TECNOLOGIE

La sicurezza informatica passa anche da Lugano

Si è svolto ieri il primo 'Lugano cybersecurity forum'

'Non possiamo farci trovare impreparati'

di Federica Ciommiento

Il conto alla rovescia è partito. Aziende, istituzioni e pubbliche amministrazioni hanno tempo un anno per adeguare le loro norme di sicurezza informatica e adempiere così agli obblighi richiesti dalla nuova legge sulla protezione dei dati, che entrerà in vigore il 1° settembre del prossimo anno in Svizzera. «La cybersicurezza e la protezione dei dati diventano così due anelli che non si separeranno più», ha detto **Alessandro Trivilini**, responsabile del Servizio informatica forense della Scuola universitaria della Svizzera italiana (Supsi), in occasione del primo 'Lugano cybersecurity forum', che si è svolto ieri al Casinò di Lugano. Il rischio di attacchi informatici è alto ed è «necessario farsi trovare preparati», ha affermato. È nato dunque un gruppo di lavoro trasversale che comprende gli aspetti tecnici, assicurativi, di protezioni dei dati e di validazione scientifica.

'Manca consapevolezza'

«Non c'è ancora la piena consapevolezza che la cybersicurezza sia una questione centrale», ha indicato l'avvocato **Rocco Talleri**. I cambiamenti legislativi, però, permettono di rivolgersi alle aziende sotto un'altra ottica: invece che una spesa, la sicurezza informatica diventa un investimento, ha ricordato l'avvocato. Infatti «il mercato la richiede e lo farà sempre di più, esigerà anche delle certificazioni».
A fargli eco c'è **Paolo Sanvido**, amministratore delegato di Casinò Lugano: «Nei consigli d'amministrazione questo tipo di discorso manca e bisogna inserirlo. Nelle direzioni c'è attenzione riguardo alla sicurezza informatica, ma spesso si pensava che bastassero una polizza assicurativa e qualche procedura per risolvere la questione. Il tema è però più ampio e con il forum vogliamo rendere attenti tutti sulla serietà della questione. Questo per evitare di avere come Paese un danno economico e come aziende un danno reputazionale: il più importante e difficile da calcolare economicamente».
Un aspetto fondamentale per la sicurezza informatica è quello tecnico: «La cybersicurezza è fatta da processi, tecnologie e persone», ha ricordato **Paolo Lezzi**, fondatore e Ceo dell'InTheCyber Group. «Tutti questi elementi devono essere tenuti al massimo livello: serve la consapevolezza delle persone per evitare errori che permettano di bypassare una parte delle difese, le tecnologie devono essere all'ultimo livello di aggiornamento e collaborare tra loro, i processi non devono permettere che vi siano vie brevi per arrivare a un determinato punto».

'Un'azienda attaccata perde immagine, produzione e clienti'

Alzare le difese, però, non basta. Sono necessarie delle sentinelle: «Bisogna verificare in maniera continua l'inizio di potenziali attacchi per poterli neutralizzare sul nascere», ha proseguito Lezzi. Per le aziende sono particolarmente problematici i 'ransomware', ovvero virus che, per esempio, limitano l'accesso ai sistemi informatici chiedendo un riscatto. Questo può provocare grandi danni per un'azienda, che si vede bloccata nella sua attività. «I pilastri descritti sono fondamentali, spesso però non sono stati implementati, sia qui sia nel resto d'Europa. Questo fa sì che i ransomware siano ancora capaci di aggredire. Non si può però più permettere che le nostre imprese e istituzioni vengano colpite e quindi ridotte del loro valore intrinseco. Perché un'azienda attaccata perde immagine, perde produzione, perde clienti».

L'assicurazione come ultimo step

Quando ci sono dei rischi si pensa quasi sempre a proteggersi con un'assicurazione. Stipulare una polizza assicurativa però non basta, ha spiegato **Régis Dubied**, Ceo di Assidu Sa Lugano. «Nelle polizze ci sono esclusioni e obblighi. Il cliente deve aver comunque raggiunto un certo livello di sicurezza e protezione». Le conseguenze in caso di un attacco possono essere economicamente molto alte. «Non è possibile avere la certezza di evitare un attacco, ma con un lavoro di prevenzione e valutazione dei rischi si possono portare i rischi in una zona accettabile e rendere l'azienda più resiliente, più sicura». Nella polizza assicurativa viene dunque trasferito il rischio residuo, «ma come ultimo stadio».