Cyber security e videosorveglianza responsabile: accettare, mitigare e prevenire il rischio di attacchi

a cura di Pietro Tonussi, Business Development Manager Southern Europe in Axis Communications

Quando parliamo di Cyber Security, dobbiamo innanzitutto fare riferimento all'utilizzo sempre più diffuso del Web e all'ambiente all'interno del quale avvengono le operazioni che fanno uso di Internet, il cosiddetto *Cyberspace*. L'evoluzione digitale della società e dell'economia ha favorito e aumentato l'interazione tra individui, aziende e istituzioni per finalità sociali, economiche e finanziarie ma, allo stesso tempo, ha creato nuove opportunità per attività criminali di vario tipo, portando a nuovi modelli di strutturazione e organizzazione di attività illecite.

L'aumento della dipendenza dal Cyberspace, se da un lato offre nuove opportunità, dall'altro introduce nuove minacce. La rete rende infatti possibili scambi e interazioni su scala internazionale e un'apertura può rendere i sistemi informatici su cui essa si basa più vulnerabili agli attacchi di criminali, hacker, terroristi. In breve, di quanti intendono comprometterli, danneggiarli o sfruttarli per ottenere informazioni personali o commerciali.

La sicurezza informatica diventa, pertanto, un tema molto sentito proprio per la crescente informatizzazione della società e dei servizi, nonchè della parallela diffusione e specializzazione dei potenziali criminali. L'interesse è aumentato notevolmente negli anni in differenti ambiti: esiste, ad esempio, un team di professionisti che si occupa delle problematiche di sicurezza legate alla trasmissione di informazioni confidenziali in rete. Ne consegue che saper sviluppare nuove capacità e nuovi strumenti per migliorare la Cyber Security rappresenta una delle sfide moderne,

anche per chi si occupa di videosorveglianza con telecamere IP, sensori che devono essere considerati come un prodotto simile a un computer collegato in rete.

Negli ultimi anni, inoltre, si è assistito a una convergenza tra sicurezza fisica e sicurezza IT, ambiti fino a poco tempo fa ben distinti. Oggi sono invece realtà che condividono strumenti comuni e lavorano in sinergia per mitigare le minacce sia fisiche che informatiche per una determinata azienda o istituzione.

Nonostante questa integrazione tra sicurezza fisica e sicurezza IT e i continui sviluppi nel settore, è necessario essere consapevoli del fatto che non è possibile creare un sistema sicuro al 100%, almeno non un sistema utilizzabile.

Tuttavia, è possibile rendere un sistema più sicuro, riducendo le aree di esposizione e attenuando i rischi. Questi ultimi ci saranno sempre, ma devono essere

conosciuti e gestiti: non si può fornire alcuna garanzia sul fatto che i prodotti, le applicazioni o i servizi non presentino difetti o vulnerabilità che possano essere sfruttati per attacchi dannosi.
La sicurezza non deve, quindi, essere vista solamente come uno stato finale ma, piuttosto, come il risultato di un processo con il coinvolgimento delle strutture che si occupano di security. Un processo che diventi parte integrante dei percorsi aziendali e che possa svilupparsi, evolvere ed attuarsi nel tempo, sulla base delle potenziali minacce.
È importante capire che le minacce devono essere gestite a livello di sistema e non a livello di singolo prodotto: la **Cyber Security è un processo, non un prodotto**. È oggettivamente impossibile eliminare tutti i rischi, anzi questo tentativo potrebbe risultare estremamente costoso e, talvolta, inutile. La raccomandazione è quindi quella di identificare i dati più sensibili e proteggerli nel modo più efficace possibile. In quest'ottica il rischio può e deve essere accettato e di conseguenza mitigato da alcune misure, ad esempio trasferendo il rischio ad enti terzi come le Assicurazioni. Ma è davvero questa la soluzione migliore?
Accettare il rischio dovrebbe essere una decisione consapevole e serena. Non sono solo i danni prodotti dagli attacchi in sé, ma soprattutto le conseguenze che questi causano nel lungo periodo ad essere i maggiori pericoli a livello aziendale. Negli ultimi tempi, si assiste sempre di più ad attacchi mirati come l'appropriazione di dati sensibili, la cancellazione degli stessi o il furto di materiale coperto da copyright.
Tuttavia, se non si conoscono questi rischi non è possibile prendere decisioni efficaci e puntuali: **un'analisi mirata delle minacce cyber potrebbe indicare realmente quali dati e informazioni andrebbero persi in caso di attacco**, un elemento concreto che aiuterebbe a capire quanto e come investire per la protezione. Un'analisi non corretta, viceversa, potrebbe portare a investimenti elevati o a protezioni non adeguate del sistema.
Il punto focale della questione, per **Axis**, è quello di contribuire ad aiutare le aziende a raggiungere un livello di sicurezza accettabile per i sistemi e ridurne i relativi costi per la protezione. La definizione di un livello di protezione accettabile dipende dalla situazione, dal livello di minaccia e dal costo di possibili violazioni.

Cyber Security: aree di vulnerabilità

Le aziende non sempre si accorgono di essere state violate e spesso non sanno come proteggersi, credendo erroneamente che le azioni da mettere in atto siano solo di tipo tecnico e che siano economicamente impegnative.
Il rischio c'è, è un dato di fatto e bisogna accettarlo. È innegabile però che ci sia bisogno di molta educazione in materia perché esistono diverse aree di vulnerabilità, che si possono raggruppare in tre diverse categorie:

1. UTENTI: in più casi negligenti e poco accorti, sono la più grande minaccia per qualsiasi sistema. Tra i pericoli più comuni che possono provocare gravi danni alla sicurezza del sistema, è possibile individuare l'utilizzo improprio dei social media; il ricorso a password errate e troppo semplici da eludere, spesso facili da decriptare perché banali o scritte su post-it incollati allo schermo del pc; il fishing, vale a dire il fenomeno di messaggi (e-mail, messaggi istantanei o tramite un sito social) per indurre gli utenti con l'inganno a fornire informazioni confidenziali o personali; l'installazione di app non attendibili e la perdita di dispositivi USB che possono contenere materiali sensibili sull'azienda.

2. SISTEMI: in generale poco protetti, risultano essere molto vulnerabili e le cause possono essere differenti. Tra queste è possibile segnalare il basso livello di configurazione e il design dell'intera infrastruttura; una scarsa conoscenza e competenza in materia di protezione; policy di protezione spesso non adeguate e una bassa o inesistente manutenzione dello stesso sistema con aggiornamenti dei software spesso insufficienti.

3. DIFETTI DI IMPLEMENTAZIONE DELLA SICUREZZA: in tal senso ci si riferisce ai "bachi" delle soluzioni o ai difetti di realizzazione e di progettazione del sistema, così come alla scarsa conoscenza delle applicazioni dei dispositivi che rendono le implementazioni dei processi di sicurezza molto bassi.

Gli esperti di Cyber Security dichiarano che oltre il **90% di tutte le violazioni e intrusioni di "successo" sono dovute a errori causati da persone, da una scarsa configurazione del sistema e dalla mancanza di manutenzione**. Un utente malintenzionato comincerà quindi il suo attacco sempre dal punto più facile e meno impegnativo, ovvero dagli utenti, per attaccare successivamente tutto il sistema.

Cyber Security: tipologie di attacchi

Quando parliamo degli attacchi perpetrati attraverso la rete è possibile classificarli in due tipologie principali:

• *Attacco opportunistico:* si verifica quando il malintenzionato sfrutta vulnerabilità ben conosciute per attaccare le vittime; se il vettore di attacco selezionato fallisce, l'attaccante procederà alla prossima vittima. Un attacco opportunistico ha come obiettivo gli utenti e i sistemi mal configurati.
• *Attacco mirato:* in genere comporta una pianificazione intelligente e si verifica quando un malintenzionato seleziona un target specifico per raggiungere un obiettivo preciso. Esso si rivolgerà agli utenti vulnerabili e ai sistemi difettosi o scarsamente protetti.

I primi sono sicuramente i più frequenti e i più facili da attuare, mentre i secondi sono indubbiamente più pericolosi in quanto vi è spesso un alto valore in gioco, come l'appropriazione dei dati sensibili, la cancellazione degli stessi o il furto di materiale coperto da copyright.

Come proteggere un sistema di videosorveglianza

Nella realizzazione di un sistema di videosorveglianza sempre di più vengono impiegate telecamere di rete IP, che da un punto di vista informatico devono essere considerate come sensori collegati alla rete alla stregua di un PC. Per avere un sistema il più protetto possibile, è necessario prestare particolare attenzione a tutti i componenti che caratterizzano una soluzione di videosorveglianza, vale a dire il server (con dischi per la registrazione delle immagini – dati), il client e il numero (variabile) di telecamere IP.
Per garantire il massimo livello di protezione è pertanto necessario che il sistema video facente parte della rete, rispetti alcuni requisiti che gli consentano di allinearsi con i livelli di protezione dell'infrastruttura esistente e con le policy di protezione definite dal responsabile della rete; inoltre il sistema deve avere una protezione adeguata a seconda del livello di rischio precedentemente calcolato in tutte le sue componenti (server, client e device connessi alla rete) secondo un'analisi del rischio preventiva che è di fondamentale importanza.
Axis Communications, consapevole dell'importanza della Cyber Security anche nel campo della videosorveglianza, si impegna, come leader del video di rete, a fornire tutti gli strumenti per proteggere i propri clienti dagli attacchi sul web e per creare soluzioni sempre più sicure da questo punto di vista. Axis offre infatti ai propri clienti una guida tecnica per seguire le corrette procedure nell'installazione di un sistema di videosorveglianza. Un impegno che si concretizza nella **"Axis Hardening Guide", un documento che facilita questo processo e contribuisce a proteggersi dagli attacchi informatici.**

Quando si sceglie di installare un sistema di videosorveglianza, bisogna fare riferimento a differenti livelli di protezione che coinvolgono in prima battuta l'intera rete, una sorta di protezione standard secondo cui adottare precisi accorgimenti, come l'utilizzo di Firewall, uno strumento di sicurezza in grado di proteggere un computer o una rete da tentativi non autorizzati di accedere al sistema; un controllo degli accessi alla rete e una segmentazione della stessa; una richiesta di autorizzazione di accesso ai vari servizi della rete e alla manutenzione; realizzare un'attività di monitoraggio costante dello "status" della rete sul fronte sicurezza.

Dal punto di vista della protezione dei Client, il reparto tecnico di Axis e coloro che si occupano di Cyber Security suggeriscono di proteggere tutti i "nodi" della rete secondo le policy dettate dal dipartimento IT mediante un'accurata e puntuale gestione delle password degli account e dei privilegi di accesso ai servizi di rete, attraverso la scelta e l'implementazione corrette di Antivirus e Firewall, mettendo in atto un attento processo di Encryption, prevedendo inoltre una gestione accurata della manutenzione dei client con un aggiornamento costante dei sistemi operativi e delle applicazioni.

Fondamentale in quest'ottica, è la protezione dei server, operazione realizzata dall'amministratore dei sistemi IT con l'implementazione dei sistemi di sicurezza già in uso che, normalmente, comprendono: la gestione degli account e dei relativi privilegi, la configurazione dei servizi e un corretto utilizzo anche in questo caso di Antivirus e Firewall, senza dimenticare l'Encryption e la manutenzione generale che sono sempre due processi fondamentali per la sicurezza generale del sistema. La protezione dei server è sempre molto importante, ma diventa fondamentale nel caso in cui ci siano dei server

di gestione del VMS (Video Management System) dove, molto spesso, sono custodite le immagine provenienti dalle telecamere e laddove un'eventuale intrusione da parte di un hacker con l'obiettivo di sottrarre immagini andrebbe a ledere le normativa della sicurezza della protezione del dato in riferimento alle ottemperanze del Garante della Privacy.

Dobbiamo inoltre considerare che effettuare il cyber hardening di dispositivi IoT è più facile rispetto a client e server, in quanto dispongono di un minor numero di servizi interni e di interfaccia. La maggior parte dei device è protetta da infrastrutture accessibili solo attraverso i servizi cloud/server e i loro utenti non installano applicazioni non sicure, non aprono allegati di posta elettronica pericolosi o accedono a siti sospetti.

Axis Communications, nella piena consapevolezza dell'importanza dell'argomento ma consapevole al tempo stesso che i propri clienti stiano già seguendo delle regole di base in materia di Cyber Security, ha redatto la guida con l'obiettivo di agevolare, attraverso semplici passaggi, un fine tunning delle telecamere considerate come device della rete.

Per maggiori informazioni e ulteriori dettagli sui livelli di protezione consigliati da Axis Communications è possibile scaricare l'AXIS Hardening Guide al seguente link:

http://www.axis.com/files/sales/AXIS_Hardening_Guide_1488265_en_1510.pdf

AXIS COMMUNICATIONS

CONTATTI: AXIS COMMUNICATIONS
Tel. +39 011 8198817
www.axis.com