L'indagine Bankitalia. Nelle aziende i responsabili della sicurezza spesso non sono esperti di cyber

In Italia scatta l'allarme intrusioni

di **Marco Ludovico**

Snobbato spesso dai non addetti ai lavori e denunciato invece a volte con fin troppa enfasi, il rischio cyber trova oggi per la prima volta dati ufficiali di rilevazione in Italia. Con la massima autorevolezza: la ricerca «Attacchi informatici: evidenze preliminari dalle indagini della Banca d'Italia sulle imprese», pubblicata nelle «Questioni di economia e finanza (Occasional papers)» di febbraio 2017, è ora sui tavoli istituzionali. Analisi citata anche dalla relazione annuale del Dis (dipartimento informazioni e sicurezza), diretto da Alessandro Pansa, presentata lunedì scorso a palazzo Chigi con il presidente del Consiglio, Paolo Gentiloni.

Il documento di via Nazionale, sede di Bankitalia, sceglie un profilo sottotono. Ma i rilievi statistici sono eloquenti. E danno torto a chi ha guardato finora alle minacce informatiche con scarsa preoccupazione. La ricerca, curata da Claudia Biancotti, si basa sulle indagini annuali di via Nazionale tra le imprese dell'industria e dei servizi, il campione totale è di 4.271 aziende. Conforta che solo l'1,5% «non adotti alcuna misura difensiva». Ma «il 30,3% - corrispondente al 35,6% degli addetti - dichiara di aver subito danni a causa di un attacco informatico tra settembre 2015 e settembre 2016».

Le cifre, tuttavia, sono ancora più allarmanti: «Correggendo i risultati per tenere conto delle intrusioni non individuate o non dichiarate, l'indice degli attacchi sale al 45,2% delle imprese e al 56% degli addetti». Statistiche forse da rivedere ancora al rialzo: «Il livello di rischio nel complesso dell'economia - scrive Bankitalia - è probabilmente ancora più alto». Nell'indagine, del resto, sono esclusi il settore finanziario, la sanità, l'istruzione e i servizi sociali, considerati però «da altre fonti particolarmente attraenti per gli attaccanti».

La ricerca conferma una serie di tendenze consolidate. Come la reticenza diffusa a rendere noto di aver subìto un attacco per non causare un contraccolpo negativo d'immagine all'azienda. Il rischio maggiore di un'incursione cyber è per le aziende di maggiori dimensioni: ha riguardato il 62,8% delle imprese con più di 500 dipendenti. E c'è la non trascurabile questione che chi si occupa di sicurezza cibernetica nelle aziende: non è detto che sia un professionista di cybersecurity.

La relazione Dis presentata la scorsa settimana a palazzo Chigi osserva come «l'intelligence ha collaborato» con Banca d'Italia per «ottenere, per la prima volta in Italia, un quadro statisticamente rilevante dell'esposizione alla minaccia cibernetica del sistema produttivo». Il documento sottolinea il confronto svoltosi tra intelligence e via Nazionale «sul fronte della costituzione di un Cert (Computer Emergency Response Team) finanziario» istituito nel dicembre 2016 in seguito a un accordo tra Banca d'Italia, Abi, e Consorzio Abi Lab: il Cert «opera quale organismo altamente specializzato nella cybersecurity nel settore bancario e finanziario». Il documento Dis fa anche emergere «la progressiva saldatura tra le finalità economiche della cyber-criminalità con quelle di comuni player di mercato, interessati, questi ultimi, a compromettere la competitività dei rispettivi concorrenti». Sotto attacco così finiscono «banche, istituti finanziari, gestori di piattaforme cloud, operatori nei settori e-commerce ed e-business e le infrastrutture critiche nazionali».

marco.ludovico@ilsole24ore.com

I target

Attacchi cyber in Italia in base alla tipologia dei soggetti privati target, in % sul totale 2016

Altri settori	41
Settore bancario	17
Agenzie di stampa/testate giornalistiche/giornalisti	11
Associazioni industriali	11
Settore difesa	5
Settore farmaceutico	5
Settore energetico	5
Settore aerospaziale	5

Fonte: Documento di sicurezza nazionale