AXIS Camera Station 5

Guida alla protezione del sistema

Introduzione

Una funzionalità unica e infallibile che può rendere qualsiasi sito e sistema di sicurezza sicuro al 100%. Per quanto allettanti possano sembrare queste parole, una funzionalità del genere non esiste e non sarà disponibile a breve. Invece, è necessario esaminare il rischio posto da minacce e vulnerabilità specifiche della propria organizzazione e, laddove il rischio sia inaccettabile, implementare controlli per mitigarlo. Criteri e procedure ben definiti garantiscono una comunicazione e un'applicazione coerenti di tali controlli in tutta l'organizzazione e gettano le basi di un programma di cybersicurezza maturo.

Un approccio consigliato consiste nel lavorare in base a framework di gestione dei rischi di sicurezza IT standard come ISO 27001, NIST CSF o altri. Sebbene questa attività possa essere scoraggiante per le organizzazioni più piccole, la definizione di un set di criteri di sicurezza delle informazioni di base e dei processi di supporto è comunque molto meglio che non avere niente. Se l'organizzazione inizia un percorso verso la cyber maturity e ha a disposizione risorse limitate, consigliamo di ricorrere al *Center for Internet Safety (CIS) Critical Security Controls Version 8*. CIS fornisce un elenco di 18 attività di controllo della sicurezza organizzate in tre gruppi di implementazione per aiutare le organizzazioni a sviluppare e maturare il proprio programma di sicurezza informatica.

Le violazioni della sicurezza si verificano in molte organizzazioni in seguito alla mancata definizione di regole, procedure e criteri chiari da utilizzare per regolarne l'uso e i diritti di accesso dei propri dipendenti. L'organizzazione ricorre a criteri e processi per le operazioni di gestione dei video? Se la risposta è no, è il momento di iniziare a definirli.

Scopo

In questo documento vengono descritti diversi criteri e procedure di sicurezza informatica utili per supportare la distribuzione e la manutenzione sicure dei sistemi . Sebbene non corrisponda direttamente a un framework di sicurezza informatica, ci affidiamo principalmente a CIS Security Controls v8 soprattutto per le seguenti attività di controllo:

- *Controllo 1: Inventario e controllo delle risorse aziendali*
- *Controllo 2: Inventario e controllo delle risorse software*
- *Controllo 3: Protezione dati*
- *Controllo 4: Configurazione sicura delle risorse e del software aziendali*
- *Controllo 5: Gestione account*
- *Controllo 6: Gestione del controllo degli accessi*
- *Controllo 7: Gestione continua delle vulnerabilità*
- *Controllo 10: Difese da malware*

I nostri consigli sono rivolti principalmente agli installatori, agli integratori e agli utenti finali affinché sia possibile ridurre i rischi comuni durante la distribuzione e la gestione dei sistemi .

Prerequisiti`

Si presuppone che i consigli e le procedure definiti e descritti nella *Guida alla protezione AXIS OS* siano stati compresi e seguiti. Inoltre, questo documento rimanda a diversi ruoli utente comuni che interagiscono con un sistema video. Assegnare questi ruoli utente in modo che corrispondano alle proprie classificazioni di utenti e ruoli. Un singolo utente può avere più ruoli, a seconda dell'organizzazione.

Ruoli definiti:

- **Installatore di sistemi**: installa, imposta, ripara, aggiorna i sistemi e ne effettua il downgrade
- **Amministratore di rete**: gestisce l'infrastruttura di rete, la connettività del nodo finale, i server e le risorse di rete nonché la protezione della rete

Introduzione

- **Amministratore di sistemi video**: definisce e gestisce il sistema video per proteggerne l'uso, le prestazioni e i privilegi dell'utente
- **Manutentore di sistemi video**: monitora e regola i componenti e ne risolve i problemi per proteggere le prestazioni del sistema per conto dell'amministratore di sistemi video
- **Utenti**: persone che utilizzano il client per accedere ai video in diretta e ai video registrati e sono in genere responsabili della protezione fisica di un'organizzazione.

Criteri di sicurezza del sistema

Sicurezza fisica

Criteri sulla protezione fisica

I server, i dispositivi, le apparecchiature di rete e i cavi sono oggetti fisici che possono subire interferenze, sabotaggi o furti. L'host su cui è in esecuzione il software del server e importanti apparecchiature di rete, come router e switch devono essere posizionati in un ambiente con accesso limitato fisicamente e logicamente. Le telecamere e gli altri dispositivi collegati devono essere montati in luoghi difficili da raggiungere e devono includere modelli o alloggiamenti resistenti agli atti vandalici. Prestare attenzione alla protezione dei cavi su pareti o canaline, poiché aumentano i rischi di manomissione e sabotaggio.

Criteri e procedure consigliati
Definire un'unità singola o organizzativa responsabile del controllo visivo della protezione fisica di server VMS, hardware di rete, dispositivi connessi e cablaggio a intervalli definiti. È essenziale mantenere un inventario accurato di tutti i server e i dispositivi, compresa la loro ubicazione.

Gestione del software

Criteri relativi al software di applicazioni di terze parti

Poiché viene installato in un ambiente Windows standard, può essere interessante utilizzare tale ambiente per applicazioni software non correlate alla gestione di video. L'installazione di altre applicazioni di terze parti offre la possibilità di introdurre malware nell'ambiente, causando tempi di inattività del sistema o fornendo a utenti malintenzionati un accesso secondario alla rete dell'organizzazione.

Criteri e procedure consigliati
Non eseguire altri software che non siano quello del server e integrazioni attendibili di terze parti sull'hardware host. Se l'hardware fisico deve essere utilizzato per altri scopi, si consiglia di utilizzare più istanze del server virtuale e di eseguire il software del server in una macchina virtuale e il software non VMS di terze parti in un'altra macchina virtuale. Le informazioni sull'esecuzione di in un ambiente virtuale sono disponibili *qui*.

Si consiglia di distribuire il software antivirus su tutti i server e i computer che si connettono al server . Se viene eseguita la distribuzione su dispositivi mobili, è necessario assicurarsi che su tali dispositivi siano installati i sistemi operativi e le patch più recenti (anche se non direttamente antivirus). Quando si esegue la scansione antivirus, non eseguire la scansione delle directory e delle sottodirectory che contengono i database di registrazione. Eseguire la scansione antivirus in queste applicazioni può influire sulle prestazioni del sistema.

Gestione account

Criteri generali sugli account

Talvolta, agli utenti normali vengono concessi diritti a livello di amministratore per motivi di praticità. In molte organizzazioni, non è sempre chiaro chi sia responsabile della revisione dei privilegi degli account e del monitoraggio dell'accesso dei dipendenti ai sistemi.

Criteri e procedure consigliati
Quando si definiscono gli account di sistema, si consiglia alle organizzazioni di seguire il principio dei privilegi minimi. Ciò significa che i privilegi di accesso degli utenti sono limitati solo alle risorse necessarie per eseguire le attività di lavoro specifiche. È inoltre consigliabile controllare periodicamente i privilegi degli utenti di sistema per proteggere gli utenti dall'"accumulo di privilegi".

Criteri dell'account amministratore di

Un errore comune quando si esegue la distribuzione di in un ambiente Windows è la definizione di un singolo account amministratore per l'host Windows. Con il tempo, la password può essere condivisa all'interno dell'organizzazione con il rischio che persone non autorizzate ottengano privilegi di amministratore per l'ambiente Windows. Questo può avere come conseguenza l'installazione di numerose applicazioni utente indesiderate o di malware sul server.

Criteri di sicurezza del sistema

Criteri e procedure consigliati
Il computer Windows che ospita il server deve avere almeno un account con privilegi di amministratore e un account con privilegi utente. Nessuno di questi account deve essere uguale all'account amministratore predefinito per Windows. Dopo aver creato gli account con privilegi di amministratore e utente, è necessario disabilitare l'account amministratore predefinito. Dopo la distribuzione, la password dell'account amministratore deve essere nota e utilizzata solo dagli **amministratori di rete**. L'account con privilegi utente deve essere utilizzato dall'**amministratore di sistemi video** se/quando questi deve accedere al server . Va notato che anche se i due ruoli precedenti vengono ricoperti dalla stessa persona, è consigliabile avere account di amministratore di rete e amministratore di sistema video separati a fini del controllo. Per supportare altri ruoli come definito in precedenza, è necessario creare ulteriori account utente senza privilegi per ogni singolo **utente** che accederà al sistema.

Se l'host su cui è in esecuzione si trova in un ambiente di dominio Windows Active Directory, è possibile creare account amministratore e utente nel contesto del dominio oppure utilizzare l'account di dominio esistente di un dipendente per eseguire l'autenticazione sull'host . In questo modo è possibile semplificare la gestione degli account poiché non è necessario creare e mantenere altri account. Ciò apre anche la possibilità di utilizzare Gestione Criteri di gruppo per far rispettare la complessità della password, la distribuzione dei certificati e altre funzionalità di sicurezza disponibili negli ambienti di dominio.

Criteri degli account utente di

Gli account utente vengono assegnati a ruoli specifici in , che a sua volta determina i diritti specifici di ciascun utente nel sistema, ad esempio le viste e i video a cui hanno il privilegio di accedere. Se più persone condividono un singolo account utente, esiste il rischio che una password venga condivisa con altri membri dell'organizzazione. La condivisione degli account rende inoltre impossibile controllare chi ha avuto accesso alla telecamera o al video e a che ora.

Criteri e procedure consigliati

Se possibile, utilizzare Microsoft Active Directory per una facile gestione di utenti e gruppi. Si consiglia inoltre di verificare che i gruppi di sicurezza pertinenti siano stati definiti per tutti i ruoli utente prima di impostare il sistema.

Active Directory fornirà inoltre:

- Un criterio relativo alla password che richiede agli utenti di modificare regolarmente la propria password
- Protezione con forza bruta, affinché l'account Windows AD venga bloccato dopo diversi tentativi di autenticazione non riusciti, in linea con i criteri per le password dell'organizzazione
- Autorizzazioni basate sui ruoli, in questo modo è possibile applicare i controlli degli accessi all'interno del dominio

Se è necessario utilizzare account Windows locali, è consigliabile creare un account univoco per ciascun utente del sistema e concedergli l'accesso solo alle entità di sistema necessarie per svolgere le proprie mansioni. L'utilizzo di gruppi per gli utenti può aiutare a semplificare l'assegnazione delle autorizzazioni qualora vi siano più utenti con autorizzazioni identiche.

Criteri degli account dei dispositivi

Gli account nei dispositivi Axis sono principalmente account computer/client. Agli **utenti** non dovrebbe mai essere consentito l'accesso diretto al dispositivo. L'unico client che deve accedere ai dispositivi durante il normale funzionamento è il server . Una strategia comune consiste nell'utilizzare la stessa password per tutti i dispositivi. Ciò comporta rischi aggiuntivi, ma può anche semplificare la gestione della password, per tale motivo è necessario valutare la propria tolleranza ai rischi. supporta l'assegnazione di password univoche a ogni dispositivo tramite la relativa interfaccia di gestione.

Un errore comune è che i dispositivi vengono aggiunti a con un singolo account condiviso da più ruoli. Quando un **manutentore di sistemi video** deve utilizzare un browser per regolare qualcosa, viene utilizzata la password (root) dell'account principale del dispositivo. Entro pochi mesi, la maggior parte delle persone nell'organizzazione conoscerà la password di tutti i dispositivi e avrà privilegi di amministratore per il sistema.

Criteri e procedure consigliati
Il dispositivo deve avere almeno due account amministratore: uno univoco creato per gli amministratori del dispositivo e l'account root predefinito per l'aggiunta di dispositivi al server . L'accesso temporaneo, ad esempio quando un **manutentore di sistemi video** accede a un dispositivo tramite un browser Web, deve essere gestito tramite l'uso di account temporanei.

AXIS Device Manager deve essere utilizzato come strumento principale per la gestione degli account e delle password del dispositivo. Una versione di AXIS Device Manager è integrata direttamente in ed è disponibile nella scheda Gestione. La password root del dispositivo deve essere utilizzata solo da AXIS Device Manager e da . Deve essere nota solo a chi utilizza AXIS Device Manager o come strumento per gestire i dispositivi.

Utilizzare per effettuare il provisioning di un account temporaneo quando una persona con il ruolo di manutentore deve utilizzare un browser Web per accedere ai dispositivi per la risoluzione di problemi o per la manutenzione. Selezionare i dispositivi e creare un nuovo account, preferibilmente con privilegi di operatore, che possa essere utilizzato dal manutentore. Una volta completata l'attività, rimuovere l'account temporaneo.

Manutenzione del sistema

Criteri di applicazione delle patch dell'host Windows

I client e il server vengono eseguiti in un ambiente Windows. È importante che questi sistemi siano sempre aggiornati per garantire che i sistemi che ospitano il software non abbiano vulnerabilità aperte che possano essere sfruttate per ottenere l'accesso non autorizzato al Video Management System.

Criteri e procedure consigliati
Per tutti i sistemi , indipendentemente dal fatto che siano in esecuzione su NVR Axis o su hardware personalizzato, si consiglia di disattivare gli aggiornamenti automatici. In passato gli aggiornamenti di Windows hanno instabilità nel sistema operativo Windows sottostante, pertanto si consiglia di testare gli aggiornamenti disponibili su computer selezionati per garantire la stabilità del sistema prima di distribuirli su tutti i sistemi host che eseguono . Tuttavia, è necessario trovare un equilibrio tra sicurezza e stabilità poiché lasciare per troppo tempo il sistema Windows senza patch può risultare rischioso per l'ambiente generale. In base al livello di esposizione alle minacce esterne del sistema del cliente, è necessario delineare un intervallo di tempo per la ricezione degli ultimi aggiornamenti nei criteri di applicazione delle patch.

Criteri di aggiornamento del software di

Nella maggior parte dei casi, l'utilizzo della versione più recente del software di garantisce l'applicazione di patch di sicurezza per tutte le nuove vulnerabilità scoperte. Lasciare il sistema senza patch per un periodo più lungo aumenterà il rischio che un utente malintenzionato possa sfruttare le vulnerabilità e compromettere il sistema.

Criteri e procedure consigliati
È importante definire criteri di applicazione delle patch con valutazioni regolari delle versioni software distribuite per assicurarsi che siano aggiornato. Il criterio di applicazione delle patch deve inoltre identificare la persona responsabile della gestione delle operazioni associate all'aggiornamento del software server e client. Per , la versione più recente è disponibile sul sito *www.axis.com*. richiede le librerie .NET più recenti, pertanto occorre fare attenzione ad allineare i criteri di applicazione delle patch di Windows ai criteri di .

Criteri di aggiornamento del firmware del dispositivo

L'utilizzo di dispositivi con versioni aggiornate del firmware mitiga i rischi più comuni poiché le versioni più recenti del firmware includono patch per vulnerabilità note che i malintenzionati potrebbero tentare di sfruttare. Axis offre una versione di supporto a lungo termine (LTS) del firmware del dispositivo che include patch di sicurezza e correzioni di bug, tuttavia le funzionalità aggiunte vengono limitate per garantire la stabilità a lungo termine della piattaforma. Per ulteriori informazioni sulla strategia di Axis per lo sviluppo del firmware, vedere il whitepaper *Gestione del firmware Axis*.

Criteri e procedure consigliati
Per i dispositivi hardware, il criterio deve indicare che tutto il firmware deve rimanere aggiornato. I processi possono sfruttare la funzionalità di aggiornamento del firmware integrata in o AXIS Device Manager Extend, per identificare se sono disponibili nuove versioni del firmware per i dispositivi Axis. È necessario definire un orario pianificato, solitamente al di fuori dell'orario lavorativo, per distribuire tutti gli aggiornamenti del firmware a tutte le telecamere. /AXIS Device Manager Extend può anche verificare se gli aggiornamenti del firmware sono stati accettati. Se il sistema dispone di integrazioni specifiche che potrebbero essere influenzate dall'aggiornamento, valutare la possibilità di standardizzare una traccia del firmware LTS.

Protezione della rete

Criteri di accesso remoto

I dispositivi e i servizi esposti a Internet aumentano il rischio che utenti malintenzionati esterni sfruttino o tentino di sfruttare vulnerabilità note. Le telecamere esposte a Internet, ad esempio da piccole organizzazioni che necessitano di accesso video remoto, cadono facilmente preda di malintenzionati se vengono utilizzate password deboli o viene scoperta una nuova vulnerabilità importante. Se possibile, l'accesso remoto all'ambiente Windows deve essere strettamente controllato o evitato. Sebbene l'ambiente Windows possa disporre della connettività Internet per poter aggiornare comodamente i sistemi, utilizzando servizi desktop remoti

come Windows Remote Desktop, TeamViewer e AnyDesk si introducono percorsi che consentono di ottenere l'accesso al sistema, se non gestito correttamente.

Criteri e procedure consigliati
Non esporre mai l'indirizzo IP e la porta di una telecamera per evitare di renderla accessibile direttamente da Internet. Se è necessario l'accesso video remoto, utilizzare Axis Secure Remote Access. utilizza un server di accesso remoto basato su cloud per agevolare l'accesso remoto crittografato al sistema tramite il client o l'applicazione per dispositivi mobili AXIS Camera Station. Oltre a essere responsabile della gestione delle connessioni per gli utenti remoti e mobili, il server di accesso remoto svolge un ruolo importante nella protezione dell'integrità se utilizzato da utenti remoti. Ulteriori informazioni su Axis Secure Remote Access sono disponibili *qui*. Axis fornisce applicazioni mobili con marchio ufficiale per Android e Apple iOS. L'applicazione per dispositivi mobili AXIS Camera Station deve essere scaricata solo da fonti ufficiali, rispettivamente da Google Play Store e Apple App Store.

Per quanto riguarda l'accesso da desktop remoto all'ambiente Windows, si sconsiglia di fornire questo tipo di accesso a un sistema su cui è in esecuzione . Tuttavia, se necessario, è necessario prestare la massima attenzione per garantire che l'applicazione desktop remota scelta sia sicura e che l'accesso venga fornito solo a coloro che lo richiedono. È consigliabile implementare ulteriori livelli di controlli, ad esempio l'autenticazione a più fattori. Si consiglia di registrare e successivamente verificare i tentativi di connessione remota per tenere traccia degli utenti che effettuano l'accesso remoto all'ambiente Windows e delle date in cui tale accesso viene effettuato.

Criteri di esposizione della rete locale

La riduzione dell'esposizione della rete locale può aiutare a ridurre molte minacce comuni riducendo la superficie di attacco. Esistono molti modi per ridurre l'esposizione della rete, tra cui la segmentazione fisica della rete (cavi e hardware di rete separati), la segmentazione logica della rete tramite LAN virtuali (VLAN) e il filtro IP. Le telecamere Axis supportano un filtro IP (tabelle IP). Tale filtro fa sì che il dispositivo risponda solo alle richieste di connessione effettuate da indirizzi IP esplicitamente consentiti.

Criteri e procedure consigliati
AXIS Camera Station S22 NVR sono server hardware con porte di rete doppie. Una delle porte crea una rete segmentata per le telecamere e l'altra si connette alla rete principale (dominio) per servire i client video. Il server funge da ponte e firewall per la rete delle telecamere, impedendo ai client di accedere direttamente alle telecamere. In questo modo si riducono le minacce da parte di utenti malintenzionati sulla rete principale.

Se il server e le telecamere sono tutti posizionati sulla rete principale, si consiglia di configurare il filtro IP della telecamera, limitando l'accesso solo ai server che ospitano , ad AXIS Device Manager e ai client di manutenzione aggiuntivi.

Criteri di crittografia di rete

Il traffico di rete trasferito su reti non sicure deve sempre essere crittografato. Internet è classificato come rete non protetta. Una rete locale può anche essere classificata come non sicura e il traffico di rete deve quindi essere crittografato. Quale criterio applicare al traffico video sulla rete dipende da come viene classificato il video e dal rischio di malintenzionati con accesso di rete al sistema video. Si consiglia di supporre che la rete sia già stata compromessa. Normalmente, le organizzazioni più grandi hanno un criterio che definisce la modalità di classificazione della rete.

Criteri e procedure consigliati

Il traffico tra il server e client video deve utilizzare la crittografia. Il traffico tra il server e le telecamere deve essere crittografato a seconda dell'infrastruttura. Le telecamere Axis dispongono di un certificato autofirmato e HTTPS abilitato per impostazione predefinita. Se esiste il rischio di spoofing di rete, ad esempio quando un computer dannoso finge di essere una telecamera, è necessario usare un'infrastruttura a chiave privata (PKI) con certificati firmati dalla CA. dispone di un'autorità di certificazione (CA) locale integrata che può gestire in modo efficiente la firma e la distribuzione dei certificati del server per i dispositivi Axis.

Versioni TLS

Si consiglia di disabilitare le versioni 1.1 e 1.0 di TLS. L'installatore di AXIS Camera Station offre assistenza durante l'installazione o l'aggiornamento.

Crittografia HTTPS

supporta e utilizza suite di crittografia TLS per crittografare le connessioni HTTPS in modo sicuro. La suite di crittografia specifica dipende dal client che si connette a o dal servizio contattato e viene negoziata da in base al protocollo TLS. Si consiglia di configurare Windows in modo che non utilizzi le suite di crittografia TLS 1.2 elencate *in RFC 7540*. La possibilità di disabilitare una suite di crittografia dipende dai dispositivi e dalle telecamere utilizzati insieme a . Se un dispositivo o una telecamera richiede una suite di crittografia specifica, potrebbe non essere possibile disabilitare la suite di crittografia debole.

Gestione dei dati

Classificazione dei video

I video in diretta e registrati devono essere classificati. Il video può essere classificato come pubblico, privato, limitato o qualsiasi altra classe definita dalle politiche dell'organizzazione. In molti casi, il video è regolato da leggi e normative regionali, nonché da politiche IT interne, pertanto è responsabilità del proprietario del sistema essere a conoscenza delle leggi e delle normative applicabili ai propri dati video

Criteri e procedure consigliati
Classificare i video in diretta, i video registrati e l'audio in conformità ai criteri di classificazione dei dati. Configurare i privilegi di accesso degli utenti e la protezione del sistema in base alla sensibilità dei dati video e audio. Se non richiesto, l'audio può essere disabilitato a livello di dispositivo.

Ulteriori controlli di sicurezza

A seconda del livello di maturità e della tolleranza di rischio dell'organizzazione, sono disponibili diversi controlli di sicurezza aggiuntivi di CIS Controls v8 che consigliamo di implementare per ridurre i rischi di sicurezza informatica nelle operazioni quotidiane.

Ulteriori controlli di CIS:

Controllo 8: Gestione registro di controllo
Raccogli, avvisa, esamina e conserva i log di controllo degli eventi che potrebbero aiutare a rilevare, comprendere o riprendersi da un attacco.

Controllo 14: Implementazione di un programma di consapevolezza e formazione sulla sicurezza
Comprendere le competenze e i comportamenti dei membri della forza lavoro. Istruire la forza lavoro su come identificare le diverse forme di attacco.

Controllo 17: Gestione e reazione agli incidenti
Utilizzare piani scritti di risposta agli incidenti con fasi di gestione degli incidenti e ruoli del personale chiaramente definiti, nonché modalità di segnalazione di un incidente di sicurezza alle autorità competenti e a terze parti

Guida alla protezione del sistema
AXIS Camera Station 5

Ver. M3.2
Data: 2024
Codice art. T10179095