PERRY JOHNSON REGISTRARS, INC.

Resilienza Aziendale con la Sicurezza Informatica

La crescente importanza alla tutela dell'azienda e dei suoi clienti dalle minacce alla sicurezza informatica è ormai evidente. Che si tratti di attacchi ransomware o di furto di dati personali, gli hacker e altri criminali informatici possono facilmente raggiungere il mondo intero e danneggiare un'azienda senza doversi spostare. Oltre alla relativa facilità di questi attacchi, sfruttare eventuali falle nella sicurezza informatica può rivelarsi incredibilmente redditizio e veloce. Rispetto, ad esempio, al furto di una carta di credito dal portafoglio (che viene prontamente rilevato e bloccato), il furto di informazioni personali via Internet può consentire al ladro di ottenere l'emissione di nuove carte a suo nome o, più in generale, di prendere di mira un database contenente migliaia e migliaia di nomi di clienti e informazioni sulle carte di credito. Poiché quasi tutte le aziende hanno a che fare con informazioni sensibili, in un modo o nell'altro, è importante che gli operatori di ogni settore sappiano difendere se stessi e i propri clienti investendo nella sicurezza informatica.

Le misure per la sicurezza informatica rispondono alle minacce contro le risorse e i sistemi informatici in tre aree: riservatezza, integrità e disponibilità. La riservatezza comprende i metodi con cui le risorse e i sistemi sono disponibili solo ai soggetti autorizzati, e protetti da chi non dispone delle autorizzazioni necessarie. L'integrità riguarda la completezza, l'accuratezza e l'aggiornamento delle risorse e dei sistemi. Infine, la disponibilità comprende la disponibilità degli asset e dei sistemi necessari ai soggetti autorizzati, in qualsiasi momento e secondo le necessità.

Come per tutti i sistemi che mirano a ridurre i rischi relativi a perdite o guasti, la definizione di un piano per la sicurezza informatica inizia con un'accurata valutazione dei rischi. L'identificazione delle misure da implementare, e la relativa intensità, costituiscono le fondamenta del sistema da costruire. Valutare le minacce e le vulnerabilità dell'organizzazione - porre domande del tipo chi, cosa, perché e come: "Chi potrebbe prenderci di mira?" "Cosa prenderanno di mira? "Come raggiungeranno il loro obiettivo? Le risposte a queste domande possono contribuire ad individuare i punti deboli. È importante ricordare che anche i requisiti normativi o contrattuali possono influenzare le vostre priorità nell'identificazione dei rischi; assicuratevi di esserne consapevoli e di tenerli in considerazione.

Una volta individuati i rischi, è possibile intervenire in modi diversi:

- **Trattando** il rischio, è possibile implementare delle misure per ridurre la probabilità o l'impatto del rischio in questione.
- **Eliminando** il rischio, lo si elimina alla fonte.
- **Trasferendo** il rischio, si trasferisce la responsabilità dello stesso a un'altra parte, come accade in caso di esternalizzazione a terzi o di stipula di un'assicurazione.
- **Tollerando** il rischio, si sceglie di mantenerlo, ad esempio perché non esiste un modo efficace per trattarlo o perché il rischio viene considerato accettabile.

Poiché non è possibile garantire al 100% l'efficacia delle misure adottate ogni volta che si presenta una minaccia, il rischio trattato va comunque considerato un rischio attivo: non è stato eliminato, ma semplicemente reso meno probabile o meno dannoso. Un approccio più articolato può aiutare a risolvere le "falle del sistema", per così dire, offrendo una protezione più sfumata e stratificata. In teoria, ogni parte del piano dovrà presentare una serie di sfide che eventuali malintenzionati dovranno superare, piuttosto che contare su un unico sistema di protezione. Un piano di sicurezza è forte quanto il suo anello più debole; individuate e rafforzate questo punto, a seconda delle tipologie di attacchi più probabili, e contribuite a ridurne i rischi.

Oltre che alle tre facce della sicurezza (riservatezza, integrità e disponibilità), è necessario considerare i tre fattori della difesa su cui occorre intervenire: persone, processi e tecnologia. Di solito, un'organizzazione tende a concentrarsi esclusivamente sull'implementazione di soluzioni tecnologiche o software, trascurando la componente umana dell'infrastruttura relativa alla sicurezza. I programmi e l'hardware coinvolti vanno implementati e mantenuti da persone; non dimentichiamolo! Altrettanto importanti sono i processi, seguiti dalle persone che si occupano della sicurezza. È fondamentale che questi siano accurati e solidi, documentati e regolarmente programmati. Infine, la tecnologia è la più ovvia delle tre, anche se imperfetta e legata al fattore umano.

La resilienza comprende anche la capacità di gestire gli incidenti che si verificano, e nella sicurezza informatica il primo passo per farlo è rilevare eventuali violazioni. Le misure di rilevamento rientrano in tre categorie:

- Il rilevamento pre-incidente può essere considerato una forma di prevenzione, che consiste nell'adottare precauzioni adeguate prima che possa aver luogo un attacco. Tra le misure adottate, si possono citare la scansione delle vulnerabilità o i test di penetrazione.
- l rilevamento in tempo reale interviene quando vengono meno le misure preventive, e l'attacco va a segno. In questa categoria rientrano le notifiche automatiche, l'allarme generato da una porta violata e altre forme di avviso.
- Sfortunatamente, è molto comune il rilevamento successivo all'incidente, poiché molti di essi vengono rilevati solo a distanza di tempo. Indipendentemente dalle falle nella sicurezza, è importante essere consapevoli dell'esistenza di un attacco e del suo successo, così da poterne limitare i danni.

La risposta agli attacchi completa la capacità di resilienza di un'azienda, poiché indica i metodi scelti per identificare, contenere, sradicare e riprendersi da un attacco. Gli insegnamenti tratti a seguito degli insuccessi in materia di sicurezza informatica offrono un'opportunità di miglioramento pari al valore di un solido sistema di sicurezza.

Per ulteriori informazioni, contattate PJR Italy - chiamateci al numero **0823/354874** o scriveteci all'indirizzo email **italy@pjr.com**.