Salvaguardia del vostro sistema di videosorveglianza dagli attacchi informatici

Consigli per valutare la sicurezza informatica della vostra soluzione video

Di Todd Robinson,
Product Manager,
apparecchi di registrazione fissi

I recenti attacchi di alto profilo contro i sistemi di videosorveglianza hanno sottolineato l'importanza di scegliere una tecnologia video sicura dal punto di vista informatico.

Le conseguenze di un attacco informatico possono essere devastanti, divulgando dati altamente sensibili su Internet, riducendo la fiducia dei clienti e aumentando il rischio di controversie e responsabilità finanziarie.

È imperativo che le aziende scelgano prodotti di cui potersi fidare e produttori con una solida reputazione per gli investimenti nella sicurezza informatica e nelle misure di protezione dei dati. A volte questo implica scavare più a fondo oltre i titoli dei giornali e nel background di un'azienda, nella sua ricerca e sviluppo e nei processi di produzione dei prodotti.

Ecco alcune cose importanti da considerare quando si valuta una soluzione di video-sorveglianza dal punto di vista della sicurezza informatica:

Todd Robinson

Cosa è crittografato e cosa no?

Mentre molti sistemi di videosorveglianza offrono la crittografia in transito, che impedisce a terzi di accedere ai dati mentre vengono trasmessi, mantenendoli crittografati fino a quando non raggiungono il loro punto finale, la crittografia completa end-to-end è il massimo livello di protezione per i vostri dati. I dati non rappresentano solo video e audio, ma includono anche metadati come i dati GPS, i dati dei pannelli di allarme, i dati degli analytics, i dati POS o i dati delle transazioni bancomat.

La crittografia completa end-to-end va oltre la semplice crittografia in transito e include la crittografia a riposo in modo che ogni aspetto dei vostri dati sia protetto. La crittografia a riposo è il processo di crittografia dei dati memorizzati su supporti fisici. Con la crittografia completa end-to-end, i dati vengono crittografati sia mentre viaggiano dalla telecamera al registratore e dal registratore al software client, sia che vengano memorizzati su supporti fisici.

Livelli più alti di crittografia possono a volte avere un impatto sulle prestazioni della CPU, quindi parlate con il vostro fornitore di video per trovare il giusto equilibrio per le vostre esigenze.

Sicurezza del sistema operativo (OS)

C'è molto dibattito sulla sicurezza di Linux rispetto a Windows nei videoregistratori di rete (NVR). Mentre in definitiva può essere utilizzato qualsiasi sistema, io sostengo che un apparecchio con un sistema operativo basato su Linux è più sicuro, qualora sia stato personalizzato per il solo scopo di registrare video. Il sistema operativo basato su Linux nei registratori di March Networks, per esempio, viene sottoposto al processo di hardening, rimuovendo i servizi non necessari, in modo che ci siano meno opportunità per gli attacchi informatici.

Inoltre, quando un sistema operativo basato su Linux viene personalizzato, non dipende da terze parti per gli aggiornamenti di sicurezza e non c'è il rischio di aggiornamenti di sistema applicati automaticamente che potrebbero avere un impatto negativo sul sistema. Ha anche un controllo più stretto su ciò a cui un'applicazione ha accesso, rendendo più difficile per il software dannoso ottenere l'accesso al sistema. E per un ulteriore livello di sicurezza, Linux ha un grande pool di sviluppatori per il suo codice OS open source, rendendo più probabile che qualsiasi falla nella sicurezza venga scoperta rapidamente.

Chi ha accesso al sistema?

La violazione di alto profilo che ha avuto luogo all'inizio di questo mese presumibilmente prevedeva l'uso di un account "Super Amministratore", dove una persona aveva accesso illimitato a tutte le telecamere del sistema basato su cloud. Ovviamente, questo tipo di accesso illimitato è una minaccia per la sicurezza, quindi parlate con il vostro fornitore di video circa le loro norme sui diritti degli utenti e l'accesso. (Per inciso, March Networks non ha una modalità "Super User" o "Super Amministratore" con accesso a tutti i sistemi dei nostri clienti).

Che sia nel cloud o presso la sede, un buon fornitore di video dovrebbe offrire controlli rigorosi sui diritti e la gestione degli utenti, permettendo agli amministratori di creare profili molto specifici che consentano o limitino l'accesso alle persone che usano il sistema. Questo garantisce che i dipendenti più giovani o di primo livello vedano solo ciò di cui hanno bisogno per svolgere il loro lavoro; permette anche agli amministratori di sistema di controllare l'accesso degli utenti e vedere chi ha avuto accesso a cosa e quando.

Protezione delle password

La sicurezza delle password sembra semplice, ma è incredibile quante violazioni avvengano a causa di password perse o rubate. Un buon fornitore di videosorveglianza non utilizzerà password a codifica fissa, o hard-coded, sui suoi dispositivi, e incoraggerà anche frequenti cambi di password e la creazione di password complesse.

Per esempio, con i registratori di March Networks ogni cliente riceve una password usa e getta per la configurazione iniziale, poi gli viene richiesto di cambiare la password con una password complessa e composta da più caratteri.

Scansione delle minacce in corso

Poiché le minacce informatiche sono in continua evoluzione, è importante considerare quali altre funzionalità possano essere integrate nella vostra soluzione di videosorveglianza per avvisarvi in caso di un potenziale attacco.

Alcuni sistemi hanno avvisi di sicurezza e allarmi integrati, in modo che riceverete un avviso in caso di tentativi insoliti di accesso al registratore, come ripetuti errori di accesso o un potenziale attacco DDoS (negazione del servizio).

Anche la scelta di un fornitore di videosorveglianza che monitori costantemente le vulnerabilità e comunichi tutte le informazioni necessarie è fondamentale in modo che i problemi possano essere risolti prima che si verifichi un attacco. Il programma di aggiornamenti di sicurezza e avvisi di March Networks valuta le vulnerabilità, determina come queste influenzino i prodotti o il software che state utilizzando e vi avvisa in modo che possano essere affrontate.

Per ulteriori informazioni sulla sicurezza informatica della videosorveglianza, visitate www.marchnetworks.com/products-services/video-surveillance-cybersecurity/

March Networks® aiuta le organizzazioni a trasformare il video in business intelligence attraverso l'integrazione di video di sorveglianza, analytics e dati di sistemi aziendali e dispositivi IoT. Le aziende di tutto il mondo utilizzano le nostre soluzioni per migliorare l'efficienza e la conformità, ridurre le perdite e i rischi, migliorare il servizio clienti e competere con maggiore successo. Con radici profonde nella videosicurezza e nel networking, March Networks è anche riconosciuta come leader nella gestione video scalabile a livello aziendale e nei servizi ospitati.

Nord America 1 800 563 5564
America Latina ..... +5255 5259 9511
Europa ..... +39 0362 17935
Asia ..... +65 6818 0963
Australia e Nuova Zelanda ..... +61 1300 089 419
Medio Oriente e Africa ..... +971 4 399 5525

MARCH networks