UNIVERSITÀ POLITECNICA DELLE MARCHE

DII Dipartimento di Ingegneria dell'Informazione

unimc

Videosorveglianza IP e Cybersecurity: come prevenire le intrusioni informatiche

Rossella de Gennaro
Dipartimento di Ingegneria dell'Informazione
Università Politecnica delle Marche

Martedì 19 Luglio 2022

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Argomento 1

Videosorveglianza e Sicurezza

Videosorveglianza e sicurezza

I sistemi di videosorveglianza rappresentano oggi gli strumenti attraverso i quali tutelare la propria sicurezza e costituiscono elementi imprescindibili nei progetti di security, di natura privata, aziendale e sociale. Il bisogno di sicurezza, infatti, così come descritto nella piramide di Maslow, è tanto personale quanto sociale, dunque prerogativa nella società del rischio e dell'incertezza. Questa è la motivazione per la quale, in quest'era tecnologica, una delle esigenze per la protezione dei propri beni è dotarsi di un impianto di videosorveglianza, a completamento di un processo di security integrata e partecipata.

A dimostrazione di ciò…

Sono sempre più numerose le richieste di realizzazione ed installazione di un impianto TVCC al livello internazionale:

- in Italia si contano circa 2mln di IPC, una ogni 35 abitanti;
- in Gran Bretagna, leader in Europa con 4mln, una ogni 14 abitanti;
- in Cina, una cam ogni 2 abitanti, per il controllo totale della popolazione e dei centri cittadini.

Cifre sicuramente imponenti, che offrono molti spunti di riflessione…

A cosa è dovuta la diffusione?

L'utilizzo della rete internet nelle telecomunicazioni e i sempre più ridotti costi di implementazione hanno permesso l'affermazione delle telecamere IP, la quale comodità è indiscutibile: per mezzo del web server interno è possibile accedere da remoto al device, visualizzare le immagini in tempo reale e salvarle su dispositivi di archiviazione o piattaforme cloud, le quali sono spesso integrate.

…Ma tali sistemi sono davvero sicuri ed affidabili?

NO!

Non basta installare un impianto di videosorveglianza per garantire maggiore sicurezza, anzi, è proprio con dispositivi di questo tipo che aumenta il rischio di intrusioni e attacchi informatici. Le IPC e i sensori IoT rappresentano un bersaglio a causa delle loro vulnerabilità, quali sistemi *nuovi*, *non protetti* e con tante *porte da cui accedere*, per raccogliere dati sensibili o attaccare la rete. Il problema della sicurezza nasce dunque nel cuore degli apparecchi, che possono avere una falla dalla quale intrufolarsi.

Il ruolo della consapevolezza

Sebbene le aziende investano molte risorse per rafforzare i sistemi di sicurezza passiva ed evitare intrusioni, spesso ignorano che sono proprio le tecnologie connesse ad internet (come, ad esempio, le TC), a rappresentare un punto di accesso alle reti. Infatti, a differenza del passato in cui gli impianti TVCC sfruttavano sistemi a circuito chiuso che conservavano le informazioni per un tempo limitato e non erano connessi a Internet o, al massimo, erano collegati alle sale di controllo per mezzo di reti cablate private, le IPC odierne sono altamente performanti, dotate di *firmware* evoluti, con potenti sensori di immagini digitali. Però, è bene tenere a mente che NON ESISTE un dispositivo immune alle violazioni ed intrusioni!

A tal proposito…

La ***prevenzione*** rimane l'unica via per mitigare il rischio. Ecco perché la sicurezza informatica è fondamentale, così come far capire che i dati raccolti dalle IPC vanno protetti tanto quanto i beni che si vuole tutelare, pertanto gli utenti dovrebbero avere più ***consapevolezza***.

Per la protezione della rete e dei dati è necessario:

- *identificare le* ***vulnerabilità*** *del sistema*: se non si è a conoscenza di possibili debolezze che possono trasformarsi in minacce, non si può prevenirle.
- *Adottare le migliori* ***misure difensive***: una volta identificato un potenziale problema, bisogna intervenire tempestivamente, prima che si trasformi in un danno irreparabile.

Argomento 2

Minacce e vulnerabilità di un sistema TVCC

Scarsa salute informatica e noncuranza dei dispositivi

Quindi, il collegamento degli apparati video in una rete di dati introduce una serie di vulnerabilità e minacce. Le cause sono molteplici**,** ma la maggior parte sono legate ad una ***scarsa salute informatica*** ed alla ***disattenzione nei riguardi del dispositivo***. La manutenzione proattiva è il metodo più efficace per garantire un sistema più stabile e sicuro, nonché avere politiche chiare per la gestione di account, password e dispositivi. I punti deboli sono le telecamere, dalle quali introdursi nei server, nei NAS o nei computer. La videocamera è il «*tallone di Achille del sistema IT*».

Se eventuali vulnerabilità rappresentino o meno un rischio dipende da:

- quanto è alta la ***probabilità*** che una debolezza possa essere facilmente utilizzata;
- l'***impatto*** che il suo sfruttamento potrebbe avere sul resto del sistema.

Le principali vulnerabilità

In molti casi le vulnerabilità sono causa di un mancato allineamento tra il reparto IT ed il team addetto alla sicurezza: gli errori come conseguenza del ***fattore umano*** sono numerosissimi. Senza dimenticare che maggiore è il numero di dispositivi connessi in rete e superiori sono le possibilità che vi siano delle intrusioni.

Le principali vulnerabilità sono:

- la presenza di ***password deboli***: ci sono attacchi in grado di carpire le password di amministratore del dispositivo e vulnerabilità che permettono di reimpostarle;
- l'uso di ***sistemi datati***: permettono di bypassare l'autenticazione dell'utente o sfruttare le *backdoor* che consentono all'intruso di accedere direttamente ai file di configurazione;
- ***falle nei dispositivi***: nella videosorveglianza, permettono di intercettare immagini-video live inviati tramite una rete privata o una connessione Internet. Oltre che il sabotaggio e la manomissione.
- la ***mancata formazione del personale***.

La tempestività dell'intervento

Sfruttando tali criticità, gli hacker potrebbero disabilitare un intero sistema di videosorveglianza posto a sicurezza di un sito di valore, di un'area protetta o persino di un'intera città, come avvenne ad esempio nel 2016 con l'attacco DDoS che ha sfruttato una botnet controllata dal malware Mirai, formata principalmente da telecamere IP prodotte dall'azienda cinese *XiongMai Technologies*, le quali erano state compromesse.

Dunque, se viene rilevata una vulnerabilità, è fondamentale reagire rapidamente. Infatti, le aziende dotate di risorse dedicate risponderanno in maniera più efficace alle minacce di sicurezza informatica, proteggendosi dagli accessi non autorizzati e dalle intrusioni, oltre a risolvere eventuali vulnerabilità applicando le patch di sicurezza.

Argomento 3

Un accenno al GDPR in materia di videosorveglianza

Il principio della security e privacy by design

Prima di illustrare gli accorgimenti da seguire per mitigare gli impatti, si ricorda che il **GDPR** si applica anche ai dati rilevati dalle TC e che non adottare le misure necessarie alla protezione di questi ultimi può portare ad una multa fino 20 milioni di euro. Pertanto, ai sensi del regolamento, qualsiasi amministratore di reti di sicurezza deve fornire informazioni in modo rapido, trasparente e comprensibile in merito ai dati trattati dai sistemi TVCC.

Il GDPR, infatti, evidenzia il concetto di *privacy by design*, poiché è fondamentale che i soggetti interessati siano tutelati, il che significa che le telecamere devono essere *GDPR compliant*, cioè devono rispettare il regolamento sia dal punto di vista giuridico che tecnico e, nel settore della videosorveglianza, ci si riferisce alla cifratura dei dati, alla gestione attenta delle password di accesso etc. Rispettare il principio della *security by design* significa integrare, sin dalle prime fasi di progettazione dei sistemi, misure di difesa informatica nei dispositivi hardware e software, secondo un approccio hardening alla stregua di rigide procedure e policy di monitoring e governance della sicurezza.

Dopo aver individuato le debolezze del sistema e le minacce alle quali sono esposte, è necessario propendere per soluzioni che comprendano la sicurezza informatica sia della rete di videosorveglianza, sia degli stessi dispositivi che la compongono.

Argomento 3

Come mitigare il rischio di un'intrusione informatica

La cybersecurity nella videosorveglianza

Rendere più sicure le reti e meno accessibili i dispositivi può rappresentare un'impresa e, d'altronde, questo non azzera mai il rischio ma, perlomeno, lo riduce e ne minimizza gli impatti. La sicurezza di un impianto TVCC deve dunque riguardare:

- I dispositivi hardware
- Le piattaforme software integrate agli apparecchi
- La crittografia ad alto livello
- Gli accessi al sistema

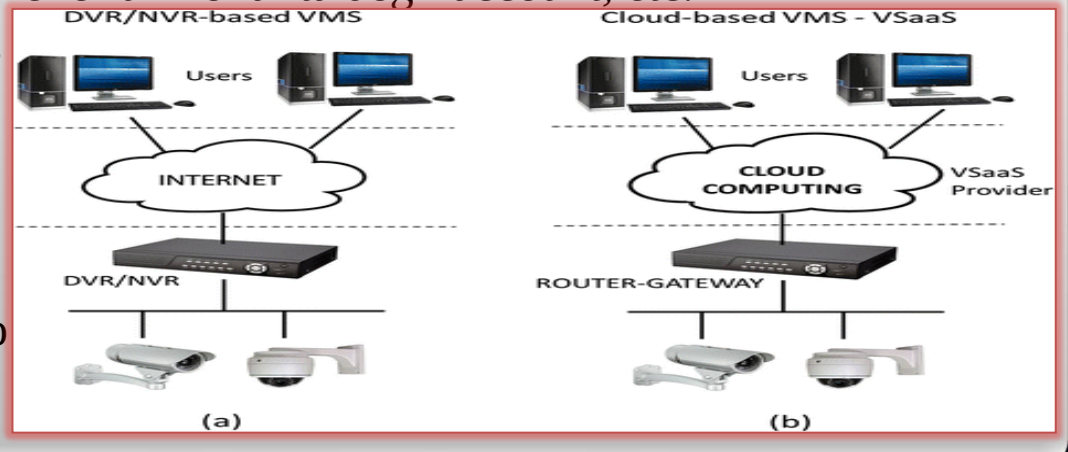
Inoltre…

Anche la scelta dei dispositivi contribuisce a raggiungere una maggiore protezione. Le telecamere con sicurezza integrata prevedono il rilevamento di eventuali vulnerabilità, rilasciando dei log, nonché avvisi di sicurezza nel caso in cui si presentino tali criticità. Sarebbe dunque sbagliato pensare al software integrato nelle videocamere come un semplice programma di controllo, poiché è un'infrastruttura a più livelli.

Le linee guida per una maggiore sicurezza TVCC

Di seguito, una serie di suggerimenti da tenere a mente, da intendersi come best practices per garantire una maggiore sicurezza informatica di un impianto TVCC, nel pieno rispetto del regolamento GDPR:

- Utilizzare ***metodi di autenticazione sicuri*** o ***cambiare periodicamente le credenziali di accesso***;
- ***Aggiornare sempre l'ultima versione del firmware***, per evitare la presenza di malware all'interno di quest'ultimo. Se non si presta attenzione, sfruttando la debolezza del *Network Time Protocol*, un hacker potrebbe mandare in crash un server di rete e prenderne il controllo, lanciando attacchi DDoS o MITM.
- ***Rafforzare i punti deboli*** dei sistemi operativi delle periferiche (modificare le porte HTTP e TCP predefinite, abilitare il protocollo HTTPS/SSL-TLS, etc.) e ***bloccare tutte le porte di comunicazione e i protocolli*** non indispensabili per il funzionamento del sistema.
- ***Inserire un blocco agli accessi***: impedire l'accesso fisico al locale degli apparati TVCC, disattivare l'accesso automatico al software di *video management system* (VMS), limitare le funzionalità degli account, etc.
- ***Posizionare il server del VMS e le telecamere su una rete isolata***, *una DMZ – Demilitarized zone*, tramite isolamento fisico o virtuale: non è raccomandato esporre una telecamera di rete come server Web pubblico, consentendo l'accesso alla stessa da parte di utenti o client sconosciuti. Si consiglia di trasmettere i flussi video delle TC su una rete eth dedicata su base hardware (DVR/NVR) corredato di specifico software (VMS).



I livelli di protezione proposti dal CIS

La tendenza è quindi quella di applicare un concetto "decentralizzato" della sicurezza. Il **CIS** suggerisce di posizionare la rete di videosorveglianza su quattro livelli di sicurezza, a seconda del tipo di infrastruttura da proteggere:

- ***Livello di protezione 0***: predefinito, raccomandato solo per unità demo o test, senza l'esecuzione di procedure standardizzate;
- ***Livello di protezione 1***: basic, per una piccola attività commerciale o ufficio, dove generalmente l'unico operatore è anche l'amministratore di sistema. Sono consigliate le seguenti procedure: installare le telecamere con le impostazioni di fabbrica, con l'ultimo firmware disponibile, impostare una password forte, creare un'utenza di accesso alle telecamere con soli scopi di visualizzazione, etc.;
- ***Livello di protezione 2***: corporate, per aziende medio-grandi che hanno personale specializzato e dedicato alla gestione del sistema. Sono consigliate le seguenti procedure: abilitazione dell'autenticazione DIGEST su protocollo HTTP, creazione di politiche di accesso al dominio e Host Name, disabilitazione dei servizi di rete non utilizzati, utilizzo dei livelli di accesso mediante filtro su indirizzi IP, abilitazione criptazione HTTPS.
- ***Livello di protezione 3***: enterprise, adatto ad una grande azienda con più sedi distribuite, che ha gruppi dedicati. Sono consigliate, oltre alle procedure già descritte, l'autenticazione tramite IEEE 802.1X, monitoraggio tramite SNMP, registro dei log in remoto.

Conclusioni

Riflessioni Conclusive

Le operazioni suggerite sono generalmente valide per ogni ambiente nel quale sono installati impianti TVCC e sistemi di sicurezza, anche se con alcune differenze nell'approccio. I data center, ad esempio, richiedono politiche di gestione molto rigide, mentre le città sottoposte a videosorveglianza devono richiedere una responsabilità condivisa, che coinvolge strutture sia pubbliche, come polizia e prefetture, sia private, come le aziende.

Considerata la diffusione delle IPC, il settore della videosorveglianza deve impegnarsi maggiormente contro le minacce informatiche, per mezzo di tecnologie, competenze e certificazioni. Infatti, l'installazione di un impianto di videosorveglianza sicuro e conforme alle norme, minimizza davvero l'impatto di un'eventuale intrusione nei sistemi, poiché i cyber criminali, così come gli artefici della criminalità comune, sono professionisti che svolgono queste attività per lavoro, pertanto non si arrendono mica dinanzi ad un ostacolo, tantomeno se facilmente eludibile.

Ecco perché è fondamentale la collaborazione nella sicurezza informatica, poiché "*proteggere una rete, i suoi dispositivi e i servizi supportati richiede la partecipazione attiva dell'intera filiera: il costruttore, l'entità che realizza l'impianto (integratore di sistemi) e l'utente finale. Un ambiente sicuro dipende quindi da utenti, processi e tecnologie*".

Bibliografia, articoli e sitografia

- *Quali sono i problemi di cybersecurity nella videosorveglianza?*, a cura di D. Testa, Axis Communication, pubblicato il 31/10/2019, https://www.axis.com/blog/secure-insights-it/2019/10/31/quali-sono-i-problemi-di-cybersecurity-nella-videosorveglianza/

- *La prevenzione dei sistemi di videosorveglianza contro i rischi di cybersecurity,* a cura di F. Quaggia, SEI Sistemi di Sicurezza, pubblicato il 12/04/2019, https://www.sei-sicurezza.it/prevenzione-videosorveglianza-rischi-cybersecurity/

- *Sistemi di videosorveglianza al sicuro con l'approccio Axitea,* Axitea spiega come proteggere in modo efficace i sistemi di videosorveglianza da malware e violazioni della privacy, a cura di M. Bavezzano, Top Trade Informatica, pubblicato il 21/06/2022, https://www.toptrade.it/sicurezza/sistemi-di-videosorveglianza-al-sicuro-con-lapproccio-axitea/

- *Sistemi di sorveglianza e sicurezza*, a cura di C. Gallotti, ICT Security Magazine, pubblicato il 3/04/2019, https://www.ictsecuritymagazine.com/articoli/sistemi-di-sorveglianza-e-sicurezza/

- *Telecamere e sicurezza: connubio possibile?*, a cura di M. Caranti, ICT Security Magazine, pubblicato il 4/03/2019, https://www.ictsecuritymagazine.com/articoli/telecamere-e-sicurezza-connubio-possibile/

Bibliografia, articoli e sitografia

- *Una cassaforte per la Cybersecurity. Una piattaforma informatica di sistema per fare un ulteriore passo verso la Cybersecurity. Integrabile con altri impianti, permette di realizzare sistemi ibridi e sicuri*, a cura di R. Quadri, Elettrico Magazine, pubblicato il 12/04/2021, https://elettricomagazine.it/blog/piattaforma-informatica-cybersecurity/

- *Videosorveglianza IP e cyber security*, a cura della redazione di SecSolution Security Online Magazine, pubblicato il 08/11/2018, https://www.secsolution.com/articolo.asp?id=653

- *Videosorveglianza, tra sicurezza informatica e rispetto della privacy: le soluzioni*, a cura di A. Vasta, Network Digital 360°, pubblicato il 9/01/2019, https://www.cybersecurity360.it/soluzioni-aziendali/videosorveglianza-tra-sicurezza-informatica-e-rispetto-della-privacy-le-soluzioni/

- *MISSION-CRITICAL: I "SEGNALI CHIAVE" DI SICUREZZA INFORMATICA DA RICERCARE NEI PRODUTTORI DI VIDEOSORVEGLIANZA*, a cura di U. Guterman, Hanwha Techwin Europe, https://www.hanwha-security.eu/it/mission-critical-i-segnali-chiave-di-sicurezza-informatica-da-ricercare-nei-fornitori-di-videosorveglianza/

Bibliografia, articoli e sitografia

- *CYBERSECURITY E SISTEMI DI VIDEOSORVEGLIANZA: COME DIFENDERSI?*, a cura della redazione di Electronic'stime, pubblicato il 31/03/2021, https://electronicstime.it/cybersecurity-e-sistemi-di-videosorveglianza-come-difendersi/

- *Cybersecurity, nel mercato mondiale della videosorveglianza, Sunell è il primo marchio ad aver ottenuto la conformità NDAA*, a cura della redazione il Corriere della Sicurezza, pubblicato il 23/12/2021, https://www.ilcorrieredellasicurezza.it/cybersecurity-nel-mercato-mondiale-della-videosorveglianza-sunell-e-il-primo-marchio-ad-aver-ottenuto-la-conformita-ndaa/

- *Cyber security nella videosorveglianza IP - La forza dell'integrazione di WatchGuard e Axis*, a cura della redazione di Elmat Always Beyond, pubblicato il 10/04/2021, https://www.elmat.com/blog/cyber-security-nella-videosorveglianza-ip/

- Gli impianti di videosorveglianza, A. Biasiotti, EPC Editore, pubblicato nel febbraio 2019 a Guidonia (RM).

- La sicurezza nelle organizzazioni aziendali. Un approccio socio-criminologico, M. Tonellotto, 2016.

Grazie per l'attenzione!