Micro Focus trendek

Útmutató a NIS2 rengetegében

„A kiberfenyegetések egyre merészebbek és összetettebbek. Elengedhetetlen volt, hogy az új realitásokhoz igazítsuk a biztonsági keretrendszerünket, és gondoskodjunk polgáraink és infrastruktúráink védelméről. A NIS2 megállapodással frissítjük az előírásokat, hogy kritikus szolgáltatásokat biztosíthassunk a társadalom és a gazdaság számára. Ez egy jelentős előrelépés."
Thierry Breton, az Európai Bizottság belső piacért felelős biztosa

Az új uniós kibervédelmi irányelv, a NIS2 számos szervezet számára támaszt új követelményeket több különféle területen. Nehéz eligazodni, kinek milyen teendői vannak, mely rendszereket és folyamatokat kell átvizsgálni, és milyen fejlesztéseket muszáj véghezvinni a megfeleléshez. A Micro Focus szakértői szerint az ellenőrzést és korszerűsítést az adatvédelemnél érdemes kezdeni, majd a hozzáférések kezelését és a hitelesítési folyamatokat ajánlott rendbe tenni, és végül az alkalmazások biztonsági tesztelését és az incidensek kezelését ajánlott automatizálni.

Az idei évben a NIS2 az egyik legfontosabb téma a hazai vállalatok életében. Az új EU-s kiberbiztonsági irányelv tengernyi teendőt ró a cégek széles körére. A legtöbb szervezetnél még folyik a tájékozódás a feladatokról. Sokan küzdenek azzal, hogy átlássák, pontosan milyen fejlesztésekre van szükség, és ezek mennyi idő alatt hajthatók végre. Érdemes azonban minél hamarabb belevágni, hogy ne legyen kapkodás a vége. Csak így lehet ugyanis felkészülni időben a megfelelő pénzügyi és szakmai erőforrásokkal arra az esetre, ha valahol szigorítani kell a gyakorlatokon vagy új megoldásokat és folyamatokat kell bevezetni. A Micro Focus szakértői összegyűjtötték a legfontosabb tudnivalókat a fókuszterületekről és a javasolt módszerekről.

Lépésről lépésre

A Micro Focus szakértői szerint a vállalati adatok átvizsgálásával és a kapcsolódó kockázatok kezelésével érdemes kezdeni a feladatokat. Az olyan fejlett, mesterséges intelligenciára támaszkodó eszközök, mint például a Voltage Fusion segítenek átfogó képet alkotni arról, hol találhatók érzékeny információk a rendszerekben, és milyen rizikók érintik ezeket. Sőt, szükség esetén a megoldás automatizált folyamatokkal növeli is az adatok biztonságát.

Ezek után ajánlott szigorú biztonsági irányelveket bevezetni és betartatni annak érdekében, hogy a bizalmas és fontos adatokhoz csak azok férjenek hozzá, akiknek erre valóban szükségük van. Ebben hatékony segítséget nyújthatnak az olyan teljes körű személyazonosság-kezelési rendszerek, mint például az Identity Governance and Administration. Egy ilyen megoldás átfogó képet nyújt az infrastruktúrán belül érvényes hozzáférésekről, és lehetőséget kínál arra, hogy azokat az illetékes üzleti vezetők rendszeresen felülvizsgálják a megfelelő információk birtokában. Az eszköz emellett olyan

pontos és gyorsan áttekinthető jelentések készítésére is alkalmas, amelyek segítségével a szakemberek igazolhatják a megfelelőséget.

Ha megvannak a hozzáférések, arról is gondoskodni kell, hogy a megfelelő hitelesítés társuljon hozzá. Nagyobb biztonságot garantál, ha a szervezetek többlépcsős hitelesítést használnak. Ehhez érdemes olyan technológiákat alkalmazni, amelyeket szívesen vesznek igénybe a felhasználók, mert egyszerűen használhatók, illetve nem okoznak plusz nehézségeket. Ezt a megközelítést jól támogatja egy olyan fejlett keretrendszer, mint például az Advanced Authentication, amelyben egyetlen felületen kezelhető minden hitelesítési eszköz. Ennek köszönhetően a vállalatok könnyen és gyorsan bevezethetik a felhasználók számára legkényelmesebb hitelesítési megoldásokat, amelyek használatát csak akkor kéri a rendszer, amikor azok biztonsági okokból valóban indokoltak.

Akkor teljes a védelmi stratégia, ha a cégek arra is felkészülnek, hogy minden intézkedés ellenére a kiberbűnözők betörnek a rendszereikbe. Ilyenkor segíthet egy olyan biztonsági információ- és eseménykezelő megoldás, mint például az ArcSight, amely közel valós időben elemzi a vállalati infrastruktúrában zajló tevékenységeket, majd gépi tanulásra és mesterséges intelligenciára támaszkodva azonosítja a szokatlan és gyanúra okot adó aktivitásokat, amelyeket a szakembereknek azonnal meg kell vizsgálniuk. Így a támadások még időben kezelhetők, mielőtt komolyabb kárt okoznának.

Csökkenti a támadási felületet és a kiberbiztonsági kockázatokat, ha a vállalatok figyelmet fordítanak az alkalmazásaikban előforduló sebezhetőségekre is. Ebben nyújt támogatást például a Fortify termékcsalád, amely képes átvizsgálni a cégek által használt alkalmazások forráskódját, azonosítja a bennük található sebezhetőségeket, és támogatja a fejlesztőket azok kijavításában.

Természetesen semmit nem érnek a kiberbiztonsági intézkedések, ha egy gyanútlan alkalmazott rákattint egy fertőzött linkre vagy csatolmányra. Érdemes tehát rendszeres oktatásokat tartani a munkavállalóknak, amelyeken keresztül megismerhetik az aktuális veszélyeket és támadási stratégiákat, és megtanulhatják, hogyan ismerjék fel, illetve kerüljék ki a kiberbűnözők kifinomult trükkjeit.