La sicurezza delle informazioni non è un’opportunità

In molti, per promuovere la sicurezza, la definiscono una risorsa o un’opportunità. Non lo è, e questo approccio danneggia proprio chi vuole promuovere la sicurezza.

Cosa non è la sicurezza delle informazioni

Nessuno dice che le cinture di sicurezza in automobile o il casco in moto sono una risorsa o un’opportunità. Eppure, si è affermata l’idea che la sicurezza informatica lo sia. O, meglio, si è affermata l’idea che per “vendere” la sicurezza informatica ai dirigenti di un’organizzazione sia importante presentarla come tale.

La sicurezza è un costo e riduce l’efficienza di alcuni lavori. **Non dobbiamo negarlo**. Acquistare un buon firewall costa almeno 500 euro; se deve essere ridondato, la cifra raddoppia; se poi bisogna installarlo e configurarlo, il costo cresce ancora.

Se ne avesse la possibilità, nessuno attuerebbe alcuna misura di sicurezza, neanche gli stessi consulenti che la vendono (per dimostrarlo, basterebbe vedere quanti di loro hanno impostato un qualche controllo accesso sul loro smartphone o tablet, o quanti usano uno schermo oscurato sui mezzi pubblici).

Sono numerosi gli articoli che parlano di sicurezza informatica e opportunità; ma, a ben vedere, solitamente il messaggio è che l’opportunità è proprio quella di prevenire gli attacchi o ridurne gli impatti. **Per un’azienda, però,**

un’opportunità è un’altra cosa: è la possibilità di aumentare i ricavi o ridurre i costi di produzione.

L’origine di questo malinteso è che “opportunità” è letto come l’inverso di “rischio” e, seguendo le risibili deformazioni del “politicamente corretto” (o dell’ “aziendalese”), alcuni hanno preferito usare un termine meno negativo.

Gli unici che dicono che la sicurezza è un’opportunità sono quelli che vogliono venderla (a clienti interni o esterni), non quelli che la attuano o che devono applicarla.

Perché è un errore parlare di opportunità

Se non si chiamano le cose con il loro nome, si viene fraintesi.

Un dirigente di un’azienda vede i costi – e l’onere organizzativo – che la sicurezza comporta. Se qualcuno sente freddo anche se la temperatura è di 40°C, non lo si riscalda dicendogli che in realtà fa caldo. A maggiore ragione, se un dirigente vede la fatica che la sicurezza comporta, non lo si convince dicendogli che è un’opportunità.

Dire che è un’opportunità mette subito l’interlocutore in un **atteggiamento difensivo**, visto che riconosce immediatamente la falsità dell’affermazione. In altre parole: si ottiene l’inverso di quello che ci si proponeva (ossia, convincerlo dell’importanza della sicurezza).

Il fatto poi che la frase fatta “la sicurezza è un’opportunità” sia usata solo dai sedicenti esperti ha un altro effetto: sposta l’argomento nell’area dell’autoreferenzialità degli esperti, lontano da chi di mestiere fa tutt’altro.

Parliamo degli attacchi? O è meglio di

no?

Un metodo molto diffuso per sensibilizzare i vertici di un'organizzazione consiste nell'elencare incidenti che hanno avuto elevati impatti.

Il rapporto Clusit del 2017 riporta i "10 attacchi rappresentativi del 2016" (nell'edizione del 2018 questa analisi non è presente): a un ospedale, a una piattaforma social di appuntamenti, a una banca del Bangladesh e una britannica, a una società produttrice di smartphone, a un sistema di trasporto pubblico, ai Democratici USA, a Yahoo!, a un provider di servizi DNS e al Ministero degli esteri italiano, quasi tutti basati su tecniche "multiple".

Quanti si possono riconoscere negli esempi? Molti pensano, giustamente, che la loro organizzazione non sia esposta come quelle che hanno subito gli attacchi, che i loro dati non siano particolarmente appetibili o che i loro sistemi informatici non siano esposti come quelli attaccati. Insomma, come spesso succede, tutti pensano di essere un caso diverso dagli altri.

Altro punto da considerare, dal rapporto del Clusit del 2018: nella prima metà del 2018 erano stati registrati 730 attacchi, di cui quasi il 30% di origine sconosciuta e il 40% da malware (per cui, per proteggersi, è sufficiente l'antivirus). Diventa difficile convincere un'organizzazione che sarà proprio lei ad essere vittima del restante 30% dei casi.

Il continuare a elencare gli attacchi da prima pagina provoca **un ulteriore effetto indesiderato:** porta a concentrare tutta l'attenzione sulle funzionalità e i sistemi esposti verso l'esterno e non a tutti gli altri. Da qui hanno origine la scorretta gestione, per esempio, degli amministratori di sistema e del BYOD.

Sicuramente è importante ricordare gli attacchi informatici

dall’esterno, ma non concentrarsi solo su di essi (dimenticando anche la sicurezza delle informazioni su supporto non informatico).

Di cosa parlare, allora?

La sicurezza delle informazioni è materia di consulenti, interni o esterni: infatti è un servizio di supporto per ogni organizzazione. Una delle regole della consulenza è che il consulente deve essere totalmente onesto con il proprio cliente, altrimenti perde credibilità.

Con questa premessa, la regola si esprime immediatamente: bisogna dire che la sicurezza delle informazioni va pianificata e realizzata **perché è necessaria per proteggere le risorse dell’organizzazione**, inclusa la sua immagine, **e perché richiesto dalla normativa vigente** e che questo comporta costi diretti (soldi) e indiretti (inefficienze, tempo da dedicare e malcontenti).

Bisogna far capire perché la sicurezza delle informazioni è utile, non perché è bella, visto che non lo è. Bisogna dire che non porta benefici, ma “solo” protezione da potenziali danni.

Elencare alcuni casi di incidenti da attacchi informatici dall’esterno è sicuramente utile, evitando però casi troppo lontani dall’interlocutore (la recente violazione di dati personali della catena alberghiera Marriott potrebbe non convincere la dirigenza di una società di ricerche di mercato o di erogazione di servizi informatici di medie dimensioni).

Forse possono essere ricordati alcuni casi molto comuni e appartenenti alla vita quotidiana, anche se spesso indegni delle prime pagine dei giornali: per esempio gli errori, i clic sbagliati e la superficialità di cui tutti sono stati, almeno una volta, testimoni.

Un esempio semplice è quello del programmatore che scrisse

“googleaspis” al posto di “googleapis” in una pagina web, creando non pochi problemi.

Nota personale

Dell’importanza dell’onestà per i consulenti, in realtà, ne parlano in pochi. Io l’ho sempre pensato, grazie agli ottimi maestri che ho avuto. Per iscritto, ho trovato il concetto nel seguente libro: Peter Block, *Flawless Consulting: A Guide to Getting Your Expertise Used*. 2nd ed. USA, Pfeier, 2000.

Articolo a cura di **Cesare Gallotti**



Lavora dal 1999 nel campo della sicurezza delle informazioni, della qualità e della gestione dei servizi IT.

Ha condotto progetti di consulenza per la pubblica amministrazione e per il settore privato. Opera, sia in Italia che all’estero, come Lead Auditor ISO/IEC 27001, ISO 9001, ISO/IEC 200000 e ISO 22301. Ha progettato ed erogato corsi di Quality Assurance e di certificazione Lead Auditor ISO/IEC 27001 e ITIL Foundation.

Tra gli attestati si segnalano: le certificazioni AICQ SICEV Lead Auditor ISO/IEC 27001, IRCA Lead Auditor 9001, CISA, ITIL Expert e CBCI, la qualifica come Lead Auditor ISO/IEC 20000 e il perfezionamento postlaurea in “Computer Forensics e investigazioni digitali”.

E’ capodelegazione del WG1 del comitato italiano ISO/IEC SC27 in UNINFO.

Ha pubblicato il libro, aggiornato nel 2017, “Sicurezza delle informazioni: valutazione del rischio; i sistemi di gestione; la norma ISO/IEC 27001:2013”.

Cura la pubblicazione, dal 2008, della newsletter “IT Service management news”

(http://www.cesaregallotti.it/Newsletter.html).

Web: www.cesaregallotti.it; Blog: blog.cesaregallotti.it

https://www.ictsecuritymagazine.com/articoli/la-sicurezza-delle-informazioni-non-e-unopportunita/