

AXIS Camera Station 5

Introducere

O funcție universală și infailibilă, care ar putea asigura 100% a securității cibernetice a oricărui sistem de securitate și a locației. Oricât de atrăgătoare ar suna aceste cuvinte, o astfel de funcție nu există și nici nu este probabil să apară în viitorul apropiat. În schimb, este necesar să se examineze riscul reprezentat de amenințările și vulnerabilitățile specifice organizației respective și, atunci când riscul este considerat inacceptabil, să se implementeze controale pentru a atenua acest risc. Politicile și procedurile bine definite asigură comunicarea și aplicarea consecventă a acestor controale în întreaga organizație și constituie baza unui program matur de securitate cibernetică.

O abordare recomandată este aceea de a lucra în conformitate cu cadrele standardizate de gestionare a riscurilor de securitate IT, precum ISO 27001, NIST CSF sau altele. Deși această sarcină poate părea descurajantă pentru organizațiile mai mici, definirea unui set de bază de politici de securitate a informațiilor și a proceselor de sprijin este mult mai bună decât a nu avea nimic. Dacă organizația dumneavoastră se afla la începutul unui proces de maturizare cibernetică și dispune de resurse limitate, vă recomandăm să investigați *Center for Internet Safety (CIS) Critical Security Controls Version 8 (Controlurile critice de securitate ale Centrului pentru siguranța pe internet (CIS), versiunea 8)*. CIS pune la dispoziție o listă cu 18 activități de control al securității, organizate în trei grupe de implementare, pentru a ajuta organizațiile să-și dezvolte și să-și perfecționeze programul de securitate cibernetică.

În multe organizații se produc breșe de securitate deoarece compania nu a stabilit politici, reguli și proceduri clare care să reglementeze utilizarea și drepturile de acces ale propriilor angajați. Organizația dvs. lucrează cu politici și procese pentru operațiunile de video management? Dacă nu, este timpul să începeți să le definiți.

Scop

Acest document prezintă o serie de politici și proceduri de securitate cibernetică utile pentru a sprijini implementarea și întreținerea în condiții de siguranță a sistemelor AXIS Camera Station 5. Deși nu sunt cartografiate direct cu un cadru de securitate cibernetică, ne bazăm în principal pe CIS Security Controls v8, cu un accent special pe următoarele activități de control:

- *Controlul 1: Inventarierea și controlul activelor întreprinderii*
- *Controlul 2: Inventarierea și controlul activelor de software*
- *Controlul 3: Protecția datelor*
- *Controlul 4: Configurația securizată a activelor și software-ului întreprinderii*
- *Controlul 5: Gestionarea conturilor*
- *Controlul 6: Gestionarea controlului accesului*
- *Controlul 7: Gestionarea continuă a vulnerabilităților*
- *Controlul 10: Măsurile de protecție împotriva programelor malware*

Recomandările noastre pun accentul pe asistarea instalatorilor, integratorilor și utilizatorilor finali în vederea reducerii riscurilor comune asociate implementării și gestionării sistemelor AXIS Camera Station 5.

Condiții prealabile

Se presupune că recomandările și procedurile definite și descrise în *AXIS OS Hardening Guide (Ghidul de securizare a sistemului de operare AXIS OS)* au fost înțelese și sunt respectate. Acest document se referă și la câteva roluri comune ale utilizatorilor care interacționează cu un sistem video. Vă rugăm să cartografiați aceste roluri de utilizator pentru a se potrivi cu propriile clasificări ale utilizatorilor și rolurilor. Un utilizator individual poate avea mai multe roluri, în funcție de organizație.

Roluri definite:

- **System Installer (Instalator de sisteme):** instalează, configurează, repară, efectuează upgrade-uri și downgrade-uri ale sistemelor
- **Network Administrator (Administrator de rețea):** întreține infrastructura de rețea IP, conectivitatea nodurilor finale, serverele și resursele de rețea, și realizează protecția rețelei
- **Video System Administrator (Administratorul sistemului video):** definește și gestionează sistemul video pentru a asigura utilizarea, performanța și privilegiile utilizatorilor acestuia
- **Video System Maintainer (Tehnician de întreținere a sistemului video):** monitorizează, ajustează și depanează componentele pentru a asigura performanța sistemului în numele administratorului sistemului video
- **Users (Utilizatori):** persoane fizice care utilizează clientul AXIS Camera Station 5 pentru a accesa videoclipuri în direct și înregistrate și care sunt, de obicei, responsabile de protecția fizică a unei organizații.

Politici de securitate a sistemului

Securitate fizică

Politica privind protecția fizică

Serverele, dispozitivele, echipamentele de rețea și cablurile sunt obiecte fizice care pot fi perturbate, sabotate sau furate. Gazda pe care funcționează software-ul de server AXIS Camera Station 5 și echipamentele importante de rețea (routere, switch-uri etc.) trebuie amplasate într-un mediu cu acces restricționat fizic și logic. Camerele și alte dispozitive conectate trebuie montate în locuri greu accesibile și trebuie să fie modele sau să aibă carcase rezistente la vandalism. Trebuie acordată atenție protejării cablurilor din pereți sau canale de cabluri, deoarece acestea cresc riscul de modificare neautorizată și de sabotaj.

Politici și proceduri recomandate

Stabiliți o persoană sau o unitate organizațională responsabilă cu controlul vizual la intervale definite a protecției fizice a serverelor VMS, a hardware-ului de rețea, a dispozitivelor conectate și a cablurilor. Este esențial să se mențină un inventar precis al tuturor serverelor și dispozitivelor, inclusiv locația acestora.

Gestionarea software-ului

Politica privind software-ul aplicațiilor terților

Deoarece AXIS Camera Station 5 este instalat într-un mediu Windows standard, poate fi tentant să utilizați acel mediu pentru aplicații de software care nu au legătură cu video managementul. Instalarea altor aplicații terțe deschide posibilitatea introducerii de malware în mediu, ceea ce ar putea duce la întreruperea funcționării sistemului sau ar putea oferi o poartă de acces pentru un atacator în rețeaua organizației.

Politici și proceduri recomandate

Nu rulați nimic altceva decât software-ul de server AXIS Camera Station 5 și integrările de încredere ale terților pe hardware-ul gazdă. Dacă hardware-ul fizic trebuie utilizat în alte scopuri, se recomandă utilizarea mai multor instanțe de server virtual și rularea software-ului de server AXIS Camera Station 5 pe o mașină virtuală și a software-ului terț care nu are legătură cu VMS pe o altă mașină virtuală. Informații cu privire la funcționarea AXIS Camera Station 5 într-un mediu virtual pot fi găsite *aici*.

Se recomandă instalarea unui software antivirus pe toate serverele și computerele care se conectează la serverul AXIS Camera Station 5. Dacă se utilizează dispozitive mobile, aceasta include asigurarea faptului că dispozitivele au instalate cele mai recente sisteme de operare și patch-uri (deși nu direct antivirus). Când efectuați scanarea antivirus, nu scanați directoarele și subdirectoarele care conțin baze de date ale înregistrărilor. Căutarea virușilor în aceste directoare poate afecta performanța sistemului.

Gestionarea conturilor

Politica generală privind conturile

Drepturile nivelului de administrator sunt uneori acordate utilizatorilor obișnuiți din motive de comoditate. În multe organizații, nu este clar cine este responsabil pentru revizuirea privilegiilor conturilor și monitorizarea accesului angajaților la sisteme.

Politici și proceduri recomandate

Recomandăm organizațiilor să respecte principiul privilegiului minim atunci când definesc conturile de sistem. Aceasta înseamnă că privilegiile de acces ale utilizatorilor sunt limitate doar la resursele necesare pentru îndeplinirea sarcinilor specifice de lucru ale acestora. De asemenea, se recomandă să se verifice periodic privilegiile conturilor utilizatorilor sistemului pentru a preveni „abuzul de privilegii”.

Politica privind conturile de administrator AXIS Camera Station 5

O greșeală frecventă la implementarea AXIS Camera Station 5 într-un mediu Windows este definirea unui singur cont de administrator pentru gazda Windows. Cu trecerea timpului, parola poate fi partajată în cadrul organizației, existând riscul ca persoane neautorizate să obțină privilegii de administrator în mediul Windows. Acest lucru poate duce cu ușurință la instalarea pe serverul respectiv a numeroase aplicații nedorite sau programe malware.

Politici și proceduri recomandate

Mașina Windows care găzduiește serverul AXIS Camera Station 5 trebuie să aibă cel puțin un cont cu privilegii de administrator și un cont cu privilegii de utilizator. Niciunul dintre aceste conturi nu trebuie să fie identic cu contul implicit de administrator pentru Windows. Contul implicit de administrator trebuie dezactivat după crearea conturilor cu privilegii de administrator și de utilizator. După implementare, parola contului de administrator trebuie să fie cunoscută și utilizată numai de **Network Administrator(s) (Administratorul (administratorii) de rețea)**. Contul privilegiat de utilizator trebuie utilizat de **Video System Administrator (Administratorul sistemului video)** dacă/atunci când are nevoie să se autentifice la serverul AXIS Camera Station 5. Trebuie menționat că, chiar dacă cele două roluri menționate mai sus sunt îndeplinite de aceeași persoană, este recomandat să existe conturi separate pentru Administratorul de rețea și pentru Administratorul sistemului video, din motive de control. Pentru a accepta alte roluri, așa cum au fost definite anterior, trebuie

create conturi de utilizator fără privilegii suplimentare pentru fiecare **User (Utilizator)** individual care se va autentifica în sistem.

Dacă gazda care funcționează pe AXIS Camera Station 5 este plasată într-un mediu de domeniu Windows Active Directory, conturile de administrator și de utilizator pot fi create în contextul domeniului sau se poate utiliza un cont de domeniu existent al unui angajat pentru autentificarea la o gazdă AXIS Camera Station 5. Acest lucru poate simplifica gestionarea conturilor, deoarece nu este necesară crearea și întreținerea de conturi suplimentare. Acest lucru deschide, de asemenea, posibilitatea utilizării Gestionării politicii privind grupul pentru a impune complexitatea parolelor, implementarea certificatelor și alte funcții de securitate disponibile în mediile de domeniu.

Politica privind conturile de utilizator AXIS Camera Station 5

Conturile de utilizator sunt atribuite rolurilor specifice din AXIS Camera Station 5, care, la rândul lor, determină drepturile specifice pe care fiecare utilizator le are în sistem, cum ar fi la ce vizualizări și videoclipuri are acces privilegiat. Dacă mai multe persoane utilizează același cont de utilizator, există un risc crescut ca parola să fie partajată cu alte persoane din organizație. Partajarea conturilor va face practic imposibilă și verificarea cine a accesat ce cameră/videoclip și la ce oră.

Politici și proceduri recomandate

Dacă este posibil, utilizați Microsoft Active Directory pentru o gestionare ușoară a utilizatorilor și grupurilor. De asemenea, se recomandă verificarea faptului că grupurile de securitate relevante au fost definite pentru toate rolurile utilizatorilor înainte de configurarea sistemului.

De asemenea, Active Directory va oferi:

- O politică privind parolele care impune utilizatorilor să își schimbe parola în mod regulat
- Protecție împotriva atacurilor de forță brută, astfel încât contul Windows AD să fie blocat după mai multe încercări eșuate de autentificare, în conformitate cu politica organizației privind parolele
- Permisuni bazate pe roluri, astfel încât controlul accesului să poată fi aplicat în întregul domeniu

Dacă este necesar să se utilizeze conturi Windows locale, se recomandă crearea unui cont unic pentru fiecare utilizator al sistemului și acordarea accesului numai entităților din sistem necesare pentru îndeplinirea responsabilităților lor. Utilizarea grupurilor pentru utilizatori poate simplifica atribuirea permisiunilor în cazul în care există mai mulți utilizatori cu permisiuni identice.

Politica privind conturile dispozitivelor

Conturile din dispozitivele Axis sunt în principal conturi de computer/client. **Users (Utilizatorii)** nu ar trebui să aibă niciodată acces direct la dispozitiv. Singurul client care trebuie să acceseze dispozitivele în timpul funcționării normale este serverul AXIS Camera Station 5. O strategie obișnuită este ca toate dispozitivele să aibă aceeași parolă. Acest lucru introduce riscuri suplimentare, dar poate simplifica gestionarea parolelor, astfel încât fiecare trebuie să își evalueze propria toleranță la risc. AXIS Camera Station 5 acceptă atribuirea de parole unice pentru fiecare dispozitiv prin intermediul interfeței sale de gestionare.

O greșeală frecventă este aceea că dispozitivele sunt adăugate la AXIS Camera Station 5 cu un singur cont partajat de mai multe roluri. La un moment dat, când un **Video System Maintainer (Tehnician de întreținere a sistemului video)** are nevoie să utilizeze un browser pentru a ajusta ceva, parola contului principal (rădăcină) a dispozitivului este dezvăluită. În câteva luni, majoritatea persoanelor din organizație vor cunoaște parola pentru toate dispozitivele și vor avea privilegii de administrator pentru sistem.

Politici și proceduri recomandate

Dispozitivul ar trebui să aibă cel puțin două conturi de administrator: unul unic, creat pentru administratorii de dispozitive, precum și contul root implicit pentru adăugarea dispozitivelor la un server AXIS Camera Station 5. Accesul temporar, cum ar fi atunci când un **Video System Maintainer (Tehnician de întreținere a sistemului video)** accesează un dispozitiv utilizând un browser web, trebuie gestionat prin utilizarea conturilor temporare.

AXIS Device Manager trebuie utilizat ca instrument principal pentru gestionarea conturilor și parolelor dispozitivelor. O versiune a AXIS Device Manager este integrată direct în AXIS Camera Station 5 și este disponibilă în fila Management (Gestionare). Parola rădăcină a dispozitivului trebuie utilizată numai de AXIS Device Manager și AXIS Camera Station 5 și trebuie cunoscută numai de cei care utilizează AXIS Device Manager sau AXIS Camera Station 5 ca instrument de gestionare a dispozitivelor.

Utilizați AXIS Camera Station 5 pentru a crea un cont temporar atunci când o persoană cu rol de tehnician de întreținere are nevoie să utilizeze un browser web pentru a accesa unul sau mai multe dispozitive în scopul depanării sau întreținerii. Selectați dispozitivul (dispozitivele) și creați un cont nou, de preferință cu privilegii de operator, pe care tehnicianul de întreținere îl poate utiliza. După ce sarcina a fost finalizată, ștergeți contul temporar.

Întreținerea sistemului

Politica de aplicare a patch-urilor pentru gazdele Windows AXIS Camera Station 5

Serverul AXIS Camera Station 5 și clienții funcționează într-un mediu Windows. Este important ca aceste sisteme să fie ținute la zi pentru a se asigura că sistemele care găzduiesc software-ul AXIS Camera Station 5 nu prezintă vulnerabilități deschise care pot fi exploatare pentru a obține acces neautorizat la sistemul de video management.

Politici și proceduri recomandate

Pentru toate sistemele AXIS Camera Station 5, indiferent dacă funcționează pe Axis NVR sau pe hardware-ul personalizat, se recomandă dezactivarea actualizării automate. Actualizările Windows au cauzat în trecut instabilitate în sistemul de operare Windows de bază, de aceea se recomandă testarea actualizărilor disponibile pe mașinile selectate pentru a asigura stabilitatea sistemului înainte de a fi distribuite către toate sistemele gazdă care funcționează pe AXIS Camera Station 5. Însă trebuie să se ajungă la un echilibru între securitate și stabilitate, deoarece lăsarea sistemului Windows fără aplicarea patch-urilor pentru o perioadă prea lungă de timp poate introduce riscuri pentru întregul mediu. În funcție de nivelul de expunere a sistemului clientului la amenințări externe, politica de aplicare a patch-urilor trebuie să prevadă un cadru de timp pentru asigurarea faptului că sistemele primesc cele mai recente actualizări.

Politica de actualizare a software-ului AXIS Camera Station 5

În majoritatea cazurilor, utilizarea celei mai recente versiuni de software pentru AXIS Camera Station 5 vă va asigura că utilizați patch-uri de securitate pentru toate vulnerabilitățile recent descoperite. Lăsarea sistemului fără aplicarea patch-urilor pentru o perioadă mai lungă va crește riscul ca un adversar să exploateze vulnerabilitățile și să compromită sistemul.

Politici și proceduri recomandate

Este important să se definească o politică de aplicare a patch-urilor cu evaluări periodice ale versiunilor de software implementate pentru a se asigura că AXIS Camera Station 5 este actualizat. Politica de aplicare a patch-urilor ar trebui să identifice, de asemenea, cine este responsabil pentru gestionarea lucrărilor asociate cu actualizarea atât a serverului, cât și a software-ului clientului. Pentru AXIS Camera Station 5, cea mai recentă versiune poate fi găsită pe www.axis.com. AXIS Camera Station 5 necesită cea mai recentă versiune. Bibliotecile .NET, prin urmare, trebuie să se acorde o atenție deosebită la alinierea politicii de aplicare a patch-urilor Windows la politica AXIS Camera Station 5.

Politica de actualizare a firmware-ului dispozitivelor

Utilizarea dispozitivelor cu versiuni actualizate de firmware reduce majoritatea riscurilor comune, deoarece cele mai recente versiuni de firmware includ patch-uri pentru vulnerabilitățile cunoscute pe care atacatorii ar putea încerca să le exploateze. Axis oferă o versiune cu suport pe termen lung (LTS) pentru firmware-ul dispozitivului, care include patch-uri de securitate și remedieri de erori, dar adăugările de funcții sunt limitate pentru a asigura stabilitatea pe termen lung a platformei. Pentru mai multe informații referitoare la strategia Axis privind dezvoltarea firmware-ului, consultați documentul tehnic *Axis firmware management (Gestionarea firmware-ului Axis)*.

Politici și proceduri recomandate

Pentru dispozitivele hardware, politica trebuie să stipuleze că toate firmware-urile trebuie să fie actualizate. Procesele pot utiliza funcția integrată de actualizare a firmware-ului din AXIS Camera Station 5 sau AXIS Device Manager Extend pentru a identifica dacă sunt disponibile versiuni noi de firmware pentru dispozitivele Axis. Ar trebui stabilit un interval de timp, de obicei în afara programului de lucru, pentru implementarea tuturor actualizărilor de firmware pentru toate camerele. AXIS Camera Station 5 / AXIS Device Manager Extend poate verifica, de asemenea, dacă actualizările de firmware au fost acceptate. Dacă sistemul are integrări specifice care ar putea fi afectate de actualizare, luați în considerare standardizarea pe o pistă de firmware LTS.

Securitate de rețea IP

Politica privind accesul de la distanță

Dispozitivele și serviciile expuse la internet cresc riscul ca adversarii externi să exploreze sau să exploateze vulnerabilitățile cunoscute. Camerele expuse la internet, de exemplu cele utilizate de organizații mici care au nevoie de acces video de la distanță, devin victime ușoare dacă se utilizează o parolă slabă sau dacă se

descoperă o nouă vulnerabilitate critică. Accesul de la distanță la mediul Windows trebuie controlat strict sau evitat, dacă este posibil. Deși mediul Windows poate avea conexiune la internet pentru a facilita actualizarea sistemelor, utilizarea serviciilor desktop de la distanță, precum Windows Remote Desktop, TeamViewer și AnyDesk, introduce căi de acces la sistemul dvs. dacă nu sunt gestionate corect.

Politici și proceduri recomandate

Nu expuneți niciodată adresa IP/portul unei camere într-un mod care să o facă accesibilă direct de pe internet. Dacă este necesar accesul video de la distanță, utilizați Axis Secure Remote Access. AXIS Camera Station 5 utilizează un server de acces de la distanță bazat pe cloud pentru a facilita accesul criptat de la distanță la sistem prin intermediul unui client AXIS Camera Station 5 sau al aplicației mobile AXIS Camera Station. Pe lângă faptul că este responsabil pentru gestionarea conexiunilor utilizatorilor de la distanță și mobili, serverul de acces de la distanță joacă un rol important la protejarea integrității atunci când este folosit de utilizatori de la distanță. Mai multe informații referitoare la Axis Secure Remote Access (Acces securizat de la distanță Axis) pot fi găsite pe *aici*. Axis oferă aplicații mobile oficiale atât pentru Android, cât și pentru Apple iOS. Aplicația mobilă AXIS Camera Station trebuie descărcată numai din surse oficiale, respectiv din Google Play Store și Apple App Store.

În ceea ce privește accesul desktop de la distanță la mediul Windows, nu se recomandă acordarea acestui tip de acces unui sistem care funcționează pe AXIS Camera Station 5. Însă dacă este necesar, trebuie să se acorde o atenție deosebită pentru a se asigura că aplicația desktop de la distanță aleasă este sigură și că accesul este acordat numai persoanelor care au nevoie de aceasta. Se recomandă implementarea unor niveluri suplimentare de control, cum ar fi autentificarea multifactorială (MFA). Se recomandă insistent înregistrarea și auditarea ulterioară a încercărilor de conectare de la distanță pentru a urmări cine și la ce ore accesează mediul Windows de la distanță.

Politica de expunere a rețelei locale

Reducerea expunerii rețelei locale poate contribui la atenuarea multor amenințări comune prin reducerea suprafeței de atac. Există multe modalități de a reduce expunerea rețelei, inclusiv segmentarea fizică a rețelei (separarea hardware-ului și a cablurilor de rețea), segmentarea logică a rețelei prin intermediul LAN-urilor (VLAN-urilor) virtuale și filtrarea IP. Camerele Axis acceptă un filtru IP (tabele IP), astfel încât dispozitivul să răspundă numai la cererile de conectare efectuate de la adrese IP permise în mod explicit.

Politici și proceduri recomandate

NVR-urile AXIS Camera Station S22 sunt servere de hardware cu două porturi de rețea. Unul dintre porturi creează o rețea segmentată pentru camere, iar celălalt se conectează la rețeaua principală (domeniu) pentru a deservi clienții video. Serverul acționează ca o punte și un firewall la rețeaua de camere, împiedicând clienții să acceseze direct camerele. Acest lucru reduce probabilitatea amenințărilor din partea adversarilor în rețeaua primară.

Dacă serverul AXIS Camera Station 5 și camerele sunt toate plasate în rețeaua principală, se recomandă configurarea filtrului IP al camerei, limitând accesul numai la serverele care găzduiesc AXIS Camera Station 5, AXIS Device Manager și clienții suplimentari de întreținere.

Aplicații și servicii suplimentare

Dacă găzduiți aplicații suplimentare pe serverul AXIS Camera Station Pro care sunt destinate să rămână limitate la localhost (serverul în sine), rețineți că administratorii pot avea acces la acestea de la distanță prin intermediul clientului. Acest lucru ar putea expune involuntar aceste aplicații.

Același risc se aplică și tuturor celorlalte servicii care funcționează în rețea. Pentru a reduce riscul, vă recomandăm să instalați un firewall între rețeaua care găzduiește AXIS Camera Station Pro și camerele sale și toate celelalte rețele care găzduiesc aplicații sau servicii necorelate. Această segmentare ajută la limitarea potențialelor compromisuri și restricționează căile de acces inutile.

Politica de criptare a rețelei

Traficul de rețea transmis prin rețele nesigure trebuie să fie întotdeauna criptat. Internetul este clasificat ca o rețea nesigură. O rețea locală poate fi, de asemenea, clasificată ca nesigură, iar traficul de rețea ar trebui, prin urmare, să fie criptat. Politica care trebuie aplicată traficului video în rețea depinde de modul în care este clasificat videoclipul și de riscul ca adversarii să aibă acces la sistemul video prin rețea. Se recomandă să se presupună că rețeaua a fost deja compromisă. Organizațiile mai mari vor avea, de obicei, o politică care definește modul în care este clasificată rețeaua.

Politici și proceduri recomandate

Traficul între clientul video și serverul AXIS Camera Station 5 trebuie să utilizeze criptarea. Traficul între serverul AXIS Camera Station 5 și cameră trebuie criptat în funcție de infrastructură. Camerele Axis sunt dotate cu un certificat semnat automat și HTTPS activat în mod implicit. Dacă există riscul de spoofing (falsificare) a rețelei, cum ar fi atunci când un computer rău intenționat încearcă să se dea drept o cameră video, ar trebui utilizată o infrastructură cu cheie privată (PKI) cu certificate semnate de CA. AXIS Camera Station 5 are o autoritate de certificare (CA) locală integrată, care poate gestiona în mod rentabil semnarea și distribuirea certificatelor de server pentru dispozitivele Axis.

Versiuni TLS

Vă recomandăm să dezactivați versiunile TLS 1.1 și 1.0. Programul de instalare AXIS Camera Station vă oferă asistență pe parcursul instalării sau actualizării.

Ciphre (algoritm de criptare) HTTPS

AXIS Camera Station 5 acceptă și utilizează suite de cifruri TLS pentru a cripta conexiunile HTTPS în mod securizat. Suita specifică de cifruri depinde de clientul care se conectează la AXIS Camera Station 5 sau de serviciul contactat, iar AXIS Camera Station 5 o negociază în conformitate cu protocolul TLS. Vă recomandăm să configurați Windows astfel încât să nu utilizeze suitele de cifruri TLS 1.2 enumerate în *RFC 7540*. Posibilitatea de a dezactiva o suită de cifruri depinde de dispozitivele și camerele utilizate împreună cu AXIS Camera Station 5. Dacă un dispozitiv sau o cameră video necesită o suită specifică de cifruri, s-ar putea să nu fie posibilă dezactivarea suitei de cifruri slabe.

Gestionarea datelor

Clasificarea videoclipurilor

Videoclipurile în direct și videoclipurile înregistrate trebuie clasificate. Videoclipurile pot fi clasificate ca publice, private, restricționate sau în orice altă categorie definită de politicile organizaționale. În multe cazuri, videoclipul este reglementat de lege și de reglementările regionale, precum și de politicile IT interne, astfel încât proprietarul sistemului are responsabilitatea de a cunoaște legile și reglementările care se aplică datelor video.

Politici și proceduri recomandate

Clasificați videoclipurile în direct, videoclipurile înregistrate și audio în conformitate cu politicile organizaționale de clasificare a datelor. Configurați privilegiile de acces ale utilizatorilor și securizarea sistemului în funcție de sensibilitatea datelor video și audio. Dacă nu este necesar, sunetul poate fi dezactivat la nivel de dispozitiv.

Controale de securitate suplimentare

În funcție de nivelul de maturitate și de toleranța la risc a organizației dvs., există mai multe controale de securitate suplimentare din CIS Controls v8 pe care vă recomandăm să le implementați pentru a reduce riscurile privind securitatea cibernetică în operațiunile zilnice.

Additional CIS Controls (Controale CIS suplimentare):

Controlul 8: Audit Log Management (Gestionarea jurnalului de audit)

Colectează, alertează, examinează și păstrează jurnalele de audit ale evenimentelor care ar putea ajuta la detectarea, înțelegerea sau recuperarea în urma unui atac.

Controlul 14: Implement a Security Awareness and Training Program (Implementarea unui program de conștientizare și instruire în materie de securitate)

Înțelegeți abilitățile și comportamentele personalului. Instruiți personalul cu privire la modul de identificare a diferitelor forme de atac.

Controlul 17: Incident Response and Management (Răspunsul la incidente și gestionarea acestora)

Utilizați planuri scrise de răspuns la incidente, cu faze clar definite de procesare/gestionare a incidentelor și rolurile personalului, precum și modul de raportare a unui incident de securitate către autoritățile competente și terțe părți.

Securitatea backup-ului bazei de date

Dacă modificați locația pentru copiile de rezervă ale bazei de date, utilizați o locație sigură, cu acces limitat. O partajare în rețea cu acces larg este mai puțin sigură.

T10179095_ro

2024- (M5.2)

© 2022 – 2024 Axis Communications AB