L’integrazione tra sicurezza fisica e sicurezza ITC secondo Kaspersky

intervista a Cesare D’Angelo, Head of Enterprise di Kaspersky

L’integrazione funzionale, tecnologica e organizzativa tra sicurezza fisica e sicurezza ITC è un’esigenza sempre più avvertita a causa dell’aumento a livello globale degli attacchi “combinati”. Quali sono le vostre valutazioni in merito?

L’avvento di nuove tecnologie, come il 5G o l’IoT, sta cambiando radicalmente le connessioni e porterà ad una naturale espansione ed intensificazione delle cyber minacce correlate. Basta guardare alle nostre case oggi dove citofoni, lavatrici, sistemi di video sorveglianza, tutto è connesso alla rete e tutto è potenzialmente attaccabile. Secondo Gartner, entro il 2025 avremo circa 25 miliardi di connessioni IoT. Questo sicuramente incrementerà il livello di comfort delle nostre abitazioni e delle nostre città, aiutandoci a risolvere i problemi relativi alla disponibilità di risorse e consentendo alle organizzazioni di misurare le performance di produzione, introdurre l’automazione e aumentare l’efficienza.

Tutti questi benefici, però, rendono l’IoT un sistema critico che va assolutamente protetto, al fine di evitare che l’impatto positivo di questa grande opportunità su imprese e persone venga annullato. Anche perché si tratta di piattaforme utilizzate anche in tutti quei settori considerati critici come ad esempio l’healthcare, le smart cities o le reti elettriche.

I sistemi di automazione degli smart building, ad esempio, sono tipicamente costituiti da sensori e controller usati per monitorare e automatizzare il funzionamento di ascensori, impianti di vario genere come quello di ventilazione, di climatizzazione, elettrici, di fornitura idrica, di video sorveglianza, o allarmi anti-incendio e sistemi di controllo degli accessi e molte altre informazioni critiche e sistemi

di sicurezza. Questi sistemi sono solitamente gestiti e controllati da normali workstation che, spesso, sono connesse a Internet.

Un attacco riuscito contro una di queste workstation può facilmente concludersi con il mal funzionamento di uno o più sistemi critici dello smart building. Inoltre, le piattaforme IoT possono essere collegate a sistemi critici come quelli per il controllo del traffico, l’erogazione dell’energia e dei trasporti, quindi è fondamentale garantire la loro continuità e integrità. In definitiva l’Internet of Things è un potente strumento di business ma per cogliere i suoi benefici le organizzazioni devono impegnarsi a fondo.

Per ottenere un’efficace implementazione, oltre a competenze specifiche, sono richiesti processi di business dedicati. Anche la sicurezza informatica è una questione che deve essere presa in considerazione sin dalle fasi iniziali dell’implementazione dell’IoT. Noi di Kaspersky vogliamo aiutare i nostri clienti ad affrontare questo compito sviluppando soluzioni di sicurezza IoT e sensibilizzandoli sui rischi e le problematiche.

Anche l'avvento dei droni ha dato nuovi accessi ai criminali informatici per minare la sicurezza e alla privacy degli utenti. Nel 2018, il mercato globale dei droni ha raggiunto un valore di circa 14 miliardi di dollari; entro il 2024 dovrebbe arrivare a toccare i 43 miliardi di dollari. Questa crescita è determinata dalle potenziali opportunità e dai tanti cambiamenti positivi che l'utilizzo di veicoli volanti privi di equipaggio può portare con sé: consegna di merci, ispezione di siti minerari, costruzioni edilizie, ma anche puro divertimento. Nonostante questi aspetti positivi, l'uso popolare di questa tecnologia rivoluzionaria potrebbe essere influenzato da alcune connotazioni negative che spesso vengono associate al mondo dei droni. I droni possono essere utilizzati anche per fare spionaggio, possono ferire le persone in caso di incidenti, possono causare danni alle infrastrutture critiche, comprese le centrali nucleari, o anche perturbare il normale funzionamento di un aeroporto, come è accaduto all'aeroporto britannico di Londra Gatwick, quando la pista è stata chiusa proprio a causa di droni in volo.
Considerando tutti questi fattori, è chiaro come sia sempre più importante contribuire alla costruzione e al mantenimento di un approccio orientato alla fiducia verso la tecnologia, in modo da salvaguardare il suo apporto innovativo - per le imprese e per i privati - e, nello stesso tempo, assicurarsi che le nuove frontiere tecnologiche non determinino rischi per la privacy o per la sicurezza.

È possibile delineare un confronto tra la situazione italiana e quella degli altri paesi dell'area EMEA e/o world in termini di attacchi conclamati?

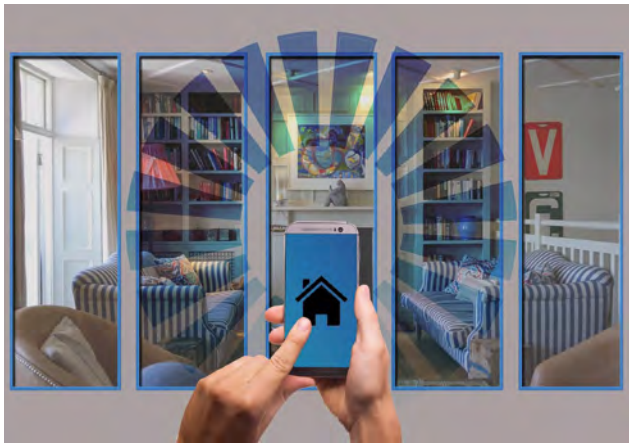
Recentemente abbiamo condotto un'indagine sulle minacce informatiche rivolte agli smart building dalla quale è emersa, in parte, la situazione a livello europeo degli attacchi rivolti ai sistemi di sicurezza di questi edifici. Secondo questa analisi, infatti, quattro computer su dieci (37.8%), usati per gestire i sistemi di automazione degli "edifici intelligenti", sono stati oggetto di attacchi malevoli. Sebbene non sia del tutto chiaro se questi sistemi siano stati deliberatamente presi di mira, questa ricerca dimostra come gli smart building siano spesso oggetto di varie minacce generiche. Per quanto non si tratti di minacce sofisticate, molte di queste possono costituire un pericolo importante per le operazioni quotidiane degli smart building. La maggior parte degli attacchi arrivava dal web ed utilizzava diverse versioni di spyware, ovvero malware che hanno l'obiettivo di rubare le credenziali degli account e altre informazioni importanti. Dall'indagine è emerso, inoltre, che l'Italia è il Paese con il maggior numero di attacchi rivolti ai computer per gli smart building (48,5%), seguito da Spagna (47,6%), Regno Unito (44,4%), Repubblica Ceca (42,1%) e Romania (41,7%).

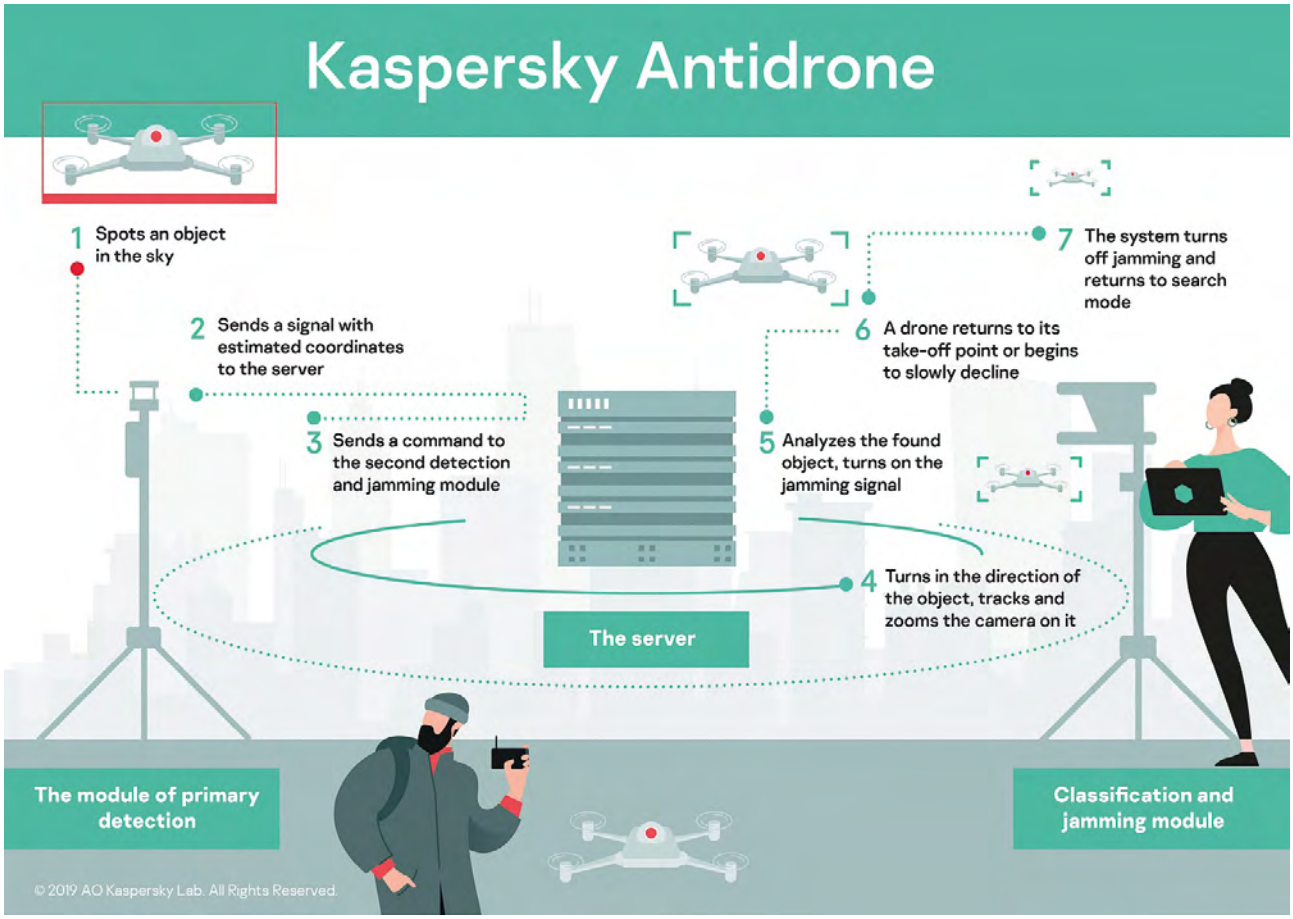
Come valutate il livello di consapevolezza sul punto delle funzioni decisionali delle organizzazioni pubbliche e private?

Quello che riscontriamo sul mercato è un livello di consapevolezza mediamente abbastanza alto, che però non corrisponde necessariamente a una prioritizzazione degli investimenti necessari a indirizzare il problema. La prima controparte con cui dialogare per condividere questa necessità sono i System Integrator e i Produttori di tecnologie, coi quali è fondamentale indirizzare il tema della vulnerabilità informatica dei prodotti fin dalla loro progettazione: lavoriamo da tempo con alcuni importanti player proprio per fare in modo che gli "oggetti" che comporranno una soluzione o che arriveranno dal cliente finale siano progettati e realizzati includendo componenti di sicurezza informatica, e che lo stesso processo di produzione di questi oggetti sia gestito da macchinari protetti anche in questo senso.

Quali sono le proposte di Kaspersky per la sicurezza integrata?

Per rispondere alle esigenze crescenti di sicurezza integrata, Kaspersky mette a disposizione Kaspersky IoT Secure





Gateway e KasperskyOS che, insieme, garantiscono il comportamento sicuro del gateway stesso, così come di tutti i dispositivi collegati e dell'intero sistema IoT.

Il mercato offre ora numerosi gateway e router descritti come "sicuri" o "affidabili". Questi dispositivi forniscono una vasta gamma di tecnologie per la protezione contro le minacce informatiche: scanner antivirus, controllo del traffico di rete, firewall, ecc. È importante capire, però, che queste tecnologie sono progettate per proteggere i dispositivi collegati al gateway, ma nessun produttore protegge effettivamente il gateway stesso.

Se è compromesso, tutte le tecnologie di sicurezza che lo accompagnano possono essere disattivate. **Kaspersky IoT Secure Gateway** contiene una gamma di tecnologie che consentono di adottare un approccio qualitativamente diverso per la sicurezza in ambito IIoT e per quella relativa ai device presenti all'interno delle smart home. Oltre alle migliori tecnologie per la sicurezza dell'infrastruttura, questa soluzione implementa tecnologie affidabili che garantiscono il comportamento sicuro del gateway o del router stesso. Abbiamo progettato la nostra soluzione per incorporare moduli e tecnologie di sicurezza nel firmware del dispositivo, in modo da poter proteggere l'hardware con diversi gradi di personalizzazione.

KasperskyOS, invece, è un sistema operativo sicuro per dispositivi embedded connessi con requisiti specifici di sicurezza informatica, che crea un ambiente in cui vulnerabilità o codici malevoli non rappresentano più un problema. Il concetto alla base di KasperskyOS è di consentire ai programmi di eseguire solo attività documentate previste dalla policy, comprese, quindi, anche le stesse funzioni del sistema operativo.

Il vantaggio per i programmatori è di poter sviluppare una politica di sicurezza insieme alle funzionalità reali di un'applicazione riducendo drasticamente la possibilità di attacchi informatici.

Inoltre, per rendere più sicuro l'uso di dispositivi volanti senza piloti o equipaggio, ridurre i possibili rischi associati e attribuire maggiori responsabilità all'operatore, Kaspersky ha sviluppato una propria soluzione "antidrone". Il software

Kaspersky Antidrone coordina il lavoro di diversi moduli hardware forniti dai partner ed è in grado di distinguere i droni da altri dispositivi. Il modulo di rilevamento primario procede con la ricerca dei droni utilizzando videocamere combinate con sensori radar, LIDAR e audio, a seconda delle esigenze del cliente e delle condizioni ambientali. L'utilizzo di uno scanner laser per determinare la posizione del drone è un "unicum" della soluzione proposta da Kaspersky, che non ha precedenti applicativi in questo campo. Quando un oggetto in movimento viene rilevato nel cielo, le sue coordinate vengono trasmesse a un server dedicato, che le invia a un'unità speciale. In base ai dati provenienti dal modulo di rilevamento primario, questa unità ruota verso l'oggetto, lo segue e la telecamera zooma sull'oggetto stesso. Contemporaneamente, una rete neurale, progettata proprio per identificare i droni e distinguerli da altri oggetti in movimento, analizza l'oggetto dal video. Se il sistema lo riconosce come drone, il server invia un comando al modulo dedicato il quale disturba, tramite interferenze, le comunicazioni tra il dispositivo e il suo controllore. Come risultato, il drone torna al luogo di partenza o atterra nel punto in cui ha perso il segnale con il controller.

Se poi pensiamo a tutti quegli oggetti molto semplici che popolano le nostre abitazioni (bollitori elettrici, telecamere di video sorveglianza, frigoriferi intelligenti) e che possono essere connessi alla rete attraverso semplici app installate sui nostri cellulari, ci rendiamo conto che uno degli inconvenienti maggiori di questi dispositivi smart

è che solo le case produttrici possono risolvere i problemi di sicurezza che potrebbero insorgere. I proprietari di tali oggetti spesso non possono fare nulla. Affinché sia più facile per gli utenti individuare le vulnerabilità nei dispositivi smart connessi alla rete domestica, abbiamo creato un'app apposita: **Kaspersky IoT Scanner**. Questa app per Android analizza la vostra rete di casa, elabora un elenco di tutti i dispositivi che vi sono connessi e individua le vulnerabilità più comuni. Dopo essere stata installata, IoT Scanner analizza la rete domestica e localizza tutti i dispositivi collegati a essa. Successivamente, analizza alcune porte di rete specifiche dei dispositivi e verifica quali porte sono aperte e quali no. Se IoT Scanner individua alcune porte che potrebbero essere sfruttate per scopi dannosi, allora l'app invia una notifica e invita l'utente a chiudere tali porte, risolvendo così la vulnerabilità.

kaspersky