Gli attacchi informatici sono sempre più micidiali e pervasivi. Che fare per fronteggiarli?

Cyber Insecurity: la protezione totale non esiste

Gli attacchi informatici in tutte le diverse forme stanno salendo d'intensità e frequenza. Non si tratta di singoli individui isolati ma di vere e proprie organizzazioni che architettano azioni sempre più invisibili e pericolose. Durante l'incontro del 12 settembre, organizzato da The Ruling Companies, un panel di esperti ha affrontato questo tema di importanza cruciale per tutte le imprese. Prendendo spunto dallo Speciale pubblicato sul numero di settembre di *Harvard Business Review Italia*, i relatori hanno fornito ai partecipanti le indicazioni più aggiornate su come affrontare queste minacce.

Marianna Vintiadis (CEO, Kroll) ha chiarito subito che la scala dei fenomeni legati alla sicurezza digitale è cambiata in modo sostanziale negli ultimi anni e si devono adottare logiche adeguate alle nuove dimensioni. Oggi bisogna pensare a una sicurezza fatta "a strati". La scelta strategica di quanti strati di protezione adottare deve essere commisurata con le probabilità di rischio, i costi e le misure a disposizione. Innanzitutto bisogna individuare con precisione cosa interessa tutelare: know-how, infrastrutture, dati o altro. Capire cosa è prioritario permette alle aziende di procedere in modo più ordinato nella messa in sicurezza dei sistemi. In secondo luogo, è bene provare a ipotizzare da chi potrebbero provenire gli attacchi. Da quale tipo di criminalità arrivano gli attacchi? E quale livello di pericolosità ha? Infine, bisogna valutare quanto controllo abbiamo sui nostri sistemi tenendo a mente che il controllo assoluto non esiste. Oggi le criticità possono arrivare da diverse fonti, hacker esperti sanno decifrare informazioni provenienti da diversi segnali come onde elettromagnetiche, ultrasuoni, calore. Quindi, sconnettersi da internet può non essere una soluzione definitiva. Il controllo dell'infrastruttura e dei sistemi è essenziale per prevenire e riconoscere eventuali problemi. La sicurezza non sarà mai totale, il vero tema è quanto e come possiamo limitare gli attacchi.

"Sono 146 - dice Walter Ruffinoni (CEO, NTT Data) - i giorni che servono mediamente per capire di essere stati attaccati". Le aziende non riconoscono le violazioni in modo tempestivo lasciando ai malintenzionati tutto il tempo di infiltrarsi e operare all'interno dei propri sistemi. Le imprese dovrebbero investire e lavorare su piani predittivi. Per capire da dove potrebbe arrivare le minacce occorrono studio e analisi dei dati e aumentare la consapevolezza e la cultura delle persone su questi temi, solo così sarà possibile anticipare e prevenire gli attacchi. Negli ultimi anni quattro casi in particolare hanno sollevato l'attenzione e cambiato la percezione della cyber security:

1- la fake news su Twitter che annunciava un attacco alla Casa Bianca. Notizia falsa che però nel 2011 ha causato un crollo reale delle borse.

2- Il blocco dell'infrastruttura elettrica in Ucraina che ha lasciato al buio la Nazione.

3- Il caso di phishing del 2015 che è valso 1 miliardo di dollari.

4- Wanna Cry che ha compromesso il sistema sanitario del Regno Unito nel 2017.

Come sottolinea Ruffinoni, chi attacca studia per anni l'organizzazione e i suoi sistemi. Ad esempio, la tecnica delle e-mail fasulle spedite a dipendenti con la firma dei propri responsabili possono risultare credibili e veritiere. Secondo Ruffinoni, assisteremo presto a un incremento esponenziale

degli attacchi che saranno sempre più veloci, mirati e invisibili. Aumenteranno le fonti e diminuirà il costo economico delle frodi. Per non farsi trovare completamente impreparati bisogna investire da subito nella formazione dei leader e di tutti i cittadini che condividono informazioni con troppa leggerezza. Le tecnologie, i software e tutti gli strumenti devono essere sicuri by design. Inoltre, le organizzazioni dovrebbero fare sistema e condividere informazioni sugli attacchi. Inoltre, servirebbe più collaborazione tra settore pubblico e privato ma anche tra i diversi Paesi.

Anche Luca Rizzi (Direttore Mercato Pubblica Amministrazione Centrale e Locale, Cisco Italia) pone l'accento sul tema della formazione e della cultura. La tecnologia in sé non è l'elemento centrale, servono strategia, competenze e processi virtuosi. I dati dimostrano che stanno aumentano gli investimenti in sicurezza e cresce anche la richiesta di personale qualificato. Cisco promuove attivamente il networking e la collaborazione con le università per sviluppare competenze e innovazione. Per prevenire gli attacchi bisogna studiare le dinamiche che avvengono in rete, analizzare i comportamenti e capire cosa sta accadendo. La difesa attiva deve essere incrementata ricorrendo all'aiuto di hacker "buoni" capaci di processare dati e informazioni. Al momento si stimano 20 miliardi di attacchi al giorno, molti dei quali automatici. Gli strumenti per combatterli ci sono, serve più consapevolezza nell'uso delle tecnologie e dei sistemi di protezione.

Secondo Roberto Saracino (Senior Vice President IGT CTO, Lottomatica) la possibilità di colpire a distanza e in modo replicabile rende gli attacchi cyber un'arma micidiale. Spesso non si tratta di singoli hacker ma di vere e proprie organizzazioni criminali che operano come un'industria composta da diverse funzioni ciascuna dedicata a un'attività specifica. Le singole azioni svolte spesso sono lecite e solo mettendo in sequenza i vari processi si comprende la frode. Per proteggersi servono diversi livelli di sicurezza e un'attenta analisi dell'ecosistema per capire la provenienza dell'attacco, gestirlo o - meglio ancora – anticiparlo. Visto che l'attacco è organizzato, la difesa deve esserlo altrettanto. Tutte le funzioni aziendali devono essere coinvolte e sensibilizzate sui temi della sicurezza.

Negli ultimi due anni l'attenzione alla sicurezza informatica è cresciuta notevolmente. La leva mediatica e quella normativa hanno contribuito ad accrescere l'interesse di cittadini e aziende sulla tutela dei propri dati e delle proprie attività in rete. Ad esempio, come ricorda Gabriele Faggioli (Presidente, Clusit), il caso Cambridge Analytica è stato molto significativo e ora i data breach devono essere denunciati tempestivamente. Tuttavia, c'è ancora poca consapevolezza sul tema della sicurezza. Molte aziende non utilizzano il cloud per paura di perdere i dati, quando in realtà è molto più improbabile che qualcuno riesca a violare i sistemi dei grandi provider. Bisognerebbe sempre controllare anche la sicurezza di tutti i nostri strumenti connessi, dallo smartphone agli utensili domestici di ultima generazione. La pubblica amministrazione ha un ruolo fondamentale nell'educazione di tutti i cittadini che si troveranno a dover gestire attacchi più organizzati e sofisticati. In Europa, dice Faggioli, l'attenzione sta crescendo sempre più e il Clusit sta collaborando alla stesura di un Cyber Security Act. Contro gli attacchi informatici è importante investire in difese appropriate e in formazione dei dipendenti. Anche se la sicurezza totale non può essere veramente ottenuta, servono perlomeno strategie innovative basate su nuove competenze e occorre predisporre misure straordinarie per garantire la sicurezza di tutti i sistemi critici.

A cura della Redazione di Harvard Business Review Italia