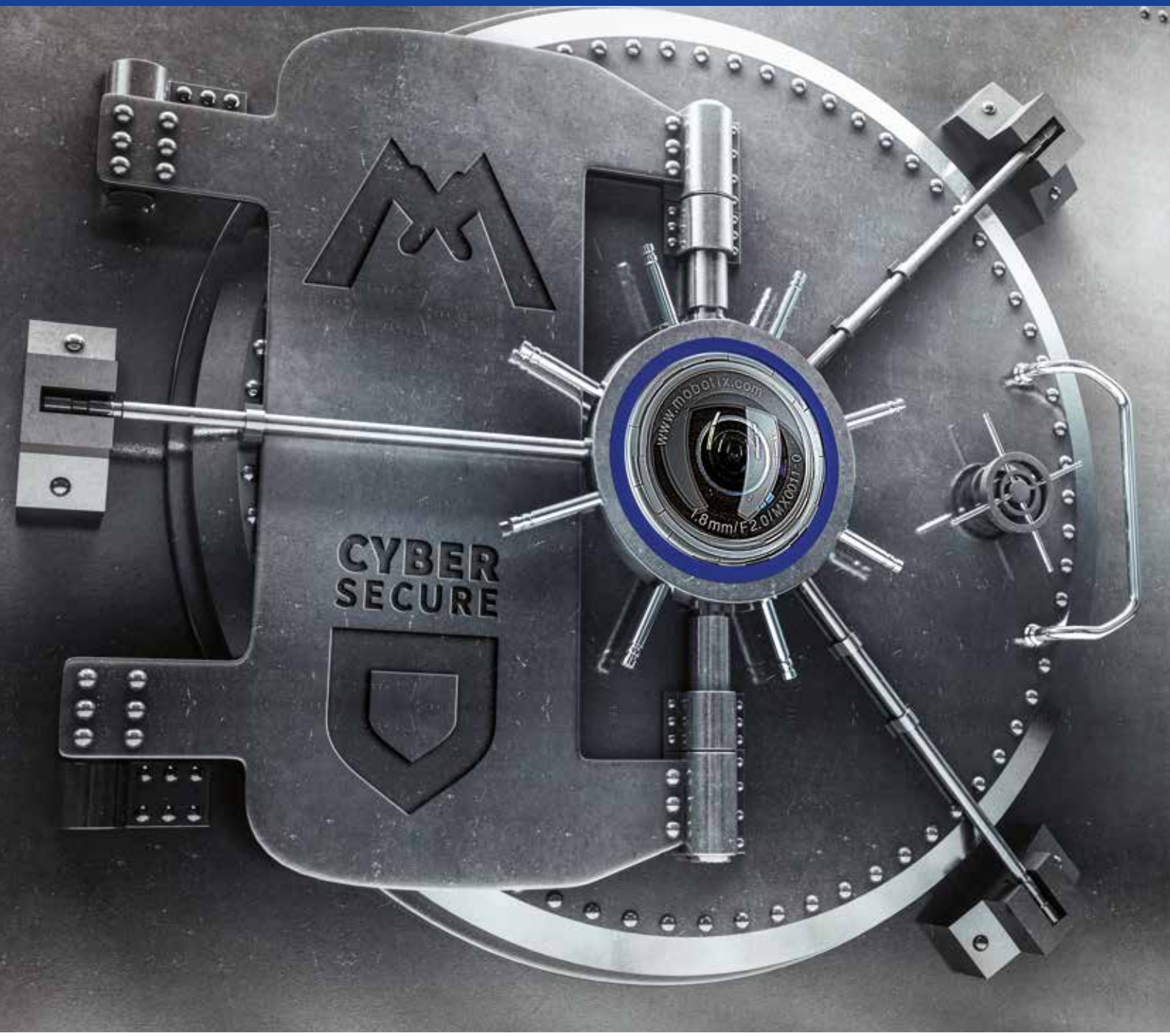
L’importanza della sicurezza informatica nei sistemi di videosorveglianza

White Paper



BeyondHumanVision

MOBOTIX

Introduzione

L'utilizzo di apparecchiature video per scopi di sicurezza, monitoraggio industriale, sanitario e di protezione rappresenta un valore aggiunto per le vite di miliardi di persone ogni giorno. Che si tratti di una famiglia in un centro commerciale protetto dall'occhio di un impianto CCTV, di un sistema video sfruttato da remoto da professionisti per rilevare difetti in una linea di produzione, o di una coppia di genitori che controlla un neonato mentre dorme, la videosorveglianza (remove the extra hyphen) può potenzialmente riguardare il quotidiano di tutti noi.

Quali sono i maggiori fattori di crescita?		
1	Maggiore preoccupazione sulla sicurezza	58%
2	Miglioramenti nell'analisi video	51%
3	Disponibilità di reti IP	50%

L'utilizzo di applicazioni video per molteplici comparti, tra cui quello della videosorveglianza, negli ultimi tempi ha registrato una forte accelerazione anche in funzione degli sviluppi dei settori dell'informazione, comunicazione e tecnologia. Se in passato le immagini video avrebbero richiesto la presenza di un operatore che osservasse la situazione per poterle valutare, oggi queste sono sempre più sfruttate e integrate con altre tecnologie quali sensori - termici, acustici, di movimento - e persino con sistemi che sfruttano intelligenza artificiale, in grado di gestire gli allarmi o di attivare azioni di risposta in maniera completamente automatizzata. I sistemi video sono dunque passati dall'essere semplici mezzi di ricezione passiva a veri e propri scenari tecnologici, in cui una serie di dispositivi di protezione sono in grado di eseguire, in modo completamente autonomo, determinate azioni di intervento sulla base di ciò che viene osservato dal sistema.

Gli ambiti di applicazione sono molteplici: si va dal semplice riconoscimento dei numeri di targa, ai sistemi più performanti, in grado di rilevare sullo schermo anche le minime avarie delle automobili sulla carreggiata. Ma è solo la punta dell'iceberg. Il settore della sicurezza rivolto al commercio al dettaglio è attento a tecnologie all'avanguardia che permettono di andare oltre la semplice videosorveglianza e di offrire ulteriore valore aggiunto alle singole attività, come ad esempio il conteggio delle persone e l'analisi dei modelli di acquisto. I benefici in questo caso arrivano perfino all'ottimizzazione della disposizione della merce all'interno del negozio e della progettazione di nuovi centri commerciali.

La richiesta è in forte e costante aumento e Cisco stima che i video per i soli scopi commerciali e di intrattenimento ingloberanno addirittura il 79% del traffico Internet entro il 2020 [1]. In questo contesto di riferimento è sicuramente necessario considerare che la creazione di video oggi è molto più semplice rispetto al passato - avvantaggiandosi di telecamere più piccole, più convenienti e con minori consumi – e che il trasferimento dal dispositivo sorgente a quello di destinazione può sfruttare connessioni Internet e reti mobili sempre più veloci.

Se però, da un lato, le riprese video - e, in particolare la videosorveglianza - vengono in gran parte considerati un vantaggio per la società perché riescono a garantire un numero inferiore di atti criminali e, dunque, ambienti più sicuri, dall'altro aumenta proporzionalmente anche il livello di esposizione agli attacchi di criminali, terroristi e informatici.

Il rischio di una videosorveglianza non sicura e dei dispositivi IoT

Gli attacchi alle reti di videosorveglianza in passato erano fenomeni rari perché si sfruttavano sistemi chiusi, spesso collegati direttamente alle sale di controllo locali tramite reti private cablate, e telecamere dotate di un collegamento diretto e di firmware semplici che permettevano unicamente di inviare video tramite un cavo coassiale, generando un potenziale di attacco molto ridotto. Oggi il panorama di riferimento è totalmente cambiato e le telecamere moderne sono diventate veri e propri computer, altamente performanti, dotate di firmware collegati a un sensore immagini digitale. Ma la complessità e la natura variabile dei processi, dei protocolli e dei meccanismi di autenticazione implicano anche una maggiore vulnerabilità dei sistemi di videosorveglianza che, con l'avvento di Internet, delle reti IP e di telecamere più a buon mercato, è aumentata a dismisura e finalizzata a carpire informazioni preziose sugli strumenti di acquisto o, ancora più grave, dati sensibili dei singoli.

La questione non è nuova. Per oltre un decennio, i ricercatori nell'ambito della sicurezza[2] hanno rilevato vulnerabilità nelle telecamere, coinvolgendo sia i maggiori vendor internazionali che i minori brand locali, stilando un elenco crescente di criticità, tra cui:

- Attacchi in grado di carpire le password di amministratore del dispositivo oltrepassando i controlli di sicurezza come l'account utente predefinito
- Vulnerabilità sulla sicurezza che consentono di bypassare l'autenticazione dell'utente per mezzo di credenziali complesse da decodificare e posizionati come "backdoor" nel dispositivo dal produttore
- L'esecuzione di un codice arbitrario nel dispositivo senza autenticazione sfruttando le vulnerabilità presenti nel pacchetto del protocollo Real Time Streaming Protocol
- Vulnerabilità sulla sicurezza che permettono di bypassare la fase di autenticazione e consentono all'aggressore di accedere direttamente ai file di configurazione
- Vulnerabilità che permettono all'aggressore di reimpostare la password del dispositivo portando quindi alla modifica non autorizzata dei file di configurazione per avere accesso alle funzioni principali della telecamera
- Attacchi alle telecamere che consentono a parti esterne di carpire stream video live inviati tramite una rete privata o una connessione Internet

Molti di questi problemi, che interessano numerosi brand minori che ricorrono alla tecnologia coperta da licenza di fornitori leader di mercato, hanno causato instabilità in milioni di dispositivi. Nonostante i fornitori più noti abbiano spesso lanciato patch per correggere le problematiche di volta in volta insorte, molte piccole realtà hanno semplicemente ignorato il problema. C'è scarsa conoscenza della materia: anche nel caso in cui sia disponibile una copertura sicura, a titolo preventivo, si tratta di aggiornamenti da eseguire con processi manuali e molti proprietari di piattaforme di videosorveglianza ne sono addirittura all'oscuro. La questione riguarda, non da meno, gli utenti domestici perché i sistemi di

videosorveglianza di molti consumatori, pur acquistati presso un rivenditore autorizzato, sono per la maggior parte esenti da patch.

Attacchi mirati e reti informatiche

Sebbene possa sembrare la trama di un film di Hollywood, la capacità di disabilitare sistematicamente un intero sistema di videosorveglianza destinato alla protezione di un sito di valore, un'area o persino una città non è un'opera considerata impossibile. Dal momento che molti fornitori di sistemi di videosorveglianza riutilizzano le stesse librerie software per gestire elementi come lo streaming, l'autenticazione e il trasferimento dei video su supporti di archiviazione, gli abili avversari sfruttano vulnerabilità note per generare attacchi informatici di tipo criminale, ma anche come mezzo per innescare terrore e panico.

Un altro aspetto riguarda la rete, che i potenziali aggressori riescono a eludere insinuandosi all'interno di un dispositivo ad essa connesso, ad esempio una telecamera, per poi sfruttare quella posizione autenticata per accedere a ulteriori risorse connesse alla stessa rete. Se da un lato le telecamere e altri dispositivi connessi all'Internet delle Cose (Internet of Things - IoT) iniziano dunque ad acquisire rilevanza ed essere integrati nei processi chiave, dall'altro rimane fondamentale l'esigenza di garantire che l'accesso ai dispositivi IoT non comporti maggiori rischi. Pur non rappresentando l'unico problema da prendere in considerazione, negli ultimi tempi sono state proprio le telecamere ad essere sfruttate come una vera e propria arma per innescare attacchi DDoS da un numero di sorgenti diverse.

L'attacco DDoS di dimensioni impressionante che nell'ottobre 2016 ha interessato Twitter, Amazon, Tumblr, Reddit, Spotify e Netflix è stato generato in parte dal botnet basato su Mirai. Come dichiara l'esperto di sicurezza Allison Nixon, Direttore area ricerche presso Flashpoint, il botnet è formato principalmente dai videoregistratori digitali (DVR) e dalle telecamere IP prodotte da XiongMai Technologies, un'azienda cinese tecnologicamente all'avanguardia. I componenti che XiongMai produce sono venduti ai fornitori che li usano nei propri prodotti, causando decine di migliaia di cooptati all'interno di queste pericolose armi cibernetiche.[3]

Il governo, i regolatori e la legge

L'esplosione dei dispositivi connessi a Internet, stimata da Gartner, Cisco e altri, ammonterà tra i 25 e i 50 miliardi [4] di oggetti entro il 2020, innescando una serie di problematiche per i governi nazionali e gli altri organismi regolatori internazionali. Diversamente dalle emittenti radio, le stazioni TV o i veicoli a motore, la legislazione in materia di ciò che può essere connesso a Internet è quasi assente. Non sono presenti standard obbligatori circa il grado di sicurezza che deve possedere un oggetto. Cosa accadrebbe se un dispositivo venisse hackerato o usato per attaccare una parte esterna? La legislazione penale, nella maggior parte delle regioni, può far fronte ai crimini informatici in cui compaiono aggressore e vittima. Tuttavia, mentre la tecnologia aumenta il proprio livello di automazione, il rischio che i dispositivi non sicuri attraggano i virus in forma pandemica, come era successo per gli utenti dei PC desktop, potrebbe iniziare a ricomparire, ad esempio nelle reti delle telecamere di videosorveglianza: in questi casi le modalità per rilevare o arginare rapidamente il problema sono ridotte.

Una questione di responsabilità economica, non solo criminale

C'è da tenere in considerazione anche la spinosa questione della responsabilità. L'installazione di sistemi di videosorveglianza può portare a una riduzione dei costi assicurativi incrementando la probabilità di cattura dei criminali. Tuttavia, nel caso in cui un sistema di videosorveglianza diventi non operativo a causa di un difetto nel sistema di sicurezza e in quel momento venga commesso un crimine non ripreso dalla telecamera, l'assicurazione potrebbe rifiutarsi di saldare il premio per non aver ottemperato ai parametri del rilevamento video richiesti. In questo caso la vittima può fare causa al produttore della telecamera? Al fornitore di un qualsiasi contratto di assistenza CCTV? Oppure, nel caso di un evento di pubblica sicurezza, è responsabilità dell'organismo di governo locale? La casistica legata all'impatto che un varco nel sistema di sicurezza potrebbe avere è davvero molteplice e questo fa sì che vi sia un'elevata incertezza nel mercato in termini di test e di risposte preventive.

Le problematiche legate alla privacy

Nonostante le questioni riguardanti la responsabilità economica e criminale che ruotano intorno all'hackeraggio dei dispositivi di videosorveglianza siano ancora in fase di dibattito, le leggi che tutelano la privacy dei cittadini si sono già evolute di conseguenza nella maggior parte dei Paesi industrializzati. Fatta salva qualche piccola differenziazione legata al caso specifico, in linea generale tutti i dati personali di natura privata pertinenti alle aree sanità, finanza, orientamento sessuale, affiliazione politica, insieme ad una serie di altri criteri, devono essere raccolti e archiviati con una modalità definibile "sicura". Questo riguarda anche i dati video. I pazienti di una clinica sanitaria per problemi psichiatrici o un individuo che partecipa a una manifestazione politica devono avere la garanzia che qualsiasi filmato di videosorveglianza riferito a quel contesto sia conservato al sicuro e lontano dal pubblico dominio. Nel caso di un attacco informatico contro un dispositivo o una rete di videosorveglianza, c'è un rischio molto elevato che le informazioni personali come immagini e altri dati sensibili legati a persone specifiche possano essere rubati e poi utilizzati senza autorizzazione, il che violerebbe il diritto alla privacy degli utenti monitorati dal sistema e potrebbe celare conseguenze legali per la persona considerata responsabile del trattamento dei dati.

La posizione dei governi

I governi in tutto il mondo si stanno muovendo per cercare la massima chiarezza in tema di sicurezza per dispositivi IoT. In Europa, alcune figure di primo piano della Commissione Europea stanno ipotizzando la creazione di un processo di certificazione per i dispositivi connessi all'"Internet delle Cose" (Internet of Things, IoT) finalizzato a garantire la protezione degli utenti. La Commissione ha già istituito l'Alliance for Internet of Things Innovation, composto da numerosi leader tecnologici nei settori energia, automotive e assistenza sanitaria e volto alla creazione di una serie di linee guida che dovranno essere adottate a livello strategico. Muovendosi sullo stesso fronte, negli USA, il Department of Homeland Security (dipartimento per la sicurezza interna) ha realizzato una guida relativa ai principi strategici per la sicurezza dell'Internet delle Cose (Strategic Principles for Securing the Internet of Things)[5]. Tra i molti concetti approfonditi, viene evidenziata la necessità di coinvolgere il tema della sicurezza già in fase di progettazione dei sistemi, il monito a eseguire con costanza gli aggiornamenti per la sicurezza nel caso specifico e il controllo delle apparecchiature in termini di loro potenziale di vulnerabilità e al conseguente impatto potenziale. Si tratta di interventi specifici, non siamo ancora di fronte a un consenso globale sia a livello amministrativo che a livello economico-finanziario, come per gli standard PCI-DSS previsti nel settore del credito. Di conseguenza, la sicurezza dei dispositivi IoT, ora come ora, si basa su un orientamento diverso da Paese a Paese e su una regolamentazione ancora troppo esigua che varia enormemente in termini di impatto ed efficacia.

In che modo MOBOTIX sta affrontando queste sfide?

In qualità di leader nel settore della videosorveglianza, MOBOTIX ricopre un ruolo a sé stante poiché sviluppa "in proprio" tutti i propri software. Questo ci permette non solo di differenziarci offrendo al mercato prodotti ad altissima tecnologia, ma garantisce un vantaggio considerevole in materia di sicurezza. Controllando direttamente lo sviluppo della componente software, MOBOTIX è meno vulnerabile agli attacchi rispetto a componenti (software e hardware) esterni. Nelle aree in cui utilizziamo gli standard di settore ampiamente supportati come l'ONVIF, disponiamo di policy in grado di emettere immediatamente qualsiasi patch richiesta non appena disponibile. Utilizzando lo stesso software per tutti i modelli di telecamere MOBOTIX, garantiamo poi che il firmware della telecamera sia aggiornato e sicuro, agevolando in questo modo anche la clientela internazionale.

La nostra filosofia aziendale si basa da sempre sulla progettazione finalizzata alla sicurezza, e questo appare evidente sotto molti punti di vista:

Sistemi operativi e aggiornamenti sicuri

Il concetto di sicurezza MOBOTIX inizia all'interno della fase di progettazione, che interessa sia il sistema operativo che lo stock applicativo. Tutti i dispositivi MOBOTIX si basano su un sistema operativo Linux modificato e sicuro che rimuove servizi e moduli standard. I moduli Linux critici come l'autenticazione sono stati completamente riprogettati dagli esperti MOBOTIX per garantire che non siano vulnerabili per difetti legati allo standard o per tecniche di aggressione tramite inserimento di codice potenzialmente pericoloso. Questo sistema operativo non è open source ed è protetto da misure di sicurezza supplementari. Ogni aggiornamento del firmware del dispositivo e degli elementi software, inoltre, è criptato e dotato di firma digitale per impedire manomissioni.

Configurazione sicura della telecamera

L'accesso all'interfaccia di configurazione della telecamera viene concesso solo agli utenti autorizzati. Per garantire la sicurezza interna, ciascun sistema consente la creazione e l'implementazione di autorizzazioni per gruppi di utenti diversi. In pratica, questo significa che le telecamere MOBOTIX non memorizzano mai le password utente con testo in chiaro, bensì vengono crittografate con un potente algoritmo di hashing unidirezionale (SHA-512) così che se il file di configurazione dovesse finire in mani sbagliate, risulterebbe estremamente difficile recuperare la password in chiaro. I servizi Linux OS non essenziali vengono disabilitati per limitare potenziali vulnerabilità e prevenire attacchi, inoltre non è presente alcun servizio telnet/SSH o "master password" non documentata: è possibile accedere e configurare una telecamera MOBOTIX tramite la propria interfaccia web . Le password possono essere conservate all'interno di sistemi di gestione con accesso privilegiato come BeyondTrust e CyberArk, protetti da un più rigido doppio fattore di autenticazione.

Rete sicura e comunicazioni tra i dispositivi

Tutti i dati scambiati tra le telecamere MOBOTIX e gli altri host nella rete possono essere criptati per garantire la riservatezza e l'integrità dei dati. Il protocollo HTTPS (SSL/TLS) ed i certificati sono supportati come standard per soddisfare le linee guida previste dalle maggiori strutture di sicurezza degli esperti come il SANS Institute. MOBOTIX inoltre include il supporto integrato per la gestione dei certificati unici X.509 in ciascuna telecamera e delle Root Certificate Authorities per consentire alle imprese di ampliare la sicurezza dei dispositivi includendo telecamere e videocitofoni autenticati tramite sistemi come OpenVPN. Questo significa che qualora una telecamera venga effettivamente rubata o hackerata, l'aggressore non potrà usare le credenziali in una telecamera compromessa per attaccare la rete residua di telecamere.

Registrazione interna sicura e anti-manomissione

Tutte le registrazioni create dalla telecamera possono essere criptate prima dell'archiviazione, partendo dal buffer ciclico che utilizza la scheda SD integrata in ciascuna telecamera. MOBOTIX ha realizzato un file system sicuro nell'ipotesi che una telecamera venga effettivamente rubata o hackerata: i video precedentemente registrati ancora presenti nella telecamera non potranno essere recuperati senza prima ottenere i diritti di amministratore protetti tramite i processi di configurazione sicura descritti precedentemente. Ciascuna immagine generata da una telecamera MOBOTIX può essere dotata di firma digitale e certificati personalizzati per prevenire manomissioni. Questo garantisce l'ammissibilità delle registrazioni qualora vengano esibite come prova in giudizio.

Funzioni di sicurezza	Telecamere IP standard	MOBOTIX
HTTPS (SSL/TLS) e certificati	✓	✓
Autenticazione digest per HTTP	✓	✓
Elenchi di controllo degli accessi	✓	✓
Utenti e gruppi con diritti personalizzati	⚠	✓
Intrusion Detection	✗	✓
Protezione anti-bot	✗	✓
Registrazioni criptate	✗	✓
Video e messaggi criptati	✗	✓
Client VPN	✗	✓

Intrusion Detection

Persino con svariati sistemi di sicurezza e i processi in esecuzione, sarebbe avventato ipotizzare che gli aggressori non tenteranno di accedere alle telecamere MOBOTIX. Questo è il motivo per cui MOBOTIX ha investito in misure aggiuntive per poter rilevare questi tentativi. Implementando una serie di elementi per il rilevamento delle intrusioni, ciascuna telecamera o videocitofono segnalerà, utilizzando un canale criptato, qualsiasi tentativo di login non autorizzato o attacchi di forza bruta. Inoltre le modifiche possono essere inviate nel caso di tentativi di login ripetuti e falliti, e l'indirizzo IP del trasgressore può essere bloccato automaticamente.

Riepilogo

L'incremento dei sistemi di videosorveglianza in termini di popolarità e come parte di altri processi sanitari, protettivi e industriali non mostra segni di rallentamento. Mentre tali elementi cominciano ad acquisire maggiore vitalità, i processi aggiuntivi come il controllo degli accessi, il monitoraggio ambientale e i processi analitici, come il riconoscimento facciale, diventeranno sempre più l'obiettivo degli attacchi informatici.

I progettisti dei sistemi di videosorveglianza insieme agli operatori per l'assistenza e persino gli organismi di regolamentazione dovranno incrementare il controllo sulla sicurezza sia sotto il profilo di un obbligo di assistenza al pubblico che per soddisfare gli obblighi legislativi futuri. Il settore industriale e i suoi leader, come MOBOTIX e altri, hanno preso in carico questi problemi e stanno lavorando alacremente per integrare la sicurezza nei dispositivi hardware e software fin dalle primissime fasi di progettazione.

Tuttavia la protezione dei dispositivi vale tanto quanto la protezione dell'ambiente complessivo. Chiudere una porta è inutile se si lascia aperta una finestra. In quest'ottica, i progettisti e gli operatori della videosorveglianza e delle reti IoT più ampie devono valutare anche altri fattori, come la rete sottostante, l'infrastruttura di archiviazione e soprattutto l'elemento umano, spesso un anello debole della catena. Numerosi gruppi industriali come il SANS Institute hanno realizzato linee guida preziose come i Critical Security Controls ad opera del Centre for Internet Security (CIS) che forniscono una serie di azioni consigliate per la difesa informatica oltre a modalità specifiche e attuabili per arrestare la maggior parte degli attacchi invasivi e pericolosi di oggi.[6]

Guardando al futuro, è evidente che la sicurezza dei dispositivi e delle piattaforme diventerà un fattore chiave nei più importanti progetti video. Mentre la formazione che riguarda le sfide dell'IoT si estende sempre più, MOBOTIX mira a collaborare con le aziende del settore, i clienti e gli organismi di governo per proteggere i dispositivi tecnologici e i sistemi che rendono la società più sicura per tutti.

Referenze

https://www.coresecurity.com/system/files/publications/2016/05/corelabs-ipcams-research-falcon-riva.pdf

https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Fonti

[1]https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.

[2]html https://www.coresecurity.com/advisories/hikvision-ip-cameras-multiple-vulnerabilities

[3]https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

[4]http://www.telecomtv.com/articles/iot/internet-of-things-to-reach-25-billion-devices-within-five-years-11931/

[5]https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

[6]https://uk.sans.org/critical-security-controls

Dal 2000 MOBOTIX sviluppa e produce in Germania sistemi video IP, sistemi di gestione video e software di analisi.

L'azienda si contraddistingue per il suo grado elevato di affidabilità. Tutte le telecamere per ambienti esterni sono sottoposte a stress test per temperature comprese tra i -30 °C e +60 °C. Prive di componenti aggiuntivi, impianti di riscaldamento o raffreddamento o parti mobili (senza auto-iris), queste telecamere non richiedono quasi nessuna manutenzione.

MOBOTIX fornisce un pacchetto perfettamente compatibile, dalla scheda MicroSD con gestione archiviazione, audio HD (microfono e altoparlante) con telefonia VoiP, all'analisi video, al software per il rilevamento del movimento senza falsi allarmi, fino al sistema di gestione video professionale.

Grazie all'architettura decentralizzata, non è necessario disporre di un computer centrale, quindi il carico sulla rete si riduce al minimo. Le telecamere intelligenti di MOBOTIX elaborano e archiviano autonomamente i dati delle immagini, attivano eventi e, in caso di accesso remoto, adeguano anche il frame rate e la risoluzione in base alla larghezza di banda a disposizione.

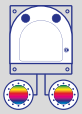
I sensori Moonlight da 6MP, integrati dalla tecnologia a immagini termiche, permettono di rilevare gli oggetti in movimento perfino in condizioni di scarsa illuminazione e a grandi distanze. In questo modo, è possibile coprire zone estese con poche telecamere. È necessaria una quantità inferiore di cablaggi, infrastrutture IT e fonti luminose supplementari. Le telecamere MOBOTIX sono alimentate tramite PoE standard e consumano al massimo 4-5 Watt.

Un sistema completo video IP intelligente di MOBOTIX permette di ridurre i costi totali. L'investimento viene ammortizzato in breve tempo e, grazie agli aggiornamenti software disponibili gratuitamente, è decisamente orientato al futuro.

Doppia ottica per ambienti esterni

M16 AllroundDual	S16 FlexMount	D16 DualDome
		
Robusta per condizioni estreme	Telecamera a doppia ottica flessibile	Telecamera a doppia ottica modulare

Termiche

M16 Thermal	S16 DualThermal
	
Termica a doppia ottica	Termica a doppia ottica

Mono-ottica per ambienti esterni

M26 Allround	S26 FlexMount	Q26 Hemispheric	D26 Dome
			
Robusta per condizioni estreme	Discreta, analisi video	Discreta, analisi video	Modulare a cupola fissa

Per ambienti interni

i26 Panorama	c26 Hemispheric	p26 Allround	v26 MiniDome
			
Emisferica 180°	Discreta, analisi video	Telecamera a soffitto modulare	Telecamera antivandalismo

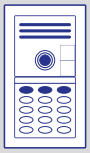
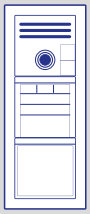
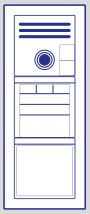
Moduli porta

Telecamera	BellRFID	Keypad
		

MxDisplay+

Terminale


Set porta

Telaio doppio		Telaio triplo	
			

IT_11/17

MOBOTIX AG
Kaiserstrasse
D-67722 Langmeil
Tel.: +49 6302 9816-103
Fax: +49 6302 9816-190
sales@mobotix.com
www.mobotix.com

MOBOTIX