LLOYD'S

Emerging Risks Report 2017

Tecnologia

Calcolare I costi
La decodifica delle esposizioni cyber

CYENCE

Disclaimer dei Lloyd’s di London

Questo rapporto è stato prodotto dai Lloyd’s e da Cyence a scopi puramente informativi. Si è presa ogni precauzione nella raccolta dei dati e nella preparazione del rapporto; ciononostante i Lloyd’s non rendono alcuna dichiarazione o rilasciano garanzie rispetto alla sua accuratezza e completezza ed escludono espressamente in base a quanto permesso dalla legge tutto ciò che potrebbe essere altrimenti implicito.

I Lloyd's non accettano alcuna responsabilità per perdite o danni di qualsivoglia natura procurati a persone in conseguenza ad azioni intraprese o non intraprese sulla base di qualsiasi dichiarazione, fatto, cifra o espressione di opinioni o convinzioni contenute in questo rapporto. Questo rapporto non è da considerarsi una consulenza di alcun tipo.

Sui Lloyd’s

I Lloyd's sono il mercato mondiale per le assicurazioni e riassicurazioni speciali. Sotto il nostro nome riconosciuto a livello globale, operiamo come custodi del mercato. Sostenuti da capitali globali diversificati e da ratings finanziari eccellenti, i Lloyd’s lavorano con una rete mondiale per far crescere il mondo assicurato – costruendo la resilienza delle comunità locali e rafforzando la crescita economica mondiale.

Grazie all’esperienza maturata nei secoli, i Lloyd’s sono le fondamenta dell’industria assicurativa ed il suo futuro. Il mercato dei Lloyd’s, guidato da sottoscrittori e broker esperti attivi in oltre 200 territori, sviluppa le assicurazioni essenziali, complesse e critiche necessarie per sostenere il progresso umano.

Su Cyence

Cyence mette a disposizione dell’industria assicurativa gli strumenti per comprendere l’impatto del rischio cyber nel contesto di dollari e probabilità. Il suo esclusivo approccio combina modellazione del rischio/economia, sicurezza cyber e analitiche dei big data allo scopo di creare una piattaforma per la modellazione economica del rischio cyber. La Piattaforma Cyence e le analitiche sono utilizzate dai leaders dell’industria assicurativa mondiale per agevolare la comprensione e la gestione del rischio cyber e per la creazione di nuovi innovativi prodotti assicurativi.

Contatti

Trevor Maynard
Head of Innovation
trevor.maynard@lloyds.com

Per domande di carattere generale relative a questo rapporto ed sui lavori dei Lloyd’s sull’innovazione, contattare innovation@lloyds.com

Sugli autori

Trevor Maynard PhD, MSc, FIA has degrees in pure maths and statistics and is a Fellow of the Institute of Actuaries. He is Head of Innovation at Lloyd’s including responsibility for horizon scanning and emerging risks. Subjects covered in recent years include: the economic and social implications of a food system shock; the effects of cyber-attacks on the US energy grid and an exploration of aggregation modelling methods for liability risks.

He is co-chairman of OASIS, an open modelling platform for catastrophe models and sits on the Board of the Lighthill Risk Network.

George Ng, a founder and Chief Technology Officer, leads major research projects and initiatives at Cyence. Previously, he was the Chief Data Scientist at YarcData. George has also worked as a Research Scientist at DARPA and US-CERT and as faculty at American University. He received his PhD from UC Irvine and B.A. from UC Berkeley, both in Economics.

Ringraziamenti

Per visionare i ringraziamenti consultare il rapporto completo.

Riassunto

Lo scopo di questo rapporto è di fornire agli assicuratori che sottoscrivono le coperture cyber alcuni scenari realistici e credibili per agevolare la quantificazione delle aggregazioni dei rischi cyber. La comprensione delle responsabilità cyber e delle esposizioni ai rischi è relativamente poco sviluppata in confronto ad altri rami di assicurazione.

Comprendendo l'esposizione al rischio cyber, gli assicuratori possono migliorarne la gestione all'interno del loro portafoglio, determinare limiti adeguati e acquisire la fiducia necessaria per espandere la propria attività in questo ramo in rapida crescita.

Il rapporto è pensato per i risk managers i cui affari sono esposti ai tipi di attacchi descritti nei due scenari del rapporto: una violazione che blocca l'operatività del loro fornitore del servizio cloud o un attacco che causa il guasto di un sistema operativo particolare della loro azienda, dei loro clienti, fornitori e/o partners di business.

Ognuno di questi scenari comprende una serie di variabili incluse la possibile attenuazione dei rischi e la risposta all'attacco cyber. Significa che le organizzazioni possono considerare l'impatto sulle loro operazioni.

Metodologia

Questo rapporto è stato sviluppato grazie alla collaborazione tra Lloyd's e Cyence che hanno messo insieme un gruppo multidisciplinare di esperti nella sicurezza cyber, nella modellazione dei rischi economici e nell'assicurazione cyber.

Cyence ha operato un processo di ricerca strutturato in sette fasi per generare gli scenari e produrre le stime delle perdite menzionate in questo rapporto. Le sette fasi sono state:

1. Revisione delle tecnologie maggiormente adottatte ed utilizzate nelle varie industrie
2. Revisione di altri fattori non tecnici
3. Raccolta ed elaborazione dei dati per le esposizioni
4. Analisi dei processi di accumulo delle esposizioni
5. Selezione degli scenari, modelli di frequenza e criticità
6. Discussione e revisione con esperti di assicurazione e sicurezza cyber
7. Calcoli delle perdite e revisione finale

I Lloyd's hanno lavorato con la Lloyd's Market Association su una serie di workshop e collaborazioni che hanno coinvolto sottoscrittori cyber del mercato dei Lloyd's per discutere ed includere le loro riflessioni nel rapporto, e identificare le implicazioni e considerazioni per l'industria assicurativa.

Attacchi cyber – una minaccia crescente

Il rischio cyber è una minaccia in crescita a livello mondiale. La digitalizzazione sta rivoluzionando i modelli di business e trasformando le vite di tutti i giorni e sta rendendo l'economia globale sempre più vulnerabile agli attacchi cyber.

Per questo motivo, stanno aumentando le conseguenze assicurative ed economiche dei crimini cyber. Nel 2016, la stima dei costi per le aziende derivanti dagli attacchi cyber si aggira intorno ai 450 miliardi di dollari all'anno a livello globale *(Graham, 2017*). Gli assicuratori stanno sempre più concretamente aiutando gli assicurati a gestire questi eventi, che vanno dalle violazioni individuali causate da insiders ed hackers dolosi, a perdite più consistenti per violazioni delle strumentazioni dei punti vendita, attacchi di ransomware (con richiesta di riscatto) come BitLocker e WannaCry, ed attacchi che impediscono la distribuzione di servizi quali Mirai.

La minaccia cyber sta aumentando e si prevede che continuerà a crescere considerando che l'economia mondiale continua a digitalizzare le operazioni, le catene di fornitura e le transazioni di business, così come i servizi per dipendenti e clienti.

Sfide per gli assicuratori

Insieme alle minacce cyber cresce la domanda di assicurazione per questi rischi. Oggi il team Lloyd's che gestisce questo settore stima che il valore del mercato cyber globale si aggira tra i 3 e 3,5 miliardi di dollari (*Stanley, 2017);* alcuni analisti stimano che entro il 2020 questo valore raggiungerà i 7,5 miliardi di dollari *(PwC, 2015)*. Nel 2016, gli assicuratori property/casualty hanno sottoscritto 1,35 miliardi di dollari di premi diretti relativi a coperture cyber, un

aumento del 35% dal 2015, secondo i rapporti di Fitch Ratings e A.M. Best.

Nonostante questa crescita, la comprensione degli assicuratori delle responsabilità cyber e delle aggregazioni dei rischi è ancora un processo in evoluzione considerando che l'esperienza e la conoscenza di questi attacchi sta aumentando. Anche l'utilizzo di internet da parte degli assicurati sta cambiando, modificando rapidamente nel tempo l'accumulo del rischio cyber in un modo che non si verifica con altri tipi di rischio.

La modellazione dei rischi assicurativi tradizionali si basa su fonti di informazione istituzionali quali dati nazionali o a livello di industria, ma non esistono fonti equivalenti per il rischio cyber e i dati per modellare gli accumuli devono essere raccolti in scala. Questo fa sì che la raccolta dei dati ed il loro aggiornamento regolare siano componenti chiave per meglio comprendere l'evoluzione del rischio.

In che modo il rapporto può approfondire la comprensione dell'aggregazione del rischio cyber

Questo rapporto è stato pensato per accrescere la comprensione di assicuratori e risk managers rispetto alle responsabilità riguardanti il rischio cyber e le relative aggregazioni. Analizza l'aggregazione attraverso il prisma di sei tendenze che contribuiscono alla vulnerabilità digitale. E' cruciale comprendere questi trends per capire l'aggregazione cyber.

Questi trends sono:

1. Volume dei contributori: Il numero delle persone che sviluppano software è cresciuto in modo significativo negli ultimi tre decenni; ogni contributore potrebbe potenzialmente aggiungere vulnerabilità al sistema attraverso l'errore umano.

2. Volume dei software: Oltre al crescente numero di persone che modificano i codici, aumenta anche il numero dei codici esistenti. Più codici significa potenziale per più errori e dunque maggiore vulnerabilità.

3. Software open source: Il movimento open-source ha portato a molte iniziative innovative. Tuttavia molte librerie open-source sono caricate online e, sebbene si ritenga che siano state riviste sotto l'aspetto della loro funzionalità e sicurezza, non è sempre vero. Errori nei codici primari potrebbero essere copiati inconsapevolmente nelle iterazioni successive.

4. Software vecchi: Più tempo un software rimane sul mercato, maggiore è il tempo a disposizione di attori dolosi per trovare le vulnerabilità. Molte persone e aziende utilizzano software obsoleti che hanno alternative più sicure.

5. Software a più livelli: I nuovi software di solito sono costruiti sui codici software precedenti. Ciò rende le operazioni di test e di correzione molto difficoltose oltre a richiedere molte risorse.

6. Software"Generati": I codici possono essere prodotti attraverso processi automatizzati che è possibile modificare per intenti dolosi.

Questo rapporto utilizza scenari per quantificare l'ampia varietà di danni che può essere causata da due diversi eventi cyber.

Scenario 1: Violazione del fornitore del servizio cloud

Un gruppo sofisticato di "hacktivists" si propone di causare danni ai fornitori di servizi cloud ed ai loro clienti per attirare l'attenzione sugli impatti ambientali provocati dalle aziende e dall'economia moderna. Il gruppo opera una modifica dolosa ad un "hypervisor" che controlla l'infrastruttura cloud. Ciò causa il blocco dei server basati su cloud dei clienti, provocando l'interruzione generalizzata del servizio e dell'attività.

Scenario 2: Attacco alla vulnerabilità di massa

Un analista cyber accidentalmente dimentica sul treno la sua borsa che contiene una copia cartacea di un rapporto su una vulnerabilità che interessa tutte le versioni di un sistema operativo in uso presso il 45% del mercato globale. Questo rapporto viene venduto sul mercato nero della rete ed acquistato da un numero indeterminato di criminali non identificati che sviluppano dei sistemi specifici ed iniziano ad attaccare le aziende vulnerabili per ottenere guadagni finanziari.

Risultati principali

Il rapporto riporta cinque importanti risultati:

- Gli impatti economici degli eventi cyber causano un'ampia gamma di potenziali perdite economiche. Per quanto riguarda lo scenario sul blocco del servizio cloud descritto nel rapporto, queste perdite vanno da 4,6 miliardi di dollari per un grande evento fino a 53,1 miliardi di dollari per un avvenimento estremo; nello scenario riguardante la vulnerabilità di un software di massa, le perdite si aggirano tra i 9,7 miliardi di dollari per un grande evento fino a 28,7 miliardi per un avvenimento estremo[a].
- Le perdite economiche potrebbero essere molto più basse o alte della media prevista negli scenari, a causa dell'incertezza circa l'aggregazione cyber. Per esempio le perdite medie nello scenario riguardante il blocco del servizio cloud sono pari a 53 miliardi di dollari per un evento estremo ma potrebbero aumentare fino a 121,4 miliardi o abbassarsi fino a 15,6 miliardi[b], in base a fattori quali le diverse organizzazioni coinvolte e la durata del blocco del servizio cloud.
- Gli attacchi cyber hanno il potenziale di causare perdite assicurate per miliardi di dollari. Per esempio, nello scenario sul servizio cloud le perdite assicurate si aggirano fra i 620 milioni di dollari per un grande sinistro fino a 8,1 miliardi per un evento estremo. Per lo scenario sulla vulnerabilità del software di massa, le perdite assicurate vanno dai 762 milioni di dollari (grande sinistro) ai 2,1 miliardi (evento estremo).
- Gli scenari evidenziano un gap assicurativo tra i 4 (per grande sinistro) ed i 45 (evento estremo) miliardi di dollari per lo scenario sui servizi cloud – ciò significa che le perdite assicurate sono rispettivamente tra il 13% ed il 17%. Il gap della sottoassicurazione è invece tra i 8,9 (grande sinistro) ed i 26,6 (evento estremo) miliardi di dollari per lo scenario sulla vulnerabilità – ciò significa che solo il 7% delle perdite economiche è coperto.
- Se si valuta la stima dei premi del mercato attuale in rapporto alle stime delle perdite previste negli scenari descritti nel rapporto, risulta evidente che un singolo evento cyber ha il potenziale di far aumentare la loss ratio dell'industria rispettivamente del 19% per grandi sinistri e del 250% per eventi estremi. Si tratta di un chiaro segnale del potenziale catastrofale del settore cyber.

[a] Queste cifre rappresentano i valori medi delle perdite simulate per anno per grandi sinistri ed eventi estremi e prendono in considerazione tutte le spese dirette previste relative agli eventi. Impatti quali danni alle proprietà, lesioni fisiche e perdite indirette come la perdita di clienti ed il danno alle reputazione non sono prese in considerazione.

[b] Questi sono illustrate con intervallo di confidenza del 95% – l'ambito dei valori che agiscono come buone stime per considerare I parametric conosciuti e sconosciuti.

Conclusioni

La domanda di assicurazione cyber cresce con l'aumento della minaccia.

Nonostante questa crescita, le conoscenze degli assicuratori relativamente alle responsabilità legate al cyber ed alle aggregazioni di rischio sono un processo in evoluzione in linea con l'aumento delle loro esperienze rispetto agli attacchi cyber. E' dunque importante che la comprensione del rischio, inclusi i calcoli tecnici dei premi e i modelli di capitale, segua la base di conoscenze dei cambiamenti riguardanti il rischio cyber.

La comprensione degli assicuratori rispetto alle responsabilità ed aggregazioni del rischio di alcuni altri settori è più sviluppata. E' generalmente riconosciuto, per esempio, che le catastrofi naturali possono causare sinistri multipli da diversi assicurati, facendo aumentare enormemente i costi dei sinistri per gli assicuratori. Le polizze di assicurazioni che coprono le catastrofi naturali solitamente tengono in considerazione tale circostanza e la riassicurazione è comunemente utilizzata per ridurre l'impatto delle aggregazioni di rischio.

I risultati del rapporto suggeriscono che le perdite economiche derivanti dagli eventi cyber hanno il potenziale di raggiungere gli stessi valori di quelle causate dai maggiori uragani. Per gli assicuratori è meglio pensare alle coperture cyber in questi termini e predisporre le misure adeguate per far fronte alle catastrofi provocate dalle aggregazioni cyber. Per far ciò, sono importanti sia la raccolta che la qualità dei dati, specialmente in considerazione del fatto che il rischio cyber si modifica in continuazione.

Per far sì che l'industria assicurativa possa capitalizzare sul crescente mercato cyber, gli assicuratori possono trarre vantaggio da una comprensione più approfondita delle conseguenze a lungo termine insite nelle coperture cyber.

I risk managers possono utilizzare gli scenari sugli attacchi cyber per verificare quale impatto gli attacchi potrebbero avere sui loro processi di business e pianificare le azioni da intraprendere per mitigare questi rischi.

Referenze

Graham, L. 2017. Cybercrime costs the global economy $450 billion [online]. CNBC Cyber Security. Available at: http://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html

PwC. 2015. Insurance 2020 & beyond: Reaping the dividends of cyber resilience [online]. Available at: http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf

Stanley, C. 2017. Cyber market estimate (interview 26 June, Christian Stanley, Casualty Executive, Class of Business Underwriting Performance, Lloyd's).