# Kibervédelem

## Koncepció és terminológia

# Tartalomjegyzék

# 1. Bevezetés

Az alábbi dokumentum tágabb betekintetést kíván adni a kibervédelem koncepciójába és terminológiájába. A szöveg leegyszerűsített meghatározásokat, modelleket és struktúrákat vázol. A célcsoportba olyan egyének és szervezetek tartoznak, akik és amelyek szeretnék megérteni a kibervédelem alapjait, különös tekintettel a fizikai védelmi rendszerekre. A dokumentum terminológiája és definíciói utalásokat tartalmazhatnak az Axis kibervédelemmel kapcsolatos dokumentumaira.

# 2. Kibervédelem

A kibervédelemnek számos definíciója létezik. A Wikipedia meghatározása a számítógépes biztonságra utal:

> *A számítógépes biztonság, más szóval kiberbiztonság vagy IT-biztonság, a számítógépes rendszerek lopás, vagy a hardver, szoftver, illetve információ sérülése elleni védelmet jelenti, beleértve az általuk nyújtott szolgáltatások – megszakítástól vagy eltérítéstől – való megóvását.*

Nincs általános recept arra, hogyan védjük meg magunkat az online térben. A digitális biztonság nem csupán arról szól, hogy milyen eszközöket használunk, sokkal inkább, a fenyegetések megértéséről és az azok elleni védekezés mikéntjéről van szó. A biztonság növelése érdekében meg kell határoznunk, hogy mit és kitől kell megvédenünk. A fenyegetések a tartózkodási helytől, az adott tevékenységtől és a munkatársaktól függően eltérők lehetnek. Éppen ezért, a legjobb megoldás kiválasztása érdekében fel kell állítanunk egy, a fenyegetéseket értékelő modellt.

# 3. Kockázatértékelés

A kibertérben zajló kockázatelemzési folyamat igencsak hasonló a fizikai védelemben végzett kockázatfelméréshez. Míg a fizikai világban jellemzően fizikai tárgyakat, épületeket, illetve magukat az embereket kell megvédeni, addig a kibertérben a biztosítani kívánt vagyont az információ és az adat jelenti, az erőforrásokat pedig szolgáltatások. A fizikai behatolást könnyebb felismerni, a lopás és a károkozás sokkal feltűnőbb.

Íme öt alap kérdés, amely segít a kockázatok felmérésében:

1. Mit akarunk megvédeni?

2. Kitől akarjuk megvédeni?

3. Mekkora a valószínűsége, hogy védelemre lesz szüksége?

4. Milyen súlyosak lehetnek a következmények, ha kudarcot vallunk?

5. Mekkora bajnak kell történnie ahhoz, hogy megelőzzük ezeket a következményeket?

Az ISO 27000 információ-védelmi szabvány hozta be az úgynevezett „CIA-hármast", amely a vagyon Bizalmas jellegét (angolul: Confidentiality), Elérhetőségét (Availability) és Integritását (Integrity) jelenti.

Milyen hatása van annak, ha nem érjük el adatainkat vagy a szolgáltatást, ha megsemmisülnek az adatok, vagy ha azok illetéktelenek kezébe kerülnek? A hatások felmérése érdekében az adatokat osztályoznunk kell, mivel az eltérő adattípusok értéke is különböző lehet.

Az ISO-szabvány az adatokat és a szolgáltatásokat három kategóriába, zárt, magáncélú és nyilvános osztályba sorolja.

Egy videórendszer például a felhasznált erőforrásokat a következőképpen osztályozza:

> Az élő videókép nyilvánosnak minősül. Ez az általános nyilvánosságot, valamint egy szervezeten belüli nyilvánosságot is jelentheti. Ha egy élő videókép a nyilvánosság számára elérhető, a károkozás is korlátozott mértékű.

> A videófelvétel magáncélúnak minősül, mivel az a szervezet egy meghatározott egysége számára érhető el, ugyanis egyes eseményekről készült felvételek érzékenyek lehetnek.

> A rendszerkonfigurációk, a felhasználói fiókok és a jelszavak zártnak minősülnek, és csupán a feljogosított személyek számára érhetők el a szervezeten belül.

# 4. Fenyegetettségi térkép

Mindig van egy mögöttes indoka annak, ha valaki kihasználja a sérülékenységet és megtámad egy rendszert. Az alkalom szülte támadások mellett külön kategóriát jelentenek a célzott behatolások. A kibervédelemben a támadókra gyakran ellenségként utalnak, akik rossz szándékból ugyanúgy okozhatnak sérülést a vagyonban, mint akár esetlegesen, véletlenszerűen is.

Napjaink jellemző támadásainak döntő többsége alkalmi támadásnak minősül: ezekben az esetekben már a lehetőség maga megadja a támadási felületet. Sok esetben az alkalom szülte támadók nem is tudják, hogy kik az áldozatok. Ezek a támadók olcsó támadási vektorokat alkalmaznak, így például nyitott hálózatok, szolgáltatások és portok után kutatnak, amelyekben aztán az alapértelmezett vagy éppen gyakran használt jelszavakkal próbálkoznak, patch nélküli szolgáltatásokat találnak és adathalász e-maileket küldenek. Az alkalmi támadóknak nem áll szándékukban további időt és erőforrást szánni egy meghiúsult támadásra, azonnal továbblépnek a következő célpont felé. Egy sztenderd szintű védelem mérsékli a legtöbb alkalmi támadás kockázatát.

A célzott támadás elleni védekezés már keményebb dió, hiszen ilyen esetekben már egy meghatározott rendszer ellen konkrét céllal végrehajtott támadásról van szó. A célzott támadások esetében ugyanazokat az olcsó támadási vektorokat alkalmazzák, amelyeket az alkalmi támadók is. Ugyanakkor, ha az első behatolási kísérlet sikertelen is, a támadók már elszántabbak, időt és energiát nem sajnálva, egyre kifinomultabb módszereket vetnek be, attól függően persze, hogy milyen értéket képvisel a támadási cél. A célzott támadások során gyakran használnak kifinomult, társadalmi kapcsolatokon alapuló, vagy éppen adathalász módszereket (egy jól felépített e-maillel támadnak egy meghatározott címzettet) azért, hogy hozzáférést szerezzenek egy rendszerhez. Ha ezek sem vezetnek sikerre, rendszer- és szoftverelemzésbe kezdenek, vagy megkeresik a sérülékenységek kihasználásának egyéb lehetőségeit.

# 5. Fenyegetések és motivációk

Ha felismerjük kik is a legvalószínűbb támadók, megérthetjük lehetséges motivációjukat, és képet kaphatunk arról, hogy mennyi időt, energiát és elszántságot fektetnek majd a támadásba, valamint azt is, hogy mely sérülékenységet célozhatják meg a legnagyobb eséllyel.

> **Hozzánk közel állók**, akik szeretnének bepillantani magánéletünkbe.

> **Alkalmazottak vagy azok**, akik szabályos hozzáféréssel rendelkeznek, és akik akaratlanul vagy épp szándékosan élnek vissza ezzel.

> **„Mókamesterek"**, akik örömöt lelnek, illetve kihívást látnak abban, ha belepiszkálhatnak számítógépes rendszerekbe.

> **Hacktivisták, azaz olyan „mozgalmárok"**, akik politikai vagy más ideológiai okok miatt támadnak egy szervezetet.

> **Kiberbűnözők**, akik csalással vagy értékes adatok eladásával igyekeznek anyagi haszonra szert tenni.

> **Ágazati versenytársak**, akik vállalatuk számára gazdasági előnyt kívánnak szerezni.

> **Kiberterroristák**, akik politikai vagy más ideológiai okokból kifolyólag szeretnének olyan támadást végrehajtani, amely riadalmat vagy pánikot kelt.

> **Nemzetállamok (külföldi titkosszolgálatok)**, amelyeket gazdasági, politikai előny megszerzése vagy a kritikus információs rendszerekben való károkozás motivál.

> **Magánszemélyek – egy adott személy vagy egy csoport –,** akik önállóan lépnek akcióba és motivációjuk eltérhet a fent felsoroltaktól. Egy oknyomozó újságíró éppúgy ide tartozhat, mint egy etikus hekker. Ez utóbbi is fenyegetést jelenthet, ha arra fordítjuk erőforrásainkat, hogy elrejtsük a hibáinkat és sérülékenységeinket, ahelyett, hogy kijavítanánk azokat.

## 6. A támadások értéke és költségei

Egy támadás értéke attól függ, hogy mekkora a sikeres behatolással megszerezhető haszonnak a támadás költségeivel arányosított nagysága. A kiberbiztonságban a cél az, hogy a támadás költségei meghaladják az azzal szerezhető hasznot, ezzel is csökkentve a támadási értéket (az érték = haszon mínusz költségek). A megfelelő védelmi szint elérése érdekében (voltaképpen megalapozva a támadási költséget), fontos tudni, milyen fenyegetések a legvalószínűbbek. Bár valamennyi rendszer kitett lehet a támadásoknak, vagy ilyen szándéknak, egyes fenyegetéseknek mégis nagyobb a valószínűsége. Annak megértése, hogy mely támadások fordulhatnak elő a legnagyobb eséllyel, segíthet beazonosítani a biztonsági intézkedések fókuszát, vagyis azt, hogy mely sérülékenységeket használhatják ki a legnagyobb valószínűséggel.

## 7. Általános szervezeti típusok és fenyegetések

Egy támadás negatív hatásai jellemzően attól függnek, hogy milyen típusú szervezet válik áldozattá.

| **Szervezeti típus** | **Példák** | **Lehetséges támadók** | **Hatás** |
|---|---|---|---|
| Kis szervezetek | > Fogyasztók<br>> Családi vállalkozások<br>> Non-profit szervezetek | > Családtagok, barátok<br>> Mókamesterek<br>> Alkalom szülte hekkerek | **Egyéni** szint<br>> Magánélet<br>> Becsület, integritás |
| Üzleti szervezetek | > Iparágak<br>> Vállalatok<br>> Kiskereskedők | A fentieken kívül:<br>> Alkalmazottak<br>> Hacktivisták<br>> Szervezett bűnözők<br>> Versenytársak | **Business** szint<br>> Anyagi veszteség<br>> Leállási idő<br>> Bizalom<br>> Szellemi tulajdon<br>> Versenyhátrány |
| Kritikus infrastruktúrák szervezetei | > Energetika, vízszolgáltatás<br>> Bank, pénzügy<br>> Távközlés, hírközlés<br>> Közlekedés<br>> Egészségügy<br>> Rendőrség, hadsereg | A fentieken kívül:<br>> Nemzetállamok<br>> Kiberterroristák | **A nyilvánosság** szintje<br>> Biztonság<br>> Ellátás<br>> Pánik |

# 8. Kockázatok

A „kockázat" fogalmát sokféleképpen definiálhatjuk. Az RFC 2828 Internet-biztonsági Jegyzék a kockázatokat a következőképpen határozza meg:

*„A kockázat a várható veszteség valószínűsége, annak függvényében, hogy egy adott fenyegetés milyen károkozási eredménnyel használ ki egy adott sérülékenységet."*

Ennek rövid verziója, amelyet számos helyzetben alkalmazunk: a „kockázat = a valószínűség és a hatás szorzata". Ez a formula a különböző fenyegetési típusok rangsorolására használható. Az RFC meghatározása tartalmazza az „adott" szót is a fenyegetés, a sérülékenység és a károkozó eredmény leírására. Minden fenyegetést egyedileg kell megvizsgálni, kezdve attól, amely a legvalószínűbb és amely a lehető leginkább negatív hatással bír.

Valamennyi védekezési típusra (a „CIA-hármasra", vagyis a bizalmas jellegre, az integritásra és az elérhetőségre) vonatkozóan egyaránt fontos, hogy megértsük egy fenyegetés negatív hatásait. Ez nehéz feladat: a becslések sok esetben szubjektívek, a hatásokat ráadásul gyakran alábecsülik. Az ISO 27000 hatástípusai (**korlátozott, komoly, súlyos és végzetes hatások**) némi segítséget nyújthatnak a prioritások felállításában. A hatástípusok az alapján is meghatározhatók, hogy mennyi időt venne igénybe a károk helyreállítás. Eszerint: a korlátozott hatás esetén órákat, napokat, a komoly hatást követően heteket vehet ez igénybe, míg a súlyos hatás után hónapokig is eltarthat a helyreállítás. A végzetes hatás után mindez évekbe telne, ha egyáltalán lehetséges a teljes helyreállítás.

# 9. Biztonsági ellenőrzések

A biztonsági ellenőrzések beiktatásának folyamatát megerősítésnek nevezzük. A biztonsági ellenőrzések azok a védelmi vagy ellenintézkedések, amelyekkel elkerülhetők, detektálhatók, ellensúlyozhatók vagy éppen minimalizálhatók a fizikai tulajdont, információt, számítógépes rendszert vagy vagyont fenyegető biztonsági kockázatok. A kompenzációs ellenőrzés alternatív védelemnek számít, amelyet akkor alkalmazhatunk, amikor a kívánt biztonsági kontroll nem alkalmazható, vagy ha a kívánt védelem túl sokba kerülne.

A hozzáférés korlátozása és a kitettség csökkentése egyaránt csökkentik egy rendszer felhasználhatóságát. A rendszer használhatósága és védelme közötti egyensúly megteremtése gyakran nehéz kompromisszumot követel felhasználók, valamint a rendszer védelméért felelős vezetők között. Ha túl sok a korlátozás, a felhasználók megtalálják a módját a védelem megkerülésének, így újabb sérülékenységeket okoznak. A felhasználhatóság és annak védelme közötti kívánatos egyensúlyt a rendszer tulajdonosának kell meghatároznia.

# 10. Sérülékenységek és kitettségek

A sérülékenységek lehetőséget jelentenek a hekkereknek, hogy hozzáférést szerezzenek egy rendszerhez. Mindez hibákból, különböző tulajdonságokból vagy felhasználói tévedésekből is fakadhat, a támadók pedig ezek bármelyikét képesek kihasználni, de akár több sérülékenység együttes használatával is célt érhetnek.

Kutatások szerint a sikeres támadások több mint 95 százaléka három tényezőhöz köthető: emberi mulasztások, gyenge rendszer-konfiguráció, valamint elégtelen karbantartás. Ezek jellemzően a megfelelő irányelvek és meghatározott felelősségi körök/szerepek hiányából fakadnak.

Egy API-eszköznek (alkalmazás-programozó felület – Application Programming Interface) és a szoftver-szolgáltatásoknak lehetnek olyan hibái, amelyeket egy támadás során kihasználnak. Egy beszállító sosem garantálhatja teljes körűen, hogy termékei hibátlanok. Ha a hibákra fény derül, a kockázatok a biztonsági kontroll fokozásával csökkenthetők. Ha egy támadó ismeretlen hibát fedez fel, vagy akár zero-day támadásra kerül sor, az áldozatnak nincs ideje megvédeni a rendszert.

A nem kritikus sérülékenységek azok, amelyeknek csekély hatása van, vagy amelyeket nagyon nehéz is kihasználni, még ha a potenciális hatás komoly is lehet. Egy kritikus hiba kihasználása több feltételhez kötött egyidejűleg, beleértve a rendszerhozzáférést és az ezzel elérhető erőforrásokat.

Az Általános Sérülékenységi Pontrendszer (Common Vulnerability Scoring System, CVSS) egyike azon lehetőségeknek, hogy a szoftver-sérülékenységeket komolyságuk alapján osztályozzuk. Az alkalmazott formula azt vizsgálja, hogy milyen könnyű kihasználni egy adott sérülékenységet, illetve, hogy az milyen negatív hatásokkal bírhat. A pontrendszerben az értékek nulla és tíz között szóródnak, ahol a tíz a legkomolyabb hatást jelenti. A CVSS számot gyakran használják az Általános Sérülékenységi és Kitettségi (Common Vulnerability and Exposure, CVE) jelentésekben. Az Axis a CVSS mérőszámmal azt mutatja meg, hogy egy azonosított sérülékenység a szoftverben vagy a termékben mennyire válhat kritikussá.

A kitettség ugyancsak nagy szerepet játszik a sérülékenységi kockázatok meghatározásában. Milyen könnyű egy támadó számára a sérülékenység kihasználása? Ez az infrastruktúrától, a szolgáltatás kitettségétől és a napi üzemeltetéstől is függ. Például: egy sérülékenységi kockázat komolynak minősülhet egy olyan nyilvános webszerveren, amely egy vállalat üzleti portálját szolgálja ki. Ugyanez a sérülékenység korlátozott is lehet például egy helyileg védett kamera-hálózatban.

## 11. Sérülékenység-vizsgálat

A sérülékenység-vizsgálat a szoftver- vagy termékauditálás egy automatizált vagy kézi megoldását jelenti. Számos ilyen vizsgálati eszköz érhető el a piacon. A vizsgálatok olyan szolgáltatásokat igyekeznek azonosítani, amelyek ismert sérülékenységet hordoznak. Egy támadó ugyanis kihasználhat ilyen szolgáltatást.

A sérülékenység-vizsgálat kizárólag ismert sérülékenységek felderítésére alkalmas. Az eredmények nem adnak pontos képet arról, hogy egy termék valójában mennyire biztonságos. Holnap egy új kritikus sérülékenységet fedezhetnek fel. A sérülékenység-vizsgálatot gyakran keverik a penetrációs (behatolási) teszteléssel, amely azt vizsgálja, miként kerülhetők meg a biztonsági intézkedések. A sérülékenység-vizsgálat csak a lehetséges sérülékenységek azonosítására alkalmas.

## 12. IP-szűrés

Az IP-szűrés egyfajta helyi tűzfalként működik a kamerában. Egy professzionális videórendszerben, a VMS (Video Management System) áll a rendszer középpontjában. A videó-kliensek nem közvetlenül a kamerából érik el videót: az élő és a rögzített kép a VMS-szolgáltatásokon keresztül jut el a felhasználóhoz. Ez azt jelenti, hogy az egyetlen számítógép, vagy szerver fog VMS-szerverként funkcionálni, amely normál működés közben eléri a kamerát. Amennyiben a videórendszer nem egy leválasztott hálózatban található, ahol a nem videó-kliensek is hálózati eléréssel rendelkezhetnek a kamerához, az IP-szűrés kiegészítő védelemként alkalmazható. Az IP-szűrésnek köszönhetően a kamera nem válaszol az olyan IP-címekről érkező lekérdezésekre, amelyek nem szerepelnek a jóváhagyott listán (whitelist). Ezen a listán szerepelnie kell a VMS szervernek, az AXIS Camera Manager (ACM) szerverének és azoknak a számítógépeknek, ha vannak, amelyeket hibakeresésre és karbantartásra használnak.

## 13. Hálózati leválasztás

A hálózati leválasztás az egyik módja annak, hogy elválasszunk egymástól kritikus hálózati erőforrásokat, ezzel is csökkentve annak esélyét, hogy ezek káros hatást fejtsenek ki egymásra. A leválasztás különösen fontos olyan erőforrások esetében, amelynek nem kell, vagy nem szabad interakcióba lépniük egymással. A hálózati leválasztás történhet virtuálisan (VLAN), amelyhez menedzselt switchek adják az infrastruktúrát, de a hálózatokat eltérő kábelezéssel vagy eszközökkel is elválaszthatunk egymástól. Az, hogy pontosan mely megoldást választjuk a hálózati leválasztásra, az a költségek, az infrastruktúra, valamint a vállalati irányelvek függvénye is lehet.

A jó, mindenre kiterjedő védelemben a fizikai biztonsági hálózatot elválasztják a többi hálózati – például a domaint kiszolgáló – erőforrástól. E két erőforrás közé tűzfalat is helyezhetünk, ha az egyik hálózat videóklienseinek el kell érniük a másik hálózat VMS szervereit. A tűzfalnak csupán a kliens és a VMS szerver közötti forgalmat szabad megnyitnia, nem adhat forgalmi elérést a kamerához.

## 14. Hálózati kódolás – HTTPS

A hálózati kódolás célja, hogy megvédje a kliens, a VMS és a kamera közötti kommunikációt. Ez akadályozza meg, hogy a hálózati forgalom megcsapolásával információ szivároghasson ki, illetve kiküszöböli azt is, hogy az átvitel során az adatokat megváltoztassák. A hálózati kódolás nem feltétlenül növeli a kamera, a VMS vagy a kliens védelmét.

Az Axis kamerái a HTTPS-t (HTTP titkosított SSL/TLS csatornán) támogatják. A kliensnek (például a VMS) ugyanígy támogatnia kell a HTTPS-t. A HTTPS titkosítja a teljes adminisztrációs forgalmat (a normál HTTP forgalmat), de nem feltétlenül titkosítja a videót, mivel azt valós idejű közvetítési protokollon, vagyis RTSP-n (Real-Time Streaming Protocol) továbbítják. A videó titkosításához arra van szükség, hogy a VMS ugyancsak támogassa az RTSP lekérést egy titkosított TLS csatornán keresztül. Nem minden VMS támogatja ezt, ezért ellenőrizni kell a VMS forgalmazójánál. Mielőtt még a HTTPS létrejönne, szükség van a kamera (akár saját, akár tanúsító hatósági) tanúsítványára, valamint a HTTPS irányelvek meghatározására.

## 15. Jogosultság-igazolás/hitelesítés igazolás

A kódolási szint szempontjából nincs jelentősége, hogy egy saját, vagy egy hitelesítő által biztosít hitelesítést alkalmazunk. A különbség abban rejlik, hogy a saját tanúsítványok nem jelentenek védettséget a hálózati „átverésekkel" szemben, vagyis olyan helyzetben, amikor egy támadó számítógép megpróbál egy jogosult kliensként vagy szerverként feltűnni. A hitelesítő cég által kiadott certifikációk azonban tovább erősítik a bizalmat a hitelesítéssel szemben, hogy az ügyfél egy valóban megbízható kamerát ér el. A hitelesítőtől származó certifikációk mind HTTPS-re (**szervertanúsítvány**), mind 802.1x-re (**klienstanúsítvány**) vonatkozhatnak.

**Nyilvános és magán tanúsítvány**

A nyilvános hitelesítések jellemzően a nyilvános szolgáltatásokra vonatkoznak – ilyenek a nyilvános weboldalak és email-szerverek. A legfelsőbb szintű megbízható hitelesítést gyárilag installálják a legtöbb operációs rendszerbe (Windows, Linux, Mac) és a böngészőkbe.

A magánhitelesítés a belső, vagy magánhálózati szolgáltatásokban jelent bizalmi pontot. A magánhitelesítést jellemzően egy dedikált szoftver vagy szerver biztosítja, a feladata pedig az, hogy valamennyi belső kliens és szerver számára kiadja a hitelesítést. A felső szintű magánhitelesítést valamennyi kliensre installálni kell, amely eléri a saját erőforrásainkat. A hitelesítés végrehajtása, a rendelkezésre álló eszközök és infarstruktúra függvényében, kézileg és automatikusan is történhet.

## 16. Hálózati hozzáférések ellenőrzése – 802.1X

Az IEEE 802.1X egy olyan szabvány, amelyet arra dolgoztak ki, hogy a helyi hálózatot ne érjék el a jogosultsággal nem rendelkező eszközök. Mielőtt egy eszköz jogosultságot kap a hálózat (vagy az erőforrás) elérésére, igazolnia kell magát. Különböző hitelesítési eljárásokat alkalmazhatunk a – MAC-cím alapján történő – MAC-szűréstől kezdve a felhasználónév és jelszó használatán át a kliens-hitelesítésig. A rendszertulajdonos dönt arról, hogy mely megoldás választja, a megfelelő választás a fenyegetés, a kockázatok és a költségek függvénye.

A 802.1X infrastruktúra működtetése befektetést jelent. Menedzselt switchekre, kiegészítő szerverekre és jellemzően egy RADIUS-ra (Remote Authentication Dial-In User Service – távoli hitelesítést biztosító behívó szolgáltatás) is szükség van. A klienshitelesítéshez jogosultság-igazolásra is szükség van. Az esetek többségében az infrastruktúrát kezelő személyzetre is szükség, aki karbantartja és figyelemmel kíséri azt. Ha a végfelhasználó még nem rendelkezik helyben 802.1X infrastruktúrával, nem valószínű, hogy ezt üzembe állítják majd a hálózati videórendszerrel. A kiegészítő ellenőrzés egy alternatívája a 802.1X-re a hálózati leválasztás, amellyel csökkenthető a kritikus hálózati erőforrások kitettsége.

## 17. SNMP

Az SNMP (Simple Network Management Protocol – Egyszerű hálózat-menedzselési protokoll) célja, hogy információt gyűjtsön az IP-hálózaton menedzselt eszközökről, illetve rendszerezze azokat. A kamerák SNMP-vel való monitorozása segít kiszűrni az eszközök hibás működését, de a kapcsolat megszakadását is, amely akár egy lehetséges támadást is jelezhet.

## 18. Syslog szerver

Minden kamerának van egy belső logja, amely a kamerában minden működési paramétert naplóz. Ez a log elveszhet, ha a kamera újrabootol, ha letörlik azt, vagy ha egy támadó módosítja azt egy sikeres behatolás során. A távoli syslog szerver begyűjtheti a kamera összes napló-üzenetét a napi működés során. A távoli syslog szerver egyben biztosítja a naplóbejegyzéseket is, ez pedig jócskán leegyszerűsítheti a hibakeresést, a normálistól eltérő események vagy egy behatolás nyomainak keresését.

## 19. További információk:

**www.axis.com/support/product-security**

> AXIS Vulnerability Policy

> AXIS Hardening Guide

> Security advisories (CVE)

> White papers

**www.axis.com/learning/online-courses**

> AXIS Academy training on cyber security

**www.axis.com/blog/secure-insights/category/cyber-security**

> Various topics on cyber security

71937/EN/R1/1805

# Az Axisról

Az Axis intelligens biztonsági megoldásokat kínál, amelyek hozzájárulnak egy intelligensebb, biztonságosabb világhoz. A hálózati videópiac vezetőjeként az Axis nyitott platformon alapuló innovatív hálózati termékek folyamatos kibocsátásával viszi előre az iparágat - globális partnerhálózatán keresztül kiváló értéket nyújt az ügyfeleinek. Az Axis partnereivel hosszú távú kapcsolattal rendelkezik, és mind a meglévő, mind az új piacokon tudást és korszakalkotó hálózati termékeket kínál számukra.

Az Axis több mint 2700 elkötelezett munkavállalót foglalkoztat a világ több mint 50 országában, akiket 90 ezernél is több partnerből álló globális hálózat támogat. Az 1984-ben alapított svédországi Axis vállalat AXIS néven szerepel a NASDAQ Stockholm tőzsde listáján.

A vállalattal kapcsolatos további információkért kérjük, látogassa meg honlapunkat a www.axis.com címen.