WHITE PAPER

Dati video come prova

Garantire l'integrità dei dati video con AXIS Camera Station

Luglio 2021

Sommario

1 Sommario

Dati video di alta qualità, credibili e non compromessi che possono essere usati come prove. Migliori prassi per la gestione di dati video come prove utilizzando AXIS Camera Station:

- Progettare, configurare e validare accuratamente il sistema per fornire l'immagine, la registrazione e la sicurezza necessarie.
- Esegui una manutenzione regolare
- Gestire ogni prova in base a procedure stabilite

2 Introduzione

La videosorveglianza è praticamente creata su misura per essere usata come prova in tribunale. Un evento catturato "su nastro", per così dire, non può essere confutato, o può? Un giudice probabilmente accetterà dati video di alta qualità, credibili e che non siano stati manomessi.

Ma vi sono anche casi in cui il valore di prova di un video viene inavvertitamente ridotto. Ad esempio, il filmato di sorveglianza con pause nelle tempistiche, i cui persone o veicoli scompaiono all'improvviso o "fanno un salto" nell'immagine, può non essere considerato sufficientemente affidabile da poter essere usato come prova. Il video può anche essere sottoposto a ulteriore scrutinio se i metadati, ad esempio le marche temporali o il MAC address della telecamera, non hanno senso. Qualsiasi sospetto che il video possa essere stato modificato, cancellato o compromesso può ridurre la credibilità del proprietario del video.

Questo documento offre consigli su come gestire i video come prove. In modo più specifico, descrive il ruolo del software di gestione video (VMS) AXIS Camera Station nella catena delle prove, nonché il ruolo del proprietario del video.

Figure 1. La videosorveglianza in punti strategici può fornire prove importanti, se impostata e gestita correttamente.

3 Prassi migliori per la gestione di dati video come prove

Le aziende e le organizzazioni che usano videosorveglianza devono seguire dei processi e delle procedure che stabiliscano come gestire e archiviare i dati video. Per essere completamente preparato per quando una delle telecamere filma un incidente, bisogna assicurarsi che il video non corra il rischio di essere sovrascritto, compromesso o rubato. Inoltre deve essere possibile esportare il filmato in modo sicuro per garantirne l'archiviazione e per consegnarlo alle forze dell'ordine.

Ma la produzione di prove video di alta qualità è un procedimento che comincia con la progettazione consapevole del sistema video. Inoltre è estremamente importante mantenere il sistema aggiornato e prendere nota di ogni irregolarità. Questo capitolo presenta i passi di questo processo, e come seguirli con l'aiuto di AXIS Camera Station e AXIS Camera Station Integrator Suite.

Se si produce un video di sorveglianza in base a questi principi di progettazione del sistema, manutenzione del sistema e gestione degli incidenti, il video sarà conforme con i requisiti di cybersecurity attuali e, fatto ancora più importante, sarà valido come prova in caso di necessità.

Figure 2. Il software di AXIS Camera Station facilita l'impostazione, il funzionamento giornaliero e la gestione strategica di un sistema di videosorveglianza.

3.1 Progetta accuratamente il tuo sistema

Un sistema di videosorveglianza deve essere progettato accuratamente. È necessario selezionare l'attrezzatura in base alle proprie esigenze e impostarla in modo che fornisca l'immagine desiderata, il tipo di registrazione desiderata e la sicurezza necessaria. AXIS Site Designer fornisce un'assistenza significativa per questi scopi.

3.1.1 Per fornire l'immagine necessaria

La qualità dell'immagine dipende dalla telecamera e dalla sua posizione. La risoluzione dell'immagine, o in modo più specifico, la densità di pixel nella scena degli eventi, può essere calcolata se si conosce il modello della telecamera, della lente e la distanza e l'angolazione della telecamera rispetto alla scena. Per una densità di pixel adeguata sul viso di una persona in una scena, potrebbe essere necessario utilizzare molte telecamere oppure telecamere con una risoluzione maggiore. È necessario investigare il campo visivo, i requisiti di illuminazione e altri parametri per telecamere specifiche su un sito specifico. Questo può essere progettato tutto senza problemi tramite AXIS Site Designer.

3.1.2 Per fornire la registrazione necessaria

Per registrare il video, usare hardware validato ad alte prestazioni con ridondanza. Per aumentare l'affidabilità del sistema, AXIS Camera Station supporta il fail over, archiviando temporaneamente immagini

sulla scheda SD della telecamera di rete. Se si usa l'analisi VMD (video motion detection), accertarsi che la registrazione sia sufficientemente lunga per poter verificare l'intero incidente. La registrazione del rilevamento di movimento che non è tarata in modo ottimale può presentare dei vuoti temporali e riprese sconnesse. In molti casi la scelta migliore è una registrazione continua, ma richiede molto più spazio di archiviazione nonché la continua disponibilità di larghezza di banda sufficiente.

3.1.3 Per fornire la sicurezza necessaria

Devi fornire al sistema la sicurezza fisica necessaria per impedire accessi non autorizzati. Tutti gli elementi hardware, comprese telecamere, apparecchiature di rete e cavi, server, archiviazione dati, cavi e dispositivi di alimentazione devono essere protetti. Le misure di sicurezza possono includere il rendere la stanza del server una zona ad accesso limitato, chiudere a chiave l'armadietto del server, mettere il server nell'armadietto, disabilitare le porte fisiche sul server, e mantenere i cavi di rete non esposti.

È importante fornire al sistema la cybersecurity necessaria per minimizzare i rischi di abuso di dati, tentativi di compromissione dei dati e attacchi dolosi. Il cosiddetto hardening può essere in parte fornito da software e tecnologia che garantisce che il sistema soddisfi gli attuali standard di sicurezza. Ma l'hardening richiede inoltre che il proprietario del sistema applichi la cybersecurity e operi attivamente per distribuirla all'interno dell'organizzazione. Ad esempio, tutti gli utenti del sistema devono essere consapevoli dell'importanza di usare password forti e difficili da indovinare e devono stare attenti a non rivelarle. Gli accessi degli utenti devono essere ridotti al minimo, così come i permessi per gli utenti, ad esempio usando l'approccio degli account utenti con meno privilegi. È responsabilità del proprietario del sistema insegnare al personale le prassi migliori e assicurarsi che queste vengano implementate con successo. Un integratore autorizzato può rafforzare il sistema, ma alcune delle misure di cybersecurity possono essere efficaci solo con la collaborazione attiva delle persone che usano il sistema.

Un modo importante per raggiungere una maggiore cybersecurity è di proteggere il video utilizzando il trasporto dati codificato. Per il trasporto dati tra il cliente e il server, AXIS Camera Station usa la codifica AES per video, audio e metadati e la codifica TLS 1.2 per altri dati. AXIS Camera Station può essere configurato per codificare i flussi di dati tra telecamere e server tramite HTTPS. Altre prassi migliori per la protezione del software includono la disattivazione di servizi non utilizzati, usando il filtraggio di IP/MAC address, l'utilizzo di IEEE 802.1X, l'utilizzo del controllo SNMP, l'impostazione della data e dell'ora corrette con un server NTP fidato (per garantire l'accuratezza della marca temporale nei metadati del video), e l'utilizzo solo di Axis Secure Remote Access per connessioni remote (invece dell'inoltro della porta o del desktop remoto). Per misure e raccomandazioni di cybersecurity dettagliate, vedere la Guida all'hardening della cybersecurity di Axis.

3.1.4 Configurare e validare il sistema

È possibile configurare parti chiave del sistema già durante la fase di progettazione utilizzando AXIS Site Designer con nomi di telecamere specifici, risoluzioni e tempi di ritenzione. Quando il sistema è progettato e installato, le configurazioni impostate in AXIS Site Designer possono essere automaticamente importate in AXIS Camera Station da dove si può continuare a modificare le impostazioni se necessario.

Dopo aver completato l'installazione, è possibile validare il sistema usando AXIS Installation Verifier, che è parte di AXIS Camera Station Integrator Suite. Lo strumento per verificare l'installazione mette a prova il sistema in modalità normale e in modalità notturna, per verificare che vi sia larghezza di banda sufficiente durante il funzionamento a luce ridotta quando i livelli di rumorosità sono più elevati ed è necessaria una larghezza di banda maggiore. AXIS Installation Verifier esegue uno stress test aumentando continuamente il volume di dati generato nel sistema fino a quando viene trovato il primo rallentamento. Questo rivelerà la capacità rimasta del sistema e indicherà se sono necessari miglioramenti.

3.2 Esegui una manutenzione regolare

Quando il sistema è in funzione, deve essere controllato e aggiornato continuamente.

Assicurarsi che sia l'hardware che il software funzionino come previsto. Controllare la qualità video, pulire le lenti della telecamera con regolarità, controllare che nulla sia stato manomesso e che il campo visivo e la direzione delle telecamere sia quella prevista. Studiare i log del sistema regolarmente, dato che forniscono informazioni su login, connessioni e problemi con i dispositivi. AXIS Camera Station fornisce delle notifiche su molte irregolarità rilevate e le registra nei log del sistema. Inoltrare i log ai punti di archiviazione remota di sola lettura, in particolare dopo che si è verificato un incidente importante. Axis inoltre fornisce un health monitoring del sistema online come parte di Integrator Suite, che permette di controllare tutte le installazioni e fornisce lo stato del sistema per facilitare servizi e manutenzione.

Sia l'hardware che il software (sistema operativo e VMS) devono essere aggiornati regolarmente. Usando sempre le ultime versioni del software e del firmware, il sistema trarrà vantaggio dalle ultime patch di sicurezza e dagli errori risolti. Idealmente, un VMS trova automaticamente tutti gli aggiornamenti di software e firmware, e richiede l'installazione dell'aggiornamento oppure lo effettua automaticamente. Qualsiasi software scaricato deve provenire da fonti fidate.

3.3 Gestire ogni prova in base a procedure stabilite

Se hai applicato in modo appropriato i principi di progettazione e mantenimento del sistema di sorveglianza, AXIS Camera Station dovrebbe essere in grado di fornire prove credibili di qualsiasi incidente rilevato dalle telecamere. Poi ci devono essere delle procedure su come procedere.

È imperativo seguire i consigli delle forze dell'ordine. In caso di crimini gravi, le forze dell'ordine hanno il diritto di decidere come proteggere le prove e devi seguire le istruzioni date.

In altri casi, il processo principale è di estrarre le prove in modo sicuro. Ciò significa essere in grado di fornire le informazioni fuori dal sistema come al suo intero, in modo non adulterato e preservandone la credibilità.

L'estrazione deve essere effettuata da un operatore dedicato, preferibilmente insieme a un testimone. Questo operatore può essere un professionista esterno, ingaggiato con l'unico scopo di fornire e documentare un'estrazione affidabile. L'utilizzo di una terza parte per l'estrazione può ridurre al minimo il rischio che il proprietario del video venga sospettato di aver compromesso le prove. L'operatore deve assicurarsi di estrarre il video che copra l'incidente ma anche fornire informazioni sufficienti su qualsiasi evento che ha portato all'accaduto o che ne è seguito.

I video selezionati possono essere estratti su dischi di sola lettura, ad esempio CD-R, DVD-R o Blu-ray (-R), che poi possono essere consegnati alle forze dell'ordine. Un'alternativa è di estrarre i video in file zip codificati e protetti da password. I file possono essere firmati in modo digitale e legati a un hash con la password dell'utente. Per confermare l'hash e controllare l'hash attuale del file, la firma deve essere inserita in AXIS File Player. Se gli hash combaciano, nessun dato è stato modificato in quel file.

Axis inoltre fornisce AXIS Camera Station Incident Report, che funziona da strumento di estrazione avanzato per gli operatori. Lo strumento deve essere impostato in anticipo ottenendo da un operatore i dati relativi a incidenti e ubicazione dell'estrazione. L'Incident Report poi realizza l'estrazione in automatico, consentendo di estrarre video organizzati in base agli incidenti, utilizzando dei tag come nomi delle cartelle. L'ubicazione deve essere impostata come una risorsa locale, ad esempio network-attached storage (NAS) o una risorsa remota, ad esempio archiviazione su cloud se è accessibile tramite protocollo SMB. Il rapporto consiste di file video, istantanee in .jpg (create manualmente in AXIS Camera Station dall'operatore durante la creazione del rapporto), preferiti in .txt e tutte le informazioni raccolte in un rapporto in formato .pdf.

4 Risorse di cybersecurity

Axis applica le migliore procedure di cybersecurity a livello di design, sviluppo e prova dei dispositivi per ridurre il rischio di difetti che potrebbero essere sfruttati durante un attacco. Ci atteniamo alle migliori procedure di cybersecurity, ad esempio in merito alla gestione delle vulnerabilità, ai requisiti di trasmissione e archiviazione sicura dei dati e alla codificazione. Ci impegniamo a semplificare e rendere più economicamente vantaggiosa l'applicazione dei controlli di sicurezza appropriati, e i nostri dispositivi supportano la codifica e la gestione della sicurezza.

Mentre Axis, in qualità d produttore e fornitore del sistema, compie gli sforzi maggiori per offrire il sistema o la soluzione più completi e sicuri, tu, in qualità di utente finale, hai la responsabilità di applicare le migliori procedure di sicurezza. Axis fornisce diversi strumenti, guide e tutorial per aiutarti. Vedi www.axis.com/cybersecurity, dove è possibile trovare, ad esempio, strumenti per l'hardening, informazioni sulla gestione della sicurezza, e messaggi sul blog sulla cybersecurity.

T10169774/IT/M1.2/2107

Informazioni su Axis Communications

Axis consente un mondo più intelligente e più sicuro creando soluzioni per migliorare la sicurezza e le prestazioni aziendali. Come società di tecnologie di rete e leader nel settore, Axis offre soluzioni nella videosorveglianza, controllo degli accessi, interfono e sistemi audio. Queste sono ottimizzate da applicazioni di analisi intelligente e supportate da formazione di alta qualità.

Axis ha circa 4.000 impiegati dedicati in più di 50 paesi e collabora con partner di tecnologia e integrazione di sistema in tutto il mondo per offrire soluzioni di clienti. Fondata nel 1984, Axis e con sede a Lund, in Svezia