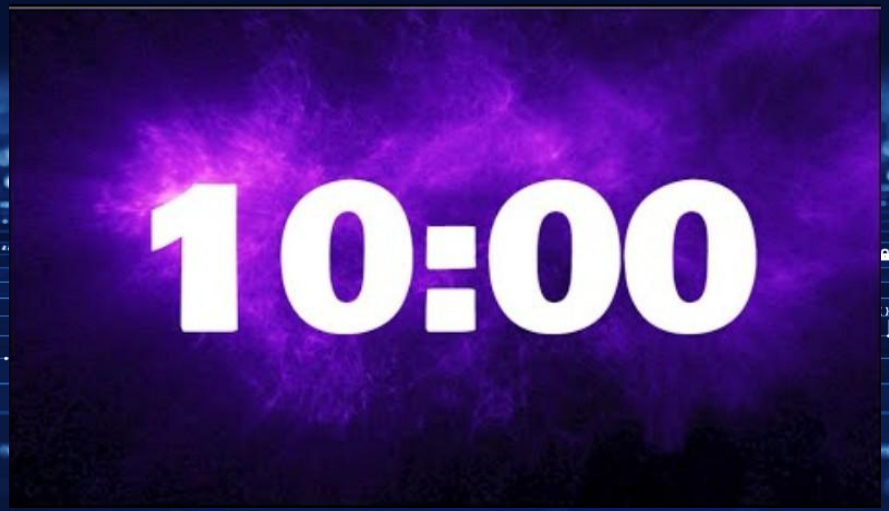
A WEBINÁRRÓL FELVÉTEL KÉSZÜL

KIBERBIZTONSÁGI WEBINÁR SOROZAT

Mikroháló

3. rész

Don’t Panic!

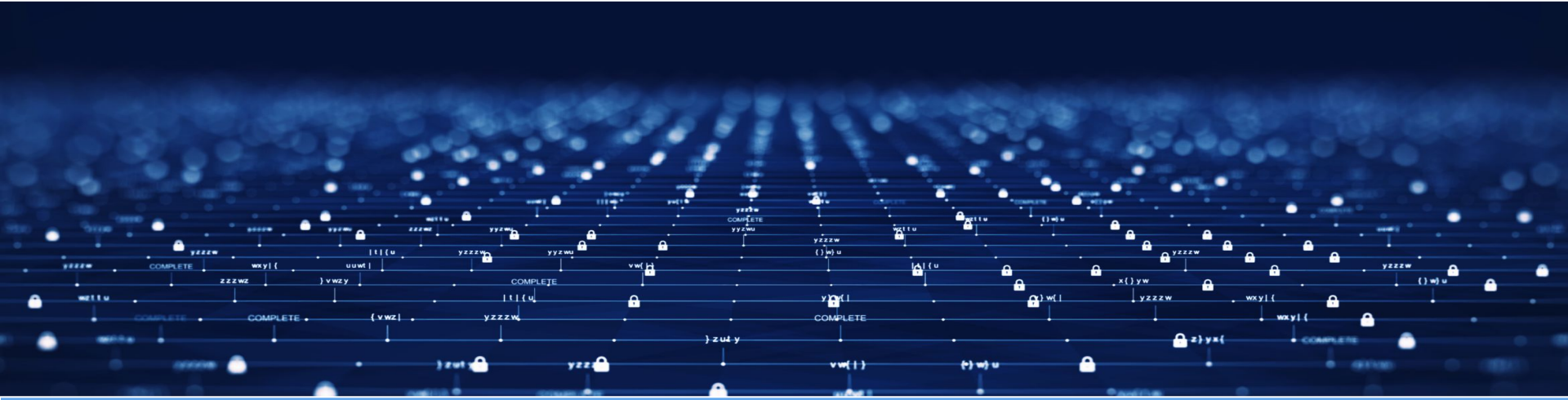


Mikroháló

KIBERBIZTONSÁGI WEBINÁR SOROZAT

3. rész

Don’t Panic!



2025.03.31

A WEBINÁRRÓL FELVÉTEL KÉSZÜL

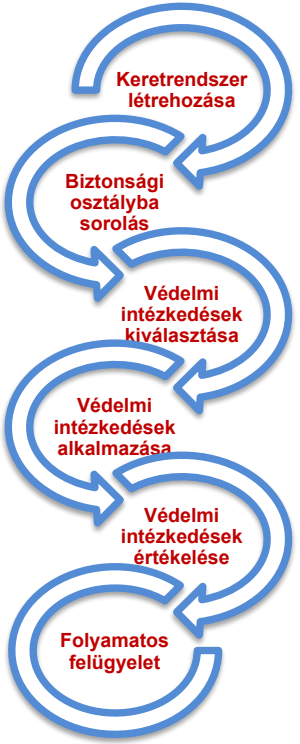
NIS2 a számok tükrében

- 72% a szervezeteknek nem rendelkezik teljes eszköznyilvántartással (ESG Global IT Survey, 2023)
- 15% soha nem végez kockázatelemzést (Nozomi, 2023)
- 34% csak alkalomszerűen értékel kockázatokat (Nozomi Networks + Vanson Bourne, 2023)
- 80% úgy gondolja, idővel meg fog felelni a NIS2-nek (Veeam, 2024)
- 66% viszont nem tudja tartani a határidőt (Veeam, 2024)
- Egészségügyi szereplők 40%-a nem hallott a NIS2-ről (Imprivata, 2024)
- Az európai cégek 90%-a szenvedett el megelőzhető kibertámadást 12 hónapon belül (Censuswide, 2024)
- 44% több mint három kritikus incidenst jelentett egy év alatt (Veeam, 2024)
- 71% magyar szervezetnek legalább 3 biztonsági incidense volt 2022-ben (Trend Micro SCALE, 2023)
- A válaszadó állami intézmények között egy sem tudott teljeskörű EIR-leltárt bemutatni (ÁSZ, 2022)
- 33% magyar közintézmények egyharmada nem végez rendszeres EIR-besorolást (ÁSZ, 2022)
- 52% az állami szervek közel fele nem ismeri vagy hibásan használja az EIR-besorolás három alapkritériumát (ÁSZ, 2022)

Mikroháló

Szervezetre vonatkozó kötelezettségek

- kockázat menedzsment rendszert kell működtetni
- elektronikus információs rendszer leltár elkészítése
- szerepkörök és felelősségek kiosztása
- adatvagyon leltár (közigazgatás)
- EIR biztonsági osztályba sorolás
- kockázatarányos védelmi intézkedések (7/2024)
- információbiztonsági szabályzat megírása
- együttműködés a hatósággal
- biztonságtudatossági oktatások bevezetése
- kiberbiztonsági gyakorlatok bevezetése
- naplózás, incidenskezelés és jelentés
- biztonsági követelmények a szerződésekbe
- IT fejlesztések 5%-át biztonságra kell költeni (költségvetési intézmények)



Mikroháló

Elektronikus információs rendszer

„24. *elektronikus információs rendszer:*
a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlési hálózat,
b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi, ideértve a kiber-fizikai rendszereket, vagy
c) az a) és b) alpontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;”

- Minden olyan rendszer, amely adatot tárol, kezel, továbbít vagy feldolgoz.
- Lehet fizikai eszköz, alkalmazás, működtető személy, eljárás.
- Akár több alrendszerből is állhat.

- Üzleti folyamatok mentén
- Hálózat alapon
- Adatokat szem előtt tartva

- Minden EIR, amely a szervezet működéséhez kapcsolódik, biztonsági osztályba sorolandó.
- Az auditköteles kör az összes osztályba sorolt EIR-re kiterjed – akár 'alap', 'jelentős' vagy 'magas' osztály.
- A nem megfelelő EIR-nyilvántartás az egyik leggyakoribb auditkockázat.

Mikroháló

Az EIR a szervezet rendelkezésében áll

- A szervezet felelős minden olyan rendszerért, amelyben saját adatot kezel vagy amely a működéshez szükséges.
- A szervezet képes befolyásolni a rendszer működését vagy biztonsági szintjét – akár közvetlen adminisztrátori jogokkal, akár szerződéses úton.
- Az érintett szervezet nem mentesülhet a felelősség alól pusztán azért, mert egy rendszert kiszervez vagy felhőben futtat.

Rendszerek lehetséges típusai

- Saját üzemeltetésű rendszer
- Kiszervezett üzemeltetésű (outsourcing) rendszer
- Felhőben futó vagy SaaS rendszer
- Bérelt, hosztolt vagy dobozos rendszer
- Partner által biztosított hozzáférés

Következő lépések a megfeleléshez

- Teljes EIR-leltár összeállítása
- Biztonsági osztályba sorolás, kockázatelemzéssel
- Külső rendszerek és szolgáltatók dokumentálása
- Felkészülés az auditálásra: nyilvántartások, szabályzatok, bizonyítékok

Mikroháló

Elektronikus információs rendszer példa

ALAPADATOK

- **EIR neve:** Irodai funkciókat biztosító elektronikus információs rendszer
- **Használat célja:** Irodai működés, kommunikáció, dokumentumkezelés
- **Futtatási környezet:** Felhő (M365), helyi rendszerek
- **Üzemeltetők:** Microsoft, belső IT, nyomtatási szolgáltató

RENDSZEREK/MODULOK

- Microsoft 365 – Exchange Online (levelezés)
- Microsoft Teams (chat, meeting)
- SharePoint Online (dokumentumtár, iktatás)
- OneDrive for Business (egyéni tárolás)
- Outlook kliens (helyi levelezőprogram)
- Active Directory / Azure AD (jogosultságkezelés)
- Papír alapú iktatórendszer
- Nyomtatási és szkennelési rendszer

BESOROLÁS

- **Bizalmasság:** Alacsony – nem tárol különleges adatokat
- **Sértetlenség:** Alacsony – sérülés nem jár súlyos következménnyel
- **Rendelkezésre állás:** Alacsony – kiesés nem kritikus
- **Összesített biztonsági osztály:** **Alacsony**

Mikroháló

Tipp - auditaltasdmagad.hu

EIR jellemzők és meghatározásuk

A tájékoztató célja

Jelen dokumentum célja, hogy útmutatót nyújtson az elektronikus információs rendszerek (továbbiakban EIR-ek) pontos azonosításához, számának meghatározásához és biztonsági osztályba sorolásához. Az előzetes osztályozás segíti a rendszerek kockázati szintjének megfelelő információbiztonsági követelmények azonosítását és integrálását.

Ez az eljárás támogatja a szervezetet abban, hogy az információbiztonsági előírások teljes körűen érvényesüljenek a rendszerek tervezése, működtetése és auditálása során.

1. Azonosítsuk a fő üzleti területeket

Első lépésként meg kell vizsgálni, hogy a szervezet mely üzleti területein működnek elektronikus információs rendszerek (EIR-ek). Az alábbiakban néhány gyakori példát említünk, amelyek segítenek az EIR-ek azonosításában:

Pénzügyi rendszer: Az olyan rendszerek, amelyek a pénzügyi tranzakciók, könyvelés és költségtervezés kezelésére szolgálnak.
Példa: Számlázási rendszer, költségvetés-tervező szoftver.

Készlet- és logisztikai rendszerek: Az árukészlet nyilvántartását, szállítási folyamatokat és logisztikai menedzsmentet támogató rendszerek.
Példa: Raktárkezelő szoftver, szállítmánykövető alkalmazás.

Ügyfélkapcsolati rendszerek (CRM – Customer Relationship Management): Az ügyfelek adatainak kezelésére, értékesítési és marketingfolyamatok nyomon követésére szolgáló eszközök.
Példa: Ügyfélnyilvántartó szoftver, automatizált marketingplatform.

Vállalati erőforrás-tervezési rendszerek (ERP – Enterprise Resource Planning): Integrált rendszerek, amelyek a szervezet különböző folyamatait támogatják, például a pénzügyi, HR, logisztikai és gyártási területeken.
Példa: Gyártási ütemezést támogató modul, készletkezelő modul.

Humán erőforrás rendszerek (HRM – Human Resource Management): Az alkalmazottak nyilvántartását, bérszámfejtést, toborzást és képzést támogató rendszerek.
Példa: Online toborzóplatform, digitális munkaidő-nyilvántartás.

Projektmenedzsment rendszerek: Az egyes projektek tervezését, ütemezését, nyomon követését és jelentését támogató eszközök.
Példa: Határidő-kezelő alkalmazás, erőforrás-elosztó szoftver.

Mikroháló

Minden informatikai rendszer, amely felett a szervezet bármilyen rendelkezési jogot gyakorol vagy amelyet a szolgáltatásai nyújtásához igénybe vesz, a szervezet EIR-jének tekintendő. A “rendelkezésében áll” kitétel arra utal, hogy a szervezet képes befolyásolni a rendszer működését vagy biztonsági szintjét – akár közvetlen adminisztrátori jogokkal, akár szerződéses úton. Az érintett szervezet nem mentesülhet a felelősség alól pusztán azért, mert egy rendszert kiszervez vagy felhőben futtat. Köteles együttműködni a külső féllel a biztonság megteremtésében, közös kockázatkezelési megállapodásokkal, és szükség esetén pótlólagos védelmi intézkedéseket hozni a saját hatáskörében. Ezáltal biztosítható, hogy a kiberbiztonsági intézkedések minden, a szervezet működésében szerepet játszó EIR-re kiterjednek, egységes védelmi szintet nyújtva.

Hatvani István
hatvani.istvan@mikrohalo.hu

2025.03.31.

Tervezett webinár témák

- A szervezeti védelem alapvető biztonsági elvei
  - bizalmasság, sértetlenség és rendelkezésre állás
  - preventív, detektív és korrektív védelmi intézkedések
  - adminisztratív, logikai és fizikai védelmi intézkedések
- Incidens kezelés és jelentési kötelezettségek
- Védelmi vektorok
- Üzleti hatáselemzés, üzletmenet-folytonosság
- Ellátási láncok biztonsága

Mikroháló

KIBERBIZTONSÁGI WEBINÁR SOROZAT

3. rész

EIR kezelés egyszerűen az ADAPTO-ban!

Mártha Csenge
martha.csenge@adapto.hu

A WEBINÁRRÓL FELVÉTEL KÉSZÜL