Annalisa Coviello

Phygital security: come raggiungerla?

“La sicurezza non può più essere solo fisica o solo digitale. Per forza di cose, anche a causa della pandemia e della conseguente “digitalizzazione” forzata alla quale siamo stati quasi tutti costretti, ormai si parla di “phygital” per ciò che riguarda la security, con tutte le conseguenze del caso, prima tra tutte la paura, e l’eventualità molto concreta, degli attacchi di hacker e cybercriminali di tutti tipi e con tutte le specializzazioni del caso.

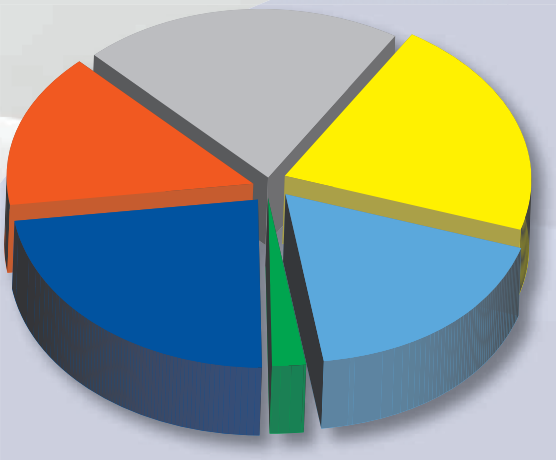
Nello scorso numero di *secsolution magazine* abbiamo dedicato ampio spazio proprio al tema dell'integrazione, ormai obbligatoria, tra sicurezza fisica tradizionale e la più moderna sicurezza digitale, intervistando i principali player del settore per capire non solo l'aria che tira, ma quali siano, in concreto, le esigenze e le necessità di chi in questo mercato ci lavora da tempo, in modo da rispondere al meglio alle richieste, sempre in continuo divenire, dell'utilizzatore finale. Anche la tavola rotonda di apertura del *secsolutionforum 2021* è stata dedicata proprio al tema "Sicurezza fisica, sicurezza logica e privacy: si riparte dal Covid?" e ha suscitato un notevole interesse, segno che la questione, più che attuale, ormai è imperativa, perché senza questa integrazione non può esistere la sicurezza *tout court*. In questo articolo vogliamo quindi sintetizzare ciò che hanno detto, partendo dalla loro esperienza e dalle esigenze espresse dai clienti, gli attori del mercato, ma anche cosa occorre fare per arrivare alla "phygital security" e contrastare gli attacchi criminali che, sia pure virtuali, sono forse ancora più pericolosi.

Come se ne esce

La prima richiesta degli operatori del settore, ribadita più o meno da tutti, è quella di cercare al più presto un accordo, un patto, tra produttori, integratori e utilizzatori per realizzare dei dispositivi che siano veramente a prova di ogni cyber e sempre continuamente aggiornati, visto che il crimine non resta mai indietro. Che sia sogno o utopia (visto che i prodotti completamente "sicuri" sotto questo aspetto, come succede con i cellulari o i computer, diventano vecchi durante il tragitto che facciamo per portarceli a casa), non si può non tentare.

Aggiornamento

E' indispensabile che, partendo dall'end-user, venga richiesto al manutentore e all'integratore di includere fra i servizi offerti anche l'aggiornamento continuo dei dispositivi. A questo punto, i produttori si devono adeguare, per non essere tagliati fuori dal mercato. Proprio per tale motivo sarebbe anche auspicabile, dicono i nostri esperti, una certificazione davvero "super partes" e rilasciata da un organismo terzo rispetto ai player del mercato, per garantire quell'imparzialità e correttezza che risultano davvero fondamentali: in questo caso, infatti, è troppo rischioso affidarsi al "fai da te" e le certificazioni rilasciate dai singoli produttori non sempre sono univoche e uniformi. Altro aspetto da non trascurare è che il pacchetto firmware dei dispositivi sia sempre allineato con le soluzioni di cybersecurity più recenti: si potrebbe ipotizzare un aggiornamento periodico, come già succede, ad esempio, con i computer o con i cellulari, che si potrebbe forse rendere obbligatorio. I penetration test che vengono eseguiti in real time dimostrano, infatti, che la sicurezza digitale è un insieme mai statico, ma molto dinamico.



Strategie da attuare per ottenere una reale integrazione tra sicurezza fisica e digitale (elaborazione dati secsolution magazine)

Cyber secure by design

Partendo proprio dalle origini, poi, molti produttori già adottano quella che viene definita "sicurezza by design", cioè già nella fase di progetto del dispositivo: è il caso, ad esempio, di numerose telecamere IP che contengono il signing oppure un firewall integrato che, in caso di banali errori di inserimento delle password di sicurezza, fa comunque entrare solo i soggetti "autorizzati" o, ancora, la disabilitazione di porte e servizi non necessari. Un'esigenza, quella della "security&privacy by design", che oggi è diventata tra le prime richieste dell'utente finale. Molti produttori, poi, prevedono una serie di corsi, durante la pandemia ovviamente on line ma da poco anche in presenza, con esame finale, in cui, grazie agli appositi tools di configurazione, è possibile verificare il livello di vulnerabilità dei dispositivi. Altri hanno realizzato una vera e propria rete di partner qualificati e sempre aggiornati proprio in materia di protezione e cybersecurity. C'è anche chi sostiene, però, che dovrebbero essere gli stessi clienti a scegliere che grado di sicurezza adottare, in piana autonomia e secondo il tipo di applicazione installata, perché in questo caso il "plug&play" troppo generalizzato può andare a discapito della sicurezza dei dati.

Lezione Covid

E concludiamo con l'attualità. Il coronavirus è stato una notevole discriminante tra chi era preparato a una gestione integrata della sicurezza fisica e logica e chi no: un esempio per tutti è quello dello smart working. Se si lavora con dati sensibili (e, oggi, quali non li sono?) è indispensabile che gli stessi non possano passare così, semplicemente, attraverso le maglie sempre troppo larghe del web "normale", perché gli hacker avrebbero davvero vita troppo facile a carpirli. Facciamo un esempio molto semplice. Il mobile banking: durante i vari lockdown, anche gli istituti di credito erano chiusi e, quindi, la gestione dei flussi finanziari era interamente on line. Ma la domanda sorge spontanea: tutti i dipendenti delle banche avevano a casa gli stessi sistemi di sicurezza della rete dell'ufficio?

Security manager

C'è una figura che è venuta fuori con preponderanza durante la pandemia: il security manager. Che è diventato un vero e proprio "regista" per garantire la sicurezza dei lavoratori che non potevano svolgere i loro compiti in smart working e, al tempo stesso, offrire ai clienti la continuità dei servizi. Il tutto cercando di coniugare sicurezza fisica, logica e, possiamo aggiungere, sanitaria, in modo che non potessero entrare persone sgradite, uscire dati sensibili e, aspetto non secondario, chiudendo anche tutte le porte possibili al virus. Cosa ci portiamo dietro, dopo più di un anno di lockdown, timide riaperture e nuove serrate? Beh, di sicuro la consapevolezza che, ormai, la sicurezza fisica e quella digitale devono diventare non solo un unico vocabolo, ma una sola realtà integrata. La strada da percorrere non è di sicuro tutta in rettilineo, però almeno sappiamo in che direzione andrà.

Per chi si fosse perso qualcosa