CTRL

MENEDZSELT VÉGPONTVÉDELEM

Az IT biztonság megteremtése a végpontokon ciklikusan ismétlődő folyamat. Célja, hogy mindig a támadók előtt legyünk egy lépéssel!

Felelős vezetőként bizonyára Ön is tisztában van a kiberbiztonsági fenyegetések veszélyeivel. Egy incidens során nem csak a folyamatos üzletmenet biztosításához elengedhetetlen rendszerek állhatnak le (konkrét pénzügyi kárt okozva), de akár rossz kezekbe is kerülhet az értékes céges adatvagyon. Ez a működési nehézségek mellett bizalomvesztéshez vagy akár a cég piaci jóhírének sérüléséhez is vezethet.

Talán Ön is feltette már magának a kérdést: a saját vállalatánál alkalmazott IT-biztonsági megoldások vajon elegendőek-e egy komplex támadás megelőzésére, felismerésére és kivédésére? Van-e elég erőforrás a kiberbiztonság megfelelő szinten tartására, valamint a folyamatos felügyeletre és fejlesztésekre? Vajon mikor készült riport utoljára a cég forgalmi adatairól és IT biztonsági eseményeiről? Egyáltalán észlelnék-e a napjainkban egyre sűrűbben előforduló biztonsági incidenseket?

Bízza szakértőinkre saját cégének informatikai biztonságát, válassza a Menedzselt végpontvédelem szolgáltatást!

CYBER THREAT RESILIENCE TEAM

CTRL

HATÉKONY VÉDELEM AZ ÖSSZETETT FENYEGETÉSEK ÉS A CÉLZOTT TÁMADÁSOK ELLEN

A vállalati hálózatok határfelületeinek elmosódása a felhőszolgáltatások térnyerésével felerősödött, ezt a tendenciát a pandémia és a távmunka lehetőségek kialakítása tovább gyorsította.
A távmunka jellegéből adódóan a végpontok a határvédelmi eszközök hatókörén kívülre kerülhetnek, ezért a végpontvédelmi megoldások jelentősége is felértékelődik.
A végpontokon megjelenhet olyan titkosított forgalom, amelyet a határvédelmi berendezéseken nem, vagy csak körülményesen lehet ellenőrizni, így a felderítési képességeket csak a kliensen telepített védelmi szoftverek biztosíthatják.
Az operációs rendszerek és széles körben használt alkalmazások sérülékenységei számtalan lehetőséget kínálnak a kiberbűnözők számára, ezért a végpontok folyamatosan fejlesztett védelmére is kiemelt hangsúlyt kell helyezni.
A zsarolóvírus támadások célpontjai már nem kizárólag a nagyvállalatok, bárki áldozatul eshet egy-egy kampánynak, amelyek egyre körmönfontabb módon próbálják a védelmi vonalakat kijátszani.

A Telekom **havidíjas szolgáltatás** keretében biztosítja ügyfelei számára a végpontok kártékony kódok elleni védelmét. A szolgáltatás a munkaállomások és szerverek folyamatos, valós idejű és ütemezett ellenőrzését végzi, hagyományos és új generációs módszerekkel egyaránt.

GYORS IMPLEMENTÁCIÓ + SZAKÉRTŐ ÜZEMELTETÉS = MEGBÍZHATÓ VÉDELEM

CTRL Menedzselt végpontvédelem szolgáltatásunk előnyei:

- A szolgáltatás igénybevételéhez nem szükséges az Ügyfél hálózatában központi felügyeleti szerver telepítése, csak a végpontvédelmi komponensek disztribúcióját kell megoldani.
- Különböző igényeknek megfelelő és rugalmasan bővíthető szolgáltatáscsomagok.
- Nincsenek ügyféloldali üzemeltetési feladatok, erőforrásigények.
- Magas rendelkezésre állás
- Havidíjas konstrukciós forma, tervezhető költségekkel.

FELÜGYELETI FUNKCIÓK

Ügyfelünk részére egyedileg kialakított, szigorúan elkülönített térben nyújtjuk a központi menedzsment szolgáltatásokat. **A felhasználói- és eszköz adatok, házirendek, telemetria adatok és riportok kezelése is elkülönítve történik** a szolgáltató **európai adatközpontjában.**
A felügyeleti funkciókat a Szolgáltató szakemberei jogosultsági szintekhez rendelt nézeteken keresztül látják el.
A Telekom szakemberei teljes körű szolgáltatásként biztosítják a a rendszer beállítását, karbantartását, a telepítő készletek kiajánlását, a házirendek módosítását, a licencek kezelését, , valamint a használattal kapcsolatos riportok elkészítését.

WEB REPUTÁCIÓ ÉS URL SZŰRÉS

A végponti URL szűrés segítségével **szabályozzuk a webhelyekhez való hozzáférést** ez által nagy mértékben növelve a **biztonságos internethasználatot**. Az URL szűrés lehetőséget ad a védelmi szintek beállítására és az egyes wbhelykategóriák elérésére vagy tiltására **kategóriák alapján történő.**
A szolgáltatás megakadályozza, hogy a felhasználók kártékony vagy tiltott oldalakhoz férjenek hozzá, és biztosítja, hogy a megtekintett oldalak mentesek legyenek a rosszindulatú programoktól, kémprogramoktól és adathalász csalásoktól, amelyek célja, hogy rávegyék a felhasználókat személyes adataik megadására.
A szűrés akkor is működik, ha a végpont a határvédelmi eszközök (proxy, tűzfal) hatókörén kívül van.

CTRL

KLASSZIKUS ANTIVÍRUS

Az első védelmi vonalat a végpontokon kezelt fájlok írási és olvasási műveleteinek **folyamatos ellenőrzése,** valamint a memóriában futó alkalmazások vizsgálata jelenti. A kreatív tömörítési módszereket használó kártevők felismerését is hatékonyan végzi a végpontvédelmünk **heurisztikus eljárás segítségével**. Az megfelelően optimalizált ellenőrzési funkciónak köszönhetően a számítógépeken csak egy kisebb méretű vírusvédelmi adatbázist tárolnunk, így **nagy mértékben csökken a teljesítményigény, valamint a kártevők felismeréséhez szükséges időtartam.** Az esetek döntő többségében elegendő a helyi adatbázis használata, ugyanakkor **kérdéses esetben felhőszolgáltatásunk is bevonásra kerülhet.**

ÚJ GENERÁCIÓS ANTIVÍRUS (NGAV)

Míg a klasszikus vírusvédelmi megoldások kódrészeket és más, nem változó ismert jeleket keresnek, **az új generációs víruskereső képes a hagyományos végpontvédelmet megkerülő fenyegetések jellegzetességei, felépítésük és viselkedésük alapján azonosítani.**
Az NGAV modul képes fájl-alapú és csak memóriában futó kártevők azonosítására is. **Képes felismerni a zsarolóvírus viselkedést és kriptovaluta bányászatot is.**
Az ismeretlen kártékony kódok felismeréséhez az NGAV egyebek mellett **gépi tanulással** és **mesterséges intelligenciával** támogatott módszereket is felhasznál.

CTRL

TESTRE SZABHATÓ CSOMAGOK VÁLASZTHATÓ KIEGÉSZÍTŐ SZOLGÁLTATÁSOKKAL

A Menedzselt végpontvédelem szolgáltatás vállalata igényeire szabható. Válassza azt a csomagot, amivel vállalata a legmegfelelőbb védelemben részesül. Amennyiben segítségre van szüksége a választásban, kérjük vegye fel velünk a kapcsolatot. Kollégáink készséggel állnak rendelkezésére.

CSOMAGOK TARTALMA	ALAP SZINTŰ	EMELT SZINTŰ
Általános szolgáltatások		
Ügyfelenként dedikált tenant	✔	✔
Európai adatközpont	✔	✔
Magas rendelkezésre állású felhőszolgáltatás	✔	✔
Több szintű adminisztratív hozzáférés, role based access	✔	✔
Ügyfelenként és termékenként beállítható házirend sablonok	✔	✔
Csoport alapú házirend kezelés elérhető	✔	✔
Végpontok bevonása többféle módon telepítő link, telepítő csomag letöltése és disztribúciója 3rd party eszközzel, közvetlen telepítés a konzolt futtató végponton	✔	✔
Biztonsági szolgáltatások		
Gyártói felhős threat adatbázis	✔	✔
Hagyományos, szignatúra alapú antivírus modul	✔	✔
Új generációs antivírus modul (behavior monitoring, predictive machine learning)	✔	✔
Kriptovírusok elleni célzott védelem	✔	✔
On-access scan	✔	✔
On-demand scan	✔	✔
Web reputációs és URL szűrés	✔	✔
URL fekete- és fehérlisták	✔	✔
Automatizált riportküldés	✔	✔
Device Control / USB control *	✔	✔
Mobile security – Android *	✔	✔
Application control *	✔	✔
Desktop Firewall *	✔	✔
Bitlocker kezelése (encrypt/decrypt) **	✔	✔
Vulnerability Protection **	✔	✔
Data Loss Prevention **	✔	✔
EDR / XDR***	–	✔
Threat intel***	–	✔
Threat investigation, threat hunting***	–	✔
Végpont izolációja***	–	✔
Sandboxing***	–	✔

* A funkció hangolása ügyfél- és szolgáltató oldali együttműködést igényel, és az alap havidíjon felül külön díjazása van. Kérje szakértőnk segítségét!
** A funkció a csomagban rendelkezésre áll, de szükséges a végpontokon aktiválni.
*** A szolgáltatást A CTRL SOC szolgáltatással együtt értékesítjük, amely tartalmazza IT biztonsági szakemberünk támogatását, érdeklődjön szakértőnknél a CTRL SOC szolgáltatásról!

TOVÁBBI INFORMÁCIÓÉRT FORDULJON ÜGYFÉLMENEDZSERÉHEZ, VAGY ÍRJON SZAKÉRTŐINKNEK A **CTRL_SOLUTIONS@TELEKOM.HU** E-MAIL CÍMRE!

CYBER THREAT RESILIENCE TEAM