-től. Az SZTFH elnökének hatásköre a szervezeti regisztráció rendeletben történő szabályozása.
  A polgári nemzetbiztonsági szolgálatok irányításáért felelős miniszter rendeletben meghatározza a biztonsági osztályba sorolás követelményeit, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedéseket.
- A törvénymódosításokat az Országgyűlés tavaszi ülésszakán tervezik elfogadni.



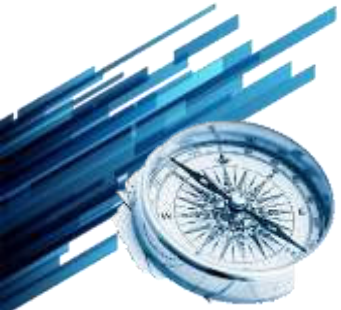
AKKOR NEM IS KELL SEMMIT TENNÜNK…

…mert nincsenek meg a jogszabályok.

NEM IGAZ! El kell kezdeni a felkészülést, mert sok követelménynek kell megfelelni. Igaz, a részletszabályozások nem állnak rendelkezésre, de irányadó az Ibtv. és a 41/2015 BM rendelet (mely átdolgozás alatt van).

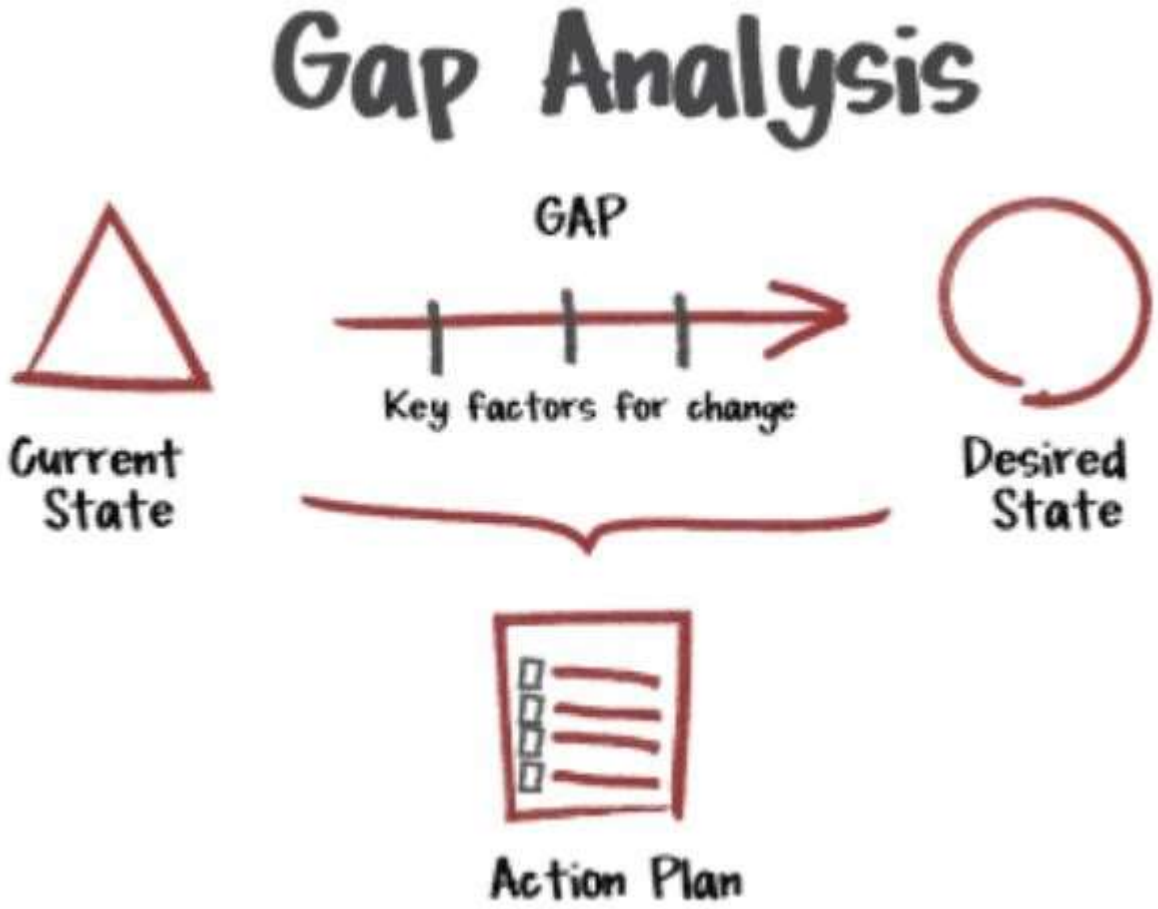
Az információbiztonság irányítási keretrendszerek követelményei is hasonlók, pl.

- Ibtv.
- ISO 27001
- NIST 800-53
- PCI DSS
- COBIT
- stb.



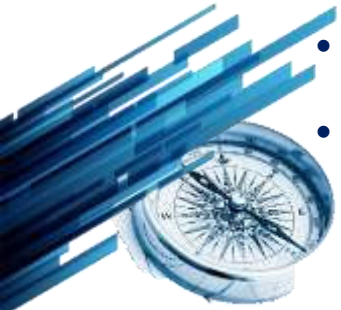
FELMÉRÉS

- GAP analízis
- Ütemterv
- Költségtervezés
- Szükséges napok: 2-4 nap



FELKÉSZÍTÉS

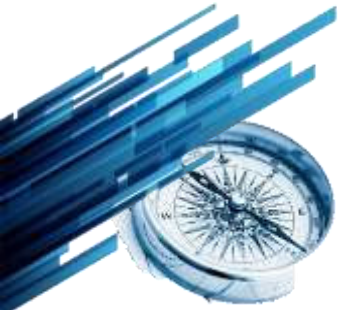
- Biztonsági osztályba sorolás támogatása
- Nyilvántartásba vételi dokumentációk elkészítése
- Információbiztonsági Felelős biztosítása
- IT Biztonsági szabályzatok elkészítése
- Incidenskezelési eljárások megalkotása, azok kialakításának támogatása (megelőzés, észlelés, reagálás, jelentés)
- BCP / DRP folyamatok kialakításának támogatása, szabályzatok elkészítése, tesztelés
- Ellátási lánc biztonsága – beszerzési folyamatok átalakítása, eljárások, követelmények megfogalmazása
- Sebezhetőségi vizsgálatok elvégzése – nem auditált
- Kiberbiztonsági kockázatelemzés és információs rendszerekre vonatkozó biztonsági szabályok kialakítása, kockázatkezelési intézkedések és eljárások kialakítása
- IT biztonságtudatossági képzések
- Szükséges napok: 25-60 nap



HATÁRIDŐK

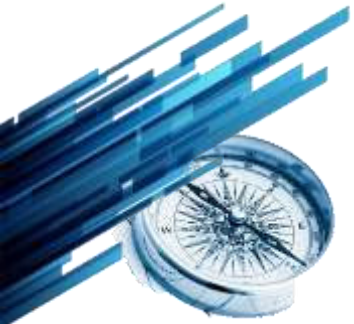
- Szervezeti regisztráció, nyilvántartásba vétel legkésőbb 2024. június 30-ig;
- A rendeletben meghatározott konkrét védelmi intézkedéseket 2024. október 18-tól kell alkalmazni;
- A kiberbiztonsági audit elvégzésére a hatósági nyilvántartásban szereplő auditorral megállapodást kell kötni, 2024. december 31-ig;
- Az első kiberbiztonsági auditot 2025. december 31-ig köteles elvégeztetni az érintett szervezet.

Ha még nem is történt meg a külső, hivatalos audit, a szervezetnek már 2024. október 18-tól biztosítani kell a teljes körű információbiztonsági megfelelőséget, a mulasztás hatósági eljárást, bírságot vonhat maga után!



Tippek, Trükkök, Biztonsági Csemegék

- Mentés –offline mentés fontossága, tesztelés
- Mentés csak a felhőbe? 27001-ben megjelenő új követelmény is
- BCP / DRP – kapacitás tervezés, képzés, tesztelés,
- Felhasználó menedzsment, kommunikáció
- Frissítések
- Zsarolóvírusok
- Közösségi média veszélyei
- Felhasználói hozzáférések korlátozása, internet elérés



NEMRÉGIBEN…

index

USD 402,39 Ft ▲ OTP 9 930 Ft ▼ 5 °C
GBP 459,09 Ft ▼ MOL 2 658 Ft ▲ 10 °C

BELFÖLD | KRÉTA | ADATHALÁSZAT | ADATBÁZIS | KÖZOKTATÁS

Adathalász támadás érte a KRÉTA-t

HORVÁTH TIBOR
+ KÖVETÉS

2022.11.07. 20:22

A diákok összes, a KRÉTA-ban kezelt adata kiszivároghatott, de nemcsak ezekhez, hanem a cég más adatbázisaihoz és a forráskódokhoz, illetve a fejlesztők belső kommunikációjához is hozzáférhettek.

A KRÉTA RENDSZER MEGTÁMADÁSA

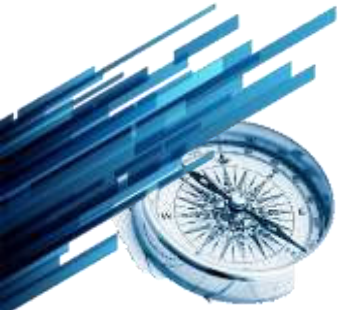
A KRÉTA mára egy komplett közoktatási informatikai rendszerré duzzadt. Összesen húszféle modul és különféle alkalmazások tartoznak hozzá, többek között olyan szolgáltatásokkal, mint az az e-napló, e-ellenőrző, intézményi adminisztrációs rendszer, digitális kollaborációs tér, e-ügyintézés, illetve egészségüggyel, étkeztetéssel, gazdálkodással, HR-ügyekkel kapcsolatos adminisztráció.

A KRÉTA A DIÁKOK ÉS A TANÁROK SZINTE MINDEN ADATÁT TARTALMAZZA VALAMILYEN MODULJÁBAN. EZ ALAPJÁN EGÉSZEN KIDOLGOZOTT PROFIL IS ALKOTHATÓ LENNE EGY-EGY DIÁKRÓL.

A FEJLESZTÉSRE RÁLÁTÓ FORRÁS SZERINT VALÓBAN TÖRTÉNT ADATHALÁSZ TÁMADÁS: EGY PROJEKTVEZETŐ KATTINTOTT EGY FERTŐZÖTT LINKRE EGY ÁTVERŐS E-MAILBEN, AZ Ő ADATAIT MEGSZEREZVE FÉRHETTEK HOZZÁ BELSŐ ADATBÁZISOKHOZ.

TANULSÁGOK A KRÉTA ESETÉBŐL

- Alkalmazzuk a „need-to-know” vagy „Least privilege” elvet,
- „Segregation of duty” jogosultságok szétválasztása, összeférhetetlenség,
- Kötelező az adminisztrátori funkciók és az office jellegű tevékenység szétválasztása,
- Felhasználói oktatás, tudatosítás,
- Legnagyobb veszély az ember (felhasználó, rendszergazda)



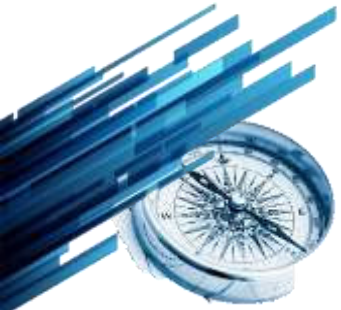
ZSAROLÓVÍRUSOK, VÉDEKEZÉS

- Zsarolóvírus támadások, leállások, hazai események:
  - autó alkatrész szállító cég
  - informatikai szállító
  - önkormányzatok
  - kórházak
  - stb.

Sokszor kiberfegyvernek fejlesztett alkalmazások (lásd: Stuxnet), de kereskedelmi forgalomban is vásárolható zsarolóvírus, vagy célzott támadás. Adattitkosítás és adatlopás egyszerre.

<u>Főbb okok:</u>

- sebezhető, nem frissített rendszerek
- kompromittálódott hitelesítő adatok
- megtévesztő e-mailek



ZSAROLÓVÍRUSOK, VÉDEKEZÉS

- **Mentés, mentés, mentés**. 3-2-1!
  Legyen legalább három másolat, 2 féle adathordozón, 1 másolat külső helyszínen (leválasztva a hálózatról) A legkorszerűbb zsarolóvírusok már megkeresik a mentéseket a hálózaton belül és visszavonhatatlanul letörlik azokat. Vigyázat! A vírusok sokszor már a támadás megtörténte előtt rejtőzködnek a hálózaton.
- Hatékony és tesztelt DRP/BCP, több helyen tárolt dokumentációval
- Szigorú jelszó politika, többfaktoros hitelesítés
- Hálózati szegmentálás, tűzfalak
- Felügyeleti rendszer, hálózati monitoring
- Oktatás, oktatás, oktatás!

VÍRUSOK MINDENÜTT

- Kapunk egy üzenetet: „XY megjelölt, hogy itt volt veled és további X személy társaságában. Az idővonaladhoz való hozzáadáshoz kattints az Idővonal felülvizsgálata hivatkozásra”
- Az üzenethez egy ígéretes videó is tartozik, ha valaki erre kattint, akkor elindítja a lavinát
- A vírus hasonló üzenetet küld valamennyi, a címlistájában szereplő személynek
- Megfertőzi a böngészőt, úgyhogy azzal már el sem lehet távolítani ezeket a hivatkozásokat - csak a böngésző újra telepítése segít

MEGFONTOLT KATTINTÁSOK

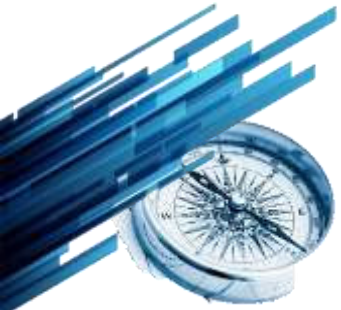
- Ismét: felhasználói tudatosítás, képzés!
- Javasolt az internet elérés korlátozása, kizárólag a szükséges szakmai tartalom legyen elérhető!
- Az ártatlannak tűnő tartalmak is rejthetnek veszélyt!

USA, Új Mexikó állam, napfizikai obszervatórium


A mysterious solar
array of co
The Sun
without p
know why.
sparking an
ies.
ated
ems to
closed and evacuated Sept. 6 due
risk. Federal officials aren't saying why it was
silence has led to international media coverage
plenty of speculation.
job
ot
are not

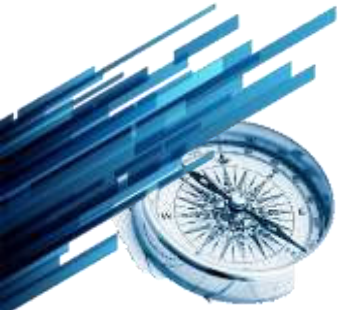
Az FBI vizsgálat igazi oka

- Az FBI gyermek pornográfia ügyében indított vizsgálatot. Egy pedofil hálózat egyik központjára mutattak a nyomozás eredményei.
- A vizsgálat idejére, 10 napra a teljes csillagvizsgálót kiürítették, még a közeli postahivatalt is lezárták.
- A gyanúsított egy karbantartó volt, akinek a gépén megtalálták a képeket. A nyomozók az objektumon belül a WiFi jeleket bemérve azonosították az elkövetőt.



TANULSÁGOK, MEGELŐZÉS

- Belső WiFi hálózat ellenőrzése, hálózat monitoring
- Internet hozzáférés szabályozása
- Hozzáférés ellenőrzés
- Naplózás, logelemzés



KÖSZÖNÖM A FIGYELMET!