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!