GIMBE EVIDENCE FOR HEALTH
Sezione:POLITICA SANITARIA

L'IDENTITÀ
Dir. Resp.:ADOLFO SPEZZAFERRO
Tiratura: n.d. Diffusione: n.d. Lettori: n.d.

Rassegna del: 08/07/26
Edizione del:08/07/26
Estratto da pag.:6
Foglio:1/2

LA VIOLAZIONE DELLE STRUTTURE SI È TRASFORMATA IN UNA CATENA DI MONTAGGIO DEL CRIMINE

La sanità sotto l'assedio degli hacker Il "borsino" dei dati rubati ogni giorno

di ANGELO VITALE

Non è più una questione di "se", ma di quanto costi la nostra identità sanitaria sul mercato nero. Se un tempo l'hacking era l'incursione di un pirata solitario, oggi la violazione delle strutture sanitarie italiane si è trasformata in una catena di montaggio del crimine ad altissimo rendimento.

I dati dell'Agenzia per la Cybersicurezza Nazionale e del Clusit parlano chiaro: nel 2025 gli attacchi in Italia sono cresciuti del 42%, con una matrice che nel 99,1% dei casi è puramente economica. La nostra salute è diventata la merce perfetta.

L'analisi dei flussi finanziari nel sottobosco digitale rivela una gerarchia precisa del valore dei dati. Mentre una carta di credito valida viene svenduta per appena 30 dollari, una singola cartella clinica completa può oscillare tra i 300 e i 1.000 dollari. Il motivo è semplice: una carta si blocca con una telefonata, una diagnosi o una storia clinica sono per sempre. È quello che gli esperti arrivano a definire un "ergastolo digitale" per la vittima.

Il confronto internazionale dei prezzi, basato sulle ultime rilevazioni del 2026 di TrendAI, posiziona l'Italia in una fascia di valore "premium".
Un database medico italiano contenente i cosiddetti "fullz" - pacchetti d'identità completi di codici fiscali e storie cliniche - è stato quotato 150mila dollari. Per avere un termine di paragone, database simili russi vengono scambiati per soli 1.000 dollari, mentre archivi indiani da oltre 200 GB si fermano a 5.000 dollari. Solo il mercato turco riesce a superare queste cifre, con database ospedalieri completi venduti a 250mila dollari, segnale di una digitalizzazione massiva non supportata da difese adeguate.

I gruppi criminali come Black Basta, Cicada3301 e Rhysida hanno abbandonato la "fiocina" - l'attacco mirato al singolo ufficio - per ampliare una sorta di "pesca a strascico". La strategia vincente non è più colpire un solo ospedale, ma i fornitori di software o le piattaforme regionali che gestiscono migliaia di cartelle cliniche contemporaneamente. È il meccanismo del moltiplicatore: bucando una singola "porta" d'accesso — spesso attraverso tecniche di inganno verso i dipendenti con il phishing o sfruttando software mai aggiornati — i criminali esfiltrano volumi immensi di file. Documentati, i casi in cui, con un solo colpo, sono stati sottratti oltre 1,5 terabyte di dati, pari a circa due milioni di file personali che finiscono istantaneamente in vendita. Il territorio milanese e lombardo, cuore della digitalizzazione italiana, è diventato l'epicentro di questo scontro.

Il caso Synlab è l'esempio più eclatante di questa nuova aggressività. Il gruppo Black Basta arrivò a paralizzare i laboratori per giorni, pubblicando poi online 1,5 TB di referti, diagnosi e documenti d'identità dopo il rifiuto dell'azienda di pagare il riscatto. Nell'attacco all'Asst Rhodense, il collettivo Cicada3301 ha dimostrato la letalità di queste ampie azioni, esfiltrando 1 TB di dati sensibili. Un blocco tale da costringere il portale web dell'azienda a rimanere in modalità provvisoria per oltre 70 giorni. All'Asst Fatebenefratelli-Sacco, anche quando l'attacco non portò al blocco totale, le falle lasciarono tracce pesanti. La struttura è stata recentemente sanzionata dal Garante Privacy per la presenza di software obsoleti e sistemi di allerta inadeguati che hanno facilitato l'incursione hacker.

Il Garante per la Protezione dei Dati Personali, nella sua relazione annuale, ha alzato il livello di allerta, segnalando criticità persistenti sulla gestione dei dossier sanitari e dei fascicoli elettronici. Non si tratta solo di multe — che per il settore pubblico e privato stanno crescendo vertiginosamente in termini di importo medio — ma di una necessità di governo dei

Peso:55%

dati. La speranza risiede nell'applicazione della Direttiva NIS2, che impone finalmente obblighi di notifica e standard di sicurezza stringenti per ospedali e laboratori, considerandoli "soggetti essenziali" per la sicurezza nazionale. perché ormai la difesa della salute non passa più solo dalle sale operatorie, ma dalla capacità di proteggere i bit che valgono ormai oro colato nel mercato nero globale.

Un database medico italiano è stato quotato 150mila dollari sul mercato illegale

(© Imagoeconomica)

Peso:55%