Sicurezza, 150 aziende in testa alla lista

La revisione della direttiva Ue sui cyber attacchi, le attività strategiche da proteggere. Rischio di multe fino a 10 milioni

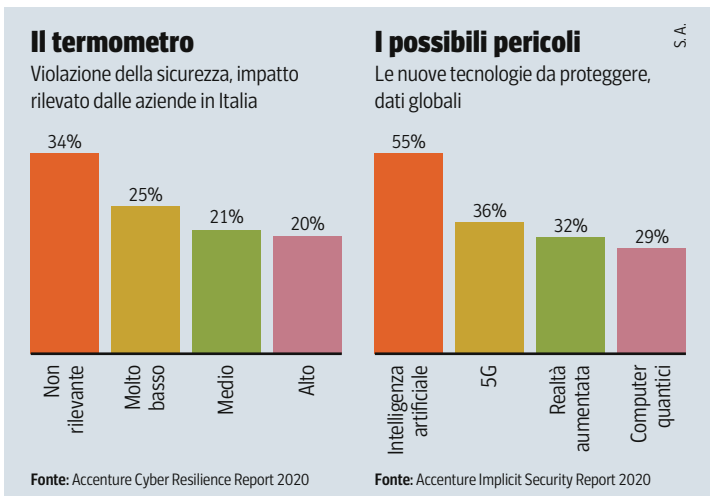
di **Umberto Torelli**

Gli hacker alzano il tiro. E sferrano cyberattacchi sempre più minacciosi. Adesso è il turno delle grandi imprese energetiche. Vedi la recente vicenda della rete di oleodotti statunitensi di Colonial Pipeline, che da Huston in Texas attraversano gli States per oltre 8 mila chilometri. Alla fine, la società ha ceduto. Per riattivare il servizio ha dovuto pagare un riscatto di 5 milioni di dollari. Così è stato tolto il ransomware installato nei software gestionali di molte stazioni di servizio. Non solo. Ora i pirati informatici puntano alle aziende pubbliche. Qualche settimana fa il sistema sanitario irlandese (Hse) ha subito un grave attacco che ha isolato in pochi minuti i computer di ospedali e centri di smistamento farmaci. Creando seri problemi alla gestione dei vaccini.

Secondo il Clusit, l'associazione italiana per la sicurezza informatica, nell'anno della pandemia si è registrato il record di attacchi. A livello globale sono stati infatti 1.871 quelli gravi di dominio pubblico. Con un impatto sistemico in ogni aspetto della società, della politica e dell'economia. Ecco perché la commissione Europea sta accelerando la revisione della direttiva NIS (Network and information security). Approvata in prima battuta nel 2016 e volta a stabilire le misure per consentire ad aziende e pubblica amministrazione di operare in ambienti digitali sicuri.

Rete
Paolo Dal Cin, Accenture security lead per l'Europa

L'ottava edizione del «Threat landscape report 2020» di Enisa (European union agency for cybersecurity) registra come l'area degli attacchi continua a espandersi. Puntando a dati di alto valore sociale come la proprietà intellettuale, informazioni mediche e segreti di Stato. Sono azioni distribuite sul territorio, di breve durata ma con finalità multiple. Nella maggiore parte dei casi estorsione finanziarie tramite ransomware. Molti incidenti passano inosservati con un tempo medio di rilevazione degli attacchi superiore ai 6 mesi. Questo ha costretto il 49,3% delle aziende a integrare l'organico con specialisti di security, con un investimento medio di 175 mila euro per impostare i programmi Nis. I dati emergono da un panel di 251 aziende europee ritenute essenziali e importanti in materia di Nis.



Fattori

«Sappiamo ormai che la cybersecurity è un requisito fondamentale per la tutela dell'economia, della sicurezza e della salute pubblica, come per la crescita — spiega Paolo Dal Cin, Accenture security lead per l'Europa —. Le aziende interessate non potranno farsi cogliere impreparate. Da un lato devono prevedere l'impatto della normativa sulla loro attività, dall'altro dotarsi di competenze, infrastrutture e tecnologie necessarie per adeguarsi». La proposta di una direttiva Nis 2.0 richiederà un ulteriore adeguamento alle nuove misure previste ed estenderà, come previsto dal legislatore, sia nuovi parametri di soglia, identificati in almeno 250 dipendenti o 50 milioni di fatturato, sia obblighi a settori aggiuntivi con una platea più ampia di aziende, valutate in Italia in oltre 500. Per ora le sanzioni per gli inadempienti prevedono multe fino a 10 milioni di euro o 2% del fatturato annuo.

Per quanto riguarda il nostro Paese gli interventi previsti a livello europeo sono stati in parte anticipati dall'impianto normativo del Dpcm 131/2020 «Perimetro di sicurezza nazionale cibernetica».

Entrato nella sua fase operativa a inizio 2021 con l'approvazione dei decreti attuativi. In questa fase sono state individuate le prime 150 aziende pubbliche e private ritenute critiche per la sicurezza nazionale. La normativa prevede tempi di segnalazione degli attacchi più restrittivi rispetto a quelli europei, con l'obbligo di denuncia di violazioni informatiche entro un'ora nei casi gravi e sei ore per i meno gravi.

«Accenture Security ha attivato in Italia un osservatorio interno in grado di monitorare e informare le aziende sulle evoluzioni normative nazionali e comunitarie – continua Dal Cin – per fornire strumenti conoscitivi e accompagnarle nei processi di trasformazione». Il processo legislativo Nis 2.0 richiederà un periodo di circa 12 mesi da oggi, ma visto il progredire delle minacce è prevedibile il completamento entro fine 2021. A questo punto i singoli paesi devono mettersi in regola entro i successivi 18 mesi dall'emanazione europea. Proroghe escluse.

Protezione

Attenti alle app camuffate e ai finti regali in bitcoin

Le truffe online stanno diventando più sofisticate. «In questi ultimi mesi, sfruttando il tema del coronavirus, sono nate app dannose e perfettamente camuffate — dice Fabio Buccigrossi, country manager di Eset Italia —. Sono andate a colpire non soltanto il singolo utente ma anche le imprese». Fondata nel 1992 a Bratislava, con uffici in tutto il mondo, Eset Italia sviluppa software e servizi di sicurezza per proteggere le imprese, le infrastrutture e i singoli utenti dalle minacce digitali.

Eset Italia
Fabio Buccigrossi, country manager: «Serve attenzione. Più minacce con lo smart working»

«Abbiamo pensato a una protezione specifica per i manager che devono mettere in sicurezza gli smartphone — dice il manager —: monitora costantemente i dispositivi e in caso di rischio interviene all'istante, senza ridurre la velocità né, in generale, la prestazione del dispositivo. La continuità lavorativa non s'interrompe».

Fra l'altro lo smart working espone a un maggior rischio, anche se le soluzioni che innalzano barriere di protezione attorno ai dati aziendali e all'utente aiutano a bloccare gli attacchi degli hacker. «Se un utente non opera attraverso una Vpn (la rete privata virtuale, *ndr.*) — avverte Buccigrossi — la minaccia aumenta in modo esponenziale».

L'azienda sviluppa da oltre 30 anni soluzioni innovative e usa l'intelligenza artificiale. Offre soluzioni legate alla tecnologia del machine learning in cloud, utili a proteggere qualunque utente. In merito agli attacchi maggiormente pericolosi del momento, il manager avverte: «Sono sempre più diffusi i ransomware, in grado di entrare in qualunque rete informatica. Dopo avere identificato quali sono i dati più importanti dell'azienda, i pirati li criptano, poi chiedono un riscatto che può raggiungere cifre consistenti. Un tempo gli attacchi degli hacker arrivavano per email a tutti indistintamente, oggi sono più mirati, dunque più pericolosi».

Oltre che alle truffe online, tra le tecniche più diffuse per derubare vittime inconsapevoli, oggi bisogna fare attenzione anche ai finti regali in criptovaluta.

«Per raggiungere il maggior numero di persone vengono utilizzati diversi canali — dice Buccigrossi —, spesso dirottando account YouTube con molti follower o cercando di diffondere la notizia attraverso Twitter. Viene richiesto l'invio di denaro digitale a un indirizzo bitcoin con la promessa, mai mantenuta, di raddoppiare la somma».

Ba. Mill.