La governance della cybersecurity: una necessità inderogabile

A colloquio con Alberto Redi, Managing Partner di Security Lab Sagl - da più di dieci anni azienda di riferimento in Ticino per i servizi di cybersecurity - e Siro Migliavacca, General Manager di Security Lab Advisory Sagl, nata recentemente dal team di management consulting di Security Lab Sagl.

Alberto Redi, qual è il contesto di rischio Cyber per le aziende?
Gli attacchi informatici, sempre più diffusi, coinvolgono indistintamente tutte le aziende e possono essere sia mirati e focalizzati, sia massivi e generalizzati. I dati, le informazioni e i sistemi informatici - importanti per la vita di ogni azienda - sono costantemente sotto minaccia; ciò aumenta il pericolo di furti patrimoniali, richieste di riscatto, spionaggio industriale, pubblicazione su internet di dati riservati, manomissione dei sistemi ed interruzione dei processi aziendali, con il rischio di pesanti ricadute sull'erogazione dei prodotti e dei servizi ai clienti.

Il Cybercrime è quindi diventato un vero e proprio mercato parallelo?
Certamente! Il cybercrime è diventato un vero e proprio business e gli hacker operano sia autonomamente che su commissione, al fine di rivendere i dati rubati e di prestare servizi a coloro che chiedono di colpire particolari obiettivi. Questo mercato del crimine sta causando danni patrimoniali e reputazionali sempre più elevati.

In questo contesto, come si stanno muovendo gli organismi regolatori?
Con l'aumentare della pervasività delle tecnologie internet, dei collegamenti e delle interconnessioni tra organizzazioni, il rischio cyber cresce anche a livello infrastrutturale e di sistema: per questo gli enti legislativi e regolatori hanno recentemente emanato nuove normative in materia di sicurezza dei dati e dei sistemi informatici, in modo da costringere tutte le organizzazioni a far evolvere il proprio sistema di difesa. Si consideri, per esempio, il nuovo Regolamento europeo per la protezione dei dati personali (Gdpr 2016/679) ed i recenti aggiornamenti delle circolari della Finma (Autorità federale di vigilanza sui mercati finanziari) per ciò che riguarda la gestione del cyber risk e la sicurezza dei servizi in outsourcing, nell'ambito della gestione dei rischi operativi.

Siro Migliavacca, cosa stanno facendo le aziende per rispondere ai crescenti pericoli derivanti dal cybercrime?
Molte aziende sono ancora ad un livello minimo di gestione della sicurezza: adottano soltanto le tecnologiche di sicurezza di base, dispongono di un sistema di backup dei dati, controllano i permessi di accesso ai dati e ai sistemi informativi e poco più. Tutto questo oggi non basta, e di fronte alla necessità di far evolvere il loro sistema di sicurezza, spesso non sanno cosa fare, da che parte iniziare.

Quali indicazioni si possono dare alle aziende?
Noi suggeriamo di fare riferimento agli standard internazionali e alle best practices accreditate. In particolare, per la protezione dei dati e la realizzazione di un modello di cybersecurity governance, allo standard Iso 27001 e al Cybersecurity Framework del Nist, istituto Usa di normazione in tema di security. Tuttavia, tali standard non fanno particolari distinzioni tra aziende con caratteristiche diverse; pertanto, il nostro compito consiste nel dare supporto affinché tali standard vengano applicati 'cum grano salis', facendo attenzione a costruire un abito su misura, coerente con le capacità di investimento e le reali esigenze dell'azienda. In questo modo evitiamo che il management si blocchi di fronte al timore che sia troppo oneroso, o complesso, far evolvere il sistema di sicurezza aziendale!

Potrebbe illustrarci, più in dettaglio, quali sono i passaggi da effettuare?
Innanzitutto, è opportuno iniziare il progetto evolutivo avendo la giusta consapevolezza su quali siano effettivamente il livello di sicurezza raggiunto e il livello di rischio al quale si è ancora esposti. Per questo motivo, il nostro approccio di consulenza prevede una fase iniziale di assessment, attraverso specifiche attività di security audit, per la valutazione del livello di sicurezza dell'ambiente tecnologico e l'individuazione delle vulnerabilità presenti, e di gap analysis normativa e organizzativa, per valutare il livello di adeguatezza delle contromisure adottate e del processo di gestione della sicurezza applicato. Raggiunta la conoscenza dello stato dell'arte, definiamo il piano degli interventi necessari per adeguare le misure di sicurezza e far evolvere il sistema di gestione.

Dopo aver definito questo piano di intervento, che cosa accade?
L'azienda realizzerà il piano, autonomamente o richiedendo il nostro supporto. Si preoccuperà di mantenere con continuità i corretti livelli di sicurezza, considerando con la dovuta attenzione le novità che interverranno sia nello scenario esterno (nuovi rischi e nuove normative), sia nel contesto organizzativo interno; inoltre, applicherà un processo ciclico di cybersecurity governance. Gestendo in modo ottimale i rischi, l'azienda potrà non da ultimo rispondere al meglio alle sempre più stringenti richieste provenienti dal mercato: molti clienti, grandi aziende e multinazionali, chiedono infatti ai loro partner di adottare modelli di security governance che garantiscano la continuità dei servizi e tutelino la catena di fornitura. A tal fine, alcune aziende ci chiedono anche di accompagnarle nel percorso di certificazione Iso 27001 del sistema di gestione della cybersecurity che abbiamo costruito insieme, per avere un attestato ufficiale, valido a livello internazionale.

Per maggiori informazioni potete contattare:
Simona Galli di AITI Servizi
Tel. 091/911 84 72
simona.galli@aitiservizi.ch
www.aitiservizi.ch