TECNOLOGIA E NUOVE MINACCE PER LE AZIENDE

GLI ATTACCHI INFORMATICI PRESENTANO ASPETTI CRITICI, CHE POSSONO RIVELARSI DEVASTANTI, IN TERMINI DI INTERRUZIONE DELL'EROGAZIONE DEL SERVIZIO E DI MODIFICA DELL'ASPETTO DEI CONTENUTI. IN MOLTI CASI, PERSINO UNA RIGOROSA POLITICA DI SICUREZZA PUÒ RIVELARSI INSUFFICIENTE

Tra i principali rischi emergenti, vista la crescente digitalizzazione, non può mancare il *cyber risk*, dove le minacce sono di vario tipo: dalla perdita di informazioni su un unico *laptop* ai pericoli derivanti dall'uso del *cloud computing*. "I presidi aziendali dell'*IT security* – afferma **Marco Dalle Vacche**, general manager di **Aig** – non sono sufficienti per far fronte ad attacchi tecnologici divenuti, oggi, sempre più raffinati. La parte più critica è rappresentata dal *denial of service* (interruzione dell'erogazione del servizio) o dal *defacement* (modifica dell'aspetto o dei contenuti). L'**80%** dei tentativi di attacco quotidiani ha un impatto trascurabile che può essere risolto o arginato attraverso una solida politica di sicurezza; ma nel **18%** dei casi, le minacce alla sicurezza informatica di un'azienda richiedono l'adozione di misure di protezione più diversificate e flessibili; infine, il 2% delle minacce è costituito da attacchi ingegnosi e mirati".

GENNAIO 2013: ATTACCO HACKER AL TRIBUNALE DI MILANO

Il sito del Tribunale di Milano è stato oggetto di attacco: al posto dell'homepage è stata visualizzata un'immagine che riportava il messaggio *Hacked by LndTm 2013 Italian crew (cioè Formazione italiana),* una maschera tricolore di V for Vendetta, usata solitamente da Anonymous. Sotto l'immagine la scritta *preparatevi ha inizio l'Apocalisse! È la fine per un nuovo inizio. Sta arrivando come l'ira di Dio il vero cambiamento per i giovani.*
Fortunatamente non sembrerebbero essere state violate le banche dati del tribunale, ma è comunque percepibile la pericolosità di un simile episodio.

ATTACCHI PER TIPOLOGIA	2011	2012	TOTALE	INCREMENTO
CYBERCRIME	170	633	803	+372,35%
UNKNOWN	148	110	258	-25,68%
HACKTIVISM	114	368	482	+322,81%
ESPIONAGE/SABOTAGE	23	29	52	+126,09%
CYBER WARFARE	14	43	57	+307,14%
TOTALE	469	1183	1652	+252,24%

Fonte: *Aig*

Nel cyber l'aspetto importante è la prevenzione: come il servizio di *loss prevention* offerto da Aig, che istruisce l'azienda, prima che avvenga il sinistro, su come contenere la crisi e prevenire il danno.

LA GESTIONE DELL'EMERGENZA

Fondamentale è che la divisione IT affronti l'emergenza senza interrompere la normale attività. "In questo frangente – spiega Dalle Vacche – è necessario capire se si è trattato di una fuga di informazioni, di una perdita di dati o di un attacco *hacker*; in che modo i dati sono stati smarriti o sottratti; dove si trovano le informazioni; se il team IT è in grado di limitare i danni; se è necessario spegnere il server o sostituirne il software; se è stato messo a punto un *disaster recovery plan* per il ripristino dei servizi informatici e in che modo sarà attuato".
Molto importante è anche l'impatto verso l'esterno. "Nell'era dei *social media*, la notizia di una fuga di informazioni si diffonde rapidamente e la fiducia di cui gode l'azienda può sgretolarsi nel giro di poche ore. La situazione deve essere gestita con cautela, tenendo presente i mezzi di informazione, i clienti, il personale, i soci/azionisti, i creditori e chiunque abbia un interesse nella società: è necessario valutare se informare o meno i clienti dell'accaduto, con quale modalità di comunicazione, cercando di riconquistare la fiducia e tutelare la reputazione dell'azienda".

LE CONSEGUENZE ECONOMICHE

È possibile, poi, che i soggetti di cui, eventualmente, si sono persi i dati, decidano di adire le vie legali. "Sono tutti costi che si sommano a quelli sostenuti per individuare l'origine della perdita o della violazione dei dati, riconfigurare le reti, ristabilire la sicurezza e ripristinare dati e sistemi. E, mentre l'attività dell'azienda è potenzialmente bloccata, gli utili dell'azienda potrebbero calare o azzerarsi, senza dire che la compromissione della sicurezza informatica può incidere in maniera significativa sul prezzo delle azioni e ripercuotersi gravemente sulla reputazione dell'azienda".
La soluzione *Cyberedge* di Aig mira a contrastare questa sorta di effetto domino avvalendosi di esperti in *incident response* (gestione degli incidenti informatici) e consulenti legali in grado di fornire un supporto nella gestione delle pubbliche relazioni oltre a servizi di *coaching* in materia di violazione della sicurezza informatica, abbinando la copertura assicurativa tradizionale a servizi di consulenza professionale.

L.S.

AZIENDE ALL'ESTERO, IL VERO PERICOLO È POLITICO

Secondo **Aon**, l'emergenza è sul rischio politico. "Il vero danno emergente – conferma **Michele Ungaro**, vice direttore generale Aon – è il rischio politico, cui sono esposte le aziende italiane che operano all'estero. Se il rischio terrorismo può essere trasferito, seppur con dei limiti, nelle polizze più classiche, sul rischio politico c'è poca informazione".
Annualmente, Aon realizza una mappa che indica la rischiosità dei diversi Paesi. "Un'azienda italiana che opera in realtà dove vi è una situazione politica a rischio, deve conoscere e valutare quale sia il rischio politico a cui va incontro e avere la possibilità di assicurarsi: ad esempio, sono assicurabili, la chiusura dei confini, la confisca o la nazionalizzazione del progetto (raffineria, diga o metropolitana) o del concessionario, la mancanza di manodopera a causa di epidemia, il cambio della normativa, l'impossibilità di convertire nella propria valuta la moneta locale con cui si viene pagati, fino all'esclusione ingiustificata delle garanzie prestate nello svolgimento dei lavori".
Il *Team Aon Crisis Management* è in grado di supportare e assistere le aziende clienti da tutti quei rischi cui si trovano esposti i loro lavoratori e rappresentanti quando operano in Paesi stranieri. "Si tratta di una combinazione tra polizze assicurative, procedure comportamentali da tenere durante il viaggio/permanenza nel Paese, e servizi di assistenza in loco".
Il valore dell'offerta di Aon sta nell'aiutare le aziende clienti a quantificare la propria esposizione e a prendere decisioni consapevoli ed efficaci per gestire e ridurne l'impatto. "La nostra *expertise* aiuta l'assicurato a proteggere il business anche all'estero, con specifiche coperture assicurative e servizi, per evitare che queste siano compromesse da azioni del governo in cui si opera o da terzi, causando un sensibile aumento dei costi, penalità, chiusure forzate o perdite di profitti".