Sicurezza convergente: quando le porte si aprono con magneti e password

a cura della Redazione

Il concetto di **sicurezza convergente** è molto attuale, si ricollega a quello di **Cyber Physical Security (CPS)** coniato solo alla fine del 2015 dal National Institute of Standards and Technologies (NIST) – **leggi** – per definire le misure di difesa da minacce che combinano le componenti fisiche e digitali dei mezzi di attacco per sottrarre sia beni materiali (tipicamente denaro) che immateriali (tipicamente dati) o compiere azioni dimostrative, terroristiche o di altra natura.
Un concetto peraltro nato e già ampiamente consolidato in ambito militare: già nella II guerra mondiale, ad esempio, gli attacchi aerei venivano anticipati da disturbi radio ai mezzi di difesa a terra e oggi perfino le battaglie navali possono avvenire in formato cyber – **leggi**.
In ambito civile, sono già innumerevoli gli episodi in cui gli attacchi sono partiti dal cyberspazio per svuotare, ad esempio, i bancomat di banche di mezzo mondo – **leggi** – o bloccare le serrature digitali di hotel – **leggi** – oppure dallo spazio materiale, per piazzare una delle innumerevoli black box in grado di interferire con i sistemi IT per sottrarre dati o altro. Con la diffusione pervasiva in corso dei dispositivi in rete, chiunque dovrà acquisire competenze specifiche per difendersi dalle insidie che potranno nascondersi nel frullatore o nel taglia erba, imparando a proprie spese che la sicurezza non è un prodotto che, una volta acquistato, dura fino a scadenza, ma un processo che deve venire aggiornato costantemente, esattamente come si è imparato a fare per le altre facce della sicurezza, la safety e la salute fisica.
E' tuttavia importante sottolineare quanto sia importante fin d'ora questo atteggiamento, senza dover aspettare l'avvento dello IoT. Due recenti fatti di cronaca, all'apparenza diversi come una serie di furti in casa in Liguria e il virus WannaCry in giro per il mondo, dimostrano inaspettate somiglianze nei sistemi di difesa delle vittime, palesemente inadeguati alla prova dei fatti per il medesimo motivo, come viene spiegato da **Giordano Turati** e **Luca Girodo** negli articoli che seguono.

Sicurezza convergente 1: quando il ladro usa il magnete invece del grimaldello…

a colloquio con Giordano Turati, CEO di TSec spa

Le cronache hanno riportato la notizia di una banda di ladri che ha compiuto di recente razzie in numerose abitazioni in una città ligure, disattivando l'impianto di allarme con un semplice magnete. Come è possibile avvenga questo?
E' possibile perché la tecnologia di base utilizzata per la fabbricazione dei più comuni contatti magnetici è molto debole. Infatti, i contatti normalmente utilizzati, soprattutto in ambito residenziale, sono semplicemente mascherabili posizionando un campo magnetico in prossimità del sensore. In un'abitazione, l'aspetto più preoccupante è che questa operazione è fattibile senza dover entrare nel del perimetro protetto. La tipica situazione notturna di un'abitazione, in cui la sicurezza degli abitanti è delegata alla sola protezione su porte e finestre, dal momento che i rilevatori volumetrici interni vengono necessariamente disinseriti per consentire il movimento delle persone, fa comprendere la criticità dell'argomento.

Quali sono le soluzioni disponibili per evitare la disattivazione dei contatti magnetici sulle porte?
Bisogna salire di livello, utilizzando soluzioni più moderne ed efficaci. La tecnologia evolve e, purtroppo, anche le capacità dei malfattori. Basta pensare che la tecnologia utilizzata per i contatti magnetici tradizionali è stata sviluppata negli anni '30 per impieghi diversi dalla sicurezza! Oggi sono invece disponibili sul mercato contatti magnetici anti-mascheramento, sensori cioè che non si possono eludere con un campo magnetico proveniente dall'esterno del perimetro protetto. Assicurano un grado elevatissimo di sicurezza fin dal semplice modello ad incasso con singolo switch, quello più comunemente utilizzato in ambito residenziale.

L'utilizzatore finale come può accertarsi che il suo installatore di fiducia utilizzi contatti magnetici adeguati?
Il suggerimento principale che mi sento di dare all'utilizzatore finale è di scegliere una soluzione il più possibile "sicura".


LA STAMPA IMPERIA SANREMO

Ladri "scientifici" in azione allarmi annullati col magnete

Furti in alloggio in strada Catocce e alle Cascine

La zona colpita dai ladri in una foto dall'alto

@ewsletter LA STAMPA

LA STAMPA CON TE DOVE E QUANDO VUOI

E-mail

Password

Potrebbe sembrare un'ovvietà, ma l'esperienza dimostra il contrario. Bisogna mettere al primo posto la sicurezza, chiedere ed avere conferma dal proprio installatore di fiducia dell'effettivo grado di sicurezza che l'impianto di allarme è in grado di offrire, in base alle proprie esigenze. La sicurezza, poi, non viene assicurata da un singolo prodotto ma da una serie di fattori e di azioni che, unite in un processo, innalzano il livello di protezione. La scelta dell'impianto più adeguato prescinde dalla comodità nell'utilizzo e dalla semplicità del montaggio, che restano elementi da considerare ma non devono essere prioritari se vanno ad inficiare il grado di sicurezza. Infine, non è detto che un impianto ben progettato e che contempli l'utilizzo di tecnologie più sicure, specie nella sensoristica, abbia dei costi più elevati. Certo, non possiamo pensare di affidare la sicurezza delle nostre abitazioni a kit autoinstallanti dal costo di poche centinaia di euro. Le persone, soprattutto le famiglie, si dovrebbero domandare: "Quanto costa la non sicurezza?". Naturalmente, queste considerazioni valgono a maggior ragione anche per ogni organizzazione pubblica e privata, dove la sicurezza non riguarda solamente le persone e i beni materiali ma, oggi, anche i dati contenuti nei server, nei videoregistratori e, in generale, tutti i dispositivi delle infrastrutture IT accessibili fisicamente.

Sicurezza convergente 2: …e quando la porta si può aprire con la password

a colloquio con Luca Girodo, esperto CCTV e sicurezza IT, docente di securindex formazione

"I ladri armati di magnete sono arrivati a Imperia, colpi in periferia"; così titolava la rivista online Riviera24.it del 1 Maggio 2017. La notizia ha attirato la mia attenzione, mi ha incuriosito ed ho voluto capirne di più. Come è possibile eludere un antifurto con un semplice magnete?

Nell'articolo parlano di un moderno Arsenio Lupin, ma non si è trattato di nessun ladro gentiluomo; molto semplicemente è stato qualcuno iscritto all'Istituto Tecnico Industriale che, con semplici nozioni di base, è stato capace di mettere fuori uso l'antifurto.

In generale, tutti gli antifurti che sono stati elusi utilizzavano dei contatti perimetrali con tecnologia elettromagnetica: è sufficiente acquistare un piccolo magnete in cartoleria, come quello con cui ci si divertiva da ragazzini, ed il gioco è fatto. Si consideri che, contatti normalmente aperti e non schermati, attaccati direttamente alle finestre, si possono mettere fuori uso in meno di 5 secondi.

Altro caso, stesso giorno, luogo diverso. Città di Milano: alcuni hacker hanno trafugato dei dati da una rete di una piccola azienda. Archivi distrutti. Questi ladri sono entrati nella rete aziendale dalla porta principale, cioè dal firewall. Hanno fatto un po' di ricerche, hanno capito la marca dell'apparato, hanno provato con la password di fabbrica...et voilà, era proprio quella!

Due episodi che posso sembrare tra di loro lontani nello spazio e nel tempo, ma che così lontani non sono. Hanno lo stesso comune denominatore, la tecnologia.

Nel furto di Imperia i proprietari si sono trovati i ladri in casa nonostante avessero utilizzato proprio la tecnologia per proteggersi, infatti avevano fatto installare l'antifurto.

Il proprietario dell'azienda, che si è ritrovato con tutti gli archivi files distrutti, aveva fatto esattamente la stessa cosa: si era affidato alle difese tecnologiche del firewall, lui si sentiva al sicuro.

Quindi, che cosa in entrambi i casi non ha funzionato? E' stata la tecnologia? Prendiamo ad esempio l'ultimo attacco del Ransomware WannaCry. Come ha fatto a mietere così tante vittime? A posteriori sembra scontato dirlo ma si è trattato semplicemente di Bug sui sistemi. Bug purtroppo noti che non sono stati aggiornati o protetti.

Le Patch erano disponibili sin da prima dell'attacco, ma molti non le hanno installate. I sistemi di difesa delle reti non hanno intercettato il Worm, non erano configurati per farlo. WannaCry, per attivarsi su un PC, controllava di essere connesso ad internet cercando di raggiungere un indirizzo web con un nome lunghissimo.

Per concludere: gli utenti credono di essere sicuri comprando un antifurto o un firewall per l'azienda, ma la sicurezza purtroppo non è un prodotto, bensì un processo. Se l'antifurto è obsoleto o un firewall non è aggiornato, non c'è sicurezza. Visto che la sicurezza è un processo, l'investimento (tempo, denaro, progettazione, etc.) deve essere continuo, affinché la difesa sia efficace. In sintesi, non esiste "l'abbastanza sicuro". O è sicuro, oppure non lo è!