LLOYD'S

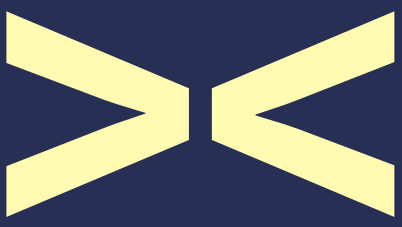
Colmare il divario

Assicurare il vostro business contro le minacce cyber in continua evoluzione

Giugno 2017

Sintesi

In collaborazione con KPMG
e DAC Beachcroft



KPMG

DAC beachcroft

Sintesi

1.1 Panoramica

Negli ultimi decenni Internet ha consentito innovazioni straordinarie, creando nuovi modelli di business e dando origine a società in grado di cambiare il mondo e generare milioni di posti di lavoro.

Ma questo progresso è stato realizzato a caro prezzo. Per loro natura, i sistemi digitali sono suscettibili di attacchi cyber da parte di individui o gruppi con ripercussioni sempre più gravi per le aziende in tutto il mondo. La natura della minaccia si sta evolvendo tanto rapidamente che le aziende trovano sempre più difficile contrastarla.

Se da una parte la minaccia informatica sta diventando sempre più complessa, dall'altra i dirigenti delle aziende non hanno la piena consapevolezza della sua portata. Secondo un recente sondaggio dei Lloyd's che ha coinvolto più di 350 dirigenti di aziende europee, solo il 42% di loro si è detto preoccupato per il ripetersi di un incidente analogo, sebbene il 92% delle aziende fosse stato vittima di una qualche forma di violazione informatica negli ultimi cinque anni.

Questo rapporto dei Lloyd's, prodotto in collaborazione con KPMG nel Regno Unito, la società di diritto internazionale DAC Beachcroft e gli assicuratori dei Lloyd's, aiuta le aziende a comprendere meglio la minaccia informatica.

La prima parte del rapporto presenta una valutazione unica delle varie minacce informatiche che le aziende si trovano ad affrontare oggi, suddivise per settore (di seguito troverete un esempio relativo ai servizi finanziari), e prende in considerazione soluzioni per mitigarle. Questa sezione mostra anche nel dettaglio l'impatto finanziario delle violazioni di dati e analizza alcuni dei costi associati ai recenti attacchi cyber più eclatanti.

La seconda parte prende in considerazione quattro motivi per cui le aziende necessitano di adottare misure più efficaci per affrontare il rischio informatico e offre, a riguardo, informazioni e consigli degli assicuratori cyber dei Lloyd's esperti nel settore.

Rischi del settore dei servizi finanziari

- Target principali
- Target frequenti
- Target occasionali
- Target meno frequenti

(L'ordine dei cerchi nella stessa categoria non indica la relativa frequenza.)

Per leggere nella sua integrità questa esclusiva analisi, settore per settore, delle minacce informatiche a cui sono esposte oggi le aziende, visitate lloyds.com/cyberriskinsight

I settori inclusi nell'analisi sono:
- Istruzione
- Servizi finanziari
- Sanità
- Ospitalità
- Information technology
- Manifattura
- Media e intrattenimento
- Petrolio e gas
- Servizi professionali
- Settore pubblico
- Retail
- Telecomunicazioni
- Trasporti
- Utilities

Per ulteriori informazioni su queste minacce, vi invitiamo a leggere il rapporto completo dei Lloyd's 'Closing the Gap' (Colmare il divario) su lloyds.com/closingthegap

1.2 Principali risultati

I tipi di attacchi cyber alle imprese variano da settore a settore e sono in continua evoluzione. Per esempio:

- Sono incrementati in modo significativo i casi di 'truffa del CEO', che sta provocando notevoli perdite finanziarie.
- Gli attacchi mirati da parte della criminalità organizzata sono diretti in particolare ai servizi finanziari, ma interessano sempre più di frequente anche il settore del retail.
- Le società che offrono servizi professionali in ambito legale e fiscale, per esempio, sono anch'esse oggetto sempre più frequente di attacchi per ottenere l'accesso ai loro clienti, che sono spesso aziende importanti.
- Sono in aumento anche gli attacchi per richiesta di riscatto e 'distributed denial-of-service', soprattutto mirati ad aziende che operano nella sanità, nei media e nell'intrattenimento.
- Il settore pubblico e quello delle telecomunicazioni sono molto esposti al rischio di attacchi cyber per spionaggio.

Le imprese devono prendere in considerazione tutti i costi di un attacco cyber, in particolare i cosiddetti costi 'slow-burn' (vale a dire i costi associati ai danni a lungo termine dell'attacco, come la perdita del vantaggio competitivo e l'aumento del tasso di abbandono della clientela). Una volta sommati ai costi immediati (come le parcelle legali, le spese per le indagini forensi e il pagamento del riscatto), i costi 'slow-burn' possono avere un impatto molto significativo per un'azienda.

Ci sono quattro fattori che aggravano i danni causati dagli attacchi informatici, rendendo ancora più importante che le aziende mitighino la loro esposizione al rischio cyber e migliorino la loro sicurezza informatica:

- L'applicazione di maggiori sanzioni per le società che violano le norme sulla sicurezza informatica nel rispetto della nuova ed imminente legislazione europea.
- Un maggior desiderio delle vittime delle violazioni cyber di citare in giudizio le aziende che hanno perso i loro dati.
- Una maggiore responsabilità per la sicurezza informatica nella catena di approvvigionamento.
- Una maggiore vulnerabilità attraverso l'uso crescente di dispositivi connessi (the Internet of things).

1.3 I prossimi passi

I Lloyd's contano più di 70 assicuratori che offrono copertura assicurativa cyber. Il rapporto si basa sulle informazioni e competenze esclusive del mercato dei Lloyd's ed evidenzia quattro soluzioni chiave che possono aiutare le aziende a prepararsi e a mitigare la minaccia informatica:

1. Comprendere le minacce specifiche per la vostra azienda, compresi i costi immediati e quelli 'slow-burn', dalla reputazione percepita dai clienti al valore dei dati in vostro possesso, dalla vulnerabilità della catena di approvvigionamento ai profili dei leader aziendali.

2. Valutare le minacce sia attuali che future: i sottoscrittori valuteranno entrambe in modo da poter offrire la copertura assicurativa più adatta alle vostre esigenze.

3. Assicurarsi che tutti i dipendenti, inclusi i dirigenti, abbiano una comprensione approfondita delle minacce informatiche che la vostra azienda deve affrontare e promuovere una cultura di gestione del rischio informatico.

4. Affidarsi all'aiuto di esperti quando si tratta di organizzare coperture assicurative informatiche adeguate ai rischi effettivi.

1.4 Conclusione

La minaccia cyber si evolve quotidianamente e quindi le aziende devono essere più preparate a gestire le conseguenze di una violazione informatica. È probabile che le spese per le aziende in seguito all'introduzione della nuova legislazione europea aumentino, ma sta anche crescendo il numero dei modi in cui possono cadere vittima di attacchi.

Se è vero che le aziende non possono proteggersi al 100% dagli attacchi cyber, tuttavia possono adottare un numero di misure che limitino l'esposizione al rischio, minimizzino le conseguenze di un'eventuale violazione e riducano i tempi di ripresa della normale attività.

L'assicurazione è un aspetto importante di questa soluzione. Ogni giorno i sottoscrittori dei Lloyd's specializzati nel settore informatico collaborano con migliaia di aziende in tutto il mondo, dalle multinazionali alle piccole e medie imprese, per comprenderne meglio i rischi e offrire loro la consulenza di esperti e la copertura assicurativa di cui hanno bisogno.

Per leggere il rapporto completo dei Lloyd's 'Closing the gap' visitate **lloyds.com/closingthegap**

Per scoprire come gli assicuratori dei Lloyd's possono aiutarvi, visitate **lloyds.com/cybercover**