Cybersecurity e aziende: se il virus peggiore è la nostra mentalità

*di Nico Abbatemarco**

Il tema della sicurezza nell'uso delle nuove tecnologie è tanto attuale, quanto controverso. Spesso sottovalutata, soprattutto in passato, la cybersecurity non può essere concepita soltanto come un'ingombrante voce di costo ma rappresenta una cruciale forma di difesa da possibili (e purtroppo reali) rischi, la cui gravità è spesso irreversibile.

Oggi, una delle debolezze principali del digital mirror è rappresentata dai rischi cyber, definiti come quei rischi che *implicano una perdita di riservatezza, integrità o disponibilità di informazioni, dati o sistemi informativi*,[1] e che, in conseguenza di ciò, possono generare *potenziali impatti negativi sulle organizzazioni*[2] (per esempio, bloccandone l'operatività quotidiana). Ogni giorno, il numero di individui e organizzazioni colpiti da una qualche forma di rischio cyber concretizzatosi in un attacco aumenta inesorabilmente. Ogni giorno, i racconti dell'orrore diffusi da chi è stato colpito contribuiscono a cambiare, lentamente ma inesorabilmente, la percezione della *cybersecurity* da parte del top management aziendale, che troppo spesso in passato ha visto in essa solo un puro costo.

Eppure, nonostante queste premesse, la maturità dei programmi di cybersecurity aziendale fa fatica a decollare. Secondo diversi report pubblicati nel periodo 2021-2023, fra le aziende globali con fatturato superiore ai 5 miliardi di dollari, quelle che si attribuiscono un livello di maturità cyber alto sono solo il 30 per cento, un numero che scende sotto la soglia del 15 per cento quando si prendono in considerazione quelle con un fatturato compreso fra i 500 milioni e i 5 miliardi

© ISTOCK - SORBETTO

* ***Nico Abbatemarco***, *Junior Lecturer, Digital Transformation presso DEVO Lab, SDA Bocconi School of Management.*

DOI: 10.1485/1120-5032-202303-15

di dollari (numeri che scendono anche al di sotto della doppia cifra quando si considerano alcuni specifici settori). Quali sono, dunque, gli ostacoli che impediscono il raggiungimento dei livelli di cybersecurity necessari nel contesto attuale?

Per evitare di sfociare in una serie di ovvietà, o peggio in una lista di sfide comuni che qualunque AI-generativa di questi tempi sarebbe in grado di creare, l'articolo assumerà come validi due presupposti: il primo è che il top management abbia già sentito parlare di cybersecurity – uno scenario estremamente probabile, a meno che non abbia passato l'ultimo decennio a vivere in una caverna – e che sia conscio del fatto che la sua mancanza può avere conseguenze gravissime, che spaziano dalla gogna reputazionale dell'azienda che ha perso informazioni sensibili dei propri clienti al blocco totale delle operations di chi ha subito un attacco *ransomware* nella sua nuova, fiammante *smart factory*. Si partirà quindi dall'assunto che il top management abbia riconosciuto un qualche tipo di rilevanza alle buone prassi di cybersecurity aziendale.

Il secondo presupposto è che la singola organizzazione possa fare poco per quelle che sono le sfide «endemiche» di questo ambito: in primo luogo, la mancanza di competenze cyber sia a livello tecnico sia manageriale. La carenza esiste ed è sentita, e i talenti lo sanno – la fuga verso gli stipendi garantiti dai grandi player del digitale o dalle grandi società di consulenza è marcata ancora più che in altre branche del digital. Tuttavia poco si può fare a proposito, se non aspettare la formazione e lo sbarco sul mercato di nuove figure professionali. Il secondo assunto è quindi che il top management debba agire con delle limitazioni esterne importanti, che però non sono per forza tali da impedire il raggiungimento di un livello di maturità cyber soddisfacente.

© ISTOCK - SORBETTO

Sulla base di questi due assunti, nei prossimi paragrafi sono presentati quattro esempi di mentalità erronei con cui il top management si approccia di frequente al mondo della cybersecurity. Seppur in maniera semplificata, ognuno di essi descrive come una mentalità sbagliata contribuisca al mancato raggiungimento degli obiettivi di cybersecurity desiderati per l'organizzazione.

PRIMO MINDSET
OK, FACCIAMO QUESTA CYBERSECURITY… MA ALLA SVELTA, E CHE SIA ECONOMICA

Il primo mindset rappresenta quello di cui è più facile vedere i limiti, anche se – sfortunatamente – non per questo risulta essere meno diffuso. Ovviamente, come tutti i progetti aziendali, anche l'implementazione di misure di cybersecurity deve essere contraddistinta da requisiti di economicità. Purtroppo, nel caso della cybersecurity, capire l'entità del beneficio apportato non è affatto semplice. In assenza di buone metriche per la misurazione degli obiettivi di cybersecurity, per ottenere tale economicità si tende a dar vita a progetti sottodimensionati in termini di risorse allocate e tempo a disposizione.

Per fare un esempio concreto, molte organizzazioni, specialmente piccole e medie imprese, affidano completamente la gestione della cybersecurity aziendale a un Managed Security Service Provider (MSSP) esterno. Affidarsi a un MSSP presenta sicuramente dei vantaggi notevoli in termini di costo e opportunità: gli MSSP eliminano la necessità di assumere e formare dipendenti a tempo pieno, di acquistare e mantenere l'infrastruttura necessaria, e offrono spesso servizi di monitoraggio 24 ore su 24 e 7 giorni su 7. Tuttavia, è molto probabile che una scelta di questo tipo porti a una perdita (almeno parziale) di controllo sulla propria postura cyber, e alla creazione di un rapporto di dipendenza dal proprio provider, che potrebbe risultare problematico in caso di interruzioni del servizio e potenzialmente lasciare l'organizzazione vulnerabile in situazioni critiche. Non è un caso che le organizzazioni più mature stiano muovendo sempre più verso un modello solo parzialmente esternalizzato, in cui l'organizzazione combina le proprie risorse interne con quelle di un MSSP. Di solito, in tale modello l'MSSP fornisce analisti di livello base, con formazione quasi esclusivamente tecnica, mentre l'organizzazione forma specialisti interni con una conoscenza profonda dei propri modelli di business. Per quanto risulti tipicamente più costoso di un'esternalizzazione completa, tale modello consente comunque di mantenere un buon bilanciamento di flessibilità, risparmio sui costi e controllo sulla propria postura cyber.

Per rimanere sul tema, un progetto cyber le cui tempistiche sono tipicamente sottostimate è l'implementa-

zione di un approccio Zero Trust. Lo Zero Trust è un approccio che presuppone che una rete sia sempre sotto attacco, e che nessun utente o dispositivo debba essere considerato automaticamente attendibile, indipendentemente dalla posizione o dal livello di accesso. Ai fini della corretta implementazione dell'approccio Zero Trust è necessario un rigoroso lavoro di identificazione di tutte le risorse aziendali a rischio (per esempio, dispositivi, utenti e applicazioni) e di classificazione degli stessi in base al loro livello di rischio. Solo una volta identificate e classificate le risorse sarà possibile stabilire criteri che limitino l'accesso a informazioni sensibili. Ovviamente, tale processo può richiedere molto tempo, sia in fase iniziale sia di aggiornamento continuativo. Sottovalutare il tempo necessario per il completamento dell'inventario – o peggio ancora procedere con un inventario parziale a causa di tempi ristretti – può vanificare del tutto gli sforzi collegati all'implementazione di questo approccio.

SECONDO MINDSET CERCHIAMO DI NON CAMBIARE TROPPO IL MODO IN CUI LAVORIAMO

Il secondo mindset, anch'esso molto diffuso, assimila la cybersecurity a una tematica di natura esclusivamente tecnica/tecnologica, quando essa include anche e soprattutto persone e processi. L'adozione di tecnologie di sicurezza è sicuramente un elemento fondamentale per raggiungere un livello di maturità cyber soddisfacente; tuttavia, altrettanto importante è il contributo fornito dalla definizione (e dalla messa in atto concreta) di policy, procedure e linee guida. Inoltre, la cybersecurity non riguarda solo la prevenzione degli attacchi, ma anche la gestione del rischio. Ciò implica che la cybersecurity debba essere trattata come un problema di business e non solo come un problema IT, e che venga percepita come tale da tutte le parti interessate all'interno dell'organizzazione. Perché questo accada, è inevitabile che diversi cambiamenti importanti abbiano luogo.

Uno dei principali ha a che fare con l'organigramma aziendale. Per anni, la responsabilità della cybersecurity è stata attribuita al Chief Information Security Officer (CISO). A dispetto della C nell'acronimo, il CISO è raramente un membro della senior leadership aziendale, e più di frequente il riporto (o il riporto di un riporto) di un top manager. Questa collocazione ha delle profonde implicazioni sulla capacità del CISO di coordinarsi con la senior leadership per garantire che la cybersecurity sia integrata in ogni aspetto della strategia aziendale. Il CISO spesso manca dell'autorità e del supporto necessari per rendere l'attuazione di una strategia di cybersecurity una priorità. Dal canto suo, il CISO moderno necessita di una formazione tale da poter esporre i rischi cyber più rilevanti per l'organizzazione in un linguaggio che risulti comprensibile al top management – una formazione che spesso è ancora carente.

Una mancanza di allineamento da entrambi i lati può facilmente portare al fallimento di approcci di cybersecurity più avanzati come il *Security-by-Design*. Il Security-by-Design comporta l'integrazione della cybersecurity in ogni fase del processo di sviluppo di un prodotto/servizio; ciò significa considerare i requisiti di cybersecurity fin dalle prime fasi di progettazione, e testarli e perfezionarli continuamente durante l'intera vita utile del prodotto/servizio. Perché questo sia possibile, è necessario che i business process owner siano pienamente consapevoli di queste esigenze e disposti ad assumersi la gestione dei rischi cyber collegati. Senza sufficiente supporto da parte della senior leadership, è quasi matematico che ciò non accada, considerate le dilatazioni in termini di budget e di tempistiche che questo cambiamento per forza di cose comporta e il cumulo di responsabilità addizionali.

TERZO MINDSET UN'ASSICURAZIONE OFFRIREBBE LO STESSO SERVIZIO

Questo mindset fa leva sull'assunto che di per sé la cybersecurity non crea alcun valore aggiunto, ma è semplicemente un mezzo per prevenire possibili incidenti. Tuttavia, il ragionamento ha diverse falle alla base. *In primis*, da un punto di vista di copertura globale, un'assicurazione cyber può coprire i costi finanziari diretti relativi a un incidente, ma non le conseguenze secondarie, come per esempio eventuali danni reputazionali, interruzioni del servizio o perdite di clienti. In secondo luogo, stipulare una polizza di assicurazione cyber sta diventando sempre più difficoltoso. In virtù del drastico aumento di attacchi cyber negli ultimi anni, sempre meno assicuratori sono disposti a coprire interamente il portafoglio di rischi cyber di un'organizzazione, e in ogni caso a prezzi significativamente più elevati che in passato. Terzo, la maggior parte delle compagnie assicurative richiede comunque ai propri clienti di dimostrare di aver adottato misure preventive per ridurre il rischio di attacchi cyber prima di emettere una polizza. Negli ultimi anni è diventato sempre più comune che le compagnie assicurative si affidino a società esterne di valutazione della cybersecurity per ottenere un'idea generale della postura cyber di un potenziale cliente e capire se e in che misura offrire una polizza adeguata.

L'assicurazione può perciò essere una componente importante della gestione del rischio cyber complessiva di un'organizzazione, ma non può sostituire l'implementazione di adeguate misure di cybersecu-

rity. Al di là del discorso assicurazione, esistono poi almeno altre due ragioni per cui la cybersecurity non può essere assimilata semplicemente a uno strumento di prevenzione incidenti. Il primo è che sempre più stati stanno vincolando aziende e settori industriali a regolamenti e standard di sicurezza informatica. In Europa il Regolamento Generale sulla Protezione dei Dati (GDPR) è sicuramente l'esempio più lampante, così come negli Stati Uniti il Cybersecurity Maturity Model Certification (CMMC), richiesto a qualunque fornitore del Dipartimento della Difesa. È ragionevole supporre che questa tendenza prosegua nel corso dei prossimi anni, sia a livello nazionale sia di singolo settore. Tornando in Europa, la direttiva Network and Information Security 2 (NIS 2) – adottata dal Consiglio Europeo nel novembre 2022 – amplierà l'ambito della precedente direttiva NIS dalle sole entità Critiche[3] alle cosiddette entità Essenziali[4] e Importanti[5]. A seconda di come verrà recepita nelle varie legislazioni nazionali, la direttiva NIS 2 potrebbe finire per includere la maggior parte delle aziende europee medio-grandi, col risultato di vincolarle al rispetto di requisiti di cybersecurity che sarà molto difficile da rispettare per quelle che oggi partono da un livello di maturità più basso.

Inoltre, in un certo senso la cybersecurity sta effettivamente diventando un mezzo per ottenere un vantaggio competitivo. Soprattutto per quanto riguarda quei prodotti e servizi dove il consumatore medio è consapevole dei possibili rischi cyber (per esempio, la privacy nei prodotti per la *smart home*), la garanzia del rispetto di standard di sicurezza adeguati può effettivamente garantire la conquista di una fascia della clientela particolarmente interessata a questa tematica.

© ISTOCK - SORBETTO

QUARTO MINDSET
OK, FACCIAMO QUESTA CYBERSECURITY... INTERNAMENTE

Per certi versi, questo mindset è forse meno pericoloso dei precedenti, ma presenta comunque delle criticità. Sicuramente, la protezione del perimetro aziendale classico è fondamentale; altrettanto sicuramente, iniziative di training e awareness dei dipendenti restano una delle armi più efficaci contro il rischio cyber, visto che oltre il 40 per cento degli attacchi cyber andati «a buon fine» nel 2022 ha usato una semplice e-mail di phishing come vettore iniziale di infezione.

Tuttavia, la cybersecurity oggi non è solo rivolta verso l'esterno, anzi. Fra gli attacchi cyber di maggior rilevanza avvenuti nell'ultimo anno diversi hanno avuto origine in un punto esterno all'azienda: per la precisione, in un servizio di terze parti (si veda, per esempio, il caso SolarWinds). La gestione della cybersecurity delle terze parti purtroppo fa parte di quelle sfide «endemiche» che oggi non dispongono di una soluzione universalmente efficace, e anche aziende con un livello di maturità cyber elevato faticano a trovare un giusto compromesso tra requisiti di sicurezza da imporre ai propri fornitori e necessità di tenerli comunque a bordo per esigenze di business. Tuttavia, a livello di mindset è importante quantomeno iniziare a pensare in quest'ottica, e capire quali sono i fornitori critici a cui sarà necessario richiedere (e verificare) la presenza di requisiti di cybersecurity di un certo livello. In futuro, è molto probabile che l'adesione a clausole di compliance cyber diventi un elemento cruciale nel processo di procurement aziendale.

Spesso sottovalutata, soprattutto nel contesto nazionale, è anche l'importanza della condivisione di informazioni di cybersecurity fra diverse organizzazioni. Storicamente, la natura confidenziale delle informazioni coinvolte e la paura di svelarne qualcuna inavvertitamente hanno reso le organizzazioni scettiche su questa pratica. Tuttavia, la condivisione delle informazioni in ambito cyber si è già dimostrata efficace in diverse occasioni. Ai fini della scomparsa di questo mindset gioca (e ragionevolmente giocherà in futuro) un ruolo molto importante l'Agenzia per la cybersicurezza nazionale, istituita nel 2021 e avente fra i suoi obiettivi quello di favorire la comunicazione e la cooperazione rispetto ai temi cyber anche nel settore privato.

CONCLUSIONI

Le sfide presentate dai mindset analizzati finora sembrano indicare uno scenario a tinte fosche e forse leggermente demoralizzante. Ma anche questo può servire a comprendere la cybersecurity. Nei fatti, ad essere brutalmente onesti, la cybersecurity aziendale è in un certo senso demoralizzante (la parte divertente al massimo è di dominio degli hacker).

L'introduzione di una funzionalità smart, come per esempio il controllo remoto della chiusura di una persiana, è intrigante perché porta con sé un senso di novità, a prescindere dalla sua effettiva utilità. L'installazione di un'inferriata per difendersi da potenziali ladri difficilmente fa lo stesso effetto, e anzi fa sentire rinchiusi in una gabbia (una frustrazione condivisa da tutti i dipendenti che hanno visto il *firewall* aziendale bloccare l'accesso a siti per loro di comune utilizzo, da quello che consente di unire due file .pdf gratuitamente al servizio di traduzione con cui leggere l'ultima policy aziendale emessa solo in inglese). Però, a differenza della persiana smart, l'inferriata è davvero utile per chi vive al piano terra.

Per molti, purtroppo, la comprensione che l'inferriata è necessaria arriverà troppo tardi, dopo essersi ritrovati i ladri in casa. Chiunque voglia evitare di ritrovarsi in questa situazione deve assolutamente superare i mindset menzionati sopra. La cybersecurity oggi è necessaria, così come è necessario fare cambiamenti importanti per implementarla in concreto, e supportarla organicamente e con continuità per darle il tempo di portare i suoi frutti, soprattutto perché a prima vista potrebbero sembrare invisibili. Inoltre, bisogna accettare l'idea che la cybersecurity non sia più uno sforzo individuale come in passato, ma uno che è tanto più di successo quanto più è partecipato.

Evitare le mentalità elencate sopra mette al sicuro da potenziali cyber attacchi? No. Ma ci permette di trasferirci al primo piano, dove molti ladri sono troppo pigri per arrivare. E per fortuna, al momento sono la maggioranza.

[1] *Adattato da NISTIR 8286.*
[2] *Adattato da NIST SP 800-60 Vol. 1 Rev. 1.*
[3] *Organizzazioni che forniscono servizi essenziali per il funzionamento della società e dell'economia.*
[4] *Organizzazioni che svolgono attività che possono avere un impatto significativo sul funzionamento delle entità critiche o sulla salute e sicurezza delle persone.*
[5] *Organizzazioni che svolgono attività che potrebbero avere un impatto significativo sulla fornitura di servizi essenziali o sull'economia in generale.*

IN SINTESI

- Investire in cybersecurity è oggi, per tutte le aziende, un'iniziativa irrinunciabile. I rischi di questo mancato investimento sono sicuramente più alti rispetto ai benefici.
- Tuttavia, nonostante si conoscano i risultati devastanti di un attacco hacker, sussistono forme di resistenza mentale all'utilizzo di sistemi di cybersecurity.
- La cybersecurity non può essere semplicemente esternalizzata o sostituita da un'assicurazione sui rischi cyber: è fondamentale acquisire competenze e sviluppare consapevolezza rispetto al tema all'interno dell'organizzazione, se non lo si è ancora fatto.