PIETRO VASSALLI, CYBER SECURITY MANAGER GRUPPO SICUREZZA SA FA IL PUNTO SULLE NOVITÀ NEL CAMPO DELLA CYBERSICUREZZA, SOTTOLINEANDO COME IL MONDO CONTEMPORANEO ABBIA TRATTO ENORMI VANTAGGI DALLA DIFFUSIONE DELLA TECNOLOGIA MA SIA ANCHE MAGGIORMENTE ESPOSTO A GRANDI RISCHI PER LA SUA STESSA SOPRAVVIVENZA.

Ph: © Foto Pavesi

COME CAMBIA IL TRATTAMENTO **DEI DATI PERSONALI**

Perché la cybersicurezza ha assunto una fondamentale importanza nell'organizzazione, nel funzionamento e in definitiva nella sopravvivenza stessa della società contemporanea?

«Per diverse ragioni. Per prima cosa siamo fortemente dipendenti dalla tecnologia. La società contemporanea è sempre più digitalizzata e siamo ormai abituati all'uso di sistemi informatizzati per svolgere una vasta gamma di attività quotidiane: comunicazioni, transazioni finanziarie, servizi di emergenza, assistenza sanitaria, approvvigionamento alimentare e molto altro. La dipendenza da questi sistemi rende la società vulnerabile a minacce cibernetiche, che stanno diventando sempre più sofisticate e diffuse: i criminali informatici mettono in atto attacchi sempre più avanzati che possono avere gravi conseguenze.
Inoltre, organizzazioni e dai governi gestiscono una grande quantità di dati sensibili e personali. Pensiamo ad esempio ai dati finanziari, a quelli medici e a tutte le informazioni che ci riguardano che sono sparse nel web. La violazione di queste informazioni può causare danni significativi alle persone e alle aziende e, di conseguenza, minacciare la privacy dei singoli individui.
Internet ha reso il mondo più interconnesso che mai. Questa interconnessione consente il rapido scambio di informazioni e la comunicazione globale, ma allo stesso tempo espone a minacce provenienti da tutto il mondo. Un attacco informatico in un paese può avere ripercussioni su scala globale. Un possibile attacco alle infrastrutture critiche, come ad esempio al settore energetico, quello dei trasporti, le telecomunicazioni e le utilities, che sono diventate sempre più automatizzate e digitalizzate, potrebbe causare interruzioni significative e mettere a rischio la sicurezza pubblica.
Possiamo fare anche qualche riflessione sull'economia: solo a titolo di esempio e-commerce e trasferimenti di denaro sono caratterizzate fortemente dalla digitalizzazione. In questo settore la cybersicurezza è cruciale per garantire che le attività continuino a funzionare in modo sicuro ed efficiente. Non va dimenticato che gli Stati utilizzano il cyberspionaggio e la guerra cibernetica per ottenere vantaggi strategici, rubare segreti industriali e influenzare gli affari internazionali. Tutto ciò può minacciare la stabilità globale e la sicurezza delle nazioni.
Va tenuto anche in debito conto che molte organizzazioni sono obbligate per legge a garantire la cybersicurezza e a rispettare determinati standard di sicurezza dei dati. La non conformità può comportare sanzioni legali e danni alla reputazione. Nel campo finanziario, le violazioni della sicurezza informatica possono comportare costi significativi, tra cui perdite economiche ingenti, danni alla reputazione e azioni legali. Investire in cybersicurezza può aiutare a mitigare questi rischi.
In estrema sintesi, la cybersicurezza è diventata fondamentale per proteggere la società contemporanea da minacce sempre più complesse e per garantire il funzionamento sicuro ed efficiente delle attività quotidiane, delle infrastrutture e dell'economia digitale. La sua importanza è destinata a crescere ulteriormente con il continuo sviluppo della tecnologia e l'aumento delle minacce che evolvono quotidianamente».

Quali sono le principali ragioni che hanno indotto la Svizzera ad una revisione totale della legge sulla protezione dei dati (nLPD)?

«La Svizzera ha intrapreso una revisione totale della sua legge sulla protezione dei dati (nota come "nLPD" o "Legge federale sulla protezione dei dati") per diverse ragioni chiave. Una delle principali è stata l'esigenza di adeguare la legislazione alla normativa europea sulla protezione dei dati, il GDPR. Poiché la Svizzera è geograficamente situata in Europa ed è fortemente interconnessa con l'Unione europea a livello economico, sociale e commerciale, la conformità al GDPR è diventata essenziale per garantire che i dati personali possano continuare a fluire senza ostacoli tra la Svizzera e i paesi dell'UE.
Inoltre, la revisione della nLPD ha come scopo il miglioramento della protezione dei diritti dei cittadini svizzeri in relazione alla loro privacy e ai dati personali. Questo comprende il diritto all'informazione, il consenso esplicito per l'elaborazione e la portabilità dei dati, oltre al diritto all'oblio.
D'altra parte, l'avanzamento della tecnologia e l'aumento delle attività digitali, il volume e la complessità dei dati personali trattati hanno registrato una crescita significativa. La legge sulla protezione dei dati, in vigore dal 1992, è stata adattata per affrontare le sfide e le opportunità create da questa evoluzione tecnologica.
Per quanto riguarda le imprese, la conformità al GDPR è molto importante per poter operare e competere a livello internazionale. Una legge sulla protezione dei dati allineata al GDPR semplifica le operazioni transfrontaliere e contribuisce alla competitività delle aziende svizzere, consentendo alla Confederazione di essere inserita nell'elenco dei Paesi cosiddetti "adeguati", ovvero dotati di norme che consentono di trattare le informazioni secondo un concetto di protezione e riservatezza delle informazioni di livello sufficiente.
La revisione della nLPD include anche provvedimenti per rendere più accessibili e praticabili i diritti degli interessati, come il diritto di accedere ai propri dati personali, il diritto di rettifica e il diritto di opposizione all'elaborazione dei dati. Va sottolineato anche che la nLPD prevede sanzioni più severe per le violazioni, al fine di disincentivare le pratiche non conformi alla protezione dei dati».

In particolare, con la nuova normativa, la protezione dei dati sarà adattata agli sviluppi tecnologici, sarà rafforzata l'autodeterminazione relativa ai dati personali e aumentata la trasparenza nella raccolta dei dati personali?

«La nuova normativa nLPD è stata progettata proprio per quegli scopi: il cardine è portare la legislazione svizzera in linea con le normative europee sulla protezione delle informazioni, oltre a garantire una maggiore protezione dei diritti individuali in merito ai dati personali.
Non va dimenticato anche l'obiettivo di avere una maggiore trasparenza e responsabilità da parte delle organizzazioni che operano dei trattamenti delle informazioni. Ritengo che queste modifiche contribuiranno in modo fattuale al miglioramento della protezione dei dati personali in Svizzera, oltre a rafforzare la fiducia degli individui nei confronti delle pratiche di gestione dei dati stessi».

Possiamo riassumere brevemente le più importanti disposizioni esecutive contenute nella nuova ordinanza sulla protezione dei dati (OPDa)?

«Certamente: vediamo un piccolo excursus delle novità introdotte. Le organizzazioni devono informare le persone in modo chiaro e completo su come vengono utilizzati i loro dati personali e sulla base giuridica del trattamento. Le persone hanno il diritto di accedere ai propri dati personali, richiederne la correzione o la cancella-

zione e opporsi al trattamento dei dati in determinate circostanze.
Il trattamento dei dati personali richiede il consenso esplicito delle persone, a meno che non esista una base giuridica alternativa. Le organizzazioni devono implementare misure di sicurezza adeguate a proteggere i dati personali da accessi non autorizzati o da violazioni della sicurezza.
Il trasferimento di dati personali al di fuori della Svizzera è consentito solo se il paese di destinazione offre un livello adeguato di protezione dei dati o se sono state prese misure di sicurezza adeguate. Le organizzazioni devono condurre una valutazione dell'impatto sulla protezione dei dati, la cosiddetta DPIA, quando il trattamento dei dati comporti un rischio elevato per i diritti e le libertà delle persone.
Sulla base di specifici criteri, alcune organizzazioni hanno l'obbligo di designare un responsabile della protezione dei dati, il DPO, e informare l'autorità di controllo dei dati della sua nomina. Le organizzazioni devono notificare all'autorità di controllo dei dati e alle persone interessate le violazioni dei dati che possano comportare un rischio per i diritti e le libertà delle persone. Inoltre, devono tenere registri dettagliati delle loro attività di trattamento dei dati. Sono previste sanzioni per le violazioni della normativa sulla protezione dei dati, comprese multe in caso di non conformità».

Che cosa prevede invece la nuova ordinanza sulle certificazioni in materia di protezione dei dati (OCPD)?
«La nuova ordinanza mira ad uniformare la norma in vigore dal 2007 alla nLPD e alla relativa OPDa. Introduce anche una importante novità rispetto alla precedente: la certificazione non più solo per i prodotti ma anche per i servizi e per i processi. Risulta essere molto interessante per le aziende il concetto per cui se ci si avvale di un sistema, di un prodotto o di un servizio certificato a monte, il titolare del trattamento, che nella maggioranza dei casi coincide con l'azienda stessa, può rinunciare ad eseguire la valutazione d'impatto, la DPIA, di cui abbiamo parlato prima. I rimandi a nLPD e OPDa sono molti e vale la pena ricordare anche che è possibile comunicare dati all'estero sulla base di una certificazione. La norma indica anche i requisiti per i certificatori, come pure quelli per certificare prodotti e servizi. Risulta interessante che, allo stato delle cose, non sia stato introdotto un marchio generale per la protezione dei dati. Una nota importante riguarda gli organismi esteri, per cui diventa stringente non solo possedere certificazioni equivalenti e avere competenza sulla nLPD, ma anche il personale assume un ruolo rilevante e pertanto deve essere qualificato. Da ultimo, ma non per importanza, vengono evidenziati i requisiti per il programma di certificazione e per la certificazione dei sistemi di gestione, dei prodotti, dei servizi e dei processi».

In che modo il Gruppo Sicurezza si è attrezzato per supportare i propri clienti di fronte alle nuove normative entrate in vigore il 1° settembre 2023?
«Sin dal 2017 Gruppo Sicurezza ha costituito Cyber. La chiave del successo è intraprendere un percorso che coniughi aspetti tecnici e procedurali. In molti casi i clienti posseggono già le componenti tecniche necessarie ma spesso queste non sono utilizzate nel modo corretto, non sono implementate o adottate da tutti. Per questo motivo supportiamo le aziende nel processo di messa in sicurezza dell'infrastruttura secondo il principio del "security by design". L'introduzione della nLPD è stato un forte volano che ha portato alla luce le criticità relative alla sicurezza presenti, oltre ad una maggiore coscienza dell'importanza che hanno i dati e le informazioni: si tratta della linfa vitale che va correttamente protetta e costantemente alimentata. A tutto questo va affiancato il supporto procedurale necessario ad introdurre un sistema di gestione della privacy. Il nostro supporto va anche in quel senso. Inoltre l'Azienda, in modo costante, offre servizi di formazione sia realizzati in modo sartoriale per i clienti e gruppi di clienti sia destinati alla divulgazione più ampia, con l'obiettivo di far crescere le competenze e la consapevolezza sul tema della sicurezza informatica di tutta la popolazione».

Infine, qual è la sua valutazione riguardo alla diffusione in Ticino di una cultura della cybersicurezza e quali ulteriori misure andrebbero eventualmente perese per migliorare l'attuale situazione?
«Il Ticino, rispetto ad altri Cantoni, si sta muovendo con grande ritardo. C'è grande difficoltà a percepire i rischi che si corrono a non intraprendere correttamente i passi necessari a mettere in sicurezza le aziende, con la falsa convinzione che tanto toccherà ad altri o che gli hacker non hanno interesse a colpire proprio me. Purtroppo riscontro che grande frequenza la confusione tra chi si occupa di sicurezza informatica chi di informatica pura: gli ambiti di attività sono profondamente differenti, soprattutto considerando che controllato e controllore non possono essere lo stesso soggetto. Da ultimo devo sottolineare che è importante comprendere che la certificazione delle competenze è fondamentale. Per avere un lavoro di qualità ci si deve affidare a professionisti qualificati e non a chi si è improvvisato. Per migliorare la situazione è fondamentale proseguire con l'informazione e la divulgazione: i toni devono essere pacati, senza terrorismo o sensazionalismo. Solo con la cultura potremo avere un cambio di mentalità che ci permetta di rendere davvero sicuro l'intero ecosistema pubblico e privato del nostro territorio».