Grayteq Classifier

Kisvállalati adatvédelem és klasszifikáció
a gyakorlatban. Esettanulmány.

Ország: Ausztria
Szektor: Informatika, fejlesztés
Ügyfél méret: 300+ alkalmazott

A feladat:

1. Fázis:
   a. Hatékony, üzlet-központú fájlklasszifikáció és címkézés kialakítása és bevezetése.
   b. A klasszifikáció napi munkára gyakorolt hatásának minimalizálása.
   c. A klasszifikáció szervezeti szintű automatizálása.
   d. A felhasználók klasszifikációra történő felkészítése, oktatása.
   e. A Microsoft Office és Adobe PDF dokumentumok címkézése besorolás-alapú kereséshez.

2. Fázis:
   a. Klasszifikáción alapuló automatikus fájlvédelem kialakítása, a Bizalmas fájlok számára.
   b. További, klasszifikáción alapuló fájlvédelem kialakítása a Grayteq DLP segítségével.

Előtörténet:

A projekt iránti igény úgy merült fel, hogy a szervezet egyik laptopját szervízbe vitték, melyen – a céges biztonsági politika által előírt – mentés és adattörlés a szervízbe vitelt megelőzően nem történt meg, így egy külső szervezethez úgy került ki egy céges gép, hogy azon valamennyi fejlesztői és egyéb a cég tulajdonát képező adat rajta maradt. Ezen hiba révén a céges adatok komoly veszélynek voltak kitéve és mivel sem klasszifikációjuk, sem azon alapuló védelmük, titkosításuk nem volt, így az eset rámutatott a felső vezetés számára az adatszivárgás figyelmen kívül nem hagyható kockázatára.

Projekt előkészítés:

Hardver és rendszer

Az ügyfél által kérésünkre biztosított két – a céges gépekkel megegyező operációs rendszerrel, szoftverekkel, beállításokkal, de céges adatoktól mentes – laptop eszközre feltelepítettük az alábbi Grayteq komponenseket:

- Grayteq Classifier Agent 20.0.0;
- Grayteq DLP Agent 20.0.0;
- Grayteq Security Server 20.0.0;
- Grayteq Dashboard 20.0.0;
- Grayteq Security Orchestrator 20.0.0;

Ezek után a két gépet egy önálló Grayteq alrendszerbe állítottuk, melyben az egyik laptopon valamennyi fenti komponens, míg a másikon csak a végponti kliensként funkcionáló gépekre telepítendő Grayteq DLP Agent és Grayteq Classifier került telepítésre. Így a két gép közül az egyik a mini rendszer „biztonsági szervereként" funkcionált, míg a másik egy klasszikus kliens számítógépet testesített meg.

Beállítások

A fenti telepítést követően beállításra került három különböző klasszifikációs szint (Publikus, Belső, Bizalmas) és a két utóbbi szinthez további két-két alszint, a GDPR érintett, illetve a GDPR által nem érintett tartalmú fájlok elkülönített kezeléséhez.

Az első körös beállítások az ügyfél IT vezetőjével egyeztetett klasszifikációs elemek beállításával valósította meg a támogatott fájltípusok klasszifikációját, úgy a felhasználók által látható

- Fájl-fejléc;
- Fájl-lábléc;
- Fájl vízjel;
- Fájl ikon jelölés;

És a felhasználók által nem látható

- Fájl címke (meta tag);
- Fájl egyedi tulajdonság (custom property)

módon.

Tesztelés

A belső tesztelések során az ügyfél által használt gépekkel, operációs rendszerekkel és szoftverekkel teljeskörű kompatibilitást mutatott valamennyi Grayteq komponens, illetve a mindkét gépen elkészített teljesítmény benchmark és felhasználói tesztek egyaránt – gyakorlatilag elenyésző léptékű terhelést és a felhasználók napi munkájában észrevehetetlen lassulást mutattak ki.

Második lépésként – ekkor még a DLP szabályokat csak limitált felhasználói körre kiterjesztve – a klasszifikációt, mint bevezetés alatt álló új munkafolyamati elemet első körben elérhetővé, majd második körben automatikussá tettük az ügyfél több, mint száz (100) felhasználója számára.

További felhasználói tesztek alapján a „corporate default” klasszifikációs szint beállítása és a felhasználók kioktatása az egyes klasszifikációs szintek közötti különbségekről és azok helyes alkalmazásáról kb. két hét alatt a fájlkészítési munkafolyamat részévé tették a klasszifikációt, míg a klasszifikáció-alapú védelme tesztelése és a DLP szabályok által védett felhasználóktól kimondottan kért, általuk választott módszer szerinti „támadó szándékú” tevékenységekről készült naplók elemzése után egyértelművé vált, hogy a klasszifikációs „kötelmek” könnyen elfogadhatóak a felhasználók által, míg a klasszifikáción alapuló DLP szabályok automatikus betartatása, naplózása és a megszegésükre tett kísérlet esetén kiváltott automatikus riasztás egyaránt beváltotta a hozzá fűzött reményeket.

A klasszifikált fájlokon a Grayteq Classifier által megjelenített ikon-jelölés a fájl megnyitása nélkül is azonnali információt nyújt a felhasználók számára a fájl besorolását illetően.

Grayteq Classifier által támogatott fájltípusok (2020.03.)

Projekt:

Kiterjesztés

Az előkészítő fázis tapasztalatait felhasználva a kiterjesztést megelőzően történt néhány „finomítás” a klasszifikációs szintek tekintetében, melyek révén a tesztek során használt 5 szint 7-re bővült ugyanis a Belső és Bizalmas szintek GDPR-érintett alszintjeit – a jogi osztály kérésére – két részre kellett bontanunk Hozzájárulás alapú és Egyéb jogalapú adatkezelési szintre.

A fenti módosítás elvégzése után – két lépésben, lépésenként egy hét „szünetet” beiktatva – az ügyfél valamennyi számítógépére és felhasználójára kiterjesztésre került a Grayteq Classifier.

Folytatás

A projekt következő lépésében a Grayteq DLP által biztosított automatikus védelmi szabályozások kerültek bevezetésre és kiterjesztésre, melyek révén a Belső illetve a Bizalmas minősítésű dokumentumok szervezeten kívülre juttatását a Grayteq DLP automatikusan megakadályozza, míg a Bizalmas minősítésű dokumentumokat a klasszifikálást követően azonnal, automatikusan erős titkosítással látja el, mely titkosítás visszafejtésére csak a Bizalmas dokumentumokba betekintéssel rendelkező felhasználók számára kerül sor.

Valamennyi Belső vagy Bizalmas minősítésű fájl szervezeten kívülre juttatási kísérletről – a tevékenység megakadályozása mellett - automatikus, heti összesítésű jelentés készül, míg a Bizalmas minősítésű dokumentumok illetéktelenek által kezdeményezett elérési kísérleteiről azonnali, valós idejű riasztást kap az IT vezető.

Ugyanakkor az ügyfél által kért címke-rendszer fájlokon történő alkalmazása révén a különböző besorolással rendelkező fájlok fizikai elhelyezkedése azonnal listázhatóvá és nyomon követhetővé vált.

2. Fázis:

Védelmek

Ebben a fázisban érkezett el végre az ügyfél eredeti igényének, a klasszifikáción alapuló védelmek bevezetésének megvalósítása, melynek során egyrészről kialakításra került a Grayteq Classifier által Bizalmas szintre klasszifikált fájlok klasszifikáció során automatikusan, valós időben történő erős, iparági sztenderd titkosítással történő védelme, másrészről a Belső klasszifikációjú fájlok „cégen belül” tartásához szükséges átfogó, valamennyi „kijáratot” lefedő biztonsági politikájának kialakítása, tesztelése és rendszerbe állítása.

A kialakított biztonsági politikák részleteiről az ügyfél rendszerének védelme érdekében részleteket nem közölhetünk.

Konklúzió:

A projekt klasszifikációs és adatvédelmi, valamint adatbiztonsági megfelelőség fejlesztő célkitűzései maximálisan teljesítésre kerültek, így az ügyfél a rendszer három (3) évre történő licensz meghosszabbítása mellett döntött.