CyberCollege *Kiberbiztonsági tudatossági képzés – törvényi megfelelés és szervezeti biztonság cégvezetők számára*
17/2025. (VII. 24.) EM rendelet 4. § (1) bekezdése alapján a szervezet vezetője részére

Képzés megnevezése:Kiberbiztonsági tudatossági képzés – vezetői

Tematika:

- **Kiberbiztonsági alapfogalmak és trendek**

Bevezető
A vezető felelőssége
Feladat- jogszabályi alap-határidő
A leggyengébb láncszem- a vezető
A vezető viselkedési kockázatai
Digitális lábnyom
CEO FRAUD/BEC
Mit tehet a vezető?
Alapfogalmak, amelyek nélkül nem lehet dönteni : Kiberbiztonság

- Információbiztonság
- Kiberhigiénia
- CIA
- PRE-DE-CO
- Adatgazda
- Adatvagyon
- EIR

Üzletmenet-folytonosság
Ellátási lánc támadások
Aktuális fenyegetések és hatásuk a cégre
Fenyegetések számokban
Az MI mint a támadók gyorsítója
Összefoglalás és következő lépések
Amit ma is tudni kell-checklist

- **Kiberbiztonsági kockázatok és szervezeti stratégiák**

A kiberkockázat ma: üzleti és jogi realitás
A rendszer logikája: miért nem elég az egyszeri intézkedés?
Jogi következmények: mi a tét a vezető számára?
A kiberbiztonsági ökoszisztéma szereplői
Harmadik fél hozzáférések és szállítói kockázatkezelés
IBF-ről vezető szemszögből

- külsős/belső
- összeférhetetlenség
- feladatok
- ellenőrzése

Kockázatarányosság elve
Milyen kockázatokkal számoljon a vezető?
A kockázatértékelés kötelező vezetői kérdései
Az EIR-nyilvántartás mint a rendszer alapj**a**
Biztonsági osztályba sorolás
Mi a Zero Trust ?
Zero Trust üzleti oldalról
A kötelező dokumentumrendszer áttekintése
IBSZ- Információbiztonsági szabályzat
A vezető mint a biztonsági kultúra meghatározója
Kiberbiztonsági KPI-ok és teljesítménymérés
A kiberbiztonsági erőforrás
Mennyibe kerül a kiberbiztonság?
Prioritizálási módszertan korlátolt erőforrás esetén
Vezetői elköteleződés
Összefoglalás: a vezető teendőlistája

- **Uniós és hazai kiberbiztonsági jogszabályi kötelezettségek és feladatok**

Hazai jogszabályok:

- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről és védelmi intézkedésekről
- 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
- 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és legmagasabb díjáról
- 2/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági felügyeleti díjról
- 17/2025. (VII. 24.) EM rendelet

EU-s szabályozás:

- GDPR – (EU) 2016/679 – Az általános adatvédelmi rendelet
- DORA rendelet – (EU) 2022/2554
- Cyber Resilience Act – (EU) 2024/2847
- Cyber Solidarity Act – (EU) 2024/2847

Összefoglalás: a vezető teendőlistája

- **Kiberbiztonsági incidenskezeléshez kapcsolódó feladatok**

A kiberbiztonsági incidens
Incidensek felismerése
Adatvédelmi incidens
Adatvédelmi incidens bejelentése
Kiberbiztonsági incidens bejelentése
Kríziskommunikáció
A pszichológiai biztonság mint a kiberbiztonsági kultúra alapfeltétele?
NO BLAME kultúra
A jelzési folyamat

A vezető döntési fája- egy zsarolóvírus esetében
Az incidens lezárul
Összefoglalás: a vezető teendőlistája

- **Kiberbiztonsági jó gyakorlatok és tapasztalatok megosztása**

Bevezető
A fizikai védelemről
Amikor a munka környezet otthon van, azaz amit a home office biztonságáról érdemes általánosságban tudni
Jelszavak- a hozzáférés valódi kulcsa
Került-e már KI adatom valahova valakinek?
A kibertámadások területei: az email
A kibertámadások területei: QR kódok
Mentális egyensúly az online térben
Kiberhigiénia

TESZT: https://forms.gle/bTpRzZ4jjHgxyq1R7