La Svizzera è nel mirino dei criminali informatici

Negli ultimi mesi gli attacchi informatici verso aziende e istituzioni presenti sul territorio svizzero sono aumentati. ©SHUTTERSTOCK

SICUREZZA DIGITALE / Un numero crescente di aziende e istituzioni della Confederazione è vittima di attacchi – Secondo il delegato del Centro nazionale per la cibersicurezza Florian Schütz, «molte imprese elvetiche hanno ancora misure di protezione insufficienti»

Giona Carcano

CPH Chemie+Papier, Emil Frey, CICR. Un'industria cartaria, un grande concessionario d'auto e un'istituzione umanitaria internazionale. Tutti e tre hanno subito gravi attacchi informatici nel mese di gennaio. Un caso? No. La tendenza è chiara: negli ultimi mesi, aziende e organizzazioni attive sul territorio svizzero sono sotto il tiro dei cibercriminali. I dati diffusi dagli esperti di Check Point Research sono allarmanti: nel 2021 gli attacchi sono aumentati del 65% rispetto all'anno precedente. Quali i motivi? E, soprattutto, come si sta muovendo la Confederazione per fronteggiare un nemico senza volto? Lo abbiamo chiesto a Florian Schütz, delegato federale alla cibersicurezza e direttore del Centro nazionale per la cibersicurezza (NCSC). «Sì, il nostro centro ha ricevuto un numero sproporzionato di segnalazioni negli ultimi mesi», conferma Schütz. «Due i motivi. Da un lato gli attacchi sono effettivamente aumentati, in particolare quelli tramite ransonware, un ricatto informatico. Dall'altro, con l'avanzare della digitalizzazione, è cresciuta la sensibilità verso la sicurezza informatica da parte di privati e imprese: pur in assenza di obblighi, gli eventi vengono denunciati sempre più spesso e c'è maggiore propensione a renderli pubblici. Di riflesso, dunque, anche le segnalazioni aumentano. Il business della cibercriminalità, purtroppo, è conveniente: chi attacca sa che ci sono vittime disposte a pagare per riavere i propri dati. E sa anche che le probabilità di successo sono buone, perché gli ostacoli sono pochi».

Alcuni negano i rischi

Pochi ostacoli, sì. Significa dunque che le aziende e le istituzioni svizzere sono vulnerabili? Ancora il delegato: «Il livello di sicurezza informatica della Svizzera è paragonabile a quello di altri Paesi europei», spiega. «Tuttavia, tra le aziende, ci sono grandi differenze in termini di cibersicurezza. Molte imprese hanno ancora misure di protezione insufficienti. La chiave sono i responsabili delle stesse società, che dovrebbero prendere seriamente la questione della sicurezza informatica e inserire nel management profili specialistici nel campo dell'IT». Si nota dunque una sottovalutazione del rischio potenzialmente molto dannosa. «Notiamo due tendenze», osserva Schütz. «La prima: alcune aziende sottovalutano o addirittura negano i rischi, e devono quindi accettare un'elevata possibilità di subire un attacco. La seconda: molte aziende riconoscono il pericolo ma non sanno come comportarsi. Spesso vengono sopraffatte dalla complessità. Un altro punto delicato riguarda il fatto che la cibersicurezza è un "mercato molto rumoroso", in cui non sempre si trovano argomentazioni professionali. Ciò rende ancora più complicato per le aziende valutare il rischio e adottare soluzioni adeguate. È proprio questo uno degli ambiti da migliorare: la maggior parte degli attacchi informatici può essere prevenuta con uno sforzo ragionevole».

+65%
è l'aumento
degli attacchi subiti da aziende o istituzioni svizzere nel 2021 rispetto all'anno prima

Gli strumenti normativi

Ma chi si cela dietro questi attacchi? «Al di là dei singoli criminali, spesso a colpire sono vere e proprie organizzazioni, ognuna con un proprio modello di business», spiega ancora il delegato. «Alcune sono organizzate a livello regionale, altre hanno membri sparsi in tutto il mondo». Nemici difficili da contrastare e da perseguire. Tuttavia, come visto, esistono strumenti facilmente reperibili utili alla prevenzione. Cosa serve, allora, per aumentare la sicurezza informatica della Svizzera? Ancora Schütz: «È importante puntare su condizioni quadro appropriate, in modo da permettere alle aziende – anche quelle con poco know-how digitale – di investire in modo mirato nella sicurezza informatica. Ciò permetterebbe di disporre di una forte protezione di base delle infrastrutture. Ma in prospettiva bisognerà anche istituire misure normative per ridurre il rischio di una crisi informatica di rilevanza sistemica».

Un primo passo è stato compiuto il 12 gennaio, quando il Consiglio federale ha posto in consultazione fino al 14 aprile il progetto di legge che introduce le basi legali per l'obbligo di segnalazione. Se attaccati, i gestori di infrastrutture critiche dovranno informare il Centro nazionale per la cibersicurezza.

Fare gioco di squadra

Sì, quando si parla di informatica, uno dei concetti chiave è «fare squadra». Nessuno può dirsi al riparo da questo tipo di eventi, eppure se tutti adottassero misure adeguate i cibercriminali incontrerebbero molti più ostacoli. «È importante che le aziende siano consapevoli dei rischi, ma è altrettanto importante rendersi conto che il comportamento individuale può influenzare la sicurezza di tutti gli altri», sottolinea l'esperto. «In questo senso, penso valga la pena investire nell'educazione e nella sensibilizzazione della popolazione sui temi inerenti la sicurezza. I cittadini, in un mondo sempre più digitalizzato, dovrebbero disporre di nozioni di base di sicurezza informatica. Non tutti devono diventare informatici, ma l'educazione aiuta a ridurre il rischio e promuove la discussione politica su questi importanti temi. In generale, dovremmo allontanarci dal concetto di attacco-difesa. Bisognerebbe insistere sulla tecnica, sviluppando e utilizzando sistemi di protezione sicuri. L'approccio "puro rischio" non è pagante». Anche lo stesso NCSC, che attualmente impiega una quarantina di collaboratori, dovrà essere potenziato. «Stiamo facendo delle valutazioni a riguardo», commenta Schütz. A mio parere, vedo sin d'ora la necessità di un'espansione. Ma come e in che misura, sarà la politica a stabilirlo».

«Berna ha colto la necessità di cambiare approccio»

L'ESPERTO / Alessandro Trivilini, responsabile del Servizio di informatica forense della SUPSI: «La nuova legge sulla protezione dei dati avrà un effetto dirompente»

Per Alessandro Trivilini, responsabile del Servizio di informatica forense della SUPSI, la Confederazione ha colto la necessità di cambiare approccio culturale verso la cibersicurezza. Eppure, «la visione che generalmente si ha di queste minacce è obsoleta», spiega. «La messa in sicurezza delle infrastrutture critiche, il loro aggiornamento, la messa a punto di un piano di risposta in caso di attacco e la formazione dei dipendenti sono purtroppo ancora visti come un costo che solo le grandi aziende possono permettersi. È sbagliato: in dieci anni di attività abbiamo seguito oltre trecento casi, e siamo giunti alla conclusione che riparare i danni di un attacco costa due volte e mezzo in più rispetto al costo della prevenzione». Anche in Ticino i dati sono allarmanti: da ottobre, osserva Trivilini, i casi si sono moltiplicati e coinvolgono sia piccole e medie imprese, sia istituzioni. «Alcuni ci contattano perché hanno paura di essere bersaglio dei cibercriminali ma non riescono a identificare l'attacco, altri invece si rivolgono a noi perché sono colpiti da un ransomware, un ricatto informatico che blocca dati sensibili». La portata di questo fenomeno? Ampia: Trivilini lo paragona a un vento che colpisce ogni angolo del cantone, senza distinzioni. E il vento, non si ferma con un fazzoletto. Anche in Svizzera c'è ancora molto da fare per raggiungere il grado di consapevolezza necessario per far fronte a questi pericoli. Anche se qualcosa si sta muovendo: la Confederazione ha colto l'importanza strategica della questione della sicurezza informatica, varando la nuova legge sulla protezione dei dati. «Di fatto, il nuovo quadro giuridico cambierà le regole del gioco del prossimo decennio», spiega l'esperto. «Le aziende e le istituzioni dovranno prestare sempre più attenzione verso il settore della sicurezza informatica, perché per la prima volta entra in gioco il concetto di responsabilità. Detto in altri termini: se i dati di un'azienda vengono resi inaccessibili in seguito a un attacco informatico, qualcuno dovrà rispondere ai propri clienti. Un sindaco di un Comune preso di mira, dovrà rispondere ai suoi cittadini». Un po' come accade in caso di incendio: bisogna capire che cosa lo ha scatenato, qual è il grado di responsabilità e se c'è stata negligenza. «Quando entrerà in vigore, la nuova legge avrà un effetto dirompente», prosegue Trivilini. «Nessuno potrà dire "non sapevo, non potevo prevedere". Ecco che allora, di riflesso, aumenterà il grado di consapevolezza e di responsabilità delle aziende o delle istituzioni nei confronti dei dati dei clienti. «In caso di denuncia, con l'introduzione della nuova legge i responsabili potrebbero venir perseguiti in sede civile per non aver fatto tutto quanto in loro potere per proteggere i dati e mettere in sicurezza l'azienda», chiosa Trivilini. «Non è soltanto una questione economica, bensì anche reputazionale. Cambierà il paradigma, e non si tornerà più indietro. È quindi arrivato il tempo di fare squadra: chi decide di correre da solo rischia, e la ricerca scientifica ha un ruolo determinante». La nuova legge entrerà in vigore nel gennaio 2023, «per dare il tempo a tutti di prepararsi».

Dal gennaio 2023
cambierà il paradigma ed entrerà in gioco la responsabilità

Sì, il settore della sicurezza informatica rappresenta il presente e il futuro: ma oltre agli strumenti giuridici, servono risorse umane, al momento piuttosto scarse. Cosa dovrebbe fare la Svizzera? Ancora Trivilini: «Siamo solo all'inizio di un percorso, la strada per raggiungere un livello di protezione agile e al passo coi tempi è lunga. Ma ci sono anche delle opportunità: la Confederazione è percepita come un Paese sicuro. Sarebbe intelligente investire risorse per diventare leader nel settore della sicurezza informatica. Il Ticino, grazie alla formazione del gruppo Cybersicuro, ha fatto grandi progressi e oggi è un riferimento. Ma anche Berna si è mossa nella dando vita lo scorso anno al centro Cyber nazionale. Ora si tratta di rendere questa rete nazionale e regionale proattiva. E di formare esperti capaci di lavorare in un settore in rapidissima evoluzione». **G.C.**