ATTUALITÀ

Cyber Security: la sfida emergente della transizione digitale

di **Fondazione AIDR** · 23 settembre 2021, 10:22

di Giuseppe Gorga, socio Aidr

La transizione digitale ha reso più urgente il tema della cybersicurezza, dilatando la richiesta nel mondo lavorativo di figure professionali esperte nella protezione delle reti informatiche e nella tutela dei dati sensibili.

È sempre più urgente assicurare la sicurezza dei dati personali. I dati statistici dimostrano chiaramente che i cyberattacchi sono aumentati del 66% in 4 anni, e i danni globali causati dalle minacce cibernetiche rappresentano ormai una cifra enorme, sia per i privati che per le aziende, senza contare tra l'altro i danni determinati dai cyerattacchi rivolti contro i sistemi informatici delle istituzioni pubbliche (Clusit, 2021).

La tutela della cybersicurezza è diventata un tema sempre più centrale, specie dopo l'avvio del processo di digitalizzazione dell'amministrazione pubblica. Lo stesso governo Draghi, creando col decreto-legge n.22 del 2021 il Ministero per l'innovazione tecnologica e la transizione digitale, si prefigura di accellerare la digitalizzazione delle pubbliche amministrazioni, rinforzando le infrastrutture digitali materiali ed immateriali. Diventa così importante innalzare i livelli di sicurezza informatica delle banche dati, in conformità alle più recenti prescrizioni in tema di sicurezza cibernetica. Il potenziamento della cybersicurezza risulta infatti fondamentale per contenere le conseguenze di incidenti ed attacchi alle reti ed ai sistemi informatici.

È infatti noto che la *cybersecurity* è da tempo in cima all'agenda della politica italiana. La priorità data a questa tematica ha trovato espressione normativa con il Decreto Legge n. 82 pubblicato il 14 giugno 2021, recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale".

La funzione del decreto è quella di potenziare la sicurezza e ridurre la vulnerabilità dei vari sistemi tecnologico-informatici contro gli attacchi informatici che vengono posti in essere per ottenere dati a scopi fraudolenti (ISACA, 2015).Il provvedimento normativo si pone come espressione di attualizzazione e continuità delle indicazioni che il Parlamento Europeo ha espresso venti anni fa, quando ha preannunciato nella "Relazione sull'esistenza di un sistema d'intercettazione per le comunicazioni private ed economiche" (2001) che il tema della sicurezza dei sistemi informatici sarebbe diventato sempre più importante di pari passo alla diffusione e all'utilizzo dei mezzi tecnologico-digitali.

Il Decreto legge, oltre ad istituire il *Comitato interministeriale per la cybersicurezza* ed il *Nucleo per la cybersicurezza*, aventi rispettivamente funzioni deliberative e preventive, ha creato anche l'*Agenzia Nazionale per la Cybersecurity*. L'ente giuridico, come si legge nel testo del Decreto, "assicura, nel rispetto delle competenze attribuite dalla normativa vigente ad altre amministrazioni, il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la una cornice di sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore" ed, inoltre, "assume tutte le funzioni in materia di cybersicurezza già attribuite dalle disposizioni vigenti al Ministero dello sviluppo economico".

Queste evoluzioni normative segnano un profondo cambiamento in materia della cybersecurity, sempre più centrale da un punto di vista strategico in un'epoca sempre più informatizzata. Come accennato, questi provvedimenti sono funzionali non solo a proteggere i sistemi informatici degli enti pubblici, ma sorgo anche a tutela di aziende e privati. Nella fattispecie dell'ambito aziendale, preme ricordare che la compromissione della sicurezza gestionale dei dati personali che i clienti affidano ai professionisti ed alle aziende causa perdita di fiducia, imbarazzo e persino azioni legali nei confronti dell'organizzazione aziendale stessa (Prandi, 2010).

Per questa motivazione, enti pubblici e privati registrano un fabbisogno crescente di esperti informatici e legali, al fine di garantire la tutela giuridica ed informatica dei dati sensibili e risolvere possibili controversie. Nella fattispecie, si fa sempre più necessaria diventa la presenza di figure specifiche, capaci di recuperare e gestire cyberinformazioni gestendo la tutela della *privacy* e della riservatezza, sia da un punto di vista legale che informatico, come appunto gli informatici forensi (Lupària & Ziccardi, 2007).

Aziende ed enti pubblici, dunque, hanno sempre più bisogno di esperti in cybersicurezza e in privacy allo scopo di proteggere, con adeguate strategie e misure giuridiche e informatiche, la sicurezza della rete dei propri servizi informatici, garantendo una corretta tutela dei dati sensibili conservati. Man mano che la transizione digitale verrà implementata, aumenterà nel mondo del lavoro la richiesta di quelle figure professionali che fanno da ponte tra informatica e giurisprudenza, primi tra tutti appunto gli informatici forensi, i *cyber security manager* ed i *data protection officer*.

In Italia sono diverse le realtà formative che erogano corsi professionalizzanti finalizzati a creare figure esperte nella gestione della sicurezza informatica. Tra i diversi istituti formativi, certamente è degna di nota la ricca offerta formativa della scuola online EuroFormation, diretta dal prof. Giuseppe Gorga, docente in Diritto Digitale, Executive Manager in tema Privacy e Cyber Security e Presidente della Confederazione Privacy e Data Protection. EuroFormation sta contribuendo al dibattito sul tema con webina, approfondimenti ed interviste ad esponenti del mondo della cybersicurezza e della politica. Oltre a questo, è sede di corsi di formazione riconosciuti a livello internazionale negli ambiti della cybersicurezza. Esperienze formative ed accademiche come queste, oltre ad essere preziose per quanti vogliono entrare in questo mondo lavorativo in continua crescita, alimentano di contributi e di risorse la ricerca di soluzioni efficaci al tema della sicurezza in ambito informatico.

Articolo pubblicato su Istituzioni24: https://www.istituzioni24.it/2021/09/23/cyber-security-la-sfida-emergente-della-transizione-digitale/

© 2026 Istituzioni24