TELJES KÖRŰ BIZTONSÁGIRÁNYÍTÁS

A vállalati biztonság ERP-je

A vállalatirányítási rendszerek előtt is volt élet, de egészen új szintre emelte a szervezetek gazdálkodását, hogy egységben láthatták és menedzselhették az üzletet. A vállalati biztonság terén mostanában kezdik ugyanezt a szerepet betölteni a GRC-rendszerek.

TÓTHMAJOR MÁTÉ, KÜRT ZRT.

FORRÁS: ITB

„Kockázatelemzés, információbiztonság, üzletmenet-folytonosság, audit, compliance, GDPR – csupa nemszeretem kifejezés egy vállalat életében, mert az eredményt nem növelik, viszont sok munkát jelentenek. A húzódozás oka többnyire az, hogy a cégek projektalapon foglalkoznak a feladatokkal, miközben az egyes funkcionális területek között minimális az együttműködés", mondja *Tóthmajor Máté,* a Kürt Zrt. termékfejlesztési vezetője. Így aztán nem alakul ki egységes kép, amely alapján átfogóan lehetne menedzselni a vállalati biztonságot.

A biztonság összes aspektusa

Ezt az egységes képet hivatottak biztosítani a GRC- (governance, risk, compliance) megoldások. Ezek valahol ugyanazt teszik a biztonságirányítással, mint tették valaha az ERP-rendszerek az üzleti működés irányításával. Megteremtik a vállalati biztonság integrált és kockázatarányos irányítását, ahol a biztonság alatt nem csak a szűkebb értelemben vett információbiztonságot kell érteni, hanem minden olyan területet, amelynek szerepe van a vállalat működőképességének fenntartásában: kockázatkezelést, BCM-et, az auditorokat, a compliance-et.

A Kürt a vállalat szakértelmét és tapasztalatait öntötte a modulárisan felépülő SeCube GRC rendszerbe, melyet a terméktámogatási visszajelzések és bevezetési projektjei alapján folyamatosan fejleszt, és amit jelenleg is már számos pénzügyi, távközlési, létfontosságú és állami szervezet használ.

Egy vállalat, egy biztonságirányítás

A SeCube GRC novemberben megjelenő 4-es főverziójának legfőbb újítása, hogy immár teljes körű vállalati biztonságirányítást kínál. Integráltan képes irányítani a céges működés biztonságának minden aspektusát, legyen szó IT-biztonságról, üzleti, fizikai vagy humán biztonságról, bevonva az összes érintett szereplőt, közéjük értve az üzleti területek menedzsereit is.

Ha ezek a szakemberek egységes rendszerben, közös folyamatok és tudásbázis mentén dolgoznak, akkor végre közös nyelvet is beszélhetnek, említi az egyik fontos előnyt Tóthmajor Máté. Eltűnnek a biztonságirányítási szigetek, eltűnnek a különféle formátumot és nyelvezetet használó jelentések, mert minden riportot ugyanabból a környezetből lehet legenerálni, így azok konzisztensek is lesznek egymással.

Egy nyelvet beszélve

A SeCube 4 másik nagy előnye az, hogy megszűnik a biztonságirányítási munka projektjellege. Ha változik az IT- vagy üzleti környezet, arra azonnal reagálni lehet minden más területen. Az egyes területek adatainak változása inputként vagy egyenesen feladatként jelennek meg más felelősöknél. Például, ha változnak az üzleti folyamatok prioritásai, az azt kiszolgáló üzemeltetési és biztonsági területeknek védelmi tervezési feladatai keletkezhetnek, de ugyanígy az IT-infrastruktúra változásai is tovagyűrűzhetnek (mondjuk, a kockázatelemzés-aktualizálási feladatokig).

Több dolog is következik ebből. Egyrészt, a felső vezetők integrált vállalati kockázati listát látnak, egységes szempontrendszer szerint tudják összevetni, hogy melyik kockázat csökkentésére mekkora erőforrásokat érdemes fordítani, valamint követhetik a kockázatkezelési folyamatokat. Másrészt nem kell külön felkészülni az auditokra, hiszen a rendszerből generált riportok mindig a biztonsági felkészültség aktuális állapotát mutatják.

„Mindez persze csak akkor valósul meg, ha használják is a GRC-szoftvert", teszi még hozzá Tóthmajor Máté. „A SeCube csak úgy tudja ellátni feladatát, ha adatokat visznek bele, ha követik a változásokat, és azokra reagálnak is az érintettek. Ugyanakkor a SeCube használatával elérhető válik a teljes vállalati biztonság átlátható és riportálható irányítása. Ha segítesz magadon, a SeCube is megsegít." ■