

La sala cyber della Farnesina ha sventato qualcosa come 630 mila eventi malevoli

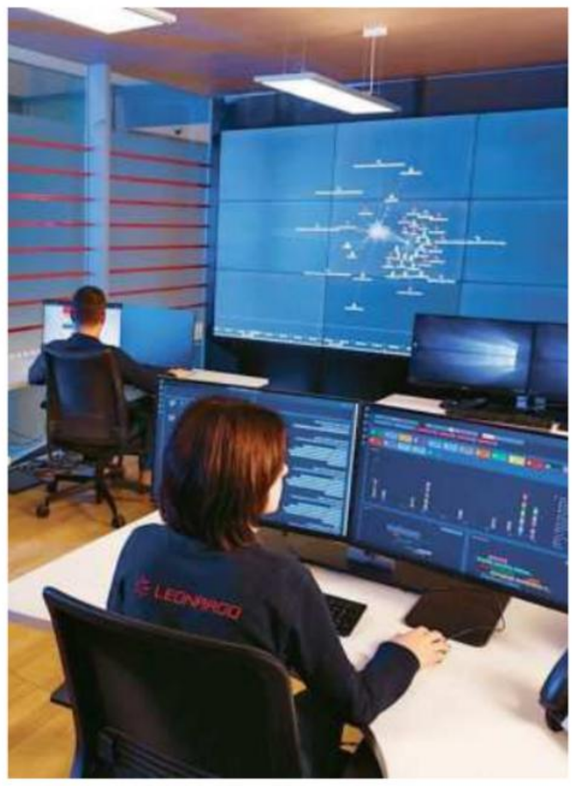
Dopo la forte escalation dei gravi attacchi ibridi che hanno colpito il Paese negli ultimi giorni, il ministro degli Esteri, Antonio Tajani, ha visitato la sala cyber della Farnesina per fare un "punto della situazione sulle misure di contrasto intraprese e sulle linee d'azione per assicurare la protezione di tutti i servizi per cittadini e imprese''.Con la riforma del dicastero fortemente voluta da Tjani ed entrata in vigore dal 1° gennaio 2026, è stata creata una Direzione Generale dedicata alle questioni cibernetiche, l'informatica e l'innovazione tecnologica e una sala operativa Cyber attiva 24 ore su 24 Quando la sala cyber registra un attacco, raccontano, attiva un raccordo immediato con l'Agenzia per la Cybersicurezza nazionale (ACN), il CSIRT Italia e il Centro nazionale anticrimine informatico per la protezione infrastrutture critiche (CNAIPIC) della polizia postale, per attuare una risposta coordinata di tutto il sistema informatico nazionale all'attacco. Subito "dopo la scoperta dell'incidente", riferiscono fonti del ministero, viene attivato un coordinamento con le strutture di sicurezza cibernetica dell'Ue. L'attività della Sala Cyber si sviluppa lungo tre direttrici principali: prevenzione delle minacce e dei rischi; monitoraggio; risposta agli attacchi. Dall'avvio delle attività nel gennaio 2026, ha «intercettato e bloccato oltre 630 mila eventi e tentativi di natura malevola diretti verso il perimetro digitale dell'amministrazione; neutralizzato circa 3,5 milioni di messaggi di posta elettronica malevoli, su un totale di quasi 23 milioni di e-mail ricevute da domini esterni; svolto migliaia di attività di analisi, di cui 817 nell'ultimo trimestre». Tra i principali attacchi respinti, riferiscono fonti della Farnesina,«vi sono quelli in occasione delle visite del presidente ucraino Zelensky in Italia, in particolare del maggio 2023 e poi del gennaio 2025, e durante le Olimpiadi invernali Milano-Cortina, nel febbraio 2026, quando sono stati presi di mira oltre a servizi collegati all'evento olimpico anche siti di sedi diplomatiche italiane». Da ultimo è stato registrato un «attacco informatico particolarmente forte al sito del Ministero a ottobre di quest'anno».Nell'attacco, «respinto senza danni alle strutture, erano stati messi nel mirino anche alcuni siti di ambasciate e consolati nel mondo». « Attacchi " DDoS - Distributed Denial of Service si verificano comunque con cadenza quotidiana.

Hacker, furti e spie: il nemico è in azienda «Modena è in ritardo»

Parla l'esperto: «Brevetti, clienti e know-how nel mirino»

«Rischiamo di trovarci dentro un conflitto senza accorgercene: siamo in piena guerra ibrida e la stiamo combattendo con i fucili col tappo. E a Modena, per scendere nello specifico, sulla protezione digitale, che tocca il cuore stesso delle aziende, c'è un ritardo culturale estremamente preoccupante». È l'opinione di Pietro Suffritti, socio amministratore della modenese Alchimie Digitali, impresa associata a CNA Modena e specializzata in trasformazione digitale, consulenza informatica, infrastrutture server, cloud e sicurezza informatica per le piccole e medie imprese. «Purtroppo molti di coloro che prendono le decisioni considerano ancora il problema una faccenda da ragazzini smanettoni, mentre in questo campo lavorano esperti con quarant'anni di esperienza alle spalle. Del resto oggi "hacker" ha una connotazione negativa, anche se deriva dal verbo inglese to hack, che significa tagliare a colpi, fare a pezzi, sfrondare. Per i criminali il termine corretto sarebbe "cracker", da to crack: spaccare, scassinare, rompere. Capisco però che sul piano comunicativo sarebbe stato complicato: tutti avrebbero pensato subito ai cracker da mangiare. In ogni caso i rischi sono enormi, tanto che l'Unione europea con la direttiva NIS 2 (Network and Information Security, del 2022, recepita in Italia con il decreto legislativo 138 del 2024) ha alzato il livello di sicurezza informatica e di resilienza agli attacchi richiesto alle imprese. Ed è una strada che funziona: secondo il Clusit, la somma delle norme europee sulla sicurezza e la tutela dei dati, dal GDPR in poi, comincia a mostrare effetti positivi, soprattutto nelle piccole e medie imprese. Eppure molti, ancora oggi, ignorano questi obblighi, mentre anche nella nostra provincia si contano fallimenti aziendali legati a questo tema».

Suffritti preferisce non fare nomi, ma racconta: «Ai tempi del terremoto del 2012 ho aiutato imprese con i capannoni quasi completamente crollati a tornare operative, con i propri sistemi di nuovo online in 48 ore: un risultato ottenuto grazie ad amministratori ben consapevoli del problema e ad accorgimenti tecnici che in quel caso hanno cambiato tutto. Per molti, purtroppo, questi restano temi da rompiscatole. Anche nel Modenese alcune aziende sono state costrette a chiudere dopo aver subito il furto dei dati che costituiscono il patrimonio stesso dell'impresa, spesso senza capire esattamente che cosa stesse succedendo. Lo schema è questo, per esempio con un'azienda presa di mira perché detiene brevetti, solide relazioni internazionali e maestranze molto qualificate. Prima vengono sottratti tutti i dati su produzione, clienti, fornitori, listini e macchinari. Poi, con quelle informazioni, si costruisce altrove, magari molto lontano, un'azienda che fa esattamente ciò che fa l'originale e vende lo stesso prodotto agli stessi clienti a un prezzo appena inferiore. In poco tempo il parco clienti dell'azienda derubata letteralmente evapora, senza che si capisca il perché. Poi l'amministratore delegato vede andarsene, una dopo l'altra, le persone chiave, non necessariamente quelle in prima fila: il magazziniere che risolve i problemi, il tecnico che conosce le procedure. E anche qui non si capisce il motivo. Infine arriva un acquirente estero sconosciuto che rileva tutto e lo rivende subito a chissà chi. Quello che racconto è accaduto davvero, e più di una volta, nel Modenese».





Pietro Suffritti, socio amministratore della modenese Alchimie Digitali Nella foto sopra il centro Cyber security Leonardo Company

C'è da rabbrividire, anche perché naturalmente c'è chi ci guadagna, e di solito non si tratta di campioni della democrazia. «Ci sono Stati, la Cina su tutti, che su queste pratiche hanno costruito vantaggi industriali enormi» prosegue l'esperto modenese. «Altri, come la Russia, si interessano a questi temi per ragioni geopolitiche e militari: basti pensare all'invasione dell'Ucraina. E infine ci sono Stati che ci finanziano le casse pubbliche: si stima che i soli furti di criptovalute valgano alla Corea del Nord oltre il 10% del suo PIL, grazie a una struttura dedicata della sua intelligence militare che ha già sottratto miliardi di dollari. Se questa non è una guerra ibrida, che cos'è? Sono attacchi costanti e continui. E le soluzioni non sono semplici: se mentre sto facendo altro mi accorgo di una vulnerabilità in un'azienda e mi espongo per avvisarla, rischio di essere denunciato per accesso abusivo e di dover dimostrare di non essere entrato nei suoi sistemi. È un reato punito fino a tre anni nell'ipotesi base e, dopo la riforma del 2024, fino a dodici nei casi più gravi». E un paio di consigli pratici: «Fate molta attenzione alla tutela delle email aziendali: anche quelle considerate a basso rischio mostrano come comunicate in azienda e come siete organizzati. Non usate password banali e non riutilizzatele in posti diversi. Usate un gestore di password, attivate la verifica in due passaggi ovunque si possa e cambiate la password subito se c'è il minimo sospetto sia compromessa».

Personaggi famosi finti, soldi spariti veri

Non soltanto le aziende, anche e soprattutto i normali utenti sempre nel mirino



Simona Baldaccini, responsabile dello sportello "SOS truffa"

«Di recente a noi Federconsumatori Modena - spiega Simona Baldaccini, responsabile dello sportello "SOS truffa" - è capitato il caso di una signora preoccupata perché il papà stava subendo una truffa amorosa. Appassionato di golf si era infatti messo a seguire via social una giocatrice nota nell'ambiente che ben presto via messaggio social lo ha contattato: ovviamente si trattava di un profilo falso e questo signore ha perso dei soldi». Si tratta di casi sempre più diffusi e che preoccupano: «Occorre stare molto attenti - prosegue l'esponente di Federconsumatori - perché i social sono come una porta spalancata e non tutti sono preparati a veder arrivare i malintenzionati. Per restare ai casi che ci sono capitati c'è stata una signora, appassionata di un noto cantante meridionale, che a un certo punto via messaggio - non era ovviamente lui - ha iniziato a chiederle dei soldi perché aveva problemi con l'automobile…».

Conclude la rappresentante dei consumatori: «A Modena , ad esempio, problemi alla catena del freddo sul tema dei frigoriferi mandati in tilt non ne abbiamo avuti, almeno noi, ma occorre sia per le aziende sia per i cittadini usare password sicure e senza riferimenti personali, cambiandole spesso, attivare efficaci antivirus, controllare le app che si scaricano e non postare le foto mentre si è in vacanza. In questo modo si rischiano visite dei ladri anche presso l'abitazione fisica».

Federconsumatori chiede l'aggiornamento immediato dei sistemi di protezione e una task force

Da qui un caloroso consiglio a tutti «Nel caso di dubbi richiamate la banca o le forze dell'ordine che si sono fatte vive, in modo da controllare. E attenzione anche ai wi-fi pubblico che non sempre è super sicuro».

Insomma, occorre stare all'erta e proprio i frigoriferi spenti da "remoto" hanno generato allarme nei rappresentanti degli utenti.

Federconsumatori chiede l'aggiornamento immediato dei sistemi di protezione e una task force dedicata presso l'Agenzia per la cybersicurezza nazionale: «Palazzo Chigi ha rassicurato e ne prendiamo atto, ma non bisogna abbassare la guardia: la strategia di chi conduce questi attacchi potrebbe cambiare, per questo dobbiamo essere pronti a individuare ogni possibile segnale di compromissione della catena del freddo. Chiediamo anche alla distribuzione della logistica alimentare e della refrigerazione di adottare immediatamente alcune misure: la verifica dell'esposizione su onternet dei sistemi di controllo e teleassistenza, la loro separazione dalle reti aziendali, accessi da remoto protetti con VPN e autenticazione a più fattori, controllo degli account e sostituzione dei dispositivi non più supportati dai produttori. E ritiene indispensabile non affidarsi solo ai sistemi di controllo collegati in rete, ma anche a sensori e registratori di temperatura non connessi a Internet».

S.L.

© RIPRODUZIONE RISERVATA