La Redazione

Phygital security: quale protezione contro gli attacchi informatici?

Non più solo physical e certamente molto digital: la security come la conoscevamo una volta è da tempo diventata "Phygital", con tutto ciò che il digitale porta con sé - a partire dal rischio di hacking. Sono diverse le strategie messe in campo dai produttori del comparto sicurezza per contenere la minaccia di attacchi cyber ai dispositivi posti in commercio, ma è evidente che per mitigare un rischio per sua natura dinamico, variabile e in continuo aggiornamento occorre un "patto di filiera" tra produttori, integratori ed utilizzatori finali che permetta di immaginare una catena di responsabilità trasparenti e condivise. Le stesse certificazioni non possono assicurare che un prodotto sia cyber security-proof, perché nell'eterna lotta tra guardie e ladri è destino che vinca il ladro (che di mestiere fa solo quello e ci pensa 24/365). Magari sarebbe utile che un ente indipendente fungesse da riferimento per l'intero comparto per definire ciò che può essere considerato "accettabilmente sicuro". Senza dubbio è essenziale (e non così scontato) mantenere aggiornati gli apparati, magari in una logica di automazione come è prassi per PC, tablet e smartphone. Su questi ed altri temi abbiamo interrogato il mercato, concentrandoci su quattro domande-chiave.

Dite la vostra

le domande

1. Quali misure ponete in essere "by design" per garantire la sicurezza cyber dei vostri prodotti?

2. Quali misure procedurali/formative ponete in essere per istruire il canale (e tramite il canale, la stessa utenza finale) alla sicurezza cyber dei vostri prodotti?

3. Se lasciato alla sola iniziativa dell'utente finale, non solo il cambio della password di default, ma anche l'aggiornamento dei firmware può non essere operato in maniera diligente, e quindi esporre i dispositivi a rischi di violazioni. Sarebbe utile prevedere degli aggiornamenti a cadenze "obbligate" (modello PC o smartphone)?

4. Ogni produttore vanta le proprie certificazioni: per armonizzare le valutazioni ed elevare la sicurezza cyber (dunque la credibilità) dell'intero comparto, sarebbe utile definire un ente di certificazione unitario cui l'intera industry mondiale possa fare riferimento?

Dite la vostra

Andrea Monteleone

National Sales Manager - Axis Communications

1 L'Azienda ha già da tempo introdotto tutta una serie di metodologie e prassi per mitigare quanto più possibile i rischi correlati alla cyber security, non solo nelle modalità con cui firmware e software sono sviluppati e testati per rispondere ai più alti standard di qualità e sicurezza, ma anche nella gestione e protezione della supply-chain in tutte le sue fasi: dall'approvvigionamento dei componenti alla delivery del prodotto.

2 Storicamente Axis ha sempre investito molto sulla educazione e formazione di Partner e Clienti finali. A tal proposito, il nostro impegno per contribuire a rendere sempre più consapevole il mercato non è destinato a diminuire, anzi. L'impegno è, principalmente, orientato a supportare tutti gli stakeholder nella fase di progettazione e implementazione dei sistemi di sicurezza, oltre che nella gestione di eventuali incidenti nel modo più proattivo e trasparente possibile.

3 Il tema è molto dibattuto e non esiste una risposta univoca e risolutiva. Più che imporre un aggiornamento obbligatorio o cadenzato – pratica che in certi ambienti potrebbe addirittura risultare controproducente o addirittura impossibile da applicare – sarei più propenso a proporre strategie condivise per mantenere sempre al massimo livello ammissibile il livello di sicurezza di un qualsiasi sistema ICT.

4 Lo spunto di riflessione è già stato recepito dalla Comunità Europea e, in certi settori, si va proprio in questa direzione. Il tema è quello di stabilire i criteri di verifica, che sono ancora lontani dall'essere ben definiti.

Il tema vero è: come stabilire i criteri di verifica della sicurezza informatica? Chi lo deve fare? Da chi deve essere accreditato?

Per leggere le interviste integrali ai player di mercato sul tema cyber security

Giampiero Miceli

Direttore Commerciale - Bettini

1 La sicurezza informatica dei dispositivi si basa sia su caratteristiche dei prodotti stessi (cifratura dei dati, profilazione accessi, mancanza di password di default, possibilità di disabilitare servizi non utilizzati), sia su procedure di controllo atte a garantire che l'intero pacchetto FW sia sempre allineato con le soluzioni delle vulnerabilità più recentemente individuate e risolte. Penetration test interni sono eseguiti frequentemente, in un processo consolidato che si completa con il rilascio di un aggiornamento e la sua pubblicazione sui nostri canali.

2 Con la pandemia Covid abbiamo adottato un nuovo modo di diffondere la cultura aziendale, abituandoci ad interagire attraverso strumenti digitali (webinar e meeting online). Formazione e informazione online per noi sono oggi validi canali comunicativi. Questi incontri trattano temi che spaziano dagli aspetti normativi a quelli tecnici, formativi e commerciali e si rivolgono a tutti coloro che appartengono al mercato della sicurezza: installatori, progettisti e vigilanze fino agli utenti finali.

3 Firmware e software degli apparati GAMS sono sviluppati in Italia e, da sempre, rilasciamo aggiornamenti periodici. Questo metodo consente ai clienti di essere informati sulle novità e di trasferirle agli utenti finali, affinché apprezzino l'attenzione che poniamo all'aggiornamento normativo e tecnico dei nostri dispositivi.

4 Crediamo che sia necessario avere regole e procedure certe. Il fai da te, pur essendo encomiabile, spesso nasce dall'impegno del singolo e non da processi normati a beneficio del mercato.

Stefano Riboli

Marketing Manager Security - Bosch Security Systems

1 Implementiamo diverse misure di sicurezza by design nelle telecamere IP, tra le quali: a) il firmware crittografato contiene il signing; b) il firewall integrato (in caso di errori di inserimento password, la modalità "autoriparante" fa continuare i soggetti autorizzati); c) il chip Trusted Platform Module (TPM) all'interno della telecamera protegge le chiavi e i dati più segreti; d) porte e servizi non necessari sono disabilitati; d) l'installatore può abilitare un sigillo alla configurazione che, in caso di modifiche alle impostazioni della telecamera, la stessa può notificare.

2 La piattaforma Bosch Security Academy prevede, per la data security, diversi corsi online e in aula con relatore ed esame finale. Durante i corsi, per mezzo del tool di configurazione, è possibile verificare il livello di vulnerabilità della telecamera IP.

3 L'aggiornamento di FW e SW sono solo una delle misure da mettere in atto e dovrebbero essere previsti durante la manutenzione. Un altro tema è la valutazione da parte del produttore del rilascio degli aggiornamenti a seguito della fine di produzione del prodotto. Per Bosch si parla di 5 anni di manutenzione del FW, considerata come una garanzia firmware estesa delle telecamere IP. Per queste attività, in base al rischio, bisognerebbe periodicamente valutare le vulnerabilità e fare test di penetrazione.

4 Un ente certificatore potrebbe essere un'ulteriore garanzia per la clientela, ma è fondamentale che il produttore testi i prodotti facendo riferimento a tutti gli standard di mercato. Nei datasheet dei prodotti, Bosch dichiara le normative di riferimento utilizzate e mette a disposizione un team di esperti PSIRT (Bosch Product Security Incident Response Team) come punto di contatto centrale per ricercatori esterni per la sicurezza, partner e clienti per segnalare informazioni sulla sicurezza relative ai prodotti. La divulgazione responsabile delle vulnerabilità consente di correggerle, informare i clienti sulle correzioni e migliorare continuamente la sicurezza dei prodotti.

Walter Pizzen
Electronic Division Director – CBC Europe

1 Da anni GANZ ha rimosso e bloccato i servizi P2P in tutte le telecamere che vengono sviluppate con firmware chiusi e stabili, testati ed approvati nei nostri uffici europei. I nostri videoregistratori vengono forniti con funzioni P2P e DDNS disabilitati.

2 La password deve essere impostata al primo avvio ed i servizi di sicurezza sono tutti abilitati di default. Sono i clienti a dover scegliere che grado di sicurezza adottare, in base alla sensibilità dell'impianto, disabilitando le protezioni e non viceversa. Capiamo la comodità di assicurarsi prodotti plug&play ma, da tempo, abbiamo scelto di non servire quel mercato che preferisce effettuare configurazioni rapide, a scapito della sicurezza dei dati.

3 Spinti da un servizio della televisione di stato, oggi non si parla d'altro che di cybersecurity. Siamo sicuri che vogliamo rendere i nostri prodotti vulnerabili esponendoli, ad esempio, ad aggiornamenti automatici, soltanto per seguire la corrente del momento? Per noi la sicurezza dei dati deve essere la priorità e gli impianti devono essere manutenuti da operatori professionali. Vendiamo sicurezza e non smartphone! Viviamo in un paese in cui si chiudono i recinti dopo che il bestiame è scappato e, per tamponare, vorremmo inserire burocrazia invece che risolvere i problemi.

4 Ritengo che il nostro settore abbia già gli strumenti per affrontare questo tipo di problematica, ma la scelta sia stata quella di "voltarsi dall'altra parte". Non credo che possa servire aggiungere un nuovo organismo, mentre far rispettare le regole già esistenti sì! Potrebbe essere una bella novità…

Daniele Sisinio
Director - Dallmeier Italia

1 Il "Made in Germany" ci impone un livello molto alto di sicurezza sia nello sviluppo sia nella produzione dei prodotti per garantire, in ogni fase del processo (sviluppo, programmazione, produzione, penetration test esterni, ecc.), che vengano prese in considerazione le più elevate esigenze degli standard internazionali (ad es. EU GDPR) e dei clienti. Disponiamo di uno dei più grandi portafogli di precauzioni: dalla crittografia end-to-end secondo gli standard più elevati alle tecniche di security gateway, ai sistemi anti-hacking e alle corrispondenti tecnologie di autenticazione (IEEE 802.1X).

2 Sempre più spesso la documentazione di "Security and Privacy by Design" è tra le prime richieste dei clienti. Noi offriamo una documentazione completa, guide alle migliori pratiche e linee guida di implementazione che vanno ben oltre le semplici funzionalità e forniscono un punto di vista olistico prima dell'implementazione.

3 Abbiamo già implementato queste linee guida. Quando gli utenti avviano una telecamera Dallmeier, sono costretti a creare la password e ID nel rispetto di rigorose sintassi di sicurezza. All'interno della nostra piattaforma software HEMISPHERE®, l'amministratore può impostare politiche di password individuali come la modifica forzata della password dopo un certo intervallo di tempo, rispettivamente, consentiamo la completa integrazione AD.

4 Alcune certificazioni vanno già in questo senso, come LGC Forensic, ma potrebbe essere utile disporre di ulteriori istituzioni di certificazione indipendenti dal fornitore. Soprattutto per prevenire abusi, come vediamo con presunte "certificazioni GDPR", che non sono in alcun modo certificati ufficiali, dal momento che le condizioni quadro per le certificazioni GDRP non sono state nemmeno ratificate.

Dite la vostra

Alberto Patella

Key Account Geovision - Gvision Italia

1 I nostri prodotti non sono concepiti con Chipset di derivazione Huawei / Hisilicon. Di conseguenza non vengono instaurate delle connessioni in uscita verso terze parti per la condivisione di dati sensibili. Oltre a ciò su tutti i nostri progetti è possibile applicare la garanzia di certificazione VA/PT nella quale viene evidenziata la totale assenza di falle informatiche.

2 Attraverso i nostri canali Social vengono argomentate tutta una serie di attività utili per i progettisti ma anche l'utenza finale.

3 E' una soluzione che abbiamo da più tempo caldeggiato, ma la disomogeneità dei prodotti e la sicurezza di molte reti IP, a volte rendono vani questi sforzi.

4 La CyberSecurity è una branca in continuo sviluppo e carente ancora di tante figure professionali estremamente necessarie. Noi come GVision e Geovision ci siamo appoggiati agli specialisti che allo stato attuale riteniamo possano essere la massima espressione di sicurezza, ma auspichiamo un'armonizzazione con un ente unico a cui far riferimento.

Potrebbe essere utile disporre di ulteriori enti di certificazione indipendenti dal fornitore

Dite la vostra

Francesco Panarelli

Key Accounts & Business Development Director - Hikvision Italy

1 I prodotti Hikvision soddisfano i più alti standard di sicurezza riconosciuti a livello internazionale da diverse certificazioni (FIPS 140-2, CC con garanzia EAL2+, ISO 27001, ISO 9001:2008, ISO 28000, CMMI Livello 5). Hikvision aderisce ad CVE, è Numbering Authority ed offre diversi strumenti di sicurezza: crittografia, strumenti di trasporto sicuri sulla rete (es. HTTPS), certificati e credenziali di accesso, codici univoci di sicurezza per ogni singolo device, programmabili solo dall'utente/utilizzatore. Anche se non impostate adeguatamente, le telecamere Hikvision non inviano immagini a server remoti e Hikvision Italy non offre soluzioni "Cloud storage" che prevederebbero l'invio di flussi ad uno storage condiviso e raggiungibile tramite una connessione ad un Cloud proprietario.

2 Hikvision Italy ha pronto un programma di formazione da "interiorizzare" e calare sulla realtà italiana, in particolare gli installatori.

3 Per mitigare un rischio dinamico come la sicurezza informatica, occorre che gli apparati vengano mantenuti aggiornati. La protezione dagli attacchi cyber può essere implementata solo grazie alla cooperazione fra Vendor, System Integrator ed End-User. Sarebbe auspicabile che, partendo dal responsabile della protezione dei dati e cioè l'End-User, diventasse prassi richiedere al manutentore di includere fra i servizi offerti anche l'aggiornamento degli apparati, in modo sistematico e rigoroso. Anche l'automazione degli aggiornamenti è un tema interessante, ma, proprio per una concezione di sicurezza dei sistemi, occorre ricordare che soprattutto in applicazioni tradizionali non sono concessi accessi verso internet per i componenti. Isolando gli apparati si ha una protezione maggiore, ma si impediscono aggiornamenti "push" (tipici dei device personali sempre connessi).

4 Ad oggi nessuno può certificare un prodotto come "cyber-sicuro", in quanto l'assenza di vulnerabilità oggi, non esclude la presenza di una vulnerabilità domani. Sarebbe però auspicabile la nascita di un ente che si occupasse almeno della definizione di un percorso di sviluppo e produzione capace di rispettare determinati parametri, che definisse i processi e gli step obbligati per poter considerare un prodotto sufficientemente sicuro da necessitare il "solo" mantenimento dei livelli di sicurezza raggiungibili con il rilascio regolare di FW.

Massimo Grassi

Security Sales Engineer - Panasonic Business

1 Il firmware di tutti i prodotti Panasonic iPRO è controllato in fabbrica e non è alterabile, criptabile né modificabile. Ogni accesso alle telecamere o al firmware stesso è bloccato o protetto, non vi sono back-door o porte di rete aperte se non quelle essenziali al funzionamento dei dispositivi. All'utente è quindi lasciata la sola possibilità di aprire porte aggiuntive in base ai servizi che vuole gestire, in piena sicurezza.

2 Tramite il Panasonic Partner Portal è possibile diventare Partner Certificato Panasonic e accedere a training di vario livello dedicate anche alla cybersecurity. Supportiamo i partner passo dopo passo, dando loro gli strumenti per realizzare un impianto di sicurezza totalmente configurato e cyber-proof.

3 I firmware Panasonic, in quanto criptati e sottoposti a continuo controllo, consentono di ridurre notevolmente i rischi di violazioni. L'i-PRO Configuration Tool (iCT) permette alle aziende di tenere costantemente aggiornato il sistema di videosorveglianza e di verificare automaticamente la disponibilità di nuovi aggiornamenti del firmware e di sistema.

4 Auspichiamo la definizione di una norma condivisa, che si affianchi alla regolamentazione degli enti di certificazione esistenti. Panasonic 5 anni fa ha siglato un accordo con la Certification Authority Symantec (poi acquisita da DigiCert) per certificare i prodotti; più recentemente ci siamo affidati all'Autorità di certificazione GlobalSign per il rilascio di certificati di encryption e di sicurezza che li rendono conformi a standard internazionali come l'americana FIPS per l'utilizzo anche in ambiti difesa, banche e PA negli USA. Al momento non esiste una norma equivalente in Europa, ma speriamo venga introdotta.

Massimiliano Marchionni

Camera Manager – Spark Security

1 In Spark lavoriamo costantemente sul firmware delle telecamere che produciamo anche per innalzare il livello di sicurezza. Per esempio, chiediamo obbligatoriamente di definire nome utente e password al primo avvio e prevediamo il blocco automatico del dispositivo in caso di troppi login falliti. Anche la Digest Authentication di default è utile nel trasferimento delle credenziali, così come la possibilità di accedere ai video solo tramite autenticazione.

2 Per Spark questo è un argomento di importanza cruciale e infatti ci facciamo spesso promotori di attività di formazione rivolte anche ai distributori e agli installatori. Inoltre, vogliamo realizzare un servizio di diagnostica che consenta a chi utilizza i nostri prodotti di verificare lo stato dei dispositivi e mantenerli costantemente aggiornati, garantendo così maggior sicurezza e performance a tutto l'impianto.

3 Sicuramente può essere utilissimo inviare periodicamente degli avvisi sull'eventuale obsolescenza della password e del firmware per mettere in guardia l'operatore sui potenziali rischi dell'impianto. Ancora una volta l'aspetto che fa la differenza è la conoscenza. Ovviamente è fondamentale investire a monte di tutto anche sulla sicurezza della rete e dei server ad essa connessi.

4 Per rendere più sicuri i nostri prodotti, in Spark prendiamo spunto dalle principali direttive europee e statunitensi in materia. Allo stesso tempo, riteniamo che sia ormai necessaria la nascita di un apposito ente certificatore, come già avviene per le certificazioni elettromagnetiche, che fornisca direttive uniche a cui tutti i produttori possano fare riferimento per elevare la cybersecurity delle loro soluzioni.

Dite la vostra

La difficoltà maggiore sarà la scelta di un Ente Certificatore che sia completamente autonomo e fuori delle dinamiche di mercato

Ermal Xhaferi

Technical Support Manager - Syac-TB

1 I prodotti SYAC-TB sono stati sviluppati interamente su sistema operativo Linux, customizzato e configurato con i soli moduli necessari al funzionamento del dispositivo. Inoltre sono stati attivati solo i servizi essenziali legati alla comunicazione del Digieye (il core tecnologico della soluzione) che non sono legati ad un server SSH o telnet. In più tutta la comunicazione viene realizzata su un protocollo proprietario sviluppato internamente. Questo ha come risultato che nessun Daemon o client di comunicazione, come aggiornamenti automatici, mascherati o meno, possa essere attivato verso un server nascosto.

2 Per noi di SYAC-TB è fondamentale creare una rete di partner qualificati per i nostri prodotti, quindi la formazione dei nostri installatori e distributori è fondamentale per garantire un corretto funzionamento e utilizzo dei nostri sistemi di protezione in termini di cyber security. Abbiamo attivato quindi una Academy attraverso la quale formiamo tutti gli operatori e partner che dovranno utilizzare i nostri prodotti di Security.

3 L'aggiornamento delle nostre macchine avviene solo tramite accesso locale di un'utenza supervisore o connessione con i nostri software di centralizzazione, sempre con diritti di supervisore. I nostri sistemi non prevedono aggiornamenti automatici e/o da Cloud, che potrebbero rendere insicuro ed instabile il sistema di protezione.

4 Sarebbe interessante stabilire degli standard di sicurezza omogenei per l'intera industria in modo che anche gli utenti riescano ad avere tutte le informazioni necessarie per una scelta più consapevole del proprio sistema. Sicuramente la difficoltà più importante sarà la scelta di un Ente Certificatore che sia completamente autonomo e fuori delle dinamiche di mercato.