

Rischi informatici

Cibercriminalità - un'industria in crescita

I metodi utilizzati dai cibercriminali sono svariati: si va dallo spionaggio e sabotaggio, ai ricatti e alla fuga di dati, fino ad arrivare alla manipolazione del mercato e al phishing. C'è stato anche un aumento dei casi originati all'interno dell'azienda, cioè atti di insider o comportamenti involontari dei collaboratori. Inoltre, interi processi dell'IT aziendale vengono sempre più spesso esternalizzati, il che comporta anche un cambiamento dei rischi ai quali queste aziende sono esposte.

Liberty protegge i beni immateriali dei suoi clienti con un approccio innovativo e creativo, fornendo soluzioni assicurative veloci e flessibili. La nostra Cyber Suite prende in considerazione tutte le sfide che le aziende si trovano ad affrontare a seguito della crescente dipendenza da reti di comunicazione, strutture informatiche di terzi, risorse digitali, nonché dai dati personali archiviati.



Ogni azienda è esposta a rischi informatici

Chiunque memorizzi dati dei propri collaboratori o di terzi deve considerare il relativo livello di sicurezza. Più i dati sono numerosi e confidenziali, più un'eventuale responsabilità verso terzi o verso il personale può risultare onerosa.

In base alla legislazione e alle disposizioni delle autorità di vigilanza, le richieste di risarcimento danni, le multe (che non sono sempre assicurabili a termini di legge), i costi per le notifiche ai clienti e il monitoraggio del credito possono assumere proporzioni considerevoli. In un numero crescente di nazioni, esiste un obbligo di legge di informare le persone i cui diritti in materia protezione dei dati siano stati violati. Se sono coinvolti dati confidenziali di cittadini dell'UE, il Regolamento generale sulla protezione dei dati dell'UE (RGPD) si applica anche alle aziende svizzere. Inoltre, laddove non esistono queste leggi, tale obbligo di informazione è spesso contenuto nelle disposizioni contrattuali o nelle linee guida settoriali.

Anche il rischio di un'interruzione della rete che causi una sospensione dell'attività e, in definitiva, una perdita di ricavi è presente per ogni azienda. Se, ad esempio, i collaboratori non possono accedere agli elenchi per la vendita o il marketing, al CRM o ai sistemi di approvvigionamento della catena di fornitura, il lavoro si blocca rapidamente. Anche edifici, fabbriche e magazzini sono spesso controllati tramite reti e, in caso di interruzione, possono verificarsi gravi compromissioni del processo di produzione.

Coperture	Massimali
Rischi informatici	fino a CHF/EUR/USD 10 milioni

Scenari della cybercriminalità

Inizialmente le attività fraudolente erano rivolte contro le istituzioni finanziarie. Ora anche studi legali, società di consulenza e soprattutto PMI di vari settori sono sempre più frequentemente bersaglio di attacchi professionali. Eccone tre esempi.

Estorsione con danni conseguenti

Una società commerciale svizzera di medie dimensioni subisce un improvviso e inatteso attacco da parte di hacker. Avendolo inizialmente sottovalutato, l'azienda viene colpita violentemente: nessun accesso alla intranet, danneggiamento di numerose applicazioni, database cancellati, server non visibili o ripristinati alle impostazioni di fabbrica – l'intero sistema informatico è fuori uso. Le interfacce attraverso le quali i grandi clienti inseriscono i loro ordini automaticamente sono state cancellate, lavorare diventa completamente impossibile e l'azienda si vede costretta ad andare offline.

A causa della situazione, c'è il rischio di perdere clienti e dover pagare penali convenzionali. Poi arrivano richieste di riscatto per diverse centinaia di migliaia di franchi. Solo dopo una costosissima attività di difesa durata tre settimane e un lavoro di ricostruzione ancora più lungo, l'azienda può tornare gradualmente alla normale operatività.

Un punto debole: il fattore umano

L'intera infrastruttura IT di un'azienda svizzera del settore dell'impiantistica per edifici è stata paralizzata: alcuni dipendenti hanno consentito l'accesso alla rete rispondendo a un'e-mail di phishing. L'attacco ha interessato il sistema centrale ERP e di gestione del magazzino, il sito Web, tutti gli indirizzi e-mail e la telefonia fissa.

La logistica di magazzino e delle consegne è stata particolarmente colpita e le consegne si sono bloccate. Alcuni specialisti informatici forensi sono stati incaricati di indagare su quanto accaduto. Sono state coinvolte tutte le sedi svizzere dell'azienda che ha oltre 1'000 collaboratori.

Attacchi mirati

Per un provider che occupa circa 50 persone, la giornata inizia in maniera frenetica: un attacco informatico ha bloccato un servizio cloud. L'attacco ransomware è stato in gran parte respinto e i server per applicazioni e dati sono stati gradualmente ripristinati. Nonostante ciò l'azienda, anche settimane dopo l'attacco, ha comunque dovuto chiedere a numerosi clienti di pazientare, in quanto sia la messa in funzione dei sistemi colpiti che il ripristino dei volumi di dati, in parte ingenti, hanno potuto essere effettuati solo gradualmente e nell'arco di diverso tempo.

Ciò che rende questo caso degno di nota è l'estorsione informatica mirata: gli attacchi di massa tramite ransomware sono infatti sempre più spesso accompagnati da estorsioni verso singole aziende. Caratteristica di questi attacchi è che si possono chiedere somme molto più alte, perché si conoscono bene gli obiettivi e si può stimare approssimativamente quanto le aziende in questione sono disposte a pagare.

Che cosa comprendono esattamente i rischi informatici?

Il termine descrive una serie di rischi di danni propri e a terzi in relazione all'utilizzo delle tecnologie dell'informazione. La Cyber Suite di Liberty offre i seguenti tipi di copertura:

Danni propri

- **Perdita o danneggiamento di dati o programmi**
Costi per riparazioni, aggiornamento, ripristino o sostituzione di dati e/o programmi danneggiati per riportarli allo stato precedente al sinistro.
- **Interruzione dell'attività**
Perdita di ricavi a causa di interruzione, deterioramento o guasto della vostra rete, nonché le spese legate alle interruzioni per la riduzione dei danni e le indagini sul sinistro.
- **Estorsione informatica**
In caso di estorsione sotto la minaccia di paralizzare o compromettere la vostra rete, pubblicare dati non autorizzati presenti sulla vostra rete o contattare i vostri clienti con falsi pretesti, gestiamo le richieste e paghiamo il riscatto.
- **Perdita di reputazione**
In caso di mancati ricavi a causa della perdita di clienti, susseguente a danno alla reputazione dovuto alla divulgazione di una violazione dei dati, vi rimborsiamo i mancati ricavi, nonché il maggiore costo del lavoro e le spese correlate alle attività di pubbliche relazioni.

Danni a terzi

- **Responsabilità civile informatica**
Spese per la responsabilità civile e la difesa legale che possono derivare da pretese fondate su un atto illecito reale o presunto.
- **Procedure delle autorità di vigilanza**
Costi per indagini, difesa e – nella misura in cui siano assicurabili secondo la legge vigente – anche multe e sanzioni.
- **Costi di notifica e gestione della crisi**
Costi legali e costi per l'assistenza alle persone colpite da violazioni delle norme in materia di protezione dei dati, ad esempio tramite monitoraggio degli atti di credito o consulenza in caso di furto di identità, anche per proteggere o ripristinare la reputazione.
- **Responsabilità civile multimediale**
Costi per indagini e difesa, nonché per richieste di risarcimento danni in caso di violazioni di diritti della proprietà immateriale o di protezione dei dati di terzi, accuse di diffamazione o pubblicazione negligente di contenuti online o offline.

Una bella domanda: la perdita di dati non è già coperta da altre assicurazioni?

Responsabilità civile professionale

Se disponete di un'assicurazione responsabilità civile professionale, è possibile che copra già i danni a terzi dovuti alla perdita di dati – di solito tuttavia solo se il danno deriva dall'esercizio dell'attività professionale.

La responsabilità civile professionale di solito non copre le pretese dei collaboratori e nemmeno un utilizzo doloso o abusivo della rete dell'assicurato che danneggi, utilizzi abusivamente o distrugga i dati dei clienti o provochi attacchi "Denial of Service".

Inoltre, sono spesso esclusi i danni derivanti dalla trasmissione di virus informatici e la copertura è limitata alle richieste di risarcimento da parte dei clienti dell'assicurato con l'esclusione delle procedure da parte di autorità di vigilanza. La maggior parte delle assicurazioni responsabilità civile professionale non fornisce copertura per i danni propri come la perdita di ricavi, la perdita o il danneggiamento di dati/programmi, l'estorsione informatica o i danni alla reputazione.

Responsabilità civile generale

Un'assicurazione responsabilità civile generale copre solo i danni alle persone e alle cose. Poiché i tribunali considerano i dati come un bene immateriale, le violazioni di diritti in materia di protezione dei dati non sono in genere coperte.

Assicurazione di cose

Di norma un'assicurazione di cose copre solo i danni ai beni materiali. I tribunali considerano i dati come beni immateriali. Per questo le perdite e i danneggiamenti di dati/programmi di solito non sono coperti. Anche se avete un'assicurazione per le interruzioni dell'attività a causa di danni alle cose, è probabile che non sia prevista alcuna copertura per interruzioni dell'attività in seguito a danni immateriali alla vostra rete. I virus informatici e i rischi di rete sono spesso esclusi dalle polizze di assicurazione di cose.

Assicurazione informatica All-Risks

L'assicurazione informatica All-Risks copre i costi per la riparazione di hardware danneggiato (bene materiale) ma, a differenza dell'assicurazione Cyber Suite, non copre le pretese in relazione a perdite di dati e i costi successivi.

Il nostro è un orizzonte di lungo periodo

Gestiamo la collaborazione con i nostri clienti in modo innovativo e deciso. Siamo veloci e abbiamo sempre il polso della situazione. Al contempo, poniamo lo sviluppo sostenibile sopra ogni altra cosa, nel rapporto con i nostri clienti e ancor di più per quanto concerne la vostra azienda.

Perché, solo ciò che va bene per voi, va bene anche per noi. Quindi agiamo sempre con una prospettiva a lungo termine: con la nostra competenza specifica nella sottoscrizione e la conoscenza dei mercati locali e internazionali, i nostri solidi rapporti con i vari partner commerciali e il nostro modo semplice di gestire i sinistri. In questo modo creiamo fiducia e affidabilità in un'era di continui cambiamenti. Anche a lungo termine.

Desiderate saperne di più su Liberty in Svizzera e sui nostri prodotti assicurativi?

Contattateci!

Liberty Specialty Markets
Lintheschergasse 19, 8001 Zurigo

+41 44 285 10 00
lsmzurich@libertyglobalgroup.com
www.libertyspecialtymarkets.com