INSURANCE Daily

LUNEDÌ 29 GENNAIO 2024 N. 2503

PRIMO PIANO

Polizze dormienti: l'indagine

Le polizze dormienti per il 2022 sono risultate essere 43.564 per un valore di poco superiore a un miliardo di euro. È quanto emerge dall'indagine promossa dall'Ivass dedicata alle polizze per il caso di morte dell'assicurato della cui esistenza i beneficiari non erano a conoscenza o di polizze "di risparmio" che, giunte alla scadenza, non sono state riscosse dagli interessati. Dal 2017, l'Autorità di vigilanza effettua ogni anno, in collaborazione con l'Agenzia delle Entrate, un incrocio tra i codici fiscali degli assicurati e l'Anagrafe Tributaria, che detiene i dati relativi all'esistenza in vita dei cittadini, per intercettare casi di decessi non noti alle compagnie assicurative, e informa queste ultime così che possano attivarsi per contattare i beneficiari e pagare le polizze. L'Ivass, inoltre, ha monitorato nel tempo l'andamento dei pagamenti e, nei casi necessari, ha richiesto alle imprese di attivarsi "per migliorare e potenziare i processi interni e gestire in modo tempestivo e sistematico le posizioni".

Per gli anni precedenti al 2022, il diritto alla prestazione è stato accertato per il 75,9% degli incroci per il 2021, il 77,7%, per il 2020, e il 63,8% per gli anni ancora antecedenti: per questi le compagnie hanno verificato rispettivamente l'88,4%, il 91% e il 92,5% delle polizze.

Beniamino Musto

MERCATO

La pubblica amministrazione italiana sotto l'attacco degli hacker

Dall'ultimo rapporto del Clusit emerge un quadro inquietante sul livello della cybersecurity italiana, che denuncia come il nostro paese sia stato oggetto di un numero di attacchi assai superiore al resto del mondo. Nel mirino dei criminali informatici sono soprattutto il settore pubblico e quello della sanità

© pixelcreatures - pixbay

Non è una novità che nel corso dell'anno appena concluso gli attacchi dei cybercriminali si siano moltiplicati, complice anche lo stato di guerra che interessa uno dei territori nei quali gli hacker si sviluppano da sempre, la Russia, e il fatto che le aziende fanno sempre più fatica a tenere il passo, vuoi per mancanza di fondi, vuoi per assenza di adeguati piani di gestione del rischio.

La pubblica amministrazione italiana, in particolare, soffre di un'endemica inefficacia in questo senso e l'ultimo rapporto del **Clusit**, pubblicato lo scorso novembre, traccia un quadro abbastanza preoccupante al riguardo.

In Italia, nei primi sei mesi del 2023, si sono verificati moltissimi attacchi, il 40% in più rispetto all'anno precedente e quasi quattro volte più che nel resto del mondo. I cybercriminali sembrano aver capito che bucare le difese dei sistemi italiani è cosa piuttosto semplice, e così vi si accaniscono.

È pur vero che la spesa in cybersecurity continua a crescere, almeno per quanto attiene alle aziende private, ma lo sforzo sembra inefficace: se dal 2018 al primo semestre del 2023 gli incidenti a livello globale sono aumentati del 61,5%, in Italia la crescita complessiva raggiunge il 300%.

Gabriele Faggioli, presidente del Clusit, ha dichiarato che a fine 2022, nel contesto delle tensioni internazionali e del conflitto russo-ucraino, l'Italia appariva per la prima volta e in maniera evidente nel mirino dei cybercriminali, ma nel 2023 questa tendenza si è decisamente consolidata.

Il settore più colpito è quello governativo con il 23% del totale, seguito a breve distanza da quello manufatturiero e da quello della sanità, col 17%.

Per quanto riguarda la pubblica amministrazione, si sono riscontrati attacchi senza precedenti, i cui risultati sono stati definiti disastrosi dagli esperti.

Alla fine dell'anno, i cybercriminali hanno sfruttato un ransomware lanciato dall'organizzazione nota come **Lockbit** per colpire la società **PA Digitale**, cliente di **Westpole**, un fornitore di servizi cloud.

PA Digitale serve 1.300 aziende pubbliche italiane, tra le quali 540 comuni.

I danni causati a un gran numero di servizi al cittadino e all'operatività interna degli enti coinvolti sono difficilmente calcolabili. I sindaci riferiscono di problemi alla gestione degli albi pretori, alla fornitura dei servizi di pagamento online offerti ai cittadini, al sistema dedicato alle carte d'identità e all'anagrafe. Grossi guai anche allo sportello unico delle attività produttive e alla Pec.

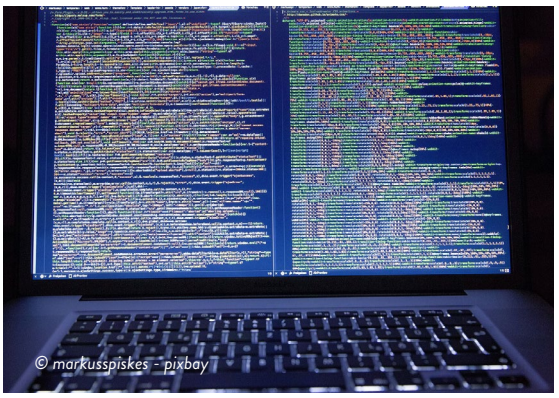
Alcuni comuni sono dovuti tornare alle modalità analogiche per molti servizi.

L'attacco è avvenuto l'8 dicembre 2023 all'alba. I danni variano da ente a ente e dipendono dal tipo di servizi affidati al Cloud Urbi, sviluppato da PA Digitale, le cui funzionalità dipendono proprio dall'infrastruttura di Westpole. *(continua a pag. 2)*

(*continua da pag. 1*) L'agenzia per la cybersicurezza nazionale, **Acn**, riferisce che è fuori dubbio che si sia trattato di un caso straordinario di attacco sistemico, che ha denunciato un'insufficienza di fondo della cybersecurity italiana.

Le fonti riferiscono che nessun dato sarebbe stato esfiltrato dagli enti, ma queste dichiarazioni vanno prese con le pinze: l'attacco alla **ASL di Modena** di pochi giorni prima (il 28 novembre 2023) è stato seguito da ampie rassicurazioni sull'assenza di furto di dati, che sono state poi smentite da quanto pubblicato dai criminali in fase di rivendicazione.

Lockbit è un gruppo criminale *RaaS* (ransomware as a service), che sviluppa e mantiene la funzionalità di una particolare variante di ransomware, un attacco cioè strutturato per estorcere denaro attraverso un ricatto. Il gruppo vende l'accesso al ransomware a individui o gruppi di operatori e ne sostiene la distribuzione in cambio di un pagamento anticipato, di quote di abbonamento, di una parte dei profitti o di una combinazione di queste cose.


© markusspiskes - pixbay

Probabilmente si tratta di un gruppo di hacker russi, o comunque dell'Europa dell'Est, perché l'unico indizio che lasciano è che ogni nuova versione pubblicata del software viene diffusa con un testo in cirillico.

Gli esperti pensano che si debba vedere di quali dati si siano impadroniti e che ci vorrà del tempo per capire come se ne serviranno.

GLI ATTACCHI ALLA SANITÀ

Gli attacchi contro la sanità pubblica continuano ad aumentare, con incursioni sempre più devastanti che denunciano un'incredibile fragilità delle protezioni adottate.

Le cartelle cliniche sarebbero infatti vendute al mercato nero, il cosiddetto *dark web*, a prezzi addirittura superiori a quelli relativi ai dati delle carte di credito.

Mentre una carta di credito può essere bloccata, infatti, i dati delle cartelle cliniche sono inalterabili e possono essere usati per ottenere farmaci, richieste di risarcimento, per furti d'identità, etc., oltre che per ricattare direttamente le vittime.

I dati trattati in sanità sono tra i più delicati e c'è un motivo per cui la legislazione europea per la difesa della circolazione dei dati personali, il Gdpr, li considera né più né meno che un'estensione della persona stessa. Un danno inflitto a un individuo attraverso un utilizzo scorretto o addirittura fraudolento dei suoi dati personali equivale a un pregiudizio grave, come se a essere colpita fosse una sua parte fisica.

Il 22 ottobre 2023 il gruppo **Rhysida** ha preso di mira l'azienda ospedaliera universitaria integrata di Verona. Dal momento che la stessa si è rifiutata di piegarsi al loro ricatto (la richiesta ammontava a 10 bitcoin, circa 350mila euro), i cybercriminali hanno pubblicato per ritorsione centinaia di migliaia di documenti sanitari. (*continua a pag. 3*)

(continua da pag. 2)

Cartelle cliniche, analisi genetiche, diagnosi oncologiche e perfino i referti di abusi sessuali: i dati più sensibili di decine di migliaia di persone sono finiti su internet.

La gang ha usato un malware, cioè un software malevolo, insomma quello che una volta chiamavamo "virus", che blocca i server e ha già messo a segno almeno 50 attacchi in tutto il mondo, incluso quello alla British Library di Londra, i cui dati sono stati messi all'asta a partire da 745mila dollari.

Le razzie ai danni della sanità sono state moltissime e hanno preso di mira ospedali e Asl, come quelle di Padova e dell'Aquila.

Dall'inizio del 2022 alla fine del 2023 il **Csirt** (il centro di risposta agli incidenti informatici), si è occupato di 42 cyber attacchi a strutture sanitarie pubbliche.

Non si tratta di un fatto squisitamente italiano: un rapporto di **Cisco Talos Incident Response** denuncia come, solo nel secondo trimestre del 2023, la sanità abbia rappresentato l'obbiettivo più colpito in tutto il mondo, con un quarto degli attacchi totali e un aumento del 30% dei tentativi di estorsione.

Anche l'**Agenzia dell'Unione Europea per la Cybersecurity** (Enisa) ha riscontrato, tra gennaio 2021 e marzo 2023, 215 casi denunciati, metà dei quali erano ransomware.

In Italia, a dire il vero, la sanità non rappresenta il settore più colpito.

Come abbiamo accennato, da noi lo sono la pubblica amministrazione e le imprese private, ma nel caso della sanità abbiamo a che fare con un impatto assai più drammatico.

Basti pensare al fatto che il blocco di un server implica che le prenotazioni e gli interventi previsti salteranno e che questi enti sono tecnicamente definiti come "infrastrutture piatte" per cui, se riesci ad accedere ad un sistema, puoi facilmente entrare in tutti.

I cybercriminali colpiscono nel mucchio, cercando una falla in cui inserirsi. È una caccia ai danni di sistemi con una data vulnerabilità che gli hacker individuano: se si rendono conto che all'interno dei server ci sono dati pregiati, come quelli sanitari, sanno che potranno rivenderli e guadagnare moltissimo denaro.


© geralt - pixbay


© TheDigitalArtist - pixbay

Dietro gli attacchi si muovono bande con differenti specializzazioni ed ogni fase è curata da gruppi diversi: in pratica, abbiamo a che fare con intere filiere criminali, i cui dettagli sono molto difficili da ricostruire ed è per questo che l'impressione comune è che i cybercriminali restino sempre impuniti.

ALTRI ATTACCHI DI LOCKBIT ALLE INFRASTRUTTURE GOVERNATIVE ITALIANE

Ma torniamo agli attacchi di Lockbit. Questo gruppo ha già rivendicato azioni assai simili nei confronti dei sistemi informatici della Regione Lazio, nel 2021, e poco dopo anche di quelli di **Thalesgroup** e **Accenture**.

Nel 2022 sarebbe stata colpita anche l'**Agenzia delle entrate**. Il gruppo ha rivendicato l'attacco, annunciando di aver sottratto all'ente 100 giga byte di dati, ma l'agenzia ha smentito il fatto.

Come si è detto, le smentite di questo tipo lasciano un po' il tempo che trovano, perché le aziende tendono a proteggersi dalle richieste di risarcimento che cittadini e clienti potrebbero avanzare, dalle multe (anche piuttosto salate) che potrebbero essere inflitte dal Garante per la protezione dei dati e dalla progressiva mancanza di fiducia che può comportare l'essere oggetto di ripetuti attacchi da parte dei cybercriminali, soprattutto per chi opera in ambito finanziario.

Un'indagine effettuata qualche anno fa da **Marsh** rivelò che il 60% dei correntisti bancari dichiaravano di voler abbandonare la loro banca di appoggio, se questa fosse stata oggetto di attacco.

Spesso, inoltre, gli hacker non lasciano segni evidenti delle loro scorrerie, anzi nascondono nel sistema colpito un software malevolo pronto a risvegliarsi, anche a distanza di molto tempo, permettendo loro di ricominciare la loro azione criminale.

Le vittime degli attacchi, in molti casi, si rendono conto di essere state violate solo al ricevimento della rivendicazione o del ricatto da parte degli hacker ed è questo uno dei problemi più difficili da affrontare per le compagnie che coprono il rischio cyber, perché impedisce loro di intervenire immediatamente, in casi in cui il fattore tempo potrebbe risultare determinante per ridurre la portata del danno.

Cinzia Altomare

INSURANCE Daily

LUNEDÌ 29 GENNAIO 2024 N. 2503

RICERCHE

Polizze catastrofi naturali, cresce l'esposizione per il settore

Il nuovo obbligo inserito nella legge di Bilancio scatterà a fine 2024 e si applicherà a tutte le imprese italiane e a quelle estere con stabile organizzazione in Italia. Secondo l'analisi di Cerved, le compagnie assicurative saranno esposte per più di 1.700 miliardi di euro. La macroarea più coinvolta è il Nord-ovest (700 miliardi), Sud e Isole le meno esposte (240 miliardi)

Ammonterà a oltre 1.700 miliardi di euro l'esposizione potenziale massima delle compagnie assicurative in base al nuovo obbligo di legge inserito nella legge di Bilancio, dove il legislatore introduce l'obbligatorietà della copertura dei danni causati da eventi quali sismi, alluvioni, frane, inondazioni ed esondazioni a beni come terreni e fabbricati, impianti e macchinari, attrezzature industriali e commerciali. Quasi mille miliardi in più rispetto ai 790 attuali, stimati su dati **Ania** (si tratta dell'esposizione teorica attuale, al netto dei limiti contrattuali previsti). L'obbligo scatterà a fine 2024 e si applicherà a tutte le imprese italiane e a quelle estere con stabile organizzazione in Italia.

La stima è il risultato di un'analisi approfondita sviluppata da **Cerved**, insieme alle società del gruppo **Mbs Consulting** e **SpazioDati**. L'approccio analitico coinvolge oltre sei milioni di aziende italiane iscritte al registro delle imprese, fornendo una panoramica completa del potenziale impatto sul mercato assicurativo. La stima non rappresenta il valore commerciale dei beni, bensì quello di ripristino che deve essere effettivamente assicurato, e non considera i possibili limiti contrattuali (la compagnia può decidere se esporsi per un indennizzo del 100% del valore assicurato o di una percentuale inferiore).


© cottonbro studio - Pexels

La distribuzione geografica dell'esposizione

Dei 1.701 miliardi, 987 fanno riferimento a fabbricati e terreni, mentre 714 a macchinari, impianti e attrezzature industriali e commerciali. Secondo un'analisi geografica, la macroarea più coinvolta è il Nord-ovest, dove l'esposizione totale si attesta a circa 700 miliardi di euro di cui 400 attribuibili a fabbricati e terreni e 300 a macchinari, impianti e attrezzature industriali e commerciali. Questi dati, che rappresentano il 40% del totale nazionale stimato, sono fortemente influenzati dalla Lombardia, che da sola ha esposizioni per più di 500 miliardi di euro. Il Nord-est manifesta un'esposizione complessiva di circa 430 miliardi di euro, con la caratteristica di mostrare un marcato equilibrio (50% ciascuno) tra fabbricati e terreni, da un lato, e macchinari, impianti e attrezzature industriali e commerciali, dall'altro. Nel Centro si registra invece un'esposizione di circa 330 miliardi di euro (19% del totale), di cui ben 120 associati al valore dei fabbricati e terreni nel solo Lazio. Infine, nel Sud e nelle Isole l'esposizione complessiva ammonta a circa 240 miliardi di euro (14% del totale). In Sicilia e Sardegna il 70% dell'esposizione riguarda fabbricati e terreni

© Pixabay

M.S.

Insurance Daily
Direttore responsabile: Maria Rosa Alaggio alaggio@insuranceconnect.it
Editore e Redazione: Insurance Connect Srl – Via Montepulciano 21 – 20124 Milano
T: 02.36768000 **E-mail:** redazione@insuranceconnect.it
Per inserzioni pubblicitarie contattare info@insuranceconnect.it
Supplemento al 29 Gennaio di www.insurancetrade.it – Reg. presso Tribunale di Milano, n. 46, 27/01/2012 – ISSN 2385-2577