

Scirge Esettanulmány

-Történet és tapasztalat, töletek, rólatok.



Kovárczi Béla-
Informatikai Védelmi
Rendszerek
Osztályvezető
Szerencsejáték Zrt.

Milyen problémákkal, kockázatokkal szembesült a Szerencsejáték Zrt. Shadow IT témában?

A Shadow IT legfontosabb kockázatai a potenciális adatszivárgás, a nem szabályozott, vagy gyenge hozzáférések, illetve adott esetben licenzelési kérdések. Sok esetben a munkatársak sem tudják miért történik regisztráció egy-egy weboldalon, ami a mélyebb tudatosítás szükségességét is jelzi.

Ezen felül a Szerencsejáték Zrt.-nél a vállalati e-mail címekkel létrehozott online fiókok közel fele nem a munkavégzéshez kapcsolódott, amelyeket törölni szükséges.

Milyen módszerrel próbálták ezt korábban megoldani, miben segített a Scirge?

A vállalat korábban tűzfal- és biztonsági logokra valamint a hétköznapi munkavégzés során kiderült információkra támaszkodva próbálta azonosítani a nem engedélyezett használatot. Ez azonban rendkívül időigényes folyamatnak bizonyult, és rengeteg vakfoltot hagyott maga után. Bár a szabályozások és az oktatások ekkor is rendelkezésre álltak, a Shadow IT felderítése így sem volt elég hatékony.

A Scirge bevezetése áttörést hozott, hiszen teljes körű átláthatóságot biztosított a vállalati e-mail címekhez kötődő webes alkalmazások használatáról. Ennek köszönhetően a kisebb, ismeretlen szolgáltatásokat is sikerült azonosítani, amelyekről korábban nem állt rendelkezésre információ. A rendszer lehetővé tette, hogy a területek vezetői áttekintsék, mely alkalmazásokra van valóban szükség, és melyek jelentenek felesleges kockázatot. Emellett azonnali visszajelzést adott a felhasználóknak kockázatos viselkedés, például jelszó-újra felhasználás esetén, ami a gyors reagálást és a tudatosítást is nagymértékben támogatta.

Mik a legfontosabb eredmények, amiket a Scirge segítségével sikerült elérni?

A vállalat rövid időn belül kézzelfogható eredményeket ért el. Nagyon pontos információkkal rendelkezünk az alkalmazásokról és felhasználókról, aminek a segítségével sikerült nagymértékben visszaszorítani a Shadow IT-t, valamint megszüntetni a felesleges regisztrációkat és online fiókokat.

A jelszóhigiéncia is jelentősen javult: a felhasználók 58 százaléka módosította jelszavát a Scirge figyelmeztetéseinek hatására.

A rendszer bevezetése teljesen új folyamatokat is elindított, például a kilépő munkatársak fiókjainak felülvizsgálatát, valamint a munkatársak személyazonosságával való visszaélések, valamint korábbi munkatársak inaktív fiókjainak kezelésére szolgáló protokoll kialakítását.

Milyen nehéz volt a rendszer implementációja, ajánlaná-e más szervezetek számára?

A Scirge telepítése mindössze két embernapot igényelt, a böngészőbővítmények bevezetése pedig zökkenőmentesen zajlott. A Szerencsejáték Zrt. tapasztalata szerint a rendszer olyan átláthatóságot biztosít, amely korábban elképzelhetetlen volt, ezért bátran ajánljuk más vállalatok számára is.

