È ora di promuovere una cultura della cybersicurezza

Norme & digitale

Giusella Finocchiaro

Mercato illecito di dati, accesso abusivo a sistemi informatici, dossieraggio... La recente inchiesta che sta portando alla luce la violazione di numerose banche dati istituzionali a danno di quasi (al momento) 1 milione di persone, sembra avere aperto un vaso di Pandora, anche per i profili delle persone indagate, che avrebbero dovuto proteggere la sicurezza.

Reati come quelli che si profilano nell'inchiesta in corso non possono che minare la fiducia di cittadini, organizzazioni e operatori nei servizi digitali e, in generale, nel mercato unico digitale, obiettivo al centro della legislazione europea. Cybersecurity Act, Direttiva NIS2, Cyber Resilience Act, Eu Cyber Solidarity Act, Regolamento attuativo per un quadro di certificazione sulla cybersicurezza: sono tutti tasselli normativi volti a promuovere la fiducia, la sicurezza e la stabilità nel cyberspazio attraverso misure di contrasto alle minacce informatiche e requisiti di sicurezza dei prodotti e dei servizi digitali.

Si muove da misure volte a garantire la continuità dei servizi essenziali e critici fino a politiche di igiene informatica e di alfabetizzazione digitale rivolte ai singoli. Sono molteplici, infatti, i livelli di protezione quando si parla di sicurezza nel digitale, così come diversi sono gli interlocutori.

Cercando di fare un po' di ordine: principalmente medie e grandi imprese che erogano servizi critici (tra cui, energia, trasporti, servizi bancari, sanitari, Tic) e fornitori di servizi digitali, reti e servizi di comunicazione elettronica, di sistemi di nomi di dominio e di servizi fiduciari, sono i diretti interessati dalle norme dettate dalla Direttiva NIS2 e dal d.lgs. 138/2024, che in Italia ha recepito la Direttiva. In capo a questi obblighi – da osservare in diversi scaglioni temporali – di registrazione alla piattaforma nazionale gestita dall'Acn (l'Autorità per la Cybersicurezza Nazionale); di comunicazione di attività e servizi svolti; di responsabilizzazione degli organi direttivi e di amministrazione; di notifica degli incidenti e, infine, (ovviamente) di adozione di misure tecniche, operative e organizzative adeguate al rischio.

Analogamente alla protezione dei dati personali, anche la gestione del rischio cyber diventa proporzionata al grado di esposizione a rischi del soggetto, alle dimensioni del soggetto, alla probabilità e alla gravità degli incidenti, compreso il loro impatto sociale ed economico. Viene introdotto un elenco minimo di misure da adottare, per assicurare la continuità operativa, inclusa la gestione di backup e un piano di *disaster recovery*; la sicurezza della catena di approvvigionamento; pratiche di igiene di base e di formazione in materia di sicurezza informatica; politiche e procedure relative all'uso della crittografia e della cifratura.

Protagonisti di questo nuovo *framework* non sono soltanto gli operatori, chiamati attraverso la propria attività ad innalzare il livello comune di sicurezza, ma anche i legislatori nazionali e le autorità designate a governare la materia.

Da un lato, gli Stati membri dovranno curare l'elaborazione e l'aggiornamento delle proprie strategie nazionali, individuando gli obiettivi strategici e le risorse necessarie per conseguirli. Dall'altro lato, l'Acn e le autorità di settore individuate dal d.lgs. 138/2024 saranno responsabili della gestione delle crisi informatiche, fungeranno da punto di contatto e di coordinamento transfrontaliero con le autorità nazionali.

La sicurezza non è soltanto un problema informatico, ma è un problema che investe molti diversi aspetti. Ha profili tecnologici, organizzativi, giuridici e va affrontata con un approccio interdisciplinare.

A poco servono misure sofisticate, se poi la password è scritta su un post-it attaccato al video del computer, o se per abitudine è condivisa. La legislazione sulla privacy ha introdotto, molti anni fa, normativamente, il tema della sicurezza, che tuttavia fatica ad affermarsi, soprattutto perché di sicurezza si parla quando non c'è, mentre se la sicurezza funziona, nessuno se ne accorge.

Oggi forse i tempi sono maturi per costruire una cultura della sicurezza, che certamente le norme favoriscono, promuovono o addirittura impongono, ma che richiede uno stretto coordinamento fra le diverse anime dell'organizzazione e un approccio culturale ed educativo condivisi.