Come si proteggono le telecamere in rete dai rischi informatici?

Tavola rotonda virtuale con Axis, Bosch, Milestone – giugno 2016

Prima domanda
Quali sono allo stato attuale le possibilità di proteggere le camere per videosorveglianza in rete dai rischi informatici che possano mettere a repentaglio la riservatezza dei dati raccolti sul campo?

Axis (Pietro Tonussi)

Prima di tutto va detto che la Cyber Security è un concetto, non un prodotto. La responsabilità di proteggere la rete, i suoi dispositivi e i servizi che supporta ricade su tutta la catena di approvvigionamento del fornitore, nonché sull'organizzazione dell'utente finale. Essa interessa persone, processi e tecnologie. Non è possibile creare un sistema sicuro al 100%. Almeno non un sistema utilizzabile. E' possibile solamente rendere il sistema più sicuro, riducendo le aree di esposizione e attenuando i rischi. Ci saranno sempre dei rischi che devono essere conosciuti e gestiti. Come ogni produttore di dispositivi in rete, Axis non può fornire garanzie sul fatto che i prodotti, le applicazioni o i servizi di rete non presentino vulnerabilità che possano venire sfruttate per attacchi dannosi, ma ci siamo impegnati a offrire suggerimenti su come ridurre ed eliminare i rischi

Bosch (Stefano Riboli)

Rispondo facendo riferimento al Cyber Security Framework, introdotto nel febbraio 2014 dal National Institute of Standards and Technology (NIST), un Framework progettato specificamente per ridurre i rischi informatici alle infrastrutture critiche e alla loro rete di dispositivi e dati ad essa collegata. Questo permette di capire i rischi collegati alla sicurezza informatica esterni ed interni all'organizzazione di qualsiasi dimensione, classificandole dal Livello 1 al Livello 4.

Nello specifico, dell'ambito di videosorveglianza si possono indicare 14 punti per migliorare la sicurezza dei dispositivi:

1. Limitare l'accesso alla telecamera tramite la restrizione degli indirizzi IP. Questo può essere fatto tramite IPAM o indirizzamento IP in congiunzione con la subnet.
2. Limitare l'accesso a specifici MAC Address e specifiche porte;
3. Proteggere tramite password: lunghezza tra 8 e 12 caratteri, con maiuscole e minuscole, un carattere speciale e almeno un numero;
4. Assicurare l'accesso via software tramite protocolli minimi, cioè disabilitando quelli non utilizzati;
5. A seconda del livello di sicurezza richiesto dall'installazione, potrebbe essere necessario cambiare le porte HTTP o HTTPS per evitare di fornire informazioni sulle porte standard alle applicazioni di discovery.
6. Disabilitare se non necessario il protocollo Telnet;
7. Impiegare il Telnet tramite "web sockets", con connessione sicura HTTPS;
8. Disabilitare i servizi Cloud se non utilizzati;
9. Se necessario usare il protocollo RTSP per video ONVIF, incapsulandolo su una connessione tunnel HTTPS
10. Disabilitare il discovery tramite UPnP
11. Ridurre l'impostazione TTL (salti di rete) così da bloccare accessi da altre reti
12. Filtrare gli indirizzi IPV4 autorizzati in rete
13. Autenticazione tramite server RADIUS 802.1x
14. Se su una rete pubblica, usare reti certificate dalla pubblica autorità per garantire le comunicazioni tra dispositivi autorizzati.

Milestone (Alberto Bruschi)
I sistemi video over IP fanno parte del mondo dell'IT e, come tali, le prime precauzioni sono quelle di realizzare una infrastruttura che segua le specifiche standard di protezione delle reti dati. Ogni prodotto dovrebbe poi avere protezioni specifiche per evitare di essere utilizzati come target o veicolo (malware).

Seconda domanda

Quale policy ha adottato la sua azienda per tutelare gli utilizzatori finali dai rischi informatici e gli integratori dalle possibili azioni di responsabilità nei loro confronti, qualora i prodotti installati non fossero ragionevolmente sicuri?

Axis (Pietro Tonussi)
Partendo dal concetto espresso prima, la missione di Axis in termini di Sicurezza Informatica è di aiutare le parti interessate a raggiungere un livello di sicurezza accettabile per i sistemi video e a ridurne i relativi costi per la protezione. oltre a fornire i prodotti, le applicazioni e i servizi più sicuri. La definizione di un livello di protezione accettabile dipende dalla situazione, dal livello di minaccia e dal costo di possibili violazioni (analisi di rischio del cliente).
Abbiamo creato una guida dedicata per i nostri clienti, siano essi partner o utenti finali, che intende fornire un supporto su come sfruttare al meglio le features che comunque sono già insite in tutti i prodotti Axis. Essa stabilisce una configurazione di base e una strategia di protezione avanzata per affrontare il panorama delle minacce in continua evoluzione. In tal modo si aumenta il valore delle soluzioni video di Axis per i propri clienti e partner commerciali.

Bosch (Stefano Riboli)
Quando si tratta di dispositivi video IP Bosch, la prima linea di protezione sono i dispositivi IP stessi. Gli encoder e le telecamere Bosch sono costruiti in un ambiente controllato e sicuro che viene continuamente sottoposto ad ispezioni. I dispositivi possono essere scritti solo tramite il firmware certificato Bosch che è costruito per una specifica serie hardware e chipset, non contraffabile. La maggior parte dei dispositivi video IP Bosch sono dotati di un chip di sicurezza integrato che fornisce funzionalità simili a crypto SmartCard e il cosiddetto "Trusted Platform Module", (TPM). Questo chip si comporta come una cassaforte per i dati critici, proteggendo i certificati, chiavi, licenze e l'accesso non autorizzato anche quando la telecamera è aperta fisicamente. I dispositivi video IP Bosch sono stati sottoposti a più di trentamila (30.000) test e della vulnerabilità e di penetrazione effettuati da società di sicurezza indipendenti. Finora, non ci sono stati casi di vulnerabilità in quanto i dispositivi sono adeguatamente protetti.
Inoltre, abbiamo prodotto una guida su come configurare i prodotti così da ridurre i rischi precedentemente indicati.

Milestone (Alberto Bruschi)
Da sempre Milestone implementa tutti i parametri di sicurezza necessari legati al sistema operativo utilizzato. Sistema operativo che deve comunque sempre essere aggiornato e curato da parte del manutentore o dal cliente finale in modo da evitare possibili minacce. Per affrontare ulteriormente questi problemi di sicurezza e dei rischi connessi, Milestone ha inoltre implementato diverse funzioni in aggiunta alle misure standard che possono essere utilizzate per aumentare l'inviolabilità del sistema video generale e delle sue registrazioni.
Milestone XProtect® Corporate e XProtect® Smart Client forniscono una serie di meccanismi di protezione che consentono agli utenti di mantenere la piena sicurezza e l'integrità dei dati video registrati. Crittografia del database, firma digitale e una funzione per impedire la riesportazione del materiale esportato sono alcune delle componenti fondamentali della soluzione di gestione video Milestone per garantire e proteggere l'integrità delle prove video.
Il team di sviluppo Milestone è sempre impegnato a mantenere alto il livello di guardia e, per quanto riguarda le nostre soluzioni, ad implementare le ultime tecnologie in fatto di gestione e protezione dei dati.