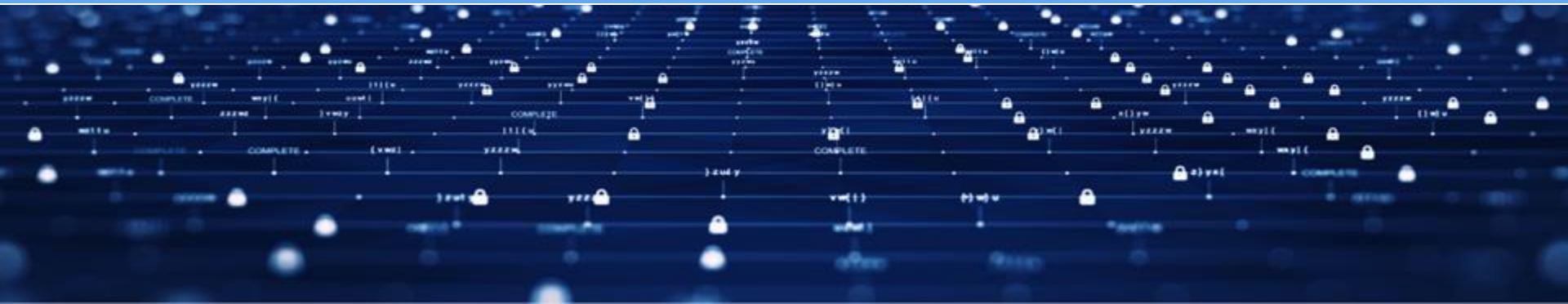
A WEBINÁRRÓL FELVÉTEL KÉSZÜL

Mikroháló

KIBERBIZTONSÁGI WEBINÁR SOROZAT

AUDIT VAGY AGGODALOM?



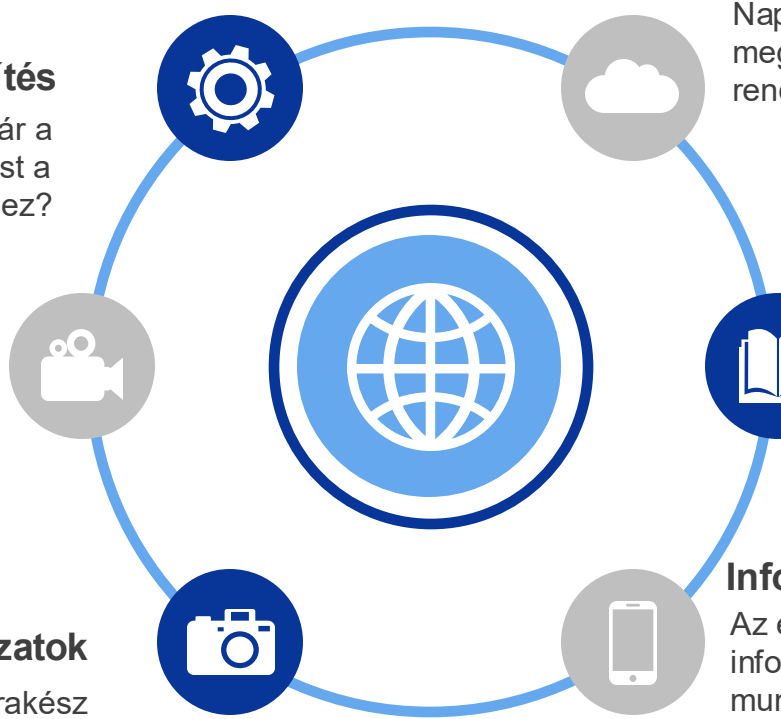
Önellenőrző Kérdések

Rendszeresemények naplózása

Naplózzák és legalább 6 hónapig megőrzik a hozzáférési és rendszereseményeket?

Kétfaktoros hitelesítés

Bevezették már a kétfaktoros azonosítást a céges rendszerekhez?



Incidenskezelési terv

Rendelkeznek incidenskezelési tervvel?

Következő 30 nap teendői

Milyen konkrét lépéseket tehet cége a következő 30 napban, hogy előkészítse a NIS2 auditot?

Információbiztonsági oktatás

Az elmúlt egy évben tartottak információbiztonsági oktatást a munkavállalók részére?

Naprakész szabályzatok

Rendelkeznek naprakész információbiztonsági szabályzatokkal?

Mikroháló

Önnek ITT a helye

Ha az előző kérdésekre akár egy kérdésre is **NEM** volt a válasz,
akkor webinárunk egyértelműen Önnek szól

1

Biztonsági hiányosságok

A nemleges válaszok biztonsági hiányosságokra utalnak, amelyek sürgős intézkedéseket igényelnek a vállalaton belül.

2

Következmények

A hiányosságok komoly következményekkel járhatnak, beleértve a pénzügyi veszteségeket és a vállalat hírnevének csökkenését.

3

Intézkedések bevezetése

Fontos a megfelelő intézkedések bevezetése a biztonság javítása érdekében, hogy minimalizáljuk a kockázatokat.

Mikroháló

A sikeres audithoz vezető út

1.) Helyzetfelmérés és GAP elemzés

Azonosítsa, hol áll most a cég a NIS2 követelményeihez képest.

2.) Intézkedési tervek és dokumentáció elkészítése

Dolgozza ki a szükséges biztonsági terveket és hiányzó szabályzatokat, folyamatleírásokat.

3.) Védelmi intézkedések bevezetése

Pótolja a feltárt hiányosságokat a technikai és szervezési intézkedések terén (pl. hozzáférés-szabályozás, mentési terv, incidenskezelés stb.).

4.) Értékelési terv és ellenőrzés

Alakítson ki rendszeres belső ellenőrzési mechanizmust az intézkedések hatékonyságának mérésére, készítsen értékelési tervet és értékelési jelentéseket az eredményekről.

5.) Tudatosság növelése és tréning

Képezze a vezetőket és a munkatársakat a kiberbiztonsági követelményekről, hogy mindenki értse a szerepét és a szabályok okát.

6.) Vezetői elköteleződés biztosítása

Vonja be a felsővezetést a folyamatba, biztosítsa a szükséges erőforrásokat és támogatást a projekthez.

Mikroháló

Mikroháló audit módszertan

✓ A szervezet kezdeményezi az auditot az auditaltasdmagad.hu portálon.

✓ Megállapodást kötünk az audit elvégzéséről.

✓ Elkészítjük és megküldjük az auditálási tervet.

✓ A szervezet első körben benyújtja az audit bizonyítékait.

✓ Hiányos vagy kiegészítő bizonyítékokat második körben kérünk be.

✓ Áttekintjük és értékeljük a beérkezett bizonyítékokat.

✓ Személyes interjúk és ellenőrzések történnek.

✓ Elkészítjük és elküldjük az auditjelentést a szervezetnek és a hatóságnak.

Milyen fő területekre kell figyelni?

Kriptográfia és titkosítás használata az érzékeny adatokra

Üzletmenet-folytonossági terv készítése

Katasztrófa utáni helyreállítási terv készítése

Incidenskezelési tervet

Információbiztonsági oktatás

Beszállítói lánc biztonsága

Szabályzatok elkészítése

Kockázatkezelés menedzsment

Hozzáférés-kezelés és azonosítás

Többfaktoros hitelesítés bevezetése

Alapvető kibervédelmi intézkedések végrehajtása

Rendszeres sérülékenységvizsgálat bevezetése

Mikroháló

Gyakori buktatók –

Hogyan kerüljük el őket?

Csak a büntetés elkerülésére fókuszálás

Az IBIR hiánya és egyszeri projekt szemlélet

Hiányos vagy nem értett követelmények

Dokumentáció hiánya vagy nem naprakész volta

Erőforrások alultervezése

IT kiszervezéséből adódó fehér foltok

Mikroháló

Tippek - A megfelelés sikeres eléréséhez

Igazodás nemzetközi szabványokhoz

Felsővezetői támogatás biztosítása

Szerepkörök és felelősségek egyértelműsítése

Kommunikáció a hatósággal és auditorral

Próba-audit végrehajtása

Folyamatos fejlesztés és naprakészen tartás

A terv NEM felesleges papírmunka!

Használja a rendszerbiztonsági tervet

Dokumentálni kell mindent

Pótolják az esetleges hiányzó szabályozásokat

A technikai intézkedések mellett az emberekre is fókuszálni kell

Mikroháló

A buktatók elkerülésének kulcsa a proaktív szemlélet.
Ne csak reagáljunk az eseményekre, tervezzünk előre, képezzünk.
Legyen világos mindenki számára, hogy miért szükség, milyen előnyökkel jár a biztonsági szint emelése a cégnél.

2025.03.27

Hatvani István
hatvani.istvan@mikrohalo.hu