KIBERBIZTONSÁGI RENDSZEREK AZ IT BIZTONSÁG 10 PONTJA

SZAKMAI BLOG | 2 PERC

Kiberreziliencia

SYSWIND

MIRŐL LESZ SZÓ?

Az NCSC 10 pontban összegyűjtötte a kibervédelemmel kapcsolatos legfontosabb teendőket. Mi egy picit kiegészítettük, hogy jobban megfogható legyen nem biztonsági szakemberek számára is. A kiberreziliencia egyik lényegi eleme az információmegosztás. A célja, hogy az informatikai infrastruktúra köré tervezett stratégiák együttesen növeljék a biztonságot a rendszerben, és csökkentsék a kibertámadások lehetőségét, illetve minimalizálják azok károkozását.

MIÉRT GYŰJTÖTTÉK ÖSSZE?

Mert még informatikai körökben is sokan tájékozatlanok a kibervédelemmel kapcsolatban, egy üzleti vezetőnek pedig kifejezetten nehéz dolga van manapság, nem várható el tőle, hogy csak úgy megfeleljen a kiberreziliencia elvárásainak. Úgyhogy, ez a rövid összefoglaló hasznos lehet minden operatív menedzsernek, ügyvezetőnek vagy cégtulajdonosnak.

MIÉRT FONTOS A 10/10?

Mert ez nem kvíz, nem egy 10 soros fogadási szelvény, amik esetenként 8 találattal is kimagasló eredményt jelentnek. A 10-ből 10 itt kötelező, mert ha csak 2-t nem teljesítesz, akkor bukik az egész koncepció. Magyarán, lehet neked 3 méter széles, 30 méter magas várfalad, ha az oldalán lyukak tátongnak.

KIKNEK SZÓL AZ AJÁNLÁS?

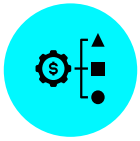
Mindenkinek, aki rendelkezik valamilyen vállalati értékkel, legyen az fizikai vagy digitális, és nem szeretné azt elveszíteni, sem azt, hogy sérüljön bármi az üzleti, gyártási, logisztikai folyamataiban. De legfőképpen olyan vállalatoknak, akik nagyban ki vannak téve az ellátási lánc függőségének vagy beszállítói, vagy felvevői oldalon. Nem mellesleg nemzeti intézményeknek, szervezeteknek sem ártana, de kiindulva a kiberreziliencia stratégiájából, őket is már biztos támogatják, és ők is biztos támogatnak más szervezeteket sikeres kiberbiztonsági tapasztalataikkal és megoldásaikkal.

KOCKÁZATKEZELÉS

Állíts fel kockázat alapú stratégiát adataid és rendszereid védelmére!
Készíts elemzést arról, hogy „mi fájna a legjobban"! Legyél tisztában azzal, hogy mivel károsíthatnának meg a legjobban, mi tenné lehetetlenné a működést, mi okozná a leghosszabb helyreállítást!

ELKÖTELEZŐDÉS ÉS KÉPZÉS

Építsd a munkavállalók elkötelezettségét a biztonság iránt!
A kompetenciafejlesztés legyen kollaboratív, és a szabályozás legyen felhasználóbarát, ne csak szigorú! Alakíts ki rendszerszemléletet és teremtsd meg az optimális eszkalációs irányokat az ITOps és a munkavállalók között! Növeld az együttműködési készséget minden irányban!



VAGYONKEZELÉS

Legyél tisztában digitális értékeiddel, adataiddal és rendszereiddel!
Mindig tudd, hogy milyen megoldások milyen üzleti igényeket szolgálnak ki! Tedd informatikád és folyamataidat transzparensé minden érintett számára! Kezeld a kritikus folyamatokat priorizáltan, és biztosítsd azok redundanciáját!

ARCHITEKTÚRA ÉS KONFIGURÁCIÓ

Minden rendszeredet tervezd és építsd biztonsági szemszögből, és folyamatosan tartsd karban!
Ne bízz félmegoldásokban, és törekedj a standardizációra, és a központosított üzemeltetésre!

SEBEZHETŐSÉGKEZELÉS

Tartsd szem előtt a sebezhetőségi pontjaidat és tartsd mindig védve a rendszereidet a teljes életciklus során!
Használj kockázat alapú, gépi tanuláson és mesterséges intelligenciával támogatott elemzéseket, és azonnal teljesítsd a kritikus problémák megoldásaira érkező ajánlásokat!

IDENTITÁS- ÉS HOZZÁFÉRÉS-KEZELÉS

Szabályozd, hogy ki és mi, illetve mikor férhet hozzá rendszereidhez, adataidhoz!
Alkalmazz Zero Trust koncepciót, és ne bízz senkiben, semmiben mindaddig, amíg nem tudod hitelesen azonosítani! Építs fel egy olyan házirendet, ami figyelembe veszi, hogy kinek, minek, mikor, honnan és miért van jogosultsága a rendszeredbe lépésre!

ADATBIZTONSÁG

Védd adataidat mindenhol, de leginkább figyelj a sérülékenységekre!
Tárold az adatokat a legkisebb rizikó mellett és oldd meg a biztonságos kiszolgálást és adatátvitelt is! Védd a végpontjaid és csatlakozási pontjaidat folyamatos állapotellenőrzéssel!

NAPLÓZÁS ÉS MONITOROZÁS

Tervezd meg a rendszereidet úgy, hogy képes legyél időben észlelni az incidenseket és tudd kivizsgálni azokat!
Legyen a rendszered összes eleme megfigyelhető és naprakész állapotú! Ne hagyd ki a BYOD eszközöket, és a vendégcsatlakozási pontokat sem! Monitorozd a hálózati és internet forgalmat felhős biztonsági proxy-n keresztül!

INCIDENSKEZELÉS

Legyen terved a kiberincidensek kezelésére és legyél képes azonnali válaszlépések megtételére!
Alakítsd házirended dinamikusan, hogy az események függvényében tudjon alkalmazkodni a kialakult helyzethez!

AZ ELLÁTÁSI LÁNC BIZTONSÁGA

Működj együtt beszállítóiddal és partnereiddel!
Vedd fel a SecOps-szal a kapcsolatot, osszátok meg a tapasztalatokat, és alakítsatok ki közös biztonsági stratégiát! Védjétek a teljes láncolatot a sérülékenységekkel szemben!

LEGYÉL TISZTÁBAN A SZERVEZETEDET ÉRINTŐ RIZIKÓ FAKTOROKKAL!
VALÓSÍTS MEG OLYAN RENDSZERT, AMI MINIMALIZÁLJA A SÉRÜLÉKENYSÉGEKET!
KÉSZÜLJ FEL A KIBERINCIDENSEKRE!

SYSWIND KFT.

1095 Budapest, Soroksári út 48. Malomudvar 11. épület, 3. emelet 11-13. iroda

+36 30 610 2707 | info@syswind.hu | syswind.hu

facebook.com/syswind

linkedin.com/company/syswind

KIBERBIZTONSÁGI RENDSZEREK