FISCALFOCUS®

5 ottobre 2019

La cibersicurezza, lo stato e i professionisti

Autore: ***Simone Carunchio***

La sicurezza informatica è sempre più richiesta e studiata. I professionisti stipulano polizze assicurative per tutelarsi nei confronti di hacker e attacchi informatici, soprattutto in relazione alle eventuali violazioni della Privacy. Ma anche lo Stato si sta muovendo per assicurare la sicurezza informatica all'interno dei propri confini, applicando e recependo, peraltro, le direttive e i regolamenti europei in proposito. Acapo del sistema di allerta vi è il Presidente del Consiglio dei Ministri, ma forse sarebbe stato più corretto prevedervi il Presidente della Repubblica. Sono poi in corso progetti visionari, quali quello di spedire i dati in orbita. Le preoccupazioni maggiori derivano dall'introduzione della rete 5G. Taluni vaneggiano di apocalissi informatiche.

Con l'arrivo della 5G, che potrà permettere di veicolare da 1000 a 5000 dati in più rispetto alla rete 3G o 4G, le informazioni che viaggeranno nell'etere saranno incalcolabili, poiché, oltre a quanto inserito dall'umano, occorre considerare anche quelle derivati dagli IdO (Internet degli Oggetti), ovverosia gli oggetti collegati direttamente a internet, come per esempio - nel campo delle città intelligenti - i semafori, le autovetture e gli impianti GPS, senza contare tutti gli altri, quali le radio, le TV, gli assistenti vocali e, naturalmente, i cellulari. I dati stoccati nel 2025 potrebbero quintuplicare rispetto a quelli immagazzinati attualmente.

Si pongono, naturalmente, questioni di privacy (di sicurezza dei dati personali), ma anche, a un differente livello, quelle di sicurezza nazionale. Occorre considerare, infatti, che la maggior parte dei servizi pubblici, sia quelli da parte dello Stato a favore dei cittadini (si pensi alla sanità) sia quelli da parte dei cittadini nei confronti dello Stato (si pensi alla fiscalità e alla fatturazione elettronica) si svolgono ormai via etere.

Per sicurezza informatica o cibersicurezza (o ancora, per chi ama gli anglicismi, cybersecurity) si intende una disciplina mediante la quale una organizzazione, titolare di un insieme di beni, tenta di proteggere il valore dei beni stessi adottando misure che contrastino il realizzarsi di eventi accidentali o intenzionali che possano danneggiarli. I beni di cui si tratta sono i più diversi. Si passa dalle informazioni personali al funzionamento di alcuni servizi, ma passando anche per una risorsa concernente i programmi o le applicazioni e i relativi macchinari.
Per quanto attiene ai dati personali si tratta di preservarne la disponibilità, l'autenticità, l'integrità e la riservatezza. In questo senso di importanza rilevante è il famoso e conosciuto GDPR, ossia il Regolamento UE n. 2016/679.

Per altro verso, sempre a livello unionale, occorre richiamare la Direttiva UE 2016/1148, conosciuta anche come direttiva Nis (Network and information security), in cui sono state stabilite le azioni che i Paesi membri devono compiere per sviluppare la sicurezza informatica. Si tratta di definire gli obiettivi strategici e le opportune misure per mantenere un elevato livello di sicurezza delle reti e dei sistemi informatici e di individuare gli OSE, ossia gli Operatori di Servizi Essenziali. Inoltre nella medesima direttiva è stato riconosciuto un ruolo fondamentale all'ENISA (Agenzia per l'Unione Europea per la cibersicurezza), la quale era stata costituita con il Regolamento CE n. 460/2004.

La centralità di tale ente è stata ulteriormente confermata mediante il Regolamento UE 2019/881, con il quale è stata

introdotta anche la certificazione della cibersicurezza. Nello specifico la certificazione si avvale di un meccanismo per attestare che i prodotti, i servizi e i processi TIC (Tecnologie dell'Informazione e della Comunicazione) siano conformi a determinati requisiti che assicurino la suddetta disponibilità, autenticità, integrità o riservatezza dei dati per tutto il ciclo della loro vita.

Si tratta di indicazioni preziose per i Data Protection Officer (DPO), ossia di coloro che si occupano si osservare, valutare e gestire il trattamento dei dati personali con l'obiettivo di far rispettare le normative europee in proposito.

Passando al livello italiano, il GDPR è stato recepito con il D.Lgs. n. 101/2018; mentre la Direttiva Nis con il D.Lgs. n. 65/2018. Per il momento sono stati individuati 465 operatori essenziali nelle categorie indicate nella direttiva, vale a dire quelle dell'energia, dei trasporti, del settore bancario e sanitario, della fornitura di distribuzione di acqua, delle infrastrutture digitali e dei mercati finanziari. Inoltre, mediante il medesimo decreto, è stato istituito presso la Presidenza del Consiglio dei Ministri il CSIRT (Computer Security Incident Response Team – chissà perché chiamato in lingua inglese!?), il quale deve prevenire gli incidenti informatici e agire di conseguenza in caso si verifichino, in coordinamento con gli altri gruppi europei del medesimo tipo. Nello stesso tempo gli OSE devono notificare al CSIRT gli attacchi informatici a cui sono sottoposti senza ritardo.

Sulla stessa linea si pone anche il D.L. n. 105/2019 del 21 settembre, titolato "disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica", il cui scopo è quello di migliorare il livello di sicurezza delle reti dei sistemi informativi e dei servizi informatici delle pubbliche amministrazioni e degli enti e degli operatori pubblici e privati nazionali.

Nel perimetro di sicurezza rientrano tutti quegli operatori che assicurano e da cui dipende una funzione essenziale dello Stato o la prestazione di un servizio indirizzato al mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato stesso. Inoltre è stabilita la procedura di notifica degli OSE al CSIRT, nonché quella per gli acquisti tecnologici sui mercati esteri. Sono state poi previste delle sanzioni amministrative in caso di non osservanza delle procedure di cui sopra.

Ma non è tutto: è stabilito che occorra monitorare i fattori di vulnerabilità della rete 5G e che, in caso di attacco informatico il capo del Governo debba seguire un preciso protocollo per disattivare uno o più apparati o prodotti impiegati nelle reti o nei sistemi informatici.
In proposito si rileva che un potere del genere lo si sarebbe potuto assegnare, più coerentemente alle funzioni costituzionali di ognuno, al Presidente della Repubblica.

In conclusione, non si può non affermare che l'apparato statale stia operando nel modo migliore e più celere per prevenire ciò che gli assicuratori asseriscono sarà una normalità: l'essere sottoposti ad attacchi informatici.

Questo processo verso la cibersicurezza è in un certo modo richiesto anche 'dal basso'. Si è appena citato il ceto assicurativo perché sono sempre di più le aziende e i professionisti che richiedono una protezione assicurativa, in particolare polizze antihacker. E alcuni rispettivi Ordini - quali quello dei dottori commercialisti, quello forense e quello del notariato - hanno già siglato delle convenzioni per questo tipo di servizi.
Qualora, infatti, il professionista sia attaccato, egli deve contattare un legale che si confronti con il Garante dei dati, cercare e trovare un esperto informatico che sappia capire la situazione di modo che la crisi possa essere gestita e i dati ripristinati.

Che tali minacce si facciano sempre più presenti nella realtà, nonché nell'immaginario di ognuno, è confermato anche da alcuni progetti che mirano a trasportare i dati nello spazio siderale in maniera che essi siano conservati in orbita. Si tratta di un progetto della start-up statunitense Cloud Costellation che mira a inviare nello spazio dei data center satellitari. Oltre alla sicurezza informatica, la start up assicura che lo stoccaggio satellitare potrebbe generare effetti positivi nell'ambiente perché il gelo spaziale sostituirebbe l'uso dell'energia necessaria per raffreddare gli apparecchi di immagazzinamento dati.

Si tratta di progetti che paiono rispondere a più o meno inconsce paure di apocalissi informatiche, ma che hanno una loro ragione d'essere in una società sempre più dipendente dalla tecnologia.

Via Alemanni 1 - 88040 Pianopoli (CZ) - ITALY
P.IVA 03426730796

E-mail: info@fiscal-focus.it