Building blocks

UNA CYBERSECURITY ‘IN REGOLA’

5 FATTORI DA CONSIDERARE PER SISTEMI ‘A PROVA DI FUTURO’, DOVE CYBERSECURITY E SICUREZZA FISICA SONO ELEMENTI IMPRESCINDIBILI E INSCINDIBILI FRA LORO

Mariagrazia Corradini

Tutti gli stakeholder aziendali sono chiamati a fare la propria parte per garantire che ogni anello della catena della cybersecurity sia il più saldo possibile

I rischi legati alla sicurezza fisica sono sotto gli occhi di tutti: una porta aperta aumenta le probabilità di ingressi non autorizzati; oggetti di valore lasciati in vista possono essere più facilmente rubati, allo stesso modo, errori e incidenti possono danneggiare persone, proprietà e cose. I rischi per la cybersecurity possono risultare meno evidenti rispetto a quella da cui dipende la sicurezza fisica, ma saperli riconoscere e affrontare nel modo corretto diventa tanto più urgente quanto più le tecnologie informatiche evolvono e, con esse, le nuove tattiche utilizzate dai cyber criminali.

Ciò è ancora più vero se si considera la crescita esponenziale del numero di dispositivi connessi e la convergenza sempre più forte tra mondo IT e OT. Sebbene, infatti, l’IoT (Internet of Things) sia una realtà ormai ampiamente diffusa nelle aziende e non solo, non tutte le organizzazioni sono consapevoli del fatto che dispositivi come le videocamere di sorveglianza, gli allarmi antincendio, i router, i sistemi di sicurezza intelligenti sono spesso i primi punti di accesso per un criminale informatico. Attacchi malware, phishing e violazione della privacy sono termini ormai entrati nella quotidianità, tuttavia, è ancora forte la necessità di creare una cultura della sicurezza informatica specificatamente per i dispositivi fisici connessi, che si basi su una maggiore consapevolezza delle minacce cyber attuali e delle pratiche per contrastarle.

Axis Communications entra nel merito di questa tematica imprescindibile per far capire ad aziende e consumatori che la protezione dei dispositivi connessi, come le telecamere di sorveglianza, non debba mai essere sottovaluta.

I principi cardine per un approccio resiliente

Sicurezza fisica e sicurezza informatica presentano delle evidenti differenze ma, in linea di massima, in entrambi gli ambiti è possibile adottare lo stesso approccio per affrontare i rischi. In particolare, i principi chiave da applicare possono essere sintetizzati come segue:

- identificare e classificare asset e risorse di cui si dispone e che devono essere protetti;
- individuare le possibili minacce e, quindi, gli aggressori da cui difendersi;
- riconoscere le possibili vulnerabilità che potrebbero essere sfruttate, definendo quindi la probabilità che ciò avvenga;
- determinare l’eventuale costo di un evento negativo, ovvero le relative conseguenze.

Ma cosa si intende per rischio? Il rischio può essere definito come la probabilità di una minaccia moltiplicata per il suo impatto in termini di danno. Una volta stabilito, occorre chiedersi cosa si è disposti a fare per prevenirlo. Vediamo quindi ora quali possono essere le minacce e le best practice analizzando 5 fattori fondamentali.

1: le minacce cyber più comuni

In ambito videosorveglianza sono tre le minacce più frequenti da tenere sotto controllo:

- *errore umano non intenzionale e ingenuità:* ha alla base la mancanza di ‘cyber awareness’ e si può verificare concretamente in modi diversi, dal social engineering, come il phishing, all’uso scorretto delle password, fino alla gestione inadeguata del sistema stesso, dettata per esempio dai mancati aggiornamenti;
- *uso improprio deliberato del sistema:* è la minaccia rappresentata da qualcuno che ha accesso

legittimo al sistema, oppure da qualcuno non autorizzato, che intende rubare i dati, manipolare il sistema o danneggiarlo;

- *manomissione fisica e sabotaggio:* i dispositivi fisicamente esposti possono essere oggetto di manomissione. Ciò non riguarda semplicemente le telecamere, ma anche i cavi che possono fornire l'opportunità per violare la rete.

2: avere un network sano e sicuro

Per raggiungere questo obiettivo è fondamentale adottare delle buone pratiche di 'cyber hygiene', ovvero quell'insieme di azioni da eseguire regolarmente per mantenere in salute dispositivi, reti e sistemi, conservandone l'integrità.

Innanzitutto, è buona prassi utilizzare password forti e uniche e installare i device nel rispetto delle policy IT e di sicurezza. Un'organizzazione dovrebbe poi definire ruoli e responsabilità, applicando il principio del 'privilegio minimo', secondo il quale a un utente vengono attribuiti solamente i permessi di accesso relativi alle risorse di cui ha bisogno per lo svolgimento delle proprie mansioni. Inoltre, lavorare a stretto contatto con l'intera supply chain può favorire la condivisione di linee guida per l'installazione e l'aggiornamento dei dispositivi.

Infine, la segmentazione di rete applicata ai dispositivi fisici, così come le Access Control List consentono di ridurre i movimenti non autorizzati nella rete.

Fonte: foto Shutterstock

Una rete è sicura solo nella misura in cui sono sicuri i dispositivi a essa connessi

3: il ruolo dell'intelligenza artificiale (AI)

Come altre tecnologie innovative, anche l'AI ha destato l'interesse dei cyber criminali. Alla domanda, quindi, se considerare l'intelligenza artificiale una nuova arma di attacco o un possibile strumento di difesa non è possibile dare una risposta univoca. Grazie all'AI gli hacker possono mettere a punto attacchi sempre più sofisticati: dai chatbot impiegati per ingaggiare i dipendenti attraverso profili social falsi, all'utilizzo di reti neurali per l'identificazione dei dati più preziosi. È altrettanto vero, però, che l'AI può trasformarsi in un valido strumento di difesa, se usata correttamente.

4: le reti zero trust

Nessuna entità che si colleghi alla rete o che sia al suo interno può essere considerata attendibile. Questo è il presupposto da cui parte la logica 'zero trust', per andare oltre il tradizionale modello basato sulla sicurezza perimetrale. Attraverso la definizione di perimetri granulari e una strategia di micro-segmentazione è quindi possibile creare policy sicure e monitorare gli accessi alle risorse protette.

5: il lifecycle management

Una rete è sicura solo nella misura in cui sono sicuri i dispositivi a essa connessi: bisogna, quindi, assicurarsi di avere una visione completa dell'intero ecosistema di rete per implementare un corretto lifecycle management dei diversi device e assicurarsi di avere software sempre aggiornati e sicuri. Di grande supporto in questo senso sono software quali Axis Device Manager, che permettono di ottenere informazioni in tempo reale sullo stato dei dispositivi.

La 'catena' della cybersecurity

Dal quadro appena delineato emerge chiaramente come la cybersecurity coinvolga le organizzazioni nella loro interezza e non solo. Si tratta infatti di una responsabilità condivisa di tutti gli stakeholder, dai produttori ai distributori, dai ricercatori agli installatori, fino agli utenti finali. Ciascuno è chiamato a fare la propria parte per garantire che ogni anello della catena della cybersecurity sia il più saldo possibile. In tal senso, svolge un ruolo chiave anche la scelta del giusto partner. Non tutti i fornitori sono uguali, occorre pertanto valutare in modo rigoroso a chi affidarsi; avere la certezza che i propri supplier siano a loro volta concentrati nel ridurre al minimo i rischi di sicurezza offre infatti una garanzia in più.

Fonte: foto Shutterstock

L'intelligenza artificiale (AI) può rappresentare sia una nuova arma di attacco per i cyber-criminali, sia un efficace strumento di difesa

Axis Communications - www.axis.com/it-it