NIS2 AUDIT

Minden, amit tudnod kell a megfeleléshez

BALASYS

Mikrohálló

Agenda

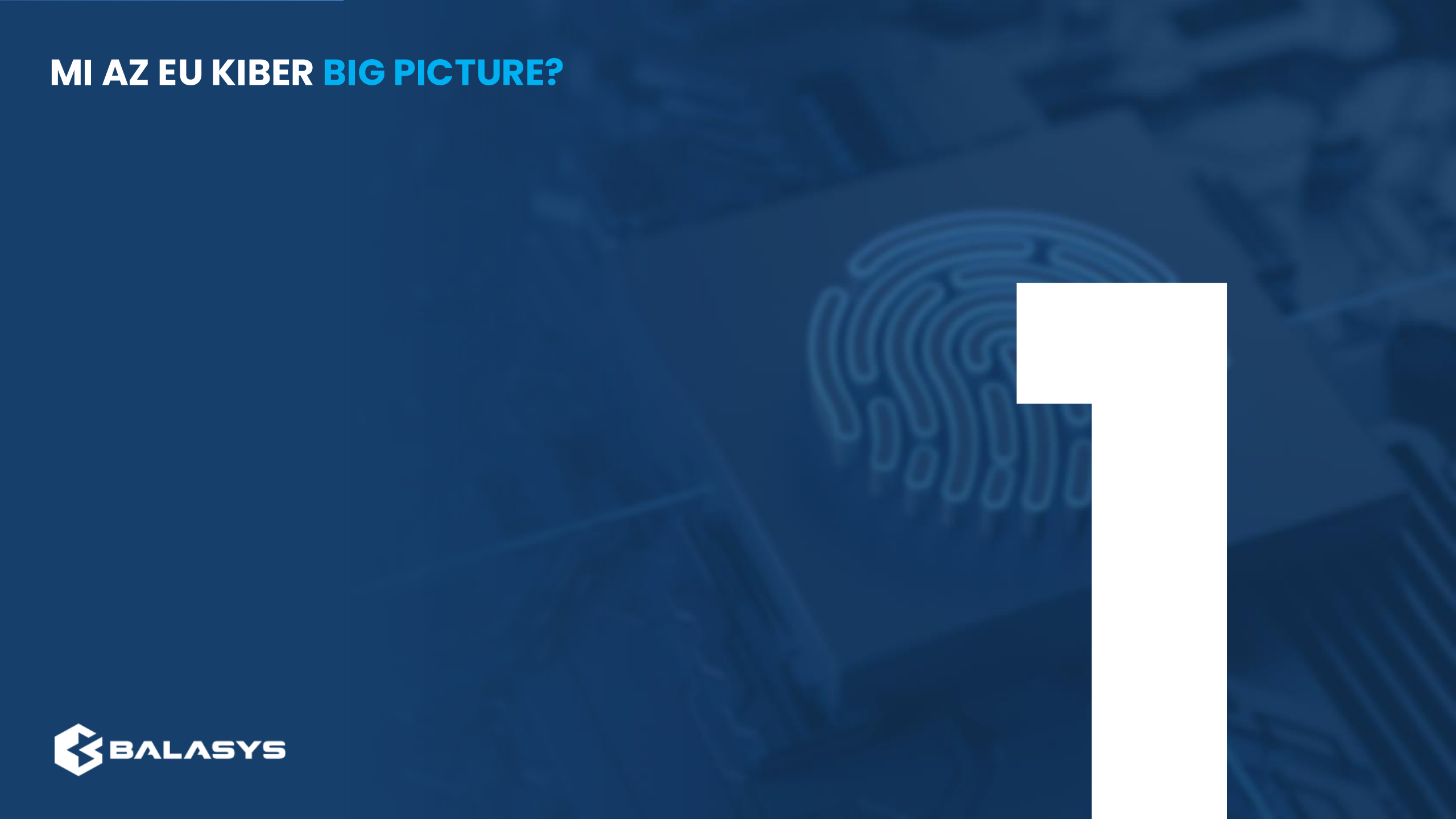
A Balasys előadásában a NIS2-t a gyakorlati, végrehajtandó és szállítandó elemek irányából vizsgáljuk.

Az megfelelés mellett rövid betekintést adunk az EU és ENISA stratégiáiba, mellyel egy időtálló rendszert tervezhetünk már az első auditra való felkészüléskor.

1. A NIS2 és az EU kibervédelmi stratégiája – Mi a NIS2 big picture?
2. Általános kibervédelmi elvárások
3. Hazai hálózatvédelem, EU megfelelésre tervezve
4. Az incidensbejelentési kötelezettség teljesítése
5. Első lépések az infrastrukturánkban

BALASYS

MI AZ EU KIBER BIG PICTURE?



BALASYS

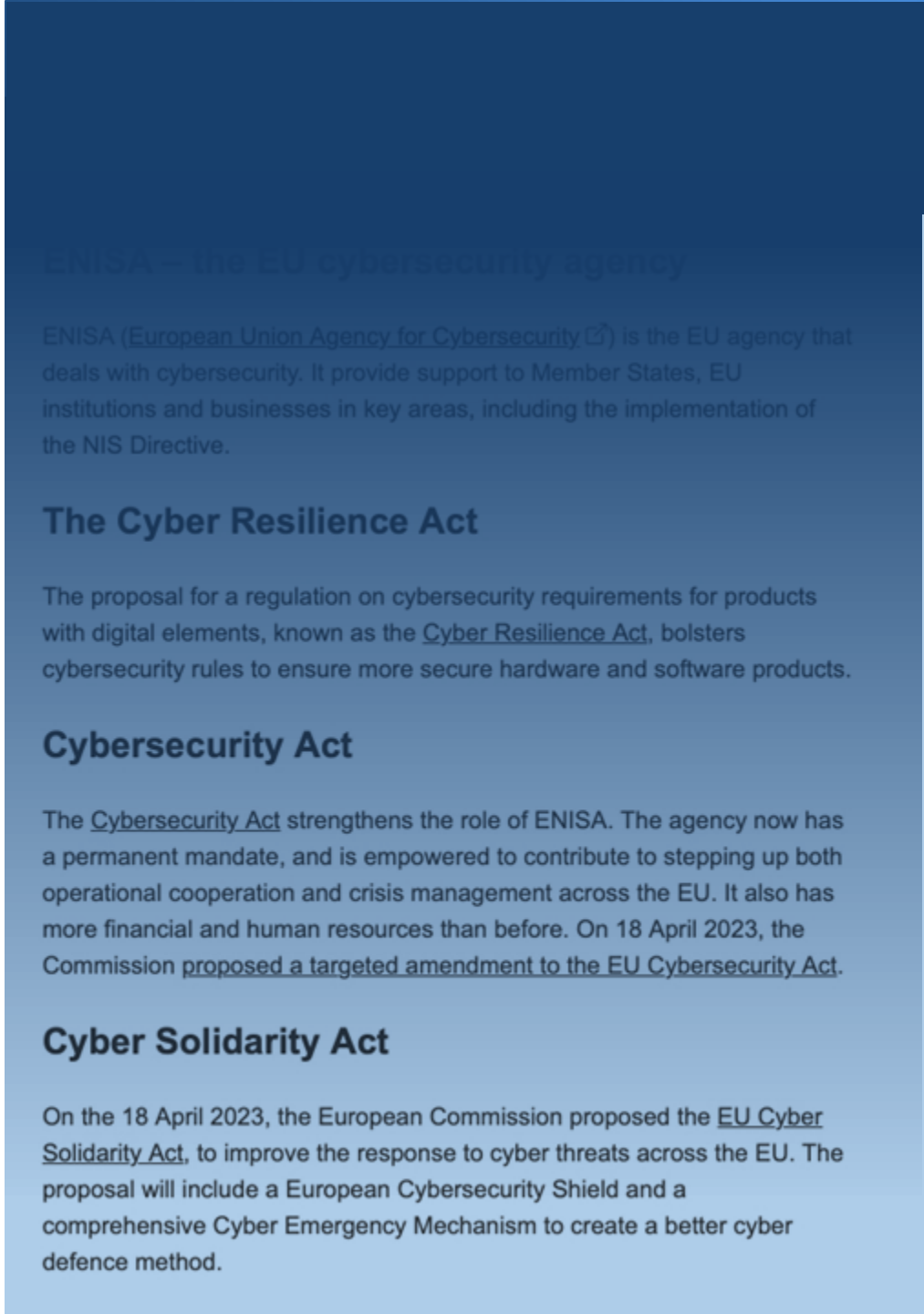
A NIS2 SZEREPE AZ EU KIBERVÉDELMI STRATÉGIÁJÁBAN

Network and Information System 2

A NIS2 nagyban **kiterjesztette a felügyelet alá tartozó szektorokat** és scope-ban hatalmasat merít a hazai vállalatok közül is

Fő vívmányai közé tartozik **az incidensbejelentési kötelezettség** és a tagállamok **CSIRT hálózat** általi bekötése az ENISA felé

Kibervédelem szempontjából akár lazának is mondható, láthatóan a reziliencia egy alapvető cél, viszont a nagyobb képet vizsgálva láthatjuk, hogy egy egységesített EU kibervédelmi stratégia alapkövét tették le a NIS2-vel



BALASYS

A KIBERVÉDELMI SZABÁLYOZÁSOK ÚJ CSALÁDJA

A NIS2 mellett számos más „reziliencia” szabályozás is érkezett, mint a **DORA, CER és CRA,** ezeket együttesen vizsgálva új irányvonalat láthatunk az EU kibervédelmében.

Az **új stratégia** egy egységesített, kiterjesztett védelmet követel meg a régió kritikus infrastruktúrájában, nemzetközi együttműködést épít és alapokat fektet le a kritikus szektorok komolyabb, központosított szabályozásának megvalósítására.

Az EU-nak nehezebb a feladata, mint az USA-nak, ahol egyetlen direktíva az összes államra érvényesen megkövetelte a Zero Trust Architektúra bevezetését, de az EU és ENISA megtették az első lépéseket, hogy itt is hasonló gyorsasággal lehessen reagálni az új kiberfenyegetésekre.

BALASYS

(87) Az illetékes hatóságok a felügyeleti feladataikkal összefüggésben olyan kiberbiztonsági szolgáltatásokat is [illegible]biztonsági auditok, a behatolási tesztek vagy az eseményekre való reagálás.

[illegible]rvezeteknek foglalkozniuk kell azon kockázatokkal is, amelyek egy szélesebb ökoszisztéman belüli más érdekelt felekkel folytatott interakcióikból és kapcsolataikból fakadnak, többek között az ipari kémkedés elleni küzdelem és az üzleti titkok védelme tekintetében. Az említett szervezeteknek különösen meg kell tenniük a megfelelő intézkedéseket annak biztosítása érdekében, hogy az egyetemekkel és a kutatóintézetekkel folytatott együttműködésük kiberbiztonsági szabályzatukkal összhangban történjen, és a bevált gyakorlatokat kövessék az információkhoz való általános hozzáférés és terjesztés, valamint különösen a szellemi tulajdon védelme tekintetében. Hasonlóképpen - tekintettel az adatoknak az alapvető és fontos szervezetek tevékenysége szempontjából fennálló fontosságára és értékére - amennyiben az adatok átalakítására és harmadik felektől származó adatelemzési szolgáltatásokra támaszkodnak, az említett szervezeteknek meg kell tenniük a megfelelő kiberbiztonsági kockázatkezelési intézkedéseket.

(89) Az alapvető és fontos szervezeteknek az alapvető kiberhigiéniai gyakorlatok széles skáláját kell alkalmazniuk, például a zéró bizalom alapelveit, a szoftverfrissítéseket, az eszközkonfigurációt, a hálózatszegmentálást, a személyazonosság- és hozzáférés-kezelést vagy a felhasználói tudatosságot, továbbá képzéseket kell szervezniük alkalmazottaik számára és fel kell hívniuk a figyelmet a kiberfenyegetésekre, illetve az adathalászatra vagy a pszichológiai manipulációs technikákra. Ezen túlmenően az említett szervezeteknek értékelniük kell saját kiberbiztonsági képességeiket, és adott esetben törekedniük kell a kiberbiztonságot erősítő technológiák, például a mesterséges intelligencia vagy a gépi tanulásra épülő rendszerek integrálására képességeik, valamint a hálózati és információs rendszerek biztonságának fokozása érdekében.

(90) Az ellátási lánc kulcsfontosságú kockázatainak további kezelése és az ezen irányelv hatálya alá tartozó ágazatokban működő alapvető és fontos szervezetek számára az ellátási lánccal és a szállítóval kapcsolatos kockázatok megfelelő kezelésének elősegítése érdekében az együttműködési csoportnak a Bizottsággal és az

Zero Trust a NIS2-ben

(87) Az illetékes hatóságok a felügyeleti feladataikkal összefüggésben olyan kiberbiztonsági szolgáltatásokat is [illegible]biztonsági auditok, a behatolási tesztek vagy az eseményekre való reagálás. [illegible]rvezeteknek foglalkozniuk kell azon kockázatokkal is, amelyek egy szélesebb ökoszisztéman belüli más érdekelt felekkel folytatott interakcióikból és kapcsolataikból fakadnak, többek között az ipari kémkedés elleni küzdelem és az üzleti titkok védelme tekintetében. Az említett szervezeteknek különösen meg kell tenniük a megfelelő intézkedéseket annak biztosítása érdekében, hogy az egyetemekkel és a kutatóintézetekkel folytatott együttműködésük kiberbiztonsági szabályzatukkal összhangban történjen, és a bevált gyakorlatokat kövessék az információkhoz való általános hozzáférés és terjesztés, valamint különösen a szellemi tulajdon védelme tekintetében. Hasonlóképpen - tekintettel az adatoknak az alapvető és fontos szervezetek tevékenysége szempontjából fennálló fontosságára és értékére - amennyiben az adatok átalakítására és harmadik felektől származó adatelemzési szolgáltatásokra támaszkodnak, az említett szervezeteknek meg kell tenniük a megfelelő kiberbiztonsági kockázatkezelési intézkedéseket.

(89) Az alapvető és fontos szervezeteknek az alapvető kiberhigiéniai gyakorlatok széles skáláját kell alkalmazniuk, például a zéró bizalom alapelveit, a szoftverfrissítéseket, az eszközkonfigurációt, a hálózatszegmentálást, a személyazonosság- és hozzáférés-kezelést vagy a felhasználói tudatosságot, továbbá képzéseket kell szervezniük alkalmazottaik számára és fel kell hívniuk a figyelmet a kiberfenyegetésekre, illetve az adathalászatra vagy a pszichológiai manipulációs technikákra. Ezen túlmenően az említett szervezeteknek értékelniük kell saját kiberbiztonsági képességeiket, és adott esetben törekedniük kell a kiberbiztonságot erősítő technológiák, például a mesterséges intelligencia vagy a gépi tanulásra épülő rendszerek integrálására képességeik, valamint a hálózati és információs rendszerek biztonságának fokozása érdekében.

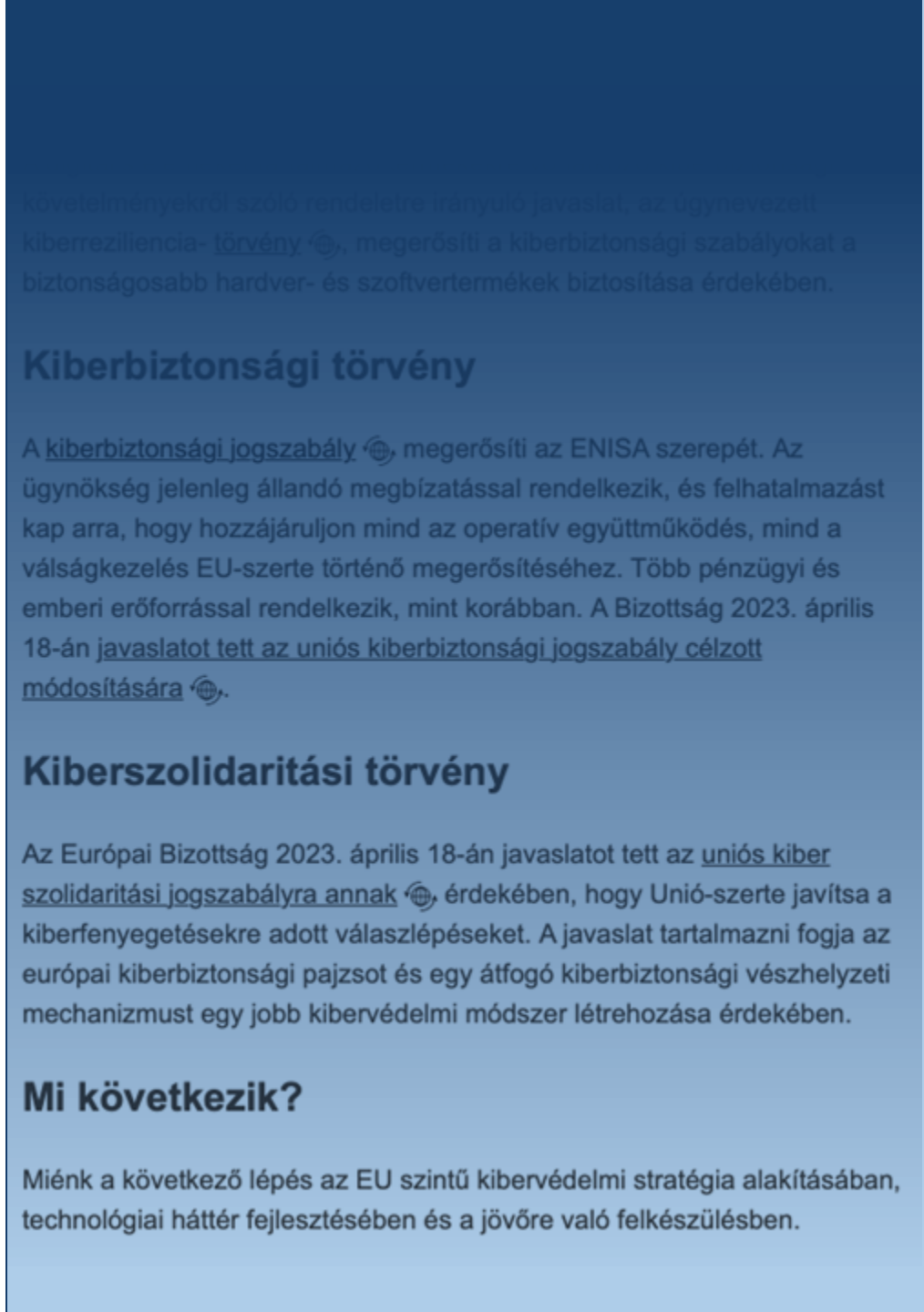
(90) Az ellátási lánc kulcsfontosságú kockázatainak további kezelése és az ezen irányelv hatálya alá tartozó ágazatokban működő alapvető és fontos szervezetek számára az ellátási lánccal és a szállítóval kapcsolatos kockázatok megfelelő kezelésének elősegítése érdekében az együttműködési csoportnak a Bizottsággal és az

A NIS2 ÉS A ZERO TRUST ÉRDEKES KAPCSOLATA

A NIS2 eredeti szövege (EUR-Lex) konkrét említést tesz a Zero Trustról, annak minden elemét viszont a jelenlegi scope és határidők mellett teljesíthetetlen feladat lenne megkövetelni.

Erős célzásnak vehetjük viszont, hogy az EU hosszútávon hasonlóan erős és kibervédelemre törekszik, mint az USA NIST által kiadott ZTA.

Az ENISA mandátumának megerősítése szintén arra utal, hogy a minőség mellett a reakcióidőkön is kívánnak javítani, erősebb, egységesített kontrollal, melyek rövid időn belül az összes tagállamban megvalósításra kerülnek.



BALASYS

ÁLTALÁNOS KIBERVÉDELMI ELVÁRÁSOK

2

BALASYS

A 2024. évi LXIX. törvény

- Szabályzatok
- Hozzáféréskezelés, Azonosítás, Hitelesítés
- Naplózás, Audit
- Naplóadatok feldolgozása, kiértékelés
- Fizikai és Környezeti védelem
- Adatvagyon, Kommunikáció, Információrendszer védelem
- Kockázatkezelés, Üzletmenet folytonosság, Ellátási lánc
- Biztonsági események kezelése, Incidensbejelentés
- Tudatosság és képzés

BALASYS

Hazai követelmények

A 2024. ÉVI LXIX. TÖRVÉNY

- Szabályzatok
- **Hozzáféréskezelés, Azonosítás, Hitelesítés**
- **Naplózás, Audit**
- **Naplóadatok feldolgozása, kiértékelés**
- Fizikai és Környezeti védelem
- **Adatvagyon, Kommunikáció, Információrendszer védelem**
- **Kockázatkezelés, Üzletmenet folytonosság, Ellátási lánc**
- **Biztonsági események kezelése, Incidensbejelentés**
- Tudatosság és képzés

BALASYS

Technológiai képességek

HAZAI HÁLÓZATVÉDELEM, EU MEGFELELÉSRE TERVEZVE

3

BALASYS

NIS2 MEGOLDÁS CSOMAGOK

NAPLÓZÁS

1. Naplóadat források bekötése
2. Napló források kiterjesztése
3. Felügyelet kikényszerítése
4. Naplóadatok feldolgozása különböző felhasználásokhoz
5. Incidensbejelentéshez szükséges jelentések elkészítése

HOZZÁFÉRÉSEK

1. Rendszerek, Szolgáltatások hozzáféréskezelésének kialakítása és kikényszerítése
2. Erős Auth folyamat megkövetelése minden kritikus rendszeren
3. Adatvagyon és kritikus rendszerek szegmentációja ZTA kialakításával

TITKOSÍTÁS

- Forgalmak titkosítása továbbítás során, titkosítás kikényszerítése
- Mgfelelő titkosítás megkövetelése tárolás közben is
- Hálózati mikroszegmentáció alkalmazása

FORGALOMSZŰRÉS

- Bejövő forgalom veszélyforrások szűrése
- Kimenő forgalom felügyelete, szűrése
- Belső hálózati forgalmak felügyelete és szűrése
- Fejlett veszélyforrás információlista alkalmazása és egyedi lista kialakítása

Hálózati forgalom felügyelete, kontrollja

BALASYS

NAPLÓZÁS

A felügyelet egyik alapköve a naplózás, a Balasys könnyen integrálható technológiáival minden rendszert a hálózati forgalmak vizsgálata alapján kényszerítjük ki a felügyeletet

- **Naplóadat generálás bármilyen rendszerből**, az átmenő forgalom alapján, akár jelen van az adat, akár hiányzik
- **Uniform naplózás** különböző rendszerek, protokollok és alkalmazások esetén is
- **Egyszerű SOC, SIEM és Big Data** Analitika integráció
- **Több, egyedi kimenet**
  Csak a releváns információkat naplózva minden csoport számára, válogatott naplóadatok küldése rendszerekbe
- **A teljes hálózati forgalom tükrözése**
  3rd party adatfeldolgozók számára

BALASYS

NAPLÓZÁS

1. Naplóadat források bekötése
2. Napló források kiterjesztése
3. Felügyelet kikényszerítése
4. Naplóadatok feldolgozása különböző felhasználásokhoz
5. Incidensbejelentéshez szükséges jelentések elkészítése

HOZZÁFÉRÉSKEZELÉS

A Balasys több megközelítést is kínál, hogy minden védendő rendszeren megvalósítható legyen a hozzáféréskezelés

Azonosítási előtétrendszer
Hálózati forgalomban kikényszerítve vagy egyedi protokoll esetén azon kívül is

MFA
Többfaktoros, erős azonosítás integrációja

Felhasználók és jogosultságok
AD és LDAP támogatás, VPN hozzáférések és Tanusítványok kezelése

Hálózati mikroszegmentáció
Kritikus rendszerek szeparálása és támadók mozgásterének minimalizálása

Legacy és Webservice környezetek támogatása

BALASYS

HOZZÁFÉRÉSEK

1. **Rendszerek, Szolgáltatások hozzáféréskezelésének kialakítása és kikényszerítése**
2. **Erős Auth folyamat megkövetelése minden kritikus rendszeren**
3. **Adatvagyon és kritikus rendszerek szegmentációja ZTA kialakításával**

TITKOSÍTÁS

Titkosítási átjáróval az átmenő forgalom mindkét irányába kikényszeríthetők a titkosítási szabályok

- **TLS1.3 támogatás**
  Titkosítás kikényszerítése és titkosítási szint emelése egyszerűen
- **Egyedi szabályrendszerek**
  Különböző forgalmakra, irányokra, adatvagyon típusokra
- **Kompatibilitás**
  Örökségrendszer, Ipari és Cloud környezetekkel
- **Titkosított forgalom feldolgozása**
  Titkosítás bontása, módosítása, TLS Offload, Flagelés
- **VPN és HSM**
  Biztonságos kommunikációs csatornák és kulcskezelés

BALASYS

TITKOSÍTÁS

- Forgalmak titkosítása továbbítás során, titkosítás kikényszerítése
- Mgfelelő titkosítás megkövetelése tárolás közben is
- Hálózati mikroszegmentáció alkalmazása

FORGALOMSZŰRÉS

Egyszerűen implementálható és kifinomult szűrési technológiák, mellyel minden forgalom, mely beérkezhet vagy elhagyhatja a védett rendszert ellenőrzött.

- **Részletes protokoll kontroll**
  Az irodai forgalomtól a mainframekig és OT/BMS protokollokig
- **Forgalommanipulációs eszközök**
  Törlés, Módosítás, Kiegészítés, Flagelés, Kompatibilitás fordítás
- **Alap szűrési képességek**
  Blacklist, Whitelist, SPAM és URL filter
- **Fejlett szűrési információforrások**
  WAF, Threat Intelligence
- **Moduláris technológia**
  DLPS, Honeypot, Analitikai felhasználás támogatása

BALASYS

FORGALOMSZŰRÉS

- **Bejövő forgalom veszélyforrások szűrése**
- **Kimenő forgalom felügyelete, szűrése**
- **Belső hálózati forgalmak felügyelete és szűrése**
- **Fejlett veszélyforrás információlista alkalmazása és egyedi lista kialakítása**

AZ INCIDENSBEJELENTÉSI KÖTELEZETTSÉG TELJESÍTÉSE

4

BALASYS

A NIS2 HANGSÚLYOS ELEME

Súlyos és gyors büntetéseket helyezett kilátásba az eredeti NIS2, a kötelezettség a hazai adaptációban sem szűnt meg.

Az incidenseket fel kell mérni, be kell jelenteni a felügyelő hatóság számára, ennek teljesítéséhez szükséges azok:

- Időben való felismerése
- Gyors reagálás (és további károk megállítása/megelőzése)
- Teljes scope felmérése, érintett rendszerek és adatvagyon tételes ismertetése
- Near-miss kategóriájú események felismerése egyedi naplózási technikákkal

NAPLÓZÁS

1. **Naplóadat források bekötése**
2. **Napló források kiterjesztése**
3. **Felügyelet kikényszerítése**
4. **Naplóadatok feldolgozása különböző felhasználásokhoz**
5. **Incidensbejelentéshez szükséges jelentések elkészítése**

BALASYS

ELSŐ LÉPÉSEK AZ INFRASTRUKTURÁNKBAN

BALASYS

NIS2 LÉPÉSRŐL LÉPÉSRE

Javasolt mihamarabb elkezdeni a közös munkát egy NIS2 tanácsadóval, mely során beazonosíthatók az erősségek és gyengeségek.

Már ez idő alatt érdemes felkeresni gyártókat, **akik képesek a meglévő rendszereink lecserélése nélkül kialakítani** a NIS2 által előírt védelmet és működést, ehhez olyan technológiákat keressünk, melyek képesek kikényszeríteni azokat és széleskörű platformtámogatással rendelkeznek.

Ne felejtsük el az **Örökségrendszereket** sem, valamint az **Ipari** és **Felhő** környezeteket.

BALASYS

A BALASYS FEJLESZTÉSEI ÉS A NIS2

Amellett, hogy megvannak a NIS2 teljesítéséhez a képességek, figyeljünk arra is, hogy **időtálló legyen a kialakított architektúra.**

A NIS2 most egy alapot fektet le és azokat az EU eszközöket hozza létre, mellyel később gyorsabban lehet emelni a régió kibervédelmi standardjein.

Érdemes EU technológiákat választani, mivel nagyon sajátosak az Unió adatvédelmi szabályozásai, gondoljunk csak vissza a GDPR-ra, melynek a teljesítése mehetett volna sokkal zökkenőmentesebben is, ha már erre a piacra készült technológiákat választunk.

A nyers képességek mellett a megfelelés támogatást is vizsgáljuk. A NIS2 erre tökéletes kezdőpont.

BALASYS

A BALASYS IRÁNYOK

- **Hálózat, Naplózás, Titkosítás és Hozzáférések, mint kiindulópont**
- **USA Zero Trust Architektúra és EU Reziliencia szabályozásokra tervezve**
- **Személyre szabható védelem és integráció a gyors megfeleléshez**
- **Meglévő rendszerek támogatása, beleértve az örökségrendszereket is**

SZALAI PATRIK
patrik.szalai@balasys.eu

Köszönöm a figyelmet!

BALASYS.EU

BALASYS

Mikroháló