INSURANCE Daily

MERCOLEDÌ 18 GIUGNO 2025 N. 2810

PRIMO PIANO

Ania promuove il ddl Furti

L'Ania accoglie con favore il disegno di legge "Modifiche al Codice penale, al Codice di procedura penale e alla legge 26 luglio 1975, n.354, in materia di furto d'auto", a firma del senatore Dario Damiani, presentato ieri in una conferenza stampa al Senato. Il ddl è volto a contrastare in modo più incisivo i furti d'auto che, sottolinea una nota dell'associazione, "rappresentano quasi una piaga sociale, fortemente monitorata dalle procure". Anche da un punto di vista assicurativo, la concentrazione di furti ha impatti sull'assicurabilità dei veicoli. Inoltre, evidenzia l'Ania, "il fenomeno spesso si rivela essere una frode". Secondo il presidente Giovanni Liverani, le frodi "non riguardano solo le compagnie, ma rappresentano un danno concreto per l'intera collettività. Ogni furto falso o gonfiato si traduce in un aggravio di costi per gli assicurati. Per questo, sosteniamo con convinzione ogni misura che favorisca controlli più efficaci, condivisione di dati e uso intelligente delle tecnologie finalizzato alla prevenzione di tali fenomeni". Pur trattandosi di un intervento normativo mirato a specifici comparti, continua la nota, "l'Ania riconosce che la proposta rappresenta un passo nella giusta direzione, contribuendo a rafforzare il sistema di prevenzione".

Beniamino Musto

MERCATO

L'urgenza di una copertura cat nat per gli edifici residenziali

Gianluca Romagnoli, docente universitario direttore del comitato scientifico della Fondazione Severo Galbusera, ritiene sia necessario pensare a una nuova forma di protezione, che non sia per forza ricalcata sulla polizza obbligatoria per le imprese, sancita dalle legge del 2023, ma che tenga conto delle specificità dei territori, delle normative e del mercato di riferimento

Fatto un obbligo, perché non farne un altro? Il riferimento è alla polizza per le imprese contro le catastrofi naturali, da poco entrata in vigore, seppur coinvolgendo i soggetti interessati con tempi diversi; ma ora (a dire il vero già da qualche anno) si pone la questione di proteggere anche gli immobili residenziali. Da questo spunto è necessario ricercare soluzioni che estendano le coperture oltre l'ambito delle imprese.


© Fondazione Galbusera

***Gianluca Romagnoli**, docente universitario e direttore del comitato scientifico della Fondazione Severo Galbusera*

Eppure, "la maggior ampiezza del tema moltiplica quelle criticità che già sono emerse in sede d'analisi dell'introduzione del primo obbligo", come ha spiegato recentemente **Gianluca Romagnoli**, docente universitario e direttore del comitato scientifico della **Fondazione Severo Galbusera**, durante il convegno *Polizze catastrofali; attualità e prospettive di estensione agli immobili non commerciali*, organizzato dalla fondazione a Padova.

Diverse iniziative parlamentari si sono susseguite su questo tema: l'ultima fu la proposta di legge presentata nel 2019 dall'onorevole **Michela Rostan**, che contemplava un programma di assicurazione obbligatoria per tutti gli edifici privati.

Con l'approvazione della legge che ha sancito l'obbligo per le imprese, come detto, finalmente il concetto di copertura contro le catastrofi naturali è entrato nel dibattito, ma sembra scontentare molti: "la legge – spiega Romagnoli – ha rotto un silenzio e ha posto in evidenza un tema d'interesse generale, quale è la sottoassicurazione, che non riguarda solo i beni impiegati per l'attività imprenditoriale. Per attenuare lo scontento, il legislatore ha delineato delle soluzioni di compromesso che possono apprezzarsi come avvio d'un percorso normativo ma che per ciò stesso hanno un impatto limitato".

L'ASSICURAZIONE? UN'OPERAZIONE RAZIONALE

C'è, ovviamente, anche la questione culturale: in un paese come l'Italia, che percepisce mediamente la polizza assicurativa come una tassa, sarebbero tante le azioni da compiere e le decisioni da prendere per innalzare il livello di protezione anche degli immobili non commerciali. Romagnoli, a questo proposito, torna sul tema della sottoassicurazione che è, appunto, "un problema eminentemente culturale". Secondo il docente dell'Università di Padova, "si dovrebbero incentivare le iniziative di educazione assicurativa" per far comprendere che l'assicurazione "è un'operazione razionale perché consente di spostare un rischio e quindi che il pagamento del premio non è una spesa inutile".

(continua a pag. 2)

(continua da pag. 1)

In questo contesto, "gli intermediari assicurativi hanno un ruolo fondamentale – sottolinea Romagnoli – perché con la loro opera offrono una prima forma di informazione e svolgono un'azione di sensibilizzazione sull'esistenza di rischi che normalmente, per tante ragioni, non sono considerati".


© Pixabay

LA VIA ITALIANA: L'OBBLIGATORIETÀ INDIRETTA

Per aggirare, in parte, lo scoglio del rigetto da parte dei consumatori di una spesa che possono percepire come ingiustificata, conviene guardare all'estero e magari prendere spunto dai paesi più simili al nostro, dove l'assicurazione property funziona meglio che da noi. In parte, le principali differenze con i modelli esteri di gestione delle catastrofi naturali si conoscono: è interessante cercare di capire quali fattori strutturali hanno impedito all'Italia di uniformarsi a quei modelli. "L'esperienza dei paesi, anche europei, è la più varia", racconta Romagnoli: si passa da sistemi che prevedono obblighi assicurativi ad altri che "ammettono una più o meno limitata libertà di sottoscrizione di polizze catastrofali". C'è però un denominatore comune: "tendenzialmente – aggiunge – tutti i paesi prevedono un ruolo fondamentale dello Stato che interviene come garante di ultima istanza degli indennizzi".

Il direttore del comitato scientifico della Fondazione Galbusera propone una via italiana: "si potrebbe pensare a un'obbligatorietà indiretta, rendere conveniente l'assicurazione e penalizzare chi non si assicura, ovviamente affiancandovi l'istituzione di consorzi assicurativi e fondi anche pubblici, supportati dallo Stato".

FRAMMENTAZIONE E COMPLICAZIONE NORMATIVA

Ma l'Italia è di fronte anche ad altri problemi e ostacoli che certamente non agevolano una soluzione al problema della sottoassicurazione nei rami elementari: la frammentazione del territorio e la stratificazione legislativa e regolamentare, da molti giudicata eccessiva, contribuiscono a sottostimare la percezione del rischio da parte di individui e aziende. Ci si chiede se sia possibile uniformare le norme senza perdere le specificità dei territori. "Il problema italiano – interviene Romagnoli – non è causato dalla frammentazione o complicazione normativa. La mancata percezione del rischio è dovuta al fatto nell'intervento dello Stato in caso di avveramento di rischi catastrofali. Non ci si assicura perché si sottovaluta il problema o, addirittura, non lo si considera – chiosa – perché è una costante che alle calamità seguono sempre delle elargizioni pubbliche".

IL MODELLO DEI RISCHI AGRICOLI

Eppure, la polizza non è il solo sistema per proteggersi. Oltre alla legge sulle catastrofi naturali, sul mercato assicurativo, e non solo, sono presenti vari modelli di gestione degli eventi estremi, per esempio in agricoltura. Anche in questo caso possono venirci in soccorso le esperienze estere, che mostrano come "l'intervento assicurativo sia solo uno dei tasselli di un sistema che intende neutralizzare i rischi catastrofali", sottolinea il docente.

"Oltre a quello, però – continua –, si devono predisporre forme consortili, per attenuare il costo dei trasferimenti dei rischi, fondi che ne assumono una parte e forme di coinvolgimento indiretto dello Stato". Un modello interessante su cui Romagnoli inviata a riflettere è appunto quello dei rischi agricoli, "dove si prevede – ricorda – che a fianco di iniziative di copertura volontarie operi un fondo, **AgriCat**, alimentato da finanziamenti pubblici e privati".

LA LISTA DELLE COSE DA FARE

Pensare a un sistema di gestione del rischio catastrofale anche per il patrimonio residenziale significa contemporaneamente stabilirne la sostenibilità: per questo Romagnoli immagina in primis una ridefinizione del ruolo di **Sace**, "di per sé limitato anche rispetto a quanto già previso per l'attuale obbligo assicurativo delle imprese", ha detto durante il convegno, e magari anche il coinvolgimento di **Cassa depositi e prestiti** per l'emissione di cat bond. Poi occorre la ridefinizione di prodotti assicurativi adeguati, che scaturiscano da "una Pog ripensata in ragione del target market di riferimento".

Tutto questo, infine, non può essere sufficiente se non accompagnato da azioni pubbliche e private di mitigazione dei rischi catastrofali, da indicazioni normative più stringenti per l'esercizio del potere di pianificazione territoriale, nonché la cantierizzazione di opere pubbliche di messa in sicurezza del territorio.

Fabrizio Aurilia

INSURANCE Daily

MERCOLEDÌ 18 GIUGNO 2025 N. 2810

GLOSSARIO

Vulnerabilità "zero-day"

Quasi tutti i software hanno delle falle attraverso le quali gli hacker riescono ad accedere ai sistemi per impadronirsi dei dati. Questa particolare tipologia viene utilizzata principalmente per gli attacchi rivolti agli sviluppatori di software e alle software house: ecco come funziona e quali sono le vittime designate

Zero-day (o anche *0-day*) è una falla nella sicurezza di un sistema informatico utilizzata principalmente per gli attacchi rivolti agli sviluppatori di software e alle software house. Questo attacco funziona generalmente hackerando il computer dello sviluppatore, prima del rilascio. Si tratta quindi di una minaccia assai pericolosa, perché le aziende di software investono molto per lo sviluppo dei loro programmi e se questi fossero oggetto di un attacco zero-day, finirebbero col buttare via buona parte del denaro investito, perché il software risulterebbe pressoché inutilizzabile, o comunque gravemente compromesso.

Quasi tutti i software contengono vulnerabilità

Nonostante l'obiettivo degli sviluppatori sia di fornire un prodotto che funzioni perfettamente, quasi tutti i software contengono dei *bug*, cioè un rischio per la sicurezza del software stesso: in gergo, si chiama *vulnerabilità*.

Le vulnerabilità variano moltissimo e possono essere sfruttate in maniera assai diversa da parte degli hacker. L'espressione zero-day è usata per descrivere vulnerabilità della sicurezza che vengono utilizzate dagli hacker per attaccare i sistemi, quando gli stessi sono sul punto di essere pubblicati.

Il termine si riferisce al fatto che il fornitore (la software house) o lo sviluppatore, una volta venuti a conoscenza della falla, hanno *zero giorni* di tempo per risolvere il problema.

Insomma, un attacco di questo tipo viene sferrato quando l'hacker riesce a sfruttare una falla, prima che gli sviluppatori abbiano la possibilità di porvi rimedio.

Differenza tra patch e codice exploit

Come si accennava, un software presenta spesso vulnerabilità della sicurezza che gli hacker possono sfruttare. D'altro canto, gli sviluppatori sono sempre alla ricerca di debolezze da correggere e si impegnano a trovare una soluzione, definita *patch* (letteralmente, cerotto o toppa), da rilasciare in un nuovo aggiornamento del programma stesso. A volte, però, gli hacker individuano tali vulnerabilità prima degli sviluppatori di software e, mentre le falle sono ancora esposte, riescono a implementare dei codici per sfruttarle: i *codici exploit*. Grazie a essi è possibile attaccare gli utenti del software (chi ha acquistato il programma o lo adopera), che diventano vittime, ad esempio, di furti di identità o di altre forme di cybercrimine.


© Franz Bachinger - Pixabay

Dopo aver identificato una vulnerabilità zero-day, gli hacker cercano di raggiungere il relativo sistema e a questo scopo si servono di un'email o di un altro tipo di messaggio, fingendo di essere un contatto noto o legittimo: si tratta della tecnica chiamata ingegneria sociale.

Lo scopo del messaggio è convincere un utente a eseguire un'azione, come aprire un file o visitare un sito web dannoso. Il risultato di questa azione è il download del malware dell'autore dell'attacco, che si infiltra nei file dell'utente e ruba i dati riservati.

Molti conoscono, ad esempio, il *phishing*: una particolare tecnica di ingegneria sociale, che utilizza canali di comunicazione come email, sms o messaggi per ingannare la vittima.

Quando una vulnerabilità diventa nota, gli sviluppatori creano una patch per fermare l'attacco, ma spesso le vulnerabilità della sicurezza non vengono scoperte subito. A volte passano giorni, settimane o addirittura mesi, prima che gli sviluppatori identifichino la vulnerabilità all'origine dell'attacco e anche dopo il rilascio di una patch zero-day, non tutti gli utenti la implementano in tempi brevi.

(continua a pag. 4)

INSURANCE Daily

MERCOLEDÌ 18 GIUGNO 2025 N. 2810

(continua da pag. 3)

In attesa nell'ombra prima di attaccare

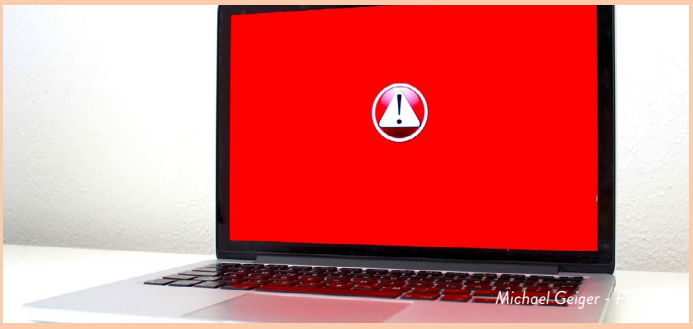
Purtroppo, gli hacker diventano sempre più veloci a sfruttare le vulnerabilità, non appena scoperte. Insomma, assai spesso arrivano prima che vi si possa porre rimedio e i codici exploit sono in vendita nel dark web a cifre esorbitanti, anche se una volta individuati e corretti non rappresentano più alcuna minaccia.

In pratica, gli attacchi zero-day sono pericolosi proprio perché gli unici a esserne a conoscenza sono proprio i loro autori, ovvero gli hacker. In più, questi attacchi sono infidi: dopo essersi infiltrati in una rete, i criminali possono attaccare immediatamente o restare in attesa del momento più vantaggioso per farlo.

Sono molte le categorie di malintenzionati che possono sferrare attacchi zero-day, come i cybercriminali (la cui motivazione è il guadagno economico), gli *hacktivist* (spinti da motivazioni politiche o sociali, che agiscono per attirare l'attenzione sulla loro causa), lo spionaggio industriale (hacker che spiano le aziende per ottenere informazioni riservate), fino al cyberwarfare, agenti politici che spiano o attaccano l'infrastruttura informatica di un'altra nazione.

Bisogna poi tener conto che un attacco zero-day può sfruttare le vulnerabilità dei sistemi più svariati, dai semplici sistemi operativi alle applicazioni office, dalle componenti open-source all'Internet of Things.

Esiste quindi un'ampia gamma di potenziali vittime, dai singoli utenti che utilizzano un sistema vulnerabile (come un browser o un sistema operativo), a quelli che accedono a dati aziendali importanti, (ad esempio, una proprietà intellettuale); dai dispositivi hardware, firmware e IoT, fino alle agenzie governative, vittime di obiettivi politici e minacce alla sicurezza nazionale.



Attacchi mirati e non mirati

È anche utile comprendere la differenza tra attacchi zero-day mirati e non mirati: i primi hanno obiettivi potenzialmente di valore, ad esempio grandi organizzazioni, agenzie governative o persone di alto profilo; i secondi sono invece rivolti contro gli utenti generici di sistemi, come sistemi operativi o browser.

Bisogna tener conto che, anche quando gli autori degli attacchi non prendono di mira utenti specifici, moltissime persone possono rimanere vittime degli attacchi zero-day, come danno collaterale. Gli attacchi non mirati, inoltre, hanno lo scopo di colpire il maggior numero di utenti, e quindi si dirigono dichiaratamente verso l'utente medio, che normalmente è assai meno protetto di un'azienda.

Può essere difficile individuare le vulnerabilità zero-day, dal momento che possono assumere diverse forme: dal criptaggio dei dati, all'assenza di autorizzazioni, dalla violazione di algoritmi ai problemi con la sicurezza delle password, e così via.

Data la natura di questi tipi di vulnerabilità, le informazioni dettagliate sugli exploit zero-day sono disponibili solo dopo che gli stessi sono stati identificati. È anche possibile che siano esplicitamente esclusi dalle coperture assicurative.

Il caso di Apple

Non parliamo di una questione lontana dalla nostra vita quotidiana: alcuni ricorderanno che **Apple** ha recentemente rilasciato aggiornamenti di emergenza per iOS e iPadOS, per correggere una vulnerabilità zero-day che l'azienda ritiene sia stata sfruttata in attacchi altamente sofisticati. La società di Cupertino non ha fornito dettagli sugli attacchi né sulle identità dei presunti attori malevoli coinvolti. Tuttavia, la falla è stata scoperta da un componente del gruppo di ricerca interdisciplinare *Citizen Lab* dell'Università di Toronto e si teme che la stessa sia stata sfruttata in offensive mirate contro giornalisti, dissidenti e oppositori politici.

Attacchi di questo tipo si basano spesso su exploit zero-day, in grado di compromettere i dispositivi, senza richiedere alcuna interazione da parte della vittima (sono anche definiti *attacchi zero-click*).

In sintesi, dunque, questo tipo di attacco può davvero coinvolgere tutti, ed è importante che l'utente medio sia al corrente dei pericoli a esso collegati.

Cinzia Altomare

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 18 giugno di www.insurancetrade.it – Reg. presso Tribunale di Milano, n. 46, 27/01/2012 – ISSN 2385-2577