Aziende a prova di hacker

Enti pubblici, grandi società e Pmi sempre più affidano i loro dati al digitale, diventando potenziali vittime di insidiosi attacchi informatici. Avere un incident response manager in azienda per fronteggiarli diventa essenziale.

Guardando all'anno appena conclusosi, la nota azienda russa Kaspersky, specializzata nella produzione di software per la sicurezza informatica, ha formulato un'osservazione che non lascia spazio all'immaginazione: "Per le cyberminacce il 2016 è stato l'anno in cui il 'prima o poi' è diventato 'ora'". Molti dei pericoli sui quali gli esperti di sicurezza IT avevano allertato si sono infatti concretizzati. Allarmanti data breach hanno colpito alcune delle maggiori compagnie mondiali. Dall'attacco al Dipartimento di Giustizia americano alla recente ammissione da parte do Yahoo di aver subìto nel 2013 il furto di informazioni personali da oltre 1 miliardo di account, i motivi di inquietudine non sono mancati. «Il proliferare di attacchi informatici di ultima generazione, sempre più sofisticati e dinamici, colpirà nel 2017 un numero crescente di piccole e medie imprese sfruttando l'anello più debole della sicurezza informatica per penetrare le infrastrutture aziendali: il fattore umano», avverte Alessandro Trivilini, dal 2011 a capo del Servizio di informatica forense del Dipartimento tecnologie innovative della Supsi. Studiando dati personali e facendo leva su abitudini comportamentali e sociali diffuse, il social engineering approfitta della scarsa consapevolezza dei rischi derivanti dal web per aggirare le barriere di protezione. A questa logica è ascrivibile lo straordinario successo ottenuto dalla corazzata ransomware, tecnica digitale di estorsione sempre più utilizzata dai cybercriminali: l'attacco si diffonde soprattutto via mail attraverso un allegato o il link a un sito contenente un malware che, una volta attivato prende possesso del sistema informatico dell'impresa, operando in backgroung fino a causarne il blocco completo. Per riavere accesso ai propri dati è necessario pagare un riscatto. «Amministratori delegati e responsabili d'azienda, confrontati con danni spesso irreparabili e inermi di fronte alla loro spietata efficacia, hanno compreso che disporre in azienda di tecnici IT preparati a rispondere rapidamente e adeguatamente agli attacchi informatici è un'esigenza ormai imprescindibile e di vitale importanza per la salvaguardia dei loro obiettivi di business», spiega Alessandro Trivilini.

Gli esperti concordano sul fatto che disporre di adeguate protezioni tecniche di sicurezza è condizione necessaria ma non più sufficiente a fronteggiare l'emergenza. «L'imprevedibilità dell'attacco cibernetico in rapporto alla prevedibilità del comportamento umano all'interno dell'azienda, nell'uso delle nuove tecnologie, è una combinazione vincente. A questo proposito, come ampiamente presentato durante la prestigiosa *Black Hat Conference* di Las Vegas, le attività di digital forensics e incident response assumeranno un ruolo sempre più centrale per una corretta ed efficace gestione del processo di information security», continua Alessandro Trivilini, recentemente nominato responsabile per la Svizzera in seno al Comitato di gestione del programma intergovernativo europeo Cost per promuovere l'innovazione tecnologica, in particolare in campo forense.

Il processo di digitalizzazione in corso e la crescente tendenza ad affidare dati lavorativi e personali alla tecnologia impongono quindi un cambio culturale nella gestione delle regole di cybersecurity, sempre più interoperabili e interdisciplinari. Da tempo impiegata in grandi aziende ad alto rischio di attacchi informatici, come per esempio banche, assicurazioni e multinazionali, l'incident response manager è una figura professionale che diventa sempre più indispensabile anche all'interno di piccole e medie imprese che non possono prescindere dall'utilizzo di nuove tecnologie per lo svolgimento del proprio business. «Si tratta di una figura di riferimento all'interno dell'azienda, specializzata e tecnicamente preparata con le più moderne competenze, per affrontare professionalmente tutte le fasi critiche che scaturiscono da un attacco cyber moderno: un esperto tecnicamente ben attrezzato, con il compito di garantire il mantenimento dei servizi di business aziendali presi di mira dall'attacco informatico», precisa il responsabile del Servizio di informatica forense della Supsi.

Lo scopo principale consiste nella definizione di un piano d'azione corretto e proporzionato da intraprendere in azienda in caso di incidente informatico di sicurezza (incident response), costruito attraverso una metodologia operativa strutturata a fasi:

- Fase di preparazione: ha come obiettivo la definizione di linee guida e policy a cui far riferimento per la gestione del caso, l'individuazione delle infrastrutture critiche da preservare, delle direttive di attivazione e coordinazione del team preposto all'intervento, e di quelle di comunicazione dell'incidente fra i collaboratori dell'azienda, la definizione dei ruoli di competenza e di comunicazione in caso di richiesta di intervento di specialisti esterni (periti, esperti in informatica forense o autorità giudiziarie) preposti alle indagini, l'identificazione degli strumenti tecnici e comportamentali necessari per fronteggiare tempestivamente l'incidente e, da ultimo, la sensibilizzazione e la formazione del personale interno all'azienda in rapporto all'evoluzione delle tecniche di attacco informatico.
- Fase di identificazione: necessaria per verificare l'effettiva presenza di un incidente informatico. In questo caso l'esperto svolge tutte le attività utili per la raccolta immediata del maggior numero di informazioni sull'incidente avvenuto, stabilisce l'assegnazione delle responsabilità delle operazioni di analisi ai singoli componenti del team, svolge una valutazione dell'incidente con lo scopo di determinare le sue caratteristiche e il suo modus operandi, definisce le modalità di salvaguardia delle prove digitali durante il loro trattamento nelle analisi e nelle ricerche (sfruttando i crismi e le linee guida dell'informatica forense) ed effettua una valutazione della potenziale scalabilità dell'attacco subìto in rapporto ad eventuali altre infrastrutture critiche non ancora infettate.
- Fase di contenimento: utile per limitare l'esposizione dell'azienda all'incidente informatico. Contempla, per esempio, le modalità di attivazione e intervento del team di incident response, l'identificazione e la notifica ai diretti interessati dell'incidente, l'esecuzione di un backup dei dati sensibili salvaguardati, la comunicazione in azienda delle azioni per il contenimento dei rischi che potrebbero avere un impatto sui servizi critici di business, la convocazione di tecnici specialisti di informatica forense per il contenimento dei danni infrastrutturali, la gestione della raccolta e della custodia delle prove digitali e la documentazione di tutte le attività intraprese per il contenimento di danni e rischi.
- Fase di eliminazione: serve a individuare le cause principali dell'incidente informatico, con lo scopo di isolarle e rimuoverle. In questo caso l'obiettivo è evitare la propagazione dell'attacco all'interno dell'azienda, effettuando un'analisi approfondita delle sue vulnerabilità.

Alessandro Trivilini, dal 2011 a capo del Servizio di informatica forense del Dipartimento tecnologie innovative della Supsi.

La formazione professionale di un incident response manager mira alla specializzazione di uno o più tecnici informatici aziendali, a dipendenza delle caratteristiche dell'infrastruttura critica da gestire, già impiegati nelle attività ordinarie di sicurezza informatica.

Per far fronte alla necessità di formare in Cantone Ticino professionisti del settore, il Servizio di informatica forense del Dipartimento tecnologie innovative della Supsi offre dal 2011 corsi di formazione continua in Digital forensics, focalizzati sulle attività di incident response, malware analysis e penetration testing, caso quest'ultimo in cui un'azienda chiede ad esperti di cercare di violare il proprio sistema informatico per metterne in luce eventuali falle.

«Si tratta di competenze altamente specializzanti utili per la definizione di un'adeguata, robusta e consapevole strategia di cybersecurity aziendale. I corsi hanno un imprinting fortemente pratico grazie alle esperienze professionali dal Servizio di informatica forense della Supsi nelle attività investigative di lotta quotidiana contro il cybercrime», conclude Alessandro Trivilini.

Susanna Cattaneo