Economy

Parte la caccia agli sceriffi della privacy per le aziende

Da maggio 2018 diventerà obbligatoria nelle aziende la figura del Data Protection Officer, per effetto di una direttiva Ue. Una scelta delicata e cruciale, più un nuovo asset che un costo

a cura della Redazione

Nel 2014 l'allora direttore dell'FBI James Comey dichiarava che negli Stati Uniti esistono soltanto due tipi di grandi aziende: quelle che hanno subito un attacco informatico e quelle che non sanno di averlo subito.

Il fenomeno del cyber attack è trasversale e in grande crescita al punto da aver conquistato la vetta delle agende governative. Per esempio, è una priorità per la Commissione europea che spinge per la creazione, nel 2018, di un centro di ricerca per la cybersecurity, il cui compito sarà quello di sostenere lo sviluppo di soluzioni a difesa della data economy. Anche il G7 Industria di settembre scorso ne ha fatto uno dei pilastri di intervento, con l'obiettivo di proteggere dati, informazioni, brevetti e segreti industriali. Nel documento finale approvato dai governi alla Reggia di Venaria compaiono anche le contromisure da prendere: educazione ai rischi informatici, cooperazione tra Stati e centri di ricerca e lo scambio di informazioni, anche tra le imprese.

Per mettersi al riparo dal rischio cyber si devono quindi affrontare simultaneamente una dimensione prettamente aziendale, una dimensione di cooperazione tra le Nazioni e una dimensione culturale che riguarda tutti.

Finora sono state numerose le aziende finite nel ciclone cibernetico. I case studies si accavallano, con effetti che superano la dimensione della singola impresa. Yahoo! e Equifax, ad esempio, lo hanno fatto capire molto bene.

Parte della ragione dell'esposizione delle aziende al rischio informatico si deve allo sviluppo delle tecnologie, digitali, interconnesse, automatizzate, che aprono continuamente nuovi fronti di vulnerabilità difficili da gestire. «Non si sottolinea abbastanza che il tema cyber è un tema che coinvolge tutto il management aziendale, e non solo chi ha la responsabilità dell'IT», chiarisce Stefano Cuzzilla (nella foto), presidente Federmanager, la Federazione dei manager industriali italiani. In particolare, la figura del Data Protection Officer, che diventerà obbligatoria da maggio 2018 per effetto della direttiva NIS, «deve qualificarsi con un profilo manageriale». Secondo Stefano Cuzzilla, infatti, «non basta affidarsi a un harware di competenze tecniche in grado di prevenire

CUZZILLA: «NON SI SOTTOLINEA ABBASTANZA CHE IL TEMA CYBER È UN TEMA CHE COINVOLGE TUTTO IL MANAGEMENT AZIENDALE»

UN VOUCHER PER L'EXPORT MANAGER

Dopo la prima sperimentazione del 2015 tornano i voucher per l'internazionalizzazione delle Pmi, estesi anche alle società di persone e alle start-up innovative. Sul piatto 26 milioni di euro di contributo a fondo perduto per chi intende avvalersi di un Temporary Export Manager - TEM per perseguire la propria strategia di export. Il TEM non è una figura qualsiasi, ma un manager specializzato, con competenze di analisi e ricerche di mercato, di individuazione e acquisizione di nuovi clienti, di assistenza legale, organizzativa, contrattuale e fiscale, capace di realizzare nel più breve tempo possibile il posizionamento all'estero del business aziendale. Per individuare il professionista più idoneo, l'azienda deve rivolgersi alle società accreditate dal ministero dello Sviluppo Economico a fornire servizi di accompagnamento ai processi di internazionalizzazione. La società CDi Manager, nata all'interno del sistema Federmanager (www.cdimanager.it), è tra quelle candidate a valutare i migliori profili di manager potenzialmente interessati a operare in questa funzione. La domanda on-line si può attivare a partire dal 21 novembre sul sito del Mise. Il termine per l'invio scatta alle ore 10.00 del 28 novembre.

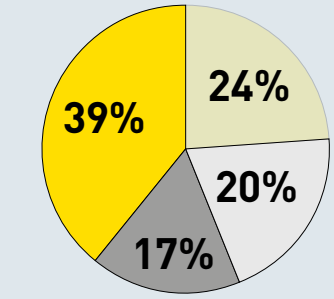
Economy

FEDERMANAGER

FONDIRIGENTI: CRESCE LA VOGLIA DI FORMAZIONE 4.0

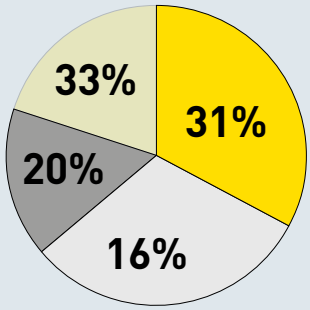
Cresce la voglia di formazione 4.0 delle aziende italiane. Il bando per l'aggiornamento delle competenze digitali lanciato da Fondirigenti, il Fondo interprofessionale per la formazione dei manager, è partito con una dotazione di 6,5 milioni di euro – pari a 15 mila euro ad azienda. La risposta? Sono arrivate richieste per ben oltre 10 milioni di euro. Analisi dei dati, cyber security e privacy, e-reputation e innovazione dei processi organizzativi/produttivi erano le 4 aree di intervento tra cui scegliere. Data la grande adesione, ora si devono valutare i singoli progetti «affinché i fondi siano assegnati secondo un sistema basato sul merito, per premiare la qualità», ci dice Carlo Poledrini, presidente Fondirigenti. «Il successo dell'iniziativa – aggiunge - ci dimostra comunque che imprese e manager rispondono con entusiasmo alle proposte formative, se si individuano giusti strumenti e obiettivi». I fondi interprofessionali rappresentano, nel nostro Paese, uno dei principali strumento per ridurre i gap formativi. Fondirigenti si conferma il maggiore tra i Fondi per i dirigenti (conta oltre 13 mila imprese aderenti per 76 mila manager) e il quinto, tra tutti i Fondi attivi in Italia, in termini di risorse raccolte.

Distribuzione per regioni della domanda di formazione



- 24% Emilia Romagna
- 20% Veneto
- 17% Lombardia
- 39% Altre regioni

Distribuzione per area tematica della domanda di formazione



- 33% Processi organizzativi/produttivi
- 31% Analisi dei dati
- 16% Sicurezza e privacy
- 20% e-reputation

e poi operare nel crisis management. Servono manager con soft skills adeguate per trasferire la cultura del rischio informatico a tutti i colleghi, anche a chi svolge mansioni diverse e in posizioni diverse».

Intervenendo a Cybertech Europe 2017 a Roma, il ministro della Difesa, Roberta Pinotti, ha utilizzato una similitudine da pelle d'oca. «Non possiamo dis-inventare le tecnologie cibernetiche offensive, come non possiamo dis-inventare le armi nucleari», ha detto, invocando azioni di sistema per fronteggiare un allarme generale.

A ben vedere, l'attacco informatico ha una ROI elevatissima. Un hacker con mezzi limitati può produrre un danno esponenziale, di ordini di grandezza superiori rispetto a quanto investito. Perciò, quella cyber è una minaccia che si definisce asimmetrica perché comporta, per chi deve garantire la difesa, un continuo e costante sforzo di ottimizzazione e efficientamento delle politiche di sicurezza cyber.

Nonostante i proclami ad effetto, sono ancora poche le aziende che hanno raggiunto un tale livello di consapevolezza. Secondo il Cybersecurity Report 2017 di Cisco, l'entità delle perdite collegate a una violazione informatica supera il 20% in termini di clienti, fatturato, opportunità di business. Mancano gli strumenti adeguati. E tra i principali ostacoli annoverati dal rapporto figurano i limiti di budget, la scarsa compatibilità dei sistemi e la carenza di talenti specializzati.

«La sicurezza digitale dovrebbe essere interpretata come un fattore di vantaggio competitivo per le imprese e una variabile sempre più determinante per l'attrazione di investimenti esteri», spiega Mario Cardoni, direttore di Federmanager. «Se si lavora sulla sensibilità aziendale, si può trasformare l'investimento nei sistemi informatici in un asset di garanzia molto apprezzato».

ANTONIO URICCHIO, RETTORE DELL'UNIVERSITÀ DI BARI, HA VOLUTO TRA I PRIMI IN ITALIA UNA LAUREA MAGISTRALE IN CYBERSECURITY

La partita si gioca molto sulla formazione universitaria. Prendiamo Taranto, dove ha sede il corso di laurea in cyber security promosso dall'Università di Bari Aldo Moro. Il Rettore Antonio Uricchio ne è convinto sostenitore: «Siamo stati tra i primi in Italia ad promuovere una laurea magistrale in questa disciplina perché volevamo dare una risposta al crescente fabbisogno espresso dalle aziende e dai poli industriali del nostro territorio. Le competenze sui sistemi informatici e la relativa sicurezza sono quelle più richieste dall'industria ad alto tasso di innovazione e l'università ha il compito di strutturare i talenti in questa direzione».

Guardare al tema della sicurezza informatica in termini di opportunità, dunque, è un approccio obbligato. Un cambio di orientamento che trova sponda nella definizione di "cyber resilience", sempre più diffusa negli accordi internazionali e nei report ufficiali.