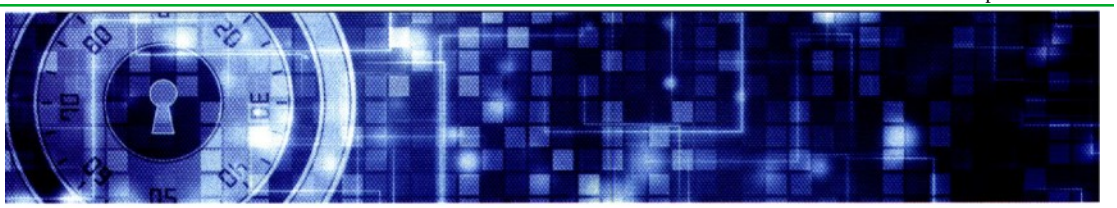
8 Ania, i consigli per assicurarsi contro i cyber rischi



Assicurarsi contro i cyber rischi

I consigli dell'Ania, Associazione Nazionale fra le Imprese Assicuratrici, sulle "garanzie-chiave" che deve avere una copertura assicurativa cyber.

La tecnologia sta costantemente trasformando le nostre vite, migliorando l'operatività delle aziende e di tutte le realtà produttive. Queste tecnologie determinano però nuove vulnerabilità che, se sfruttate, possono causare danni irreparabili. Le continue notizie sull'attività criminale online, che prosegue e si incrementa senza sosta, dimostrano come gli attacchi informatici costituiscano oggi per le aziende una grave minaccia. L'uso intensivo di Internet e di tutte le connessioni da parte delle realtà produttive, dei loro collaboratori, dei fornitori e dei clienti incrementa i possibili obiettivi. Secondo Enisa, l'Agenzia europea per la sicurezza delle reti e dell'informazione, la minaccia più importante registrata nel 2017 è stata quella degli attacchi malware, ossia software che disturbano le operazioni di un computer, rubano informazioni sensibili, violano sistemi informatici o mostrano pubblicità indesiderata, danneggiando la reputazione dell'azienda. Seguono gli attacchi via web e il phishing, ossia truffe internet in cui la vittima fornisce impropriamente dati personali o codici di accesso.

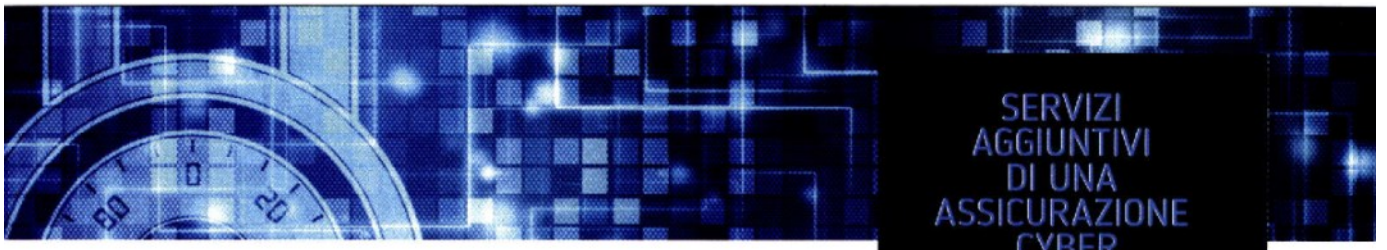
In Italia i danni da cybercrime nel 2017 ammontano a circa 10 miliardi di euro. Il danno medio è pari a 2 milioni di euro ed è aumentato del 70% rispetto a tre anni prima. Le realtà più colpite sono quelle appartenenti al comparto finanziario, a quello farmaceutico e a quello dei beni di consumo. Secondo un'indagine della Banca d'Italia sulle imprese non finanziarie, nonostante quasi tutte le aziende abbiano adottato misure di prevenzione da rischi informatici, il 30% delle stesse dichiara di avere subito comunque danni da attacchi cyber nel periodo settembre 2015 – settembre 2016. E si tratta di un dato che sottostima la realtà, perché una percentuale significativa dei casi non viene dichiarata.

Infatti, l'AIBA, Associazione Italiana Brokers di Assicurazioni, stima per il 2017 che il 50% delle piccole e medie aziende sono state colpite da un attacco di questo tipo, per un costo medio di 35.000 euro.

Per il resto, dall'indagine non

LE SEI "GARANZIE-CHIAVE" DI UNA COPERTURA ASSICURATIVA CYBER

	COSA COPRE	A CHI È CONSIGLIATA
DANNI DA INTERRUZIONE DI ESERCIZIO	Copre la perdita di reddito causata dall'interruzione di attività a seguito di un incidente	*Rilevante per tutte le realtà produttive*
COSTI PER VIOLAZIONE DATI	Copre: costi per affrontare la violazione dei dati, per esempio la notifica ai clienti dell'avvenuta violazione; costi di un call center per rispondere ai clienti; costi della consulenza per le pubbliche relazioni; l'assistenza legale necessaria; le richieste di risarcimento per danni a terzi (responsabilità civile)	*Rilevante, in particolare, per realtà che gestiscono informazioni personali dei loro clienti*
ESTORSIONE CYBER	Copre da ransomware e altri tentativi malevoli di sequestrare e bloccare l'accesso ai dati operativi o personali a fronte del pagamento di un riscatto	*Rilevante per tutte le realtà produttive, data la crescente frequenza di tali attacchi*
ATTACCHI HACKER	Copre dai danni inflitti da un hacker, in particolare la perdita o l'alterazione di dati o l'abuso di programmi e sistemi informatici	*Rilevante, in particolare, per realtà che operano online o con sistemi di produzione automatizzati*
RESPONSABILITÀ PER ATTIVITÀ MULTIMEDIALE E PUBBLICITARIA	Assicura un risarcimento dei danni provocati a terzi, per esempio: per calunnia, diffamazione o violazione dei diritti di proprietà intellettuale, tramite i media digitali (danno reputazionale), plagio, violazione dei copyright	*Rilevante, in particolare, per realtà produttive che trasmettono dati via e-mail o sito web, o che si affidano ai social media o altri contenuti digitali*
ASSISTENZA	Garantisce un supporto H24 da parte di specialisti cyber nel periodo successivo a una violazione di dati o hackeraggio. Gli specialisti valutano i sistemi, identificano la causa e suggeriscono misure preventive. Possono anche dare consigli legali e dare indicazioni su cosa fare per informare i clienti	*Rilevante, in particolare, per realtà che non hanno un ufficio competente a svolgere l'attività di gestione del rischio cyber*



emerge una significativa distinzione dell'esposizione al rischio per area geografica, né fra imprese più o meno tecnologiche. L'unico fattore chiave sembra essere la dimensione della realtà produttiva: più è alto il numero di dipendenti, maggiore è la frequenza di incidenti cyber, in quanto si tratta di aziende solitamente più visibili e, dunque, più attraenti per gli hacker. Queste, oltre a essere più presenti online, tendono a gestire quantità maggiori di dati sensibili.

Le realtà più piccole sono quelle che investono meno in sicurezza informatica – perché ancora non sono del tutto consapevoli del pericolo o perché non hanno risorse per la gestione del rischio cyber – e delegano spesso all'esterno tutte le funzioni di sicurezza. Questo si traduce in una maggiore vulnerabilità e può bastare un solo attacco informatico a interrompere l'attività produttiva determinando danni non sostenibili.

L'ASSICURAZIONE È LA SOLUZIONE

Assicurare la propria realtà produttiva protegge da imprevisti che possono comprometterne la reputazione, i risultati o la stessa sopravvivenza.

Si può trovare protezione con prodotti assicurativi specializzati per il rischio cyber che coprono i danni subiti e quelli provocati a terzi – per esempio, ai clienti – per violazione di dati sensibili o disservizi. •

ALTRE POSSIBILI GARANZIE DELL'ASSICURAZIONE CYBER

SERVIZI AGGIUNTIVI DI UNA ASSICURAZIONE CYBER

Infine, quello che contraddistingue alcune polizze cyber è la presenza di servizi per la gestione completa del rischio, sia in termini di prevenzione sia in termini di risposta alla crisi causata dall'attacco.

PREVENZIONE

Consulenza sulla sicurezza informatica (test di vulnerabilità, formazione, valutazione del rischio, analisi delle minacce in corso)

Consulenza manageriale sulla gestione del rischio

Consulenza legale sul rischio privacy

RISPOSTA ALLA CRISI

Consulenza legale (adempimenti verso Autorità amministrative, comunicazioni a terzi, risposte a reclami)

Servizi IT (risanamento dei sistemi e ripristino dei dati)

Consulenza manageriale (valutazione dei rischi e analisi costi-benefici)

Consulenza pubbliche relazioni (supporto per la comunicazione e la salvaguardia del brand)

Unità di crisi (monitoraggio del furto dei dati, call center, servizi di notifica, azioni per il contenimento del danno reputazionale)