

“A rendszer azóta is több nulladik napi kártevőt – köztük titkosító vírust is – blokkolt, megóvva ezáltal az intézményi adatvagyonot. Nem mellékes az sem, hogy egy ilyen incidens - még ha az adatvesztés el is kerülhet - milyen hatással van az üzletmenet folytonosságára, mennyire kerülhet veszélybe az intézmény napi működése a helyreállítás idejére.

A Microsoft Azure alapú Panda Adaptive Defense 360 és a Systems Management mára szerves részévé vált intézményünk IT ökoszisztémájának.”

Soós Tamás

Informatikai irodavezető



Intézmény

Eszterházy Károly
Egyetem Oktatókutató
és Fejlesztő Intézet

Megoldás

Panda Fusion with
Adaptive Defense 360 +
Advanced Reporting Tool

Számítógépek száma
200

Információk az intézményről

Az Oktatókutató és Fejlesztő Intézet az oktatási ágazat stratégiai kutató-fejlesztő és szolgáltató intézménye. Alapfeladatát a magyar közoktatás, esetenként a felsőoktatás fejlesztése érdekében végzett kutatási, fejlesztési, innovációs és szolgáltatási tevékenység jelenti. Az intézet tevékenysége a közoktatási és felsőoktatási kutatásokra és fejlesztésekre, nemzetközi elemzésekre, az oktatásirányítás szakmai döntéseit előkészítő szakértői tevékenységekre, adatszolgáltatásokra, valamint a szakmai eredmények széles körű disszeminációjára is kiterjed. Az Oktatókutató és Fejlesztő Intézet feladata továbbá a Nemzeti alaptantervnek megfelelő állami tankönyvek fejlesztése, előállítás.



OKTATÓKUTATÓ
ÉS FEJLESZTŐ
INTÉZET



Előzmények

Korábban előfordult, hogy egy nulladik napi kártevő átcsúszott a rendszeren, és bár az adatokat a megfelelő mentési struktúrának köszönhetően adatvesztés nélkül vissza tudták állítani, az esetet tanulságként kezelték és a menedzsmenttel közösen úgy döntöttek, itt az ideje felülvizsgálni a végpontvédelmi rendszerüket, hogy mennyire felel meg a kor kihívásainak.

Az intézmény kiemelt feladatot lát el az oktatás-támogatás terén, így nagyon fontos, hogy az informatikai rendszerük naprakész és védett legyen a legújabb típusú kártevők ellen is.

Kihívások

Az informatikai infrastruktúra főként virtualizált környezetbe helyezett Microsoft Windows szerverekből és Windows 10-es, tartományba léptetett munkaállomásokból áll. Minden munkatárs (kutatók, tankönyvírók, projekttes és funkcionális egységek dolgozói) a hálózati fileszerverekre dolgozik. Ezeket tárolják az állami tankönyvfejlesztéshez szükséges munkaállományokat, melyek száma az évek során több mint százmillióra nőtt és közel 200 TB-nyi helyet foglalnak a storage szervereken.

Megoldás

Piackutatásuk során került látóterükbe a Panda Security megoldása, amely a nulladik napi kártevők ellen is védelmet nyújt, valamint egy komplex felügyeleti rendszerrel kiegészülve az üzemeltető kollégák részére is komoly segítséget jelent.

Egy bemutató után elkezdtek a saját rendszerükön tesztelni, és igyekeztek a lehető legtöbb szempont alapján megvizsgálni, hogy megfelelően tudják-e alkalmazni. Már a bevezetés kezdetén tapasztalták, hogy a felhő alapú központi menedzsment infrastruktúrának köszönhetően mennyire egyszerű a telepítés, a monitorozás, a rendszereik up-to-date állapotban tartása, ezáltal csökkent az IT-s kollégák leterheltsége is.

A teszt időszaka alatt folyamatos kapcsolatban voltak a Panda Security képviselőivel, így a tesztidőszak gördülékenyen zajlott, a szoftver megfelelt az elvárásoknak, mind az üzemeltetés, mind pedig a biztonsági szint és az erőforrás tekintetében, így úgy döntöttek, hogy a jövőben a Panda Security megoldását fogják alkalmazni.

Költségvetési intézményként természetesen az anyagi szempontokat is figyelembe kellett venniük. Felmérve, hogy mit kockáztatnak, a biztonság mellett tették le a voksukat. A választásukat megkönnyítette az egységes licencelés, mert a szerverekre, munkaállomásokra és a mobil eszközökre is ugyanaz használható. Kiemelték az integrált MS Exchange szerver védelmet, melynél - felhasználószámától függetlenül - egyetlen licenc felhasználásával meg tudják védeni a levelezésüket a szofisztikált zsarolóvírusok és egyéb kiberkémkedési metódusok ellen.