SZABÓ ZOLTÁN
EIV, ISO 27001 LA

FORTIX Consulting – vezető tanácsadó

Tapasztalat:

- *Kritikus rendszerelemek védelme*
- *IBF*
- *PCI-CP és PCI-DSS*
- *Pénzügyi szervezetek*
- *NIS 2*

- *Saferinternet*


adminisztráció
!?

Volt egyszer egy NIS …

NIS 2

gyakorlati tapasztalatok

2022. december 27 (hatályba 2023. január 16-án lépett)
2024. október 17-ig a tagállamoknak át kell ültetniük a saját jogrendszerükbe, mely szabályozások **kötelező** érvényűek az érintett szervezetek számára.

https://eur-lex.europa.eu/eli/dir/2022/2555

NIS 2 - az EU ’22 decemberében elfogadta a korábbi, 2016-os Network and Information Security (NIS) irányelv módosítását a NIS 2-t, kötelezően magasabb felkészültséget írva elő a kiberbiztonság területén az Uniós országokban.

- Kockázatarányos védelem, ISMS kialakítása
- Incidenskezelés folyamata, kommunikációja
- Üzletmenet folytonosság biztosítása
- Ellátási lánc védelme

Üzenet annak, aki elvileg mindent jól csinál:
Nem elég biztonságosnak lenni, annak is kell látszani.

Alapvető elemek

Nemzeti CSIRT (NKI)

Kockázatarányos biztonsági intézkedések

Vezetés felelőssége, oktatások

10M € v. 7M €
2% v. 1,4%


AZ AUDIT ELŐTT SZÉPÉ TESSZÜK AZ IRODÁT.
HOLNAP A SZERVERSZOBA JÖN.

Az irányelv hatálya:

Alanyi hatálya:

alapvető szerveztek /kiemelten kritikus ágazatok/

Energia, ivóvíz, közigazgatás…digitális szolgáltatások … világűr.

fontos szervezetek /egyéb kritikus ágazat/

postai és futárszolgáltatások, hulladékgazdálkodás, gyártás (számtech, orvostechnika, gépjármű) …

Az irányelv hatálya
méret

Szervezet méretétől függően a közép és

nagyvállalatok:

Több mint 50 fő foglalkoztatott
10 M €

„Azon önálló vállalkozások elektronikus információs rendszereire vonatkozik a törvény, melyek minimum 50 fő alkalmazottal rendelkeznek vagy éves nettó árbevételük meghaladja a 10 millió eurónak megfelelő forintösszeget”

De a szervezet elvárhatja a beszállítóktól a tanúsítást és az irányelvnek történő megfelelést, így kisebb, akár mikrovállalkozás is válhat az irányelv alanyává!

Aki mindenképp
a méretkorláttól függetlenül az irányelv hatálya alá tartoznak:

Nyilvános elektronikus hírközlés, bizalmi szolgáltatók, TLD-nyilvántartók, DNS szolgáltatók, domainnév nyilvántartók;
Kritikus szervezetek a CER (2022/2557 EU) irányelv alapján azonosítva;
Köz-szempont: szolgáltatás zavara jelentős hatású lehet a közvédelemre, közegészségre, közbiztonságra;
Közigazgatási szerv: nemzeti jog alapján;
Különös fontosságú: nemzeti vagy regionális szinten;
Egyetlen szolgáltatásnyújtó: szolgáltatása a kritikus társadalmi vagy gazdasági tevékenységek fenntartásához elengedhetetlen.


Írja már alá a biztonság-
tudatossági oktatást Mari néni
mert megbukunk az auditon.

A NIS 2-irányelv célja a kiberreziliencia növelése!

- a biztonsági követelmények megerősítése,
- az ellátási láncok biztonságának figyelembevétele
- a jelentési kötelezettségek

A rendelet kockázatarányos védekezést vár el mind technológiai, mind szabályozás téren, a rendszerek és környezet biztonsági szintbe sorolását várja el. (**3 szintű skála**)

Érintett szervezet feladatai

Önazonosítás, nyilvántartásba vétel-re bejelentkezés – **2024.01.01-től 06.30-ig**.
Biztonsági osztályba sorolás – **2024.01.01-től,** de nem ugrik a nyakunkba senki, hiszen a részletszabályok még nem ismertek.
Elektronikus információs rendszerek biztonságáért **felelős személy kijelölése** – **2024.01.01-től**,
KOCKÁZATARÁNYOS Védelmi intézkedések bevezetése – folyamatosan
Felügyeleti díj megfizetése Hatóság felé – **2024.10.18-ig**. (0,015% / max. 10mHUF)
Első kiberbiztonsági audit vonatkozásában **szerződéskötés auditorral** – **2024.12.31-ig**
Első kiberbiztonsági audit lefolytatásának határideje – 2025.12.31-ig

A NIS 2-irányelv célja a kiberreziliencia növelése!

- A cégvezetés többlet felelősségének nyomatékosítása
- Információbiztonsági irányítási rendszer működtetése
- Kockázatelemzési és kezelési folyamatok fenntartása, védelmi intézkedések a kockázatok csökkentésére
- Incidenskezelési folyamat működtetése
- Üzletmenet-folytonosság erősítése
- Személyi- és fizikai biztonság
- Biztonságtudatosság növelése
- Ellátási láncok biztonságának növelése

A rendelet kockázatarányos védekezést vár el mind technológiai, mind szabályozás téren, a rendszerek és környezet biztonsági szintbe sorolását várja el. (**3 szintű skála**)


MAGA LESZ AZ IBF...
DE MIÉRT?!
A TEHETSÉGE MEGVA
LÁTTAM HOGY AZ FKERES() FÜGGVÉNYT HASZNÁLJA.

FORTIX

Hatóság

SZTFH

*Szabályozott Tevékenységek Felügyeleti Hatósága

Az Országgyűlés megszavazta a 2021. évi XXXII. törvényt, mely a Szabályozott Tevékenységek Felügyeleti Hatóságának 2021. október 1-jei megalakulását – szerencsejáték, bányafelügylet…

és….

Magyar Közlöny 2023. évi 72. szám – kibertanúsítási rendelet - 23/2023 Kibertan tv.

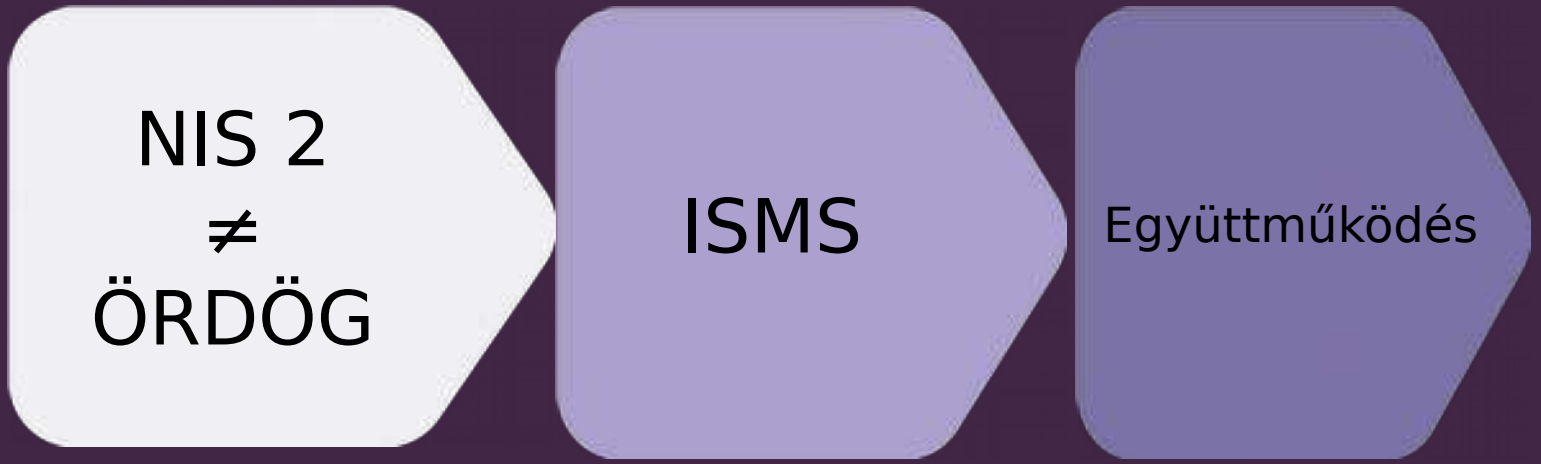
- **Tanúsítási rendszer kialakítása és fejlesztése**
- **Szintekhez tartozó elvárások meghatározása, értékelése – alap / jelentős / magas**
- **A tanúsítás felügyelete – tanúsító szervezetek koordinálása és nyilvántartásba vétele**
  - **szolgáltatási díj**
  - **kötelező tanúsítási szerződés**
- **Hatósági és rendkívüli ellenőrzések**

Mit csinál az auditor?

- Személyes interjúk
- Sérülékenységtesztek
- Vizuális ellenőrzések, műszaki helyszíni vizsgálatok
- Adatok, dokumentumok elemzése, írásbeli információkérés

Az elkészülő kiberbiztonsági audit jelentést az auditor az érintett mellett **a Hatóság részére is** megküldi. A Hatóság az audit jelentés alapján folytathat további vizsgálatot is.


HOGY LEHET AZ RTO TÖBB MINT EGY HÉT?!
AZ UTOLSÓ NAGYOBB LEÁLLÁSNÁL ÖRÖMTÜZEK GYÚLTAK ORSZÁGSZERTE...
IT


NIS 2
≠
ÖRDÖG
ISMS
Együttműködés

Köszönöm a figyelmet!