POLIZZE PROPERTY

© Jakarin2521 - iStock

CHE FARE CON LE ESCLUSIONI DI CYBERWAR

NEL CONTESTO INTERNAZIONALE SEMPRE PIÙ TESO IN CUI STIAMO VIVENDO DALL'AGGRESSIONE RUSSA ALL'UCRAINA, ANCHE LE ASSICURAZIONI DEVONO CAPIRE MEGLIO COME PROTEGGERSI DAGLI ATTACCHI INFORMATICI CHE SONO SEMPRE PIÙ ASSIMILABILI AD ATTI DI GUERRA.
LE INFRASTRUTTURE E LE AZIENDE DI TUTTO IL MONDO SONO A RISCHIO COSTANTE DELL'AZIONE DEGLI HACKER

di Cinzia Altomare

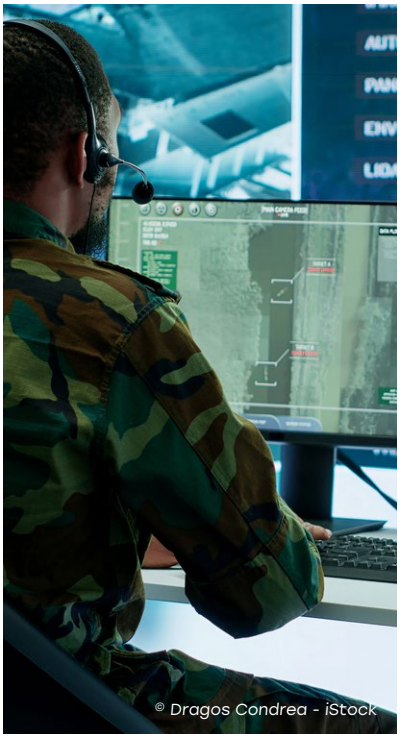
Gli assicuratori cyber stanno attraversando un doloroso processo di adattamento, nel tentativo di trovare un equilibrio tra le aspettative degli assicurati e la possibilità di fronteggiare il rischio massivo che un attacco di *cyberwar* potrebbe comportare. Il dibattito ha visto una continua riformulazione delle diverse clausole di esclusione proposte, con wording sempre diversi e sempre vulnerabili a critiche sulla chiarezza della loro portata. Gli assicuratori dei rami property, d'altro canto, preferiscono spesso non insistere sulla presenza di tali esclusioni nelle loro polizze, probabilmente perché incerti sulle reali conseguenze che una guerra informatica potrebbe avere sui loro portafogli. È possibile che si sia trattato di una strategia per rimanere in disparte, finché non sia stato raggiunto il consenso da parte degli specialisti di cyber risk, ma ciò può comportare dei problemi.

Anche qualora abbiano previsto un'esclusione specifica, i sottoscrittori property non possono sentirsi interamente al sicuro, perché molti loro testi condividono con quelli delle polizze cyber una certa mancanza di chiarezza. Anche in questo caso, si vedono poche esclusioni davvero complete, in particolar modo all'interno delle polizze *all risks*. Nonostante i loro sforzi, insomma, molti assicuratori property si trovano a essere esposti a questo particolare rischio, il che suggerisce che si debba trovare una soluzione, se non si vuole rischiare di dover fronteggiare sinistri massivi da cyberwar, pur avendo pensato di averli esclusi.

Come sappiamo, ciò che fa davvero paura agli assicuratori non sono certo i sinistri, ma la possibilità di dover indennizzare eventi del tutto imprevisti, per i quali non siano state allocate riserve di alcun tipo.

COS'È E COME SI COPRE IL RISCHIO CYBER

Col termine *cyber risk* o *rischio informatico* ci riferiamo a perdite di dati causate da terzi in genere, come dipendenti dell'azienda assicurata, collaboratori esterni e soggetti sconosciuti. Queste perdite possono includere il furto, la compromissione dell'integrità e il dan-


© Dragos Condrea - iStock

neggiamento di qualunque tipo di risorse informatiche e tecnologiche, interne ed esterne. Ciò comprende le frodi e, ovviamente, gli atti di guerra informatica.

Per quanto le coperture assicurative per alcuni tipi di rischi informatici siano offerte già dalla fine degli anni '80, la nascita di un prodotto autonomo di assicurazione cyber rappresenta un'aggiunta relativamente nuova nei portafogli di broker e assicuratori.

Al momento, le coperture assicurative cyber possono esistere in tre forme principali:

a) polizze autonome che coprono i rischi informatici;
b) estensioni speciali su polizze esistenti, di solito property, che offrono una copertura informatica più o meno estesa;
c) coperture fornite da polizze tradizionali, generalmente all risks, in modo non esplicito, per la mancanza di esclusioni relative a questa tipologia di rischio.

Possiamo considerare le prime due forme come normali tipi di protezione offerti dal mercato, ma l'ultima riflette ciò che gli esperti definiscono esposizione silente (*silent exposure*) e qui potremmo trovarci di fronte a problemi anche seri.

UNA POLIZZA CHE COMPRENDE ANCHE LA RESPONSABILITÀ

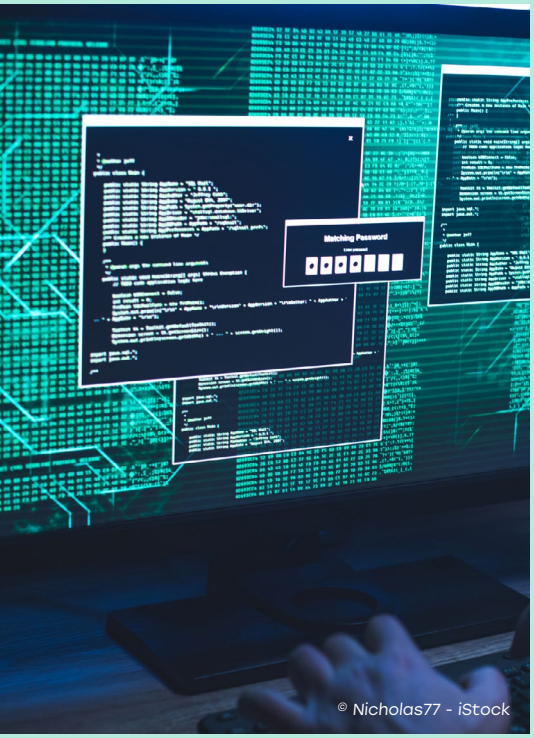
Un altro aspetto da non dimenticare è che nei rami danni distinguiamo le coperture *first party* cioè quelle property, dalle *third party*, che sono associate ai rischi di responsabilità. Ma quando parliamo di cyber risk o comunque di rischi inerenti al rischio informatico, la copertura offerta comprende entrambe: la parte property e quella di responsabilità. La prima risarcisce l'assicurato per i danni subiti in seguito alla violazione o distruzione di dati, l'estorsione, il furto degli stessi, la riparazione di sistemi, ecc. La seconda si riferisce invece ai danni subiti da terzi a causa della violazione subita.

Le assicurazioni diverse da quelle cyber escludono generalmente il rischio cyber, inteso come fattore scatenante del sinistro, le polizze cyber, invece, escludono spesso le lesioni personali e i danni fisici alla proprietà.

Un'esposizione *silent*, anche nota come *esposizione informatica non affermativa*, si verifica quando la copertura per un evento informatico non è esplicitamente esclusa da una polizza assicurativa, ovvero quando la relativa esclusione non sia sufficientemente chiara, e si sono verificati casi piuttosto interessanti in questo senso.

L'AZIONE DI NOTPETYA E LE SUE CONSEGUENZE

Un esempio è rappresentato da un sinistro del 2017, quando il mercato fu colpito dal malware denominato **NotPetya**, uno degli attacchi informatici più devastanti dall'invenzione di internet, che costò più di 10 miliardi di dollari. Le aziende colpite dall'attacco includevano: **Merck** (danni stimati in 870 milioni di dollari); **FedEx** (danni stimati in 400 milioni) e **Maersk** (danni stimati in 300 milioni).



© Nicholas77 - iStock

Un'altra azienda che subì l'attacco NotPetya fu la **Mondelez**, nota per i biscotti *Oreo* e i cioccolatini *Cadbury*. Il malware NotPetya infettò due dei suoi server, colpendo una parte significativa delle applicazioni Windows utilizzate, nonché le reti di vendita e distribuzione. Questo caso dimostra quanto un'esposizione silent possa costare a un'azienda: l'attacco provocò perdite per circa 100 milioni di dollari che Mondelez cercò di recuperare attraverso la sua polizza all risks, dal momento che la copertura della stessa includeva:

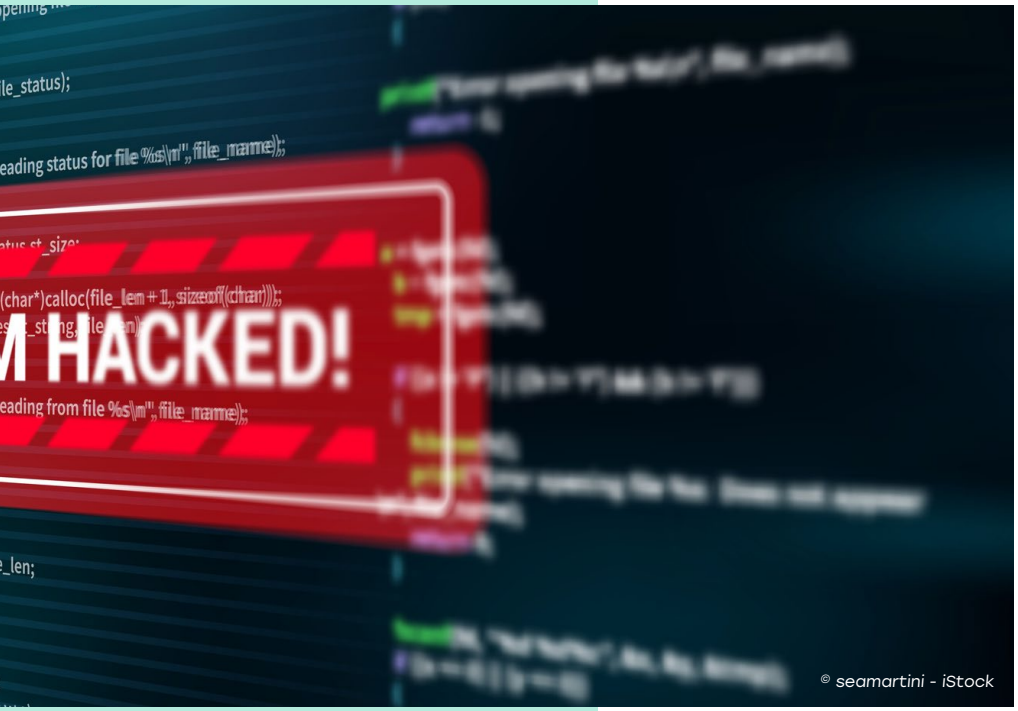
- la perdita fisica o il danno a dati elettronici, programmi o software, inclusa perdita fisica o danno causato dall'introduzione malevola di un codice macchina o di un'istruzione;
- la perdita effettiva e le spese aggiuntive sostenute dall'assicurato durante il periodo dell'interruzione derivante dal mancato funzionamento degli strumenti o dei supporti elettronici di elaborazione dati dell'assicurato.

Dunque, la copertura includeva specificamente la perdita fisica o il danno a dati elettronici, programmi o software, causato dall'introduzione dannosa di un codice macchina o di un'istruzione. L'assicuratore, però, decise di respingere la richiesta di indennizzo, sulla base di un'esclusione che limitava il risarcimento in caso di danni derivanti direttamente o indirettamente da un "atto ostile o bellicoso [...] da parte di qualsiasi governo o potere sovrano". È abbastanza probabile che tale esclusione riflettesse quella contenuta nei trattati di riassicurazione della compagnia.
Seguirono molte discussioni sulla natura dell'attacco NotPetya e se lo stesso costituisse un "atto bellicoso" o "paragonabile a un atto di guerra". Alla fine, la questione fu risolta con un accordo

negoziato, che fu mantenuto riservato.
In sintesi, comunque, l'incidente di NotPetya ha fatto capire all'intero mercato che le esclusioni di war risk e cyberwar incluse nella maggior parte delle polizze property non erano adatte allo scopo, perché in realtà non erano state redatte tenendo conto di un contesto cyber. Pertanto, le conseguenze di NotPetya hanno portato assicuratori e riassicuratori a rivedere i termini e le condizioni delle loro polizze, per evitare che una situazione del genere si ripeta.

PACTA SUNT SERVANDA

Anche coloro che non sono pratici di termini legali conoscono l'espressione latina *pacta sunt servanda*. Essa prevede che un contratto faccia legge tra le parti, cioè, che i termini dei contratti debbano essere rispettati. È un principio antico, probabilmente consolidatosi



© seamartini - iStock

durante il Medioevo, che è stato recepito nelle legislazioni di tutto il mondo. Come tutti i principi, ha le sue eccezioni, ma avere condizioni scritte chiaramente rappresenta il primo passo per evitare future controversie.

Quando parliamo di assicurazione e riassicurazione, è fondamentale garantire che termini e condizioni siano al passo con i tempi e riflettano l'intenzione comune delle parti. Una clausola scritta in modo non chiaro o un'esclusione ambigua possono generare costi aggiuntivi, non necessari e soprattutto imprevisti.

Per evitare interpretazioni errate e dibattiti, un'esclusione informatica ben ponderata e ben scritta è basilare. È dunque evidente che le clausole contrattuali progettate per escludere le perdite derivanti dalla guerra informatica, o cyberwar, non sono così solide come si pensava e continuano a essere messe alla prova nei tribunali.

DEFINIRE UN ATTACCO INFORMATICO OSTILE O BELLICOSO

Un primo passo che può aiutare a mitigare un'esposizione silente di tale tipo è quello di eseguire un'analisi delle polizze e dei contratti in corso, per verificare la posizione della copertura cyber in genere. Più specificamente, l'analisi dovrebbe valutare se l'esposizione al cyberwar sia adeguatamente affrontata e se è presente nel contratto (tramite inclusione affermativa) o esclusa, sempre in modo affermativo, cioè chiaro.

Invece, la presenza di esclusioni silent nelle polizze property parte dal presupposto che la stessa non sia coperta e, in tal caso, non risulterebbero coperte nemmeno le perdite derivanti dalla mancata disponibilità dei dati o da malfunzionamenti del sistema, ad esempio nel caso in cui i dati stessi siano stati danneggiati o cancellati.

Tuttavia, perché l'esclusione abbia un senso sul piano tecnico, è necessario che vi siano definizioni dettagliate sui sistemi informatici e gli attacchi cyber in genere e, soprattutto, su ciò che possa rappresentare un *attacco informatico ostile o bellicoso*.

GLI ATTACCHI INFORMATICI SONO ATTI DI CYBERWAR

In un altro caso rimasto famoso, quello di Merck e International Indemnity contro **Ace American Insurance Company** e altri assicuratori, è risultata piuttosto evidente la collisione tra le esclusioni presenti in una polizza property e quelle delle cyber. Il tribunale ha ritenuto che un'esclusione standard per *atti di guerra* avrebbe tenuto gli assicuratori property al sicuro solo se si fosse trattato di atti di *guerra convenzionale* e dunque non informatica. Anche recentemente, nel Regno Unito, una dichiarazione della Corte d'appello sulle *war risk exclusion* (sempre in ambito property), ha illustrato che tale esclusione può avere effetto solo nel caso in cui si parli di attacchi di tipo convenzionale e cioè, ancora una volta, non informatica.

Ancora oggi questo problema è suscettibile di più soluzioni, ma è davvero il momento di fare chiarezza. La guerra in Ucraina ha dimostrato quanto possa essere importante risolvere la questione, perché, mai come prima, i casi di attacchi informatici che colpiscono ovunque nel mondo si configurano come atti di cyberwar, o per lo meno, come qualcosa di molto simile a essi.

La maggior parte degli assicuratori cyber ha ormai riconosciuto il rischio: è giunto il momento che sul lato property si faccia lo stesso.