ITAS CYBER PROTECTION

SFATIAMO I LUOGHI COMUNI

Non ho bisogno di assicurarmi perché…

- non gestiamo noi i dati dei nostri clienti
- il rischio cyber è solo online
- diamo tutto in outsourcing sul cloud
- il nostro team IT è molto competente, se ne occupano loro!
- le PMI sono meno esposte ad attacchi cyber
- l'assicurazione è utile ma non ci aiuterebbe a gestire l'incidente
- abbiamo già una polizza di RC Professionale

In caso di incidente cyber
le decisioni da prendere in poco tempo riguardano:

- Coinvolgo l'Ente Regolatore? Se sì, quando?
- Quando notificare il Garante?
- Ci serve un legale esperto in privacy?
- Dobbiamo offrire un prodotto di monitoraggio di identità?
- L'incidente che stiamo gestendo, è di fatto un breach?
- Quando tempo ci vuole per notificare i soggetti interessati?
- Utilizziamo i nostri IT interni o occorrono consulenti esterni specializzati?

Aspetti sensibili legati alla tematica del “cyber risk”

- All’interno delle aziende è raro avere una persona in grado di affrontare questi rischi specifici;
- Il danno può essere causato da azioni diversissime fra loro (attacco telematico, truffa via email, smarrimento chiavetta usb o laptop);
- Anche nelle grandi aziende la presenza di personale specializzato non garantisce sicurezza assoluta;
- Il GDPR ha introdotto nuove responsabilità e doveri in materia privacy;
- L’individuazione del responsabile danneggiante può essere difficoltosa o impossibile … o inutile;
- La tutela legale ex-post può rivelarsi inefficace rispetto ai bisogni commerciali immediati dell’azienda (riavvio della produzione, risarcimento immediato ai clienti, procedure giudiziarie lunghe, difficoltà di individuare il responsabile).

Una violazione dei dati non è sempre un disastro.

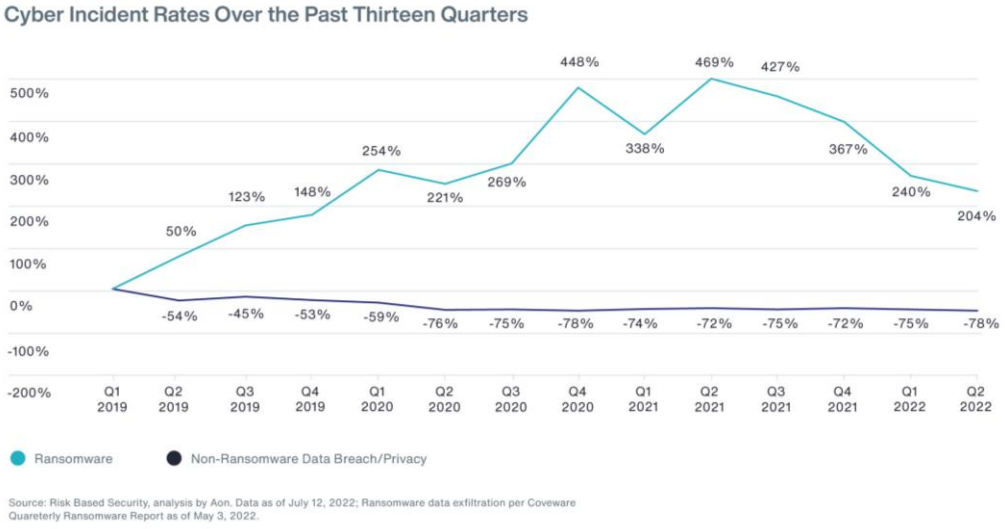
GESTIRLA MALE LO È!

Principali rischi “cyber” corsi dalle imprese

- Perdita di dati personali riguardanti i clienti o i contatti
- Interruzione dell’attività commerciale
- Perdita di dati riservati riguardanti brevetti o strategie aziendali
- Costi di ripristino delle strutture network aziendali
- Rischio reputazionale
- Adempimenti regolatori - costo delle notifiche
- Sanzioni

Fonte: report AON 2022

La frequenza e la gravità dei sinistri per errori e omissioni e per la responsabilità civile verso i media sono rimaste piuttosto costanti fino alla prima metà del 2022. I dati di Aon mostrano che la frequenza dei sinistri cyber è diminuita di trimestre in trimestre, ma risulta ancora decisamente elevata e pericolosa



Source: Risk Based Security, analysis by Aon. Data as of July 12, 2022; Ransomware data exfiltration per Coveware Quareterly Ransomware Report as of May 3, 2022.

Osservazioni chiave:

- La frequenza degli attacchi Ransomware **ha superato in modo stabile la frequenza degli eventi di Data e Privacy Breach non correlati ad attività di Ransomware.**
- **L'attacco Ransomware è incrementato del 204%** dal momento Q1 2019 al momento Q2 2022
- Comparato al momento Q2 2021 gli attacchi ransomware risultano in calo ma ancora costanti e con conseguenze decisamente impattanti
- Come nel momento Q1, le industrie più comunemente colpite dal Ransomware nel Q2 2022 sono: Settore Pubblico, Industrie Manifatturiere, Sanità, Servizi professionali & Business.
- Le esfiltrazioni di dati, nel Q1 2022, sono accadute nel 77% dei casi Ransomware secondo quanto riportato da Coveware.

Fonte: Insurance Daily N. 2260- martedì 15 novembre 2022

LE PMI SONO PIÙ A RISCHIO

Prima dell'attacco NotPetya del 2017, i rischi informatici erano incentrati soprattutto sulle violazioni dei dati e sulla responsabilità verso terzi. [omissis]…, la proliferazione delle normative sulla privacy dei dati ha aperto le porte a procedure di contenzioso e ha aumentato l'esposizione al rischio a coda lunga (long tail risk).

Negli ultimi due anni, invece, i sinistri puri sono diventati dominanti, con l'esplosione di ransomware da parte della criminalità organizzata, che hanno spostato i danni al core business.

Le imprese, i riassicuratori, le associazioni di settore e le autorità pubbliche hanno moltiplicato gli sforzi di gestione del rischio e hanno collaborato per fornire non solo il trasferimento, ma anche la mitigazione della minaccia cyber, contribuendo a monitorare gli attacchi informatici.

Ma il divario di protezione, come si diceva, rimane ampio. La maggior parte delle aziende non è assicurata o è significativamente sottoassicurata, …[omissis]. In una recente ricerca è emerso che solo il 55% delle aziende ha dichiarato di avere una copertura contro il cyber risk e meno di una su cinque ha limiti di copertura superiori alle necessità per i danni da ransomware.

Gli analisti hanno stimato che il costo totale di un incidente informatico che colpisce una PMI è, in termini relativi, tre volte superiore a quello di una grande azienda, con costi legali che generalmente vanno dai 20mila ai 100mila dollari per una società con un fatturato inferiore ai 50 milioni.

ITAS MUTUA

ESEMPI DI SINISTRO / 1

- Viene rubato un pc portatile che conteneva dati personali di migliaia di clienti. Successivamente i ladri utilizzano queste informazioni come furto di identità. I clienti fanno causa all'azienda assicurata.
- Infedeltà dei dipendenti: un dipendente, all'insaputa dei propri responsabili, sottrae il database dei clienti dell'azienda assicurata e li vende all'azienda concorrente. I clienti lo vengono a sapere e fanno causa all'azienda assicurata.
- Un hacker, attraverso un virus riesce a penetrare nei sistemi aziendali, e viene in possesso di tutte le email e numeri di telefono dei clienti, i quali vengono poi tempestati di chiamate e di messaggi nelle loro caselle email. I clienti vengono a sapere che i loro dati sono stati violati e fanno causa all'azienda assicurata.

Il costo medio per ogni record violato è di circa € 158 ***(fonte : The Ponemon Institute Report - 2016)***

Le perdite economiche previste per un breach minore di 1000 record ammonta ad una cifra tra i € 52.000 e € 87.000 ***(fonte : Avv. Giorgio Grasso, PHD Senior Partner BTG Legal - 2019)***

ITAS MUTUA

ESEMPI DI SINISTRO / 2

- Denial of service attack: un hacker attacca la nostra azienda assicurata ed installa un programma che permette di inviare migliaia di email ai propri clienti, bloccandone di fatto la loro operatività e/o causando loro un danno.
- I dati dei clienti sono stati violati (ad esempio per un malicious code) ma l'azienda assicurata nonostante siano passati molti mesi non ne ha dato la notifica ai loro clienti. I clienti fanno causa all'azienda assicurata ai sensi della Legge sulla Notifica della Violazione.
- Violazione della politica privacy. I dati dei clienti sono stati correttamente raccolti tramite i moduli cartacei firmati, ma la donna delle pulizie li ha buttati via pensando che fossero carta straccia. Successivamente i dati dei clienti vengono venduti a Società terze che li utilizzano per fare una campagna pubblicitaria nei loro confronti. I clienti vengono a sapere che i loro dati sono stati venduti e fanno causa all'azienda assicurata, che sebbene avesse raccolto i moduli non può provare ciò. (*il rischio cyber non è solo online*)

ITAS MUTUA

ESEMPI DI SINISTRO / 3

- A seguito di un incendio viene perso l'archivio di un cliente che conteneva informazioni riservate importantissime. Il cliente fa causa all'azienda assicurata.
- Ransomware (caso reale ITAS): il titolare di una azienda ha aperto una email e che ha criptato tutti i dati dei PC e anche di quello che gestiva il macchinario di produzione. L'attività si è fermata, fino a quando si è fatta la pulizia dei PC e la reinstallazione dei software e dei dati dal back-up.
- Ransoware: nel periodo di Natale, un hacker è riuscito ad entrare nel sistema informatico di un hotel e ha bloccato tutti gli accessi alle camere. È stato richiesto un riscatto per poter riavere il controllo degli accessi.
- E-Crime (caso reale ITAS): due hostess presso lo stand di una fiera per conto di una azienda, ricevono dal titolare dei messaggi (il tono era quello confidenziale che intrattenevano sempre) nei quali gli veniva chiesto di fare delle spese necessarie per lo stand con la loro carta di credito, poi gli avrebbero rimborsato tutto. Ovviamente il era falso ma talmente fatto bene da ingannare le due ragazze. Si è quindi trattato di una frode con perdita patrimoniale

ITAS MUTUA

ESEMPI DI SINISTRO / 4

- Ransomware: l'HR manager riceve un'email con un curriculum vitae in allegato Word; aprendo il file, abilita accidentalmente una macro che scarica ed esegue un file DLL; utilizzando un processo, il DLL crittografa i file.
- Errore umano: le informazioni personali sono state inavvertitamente inviate a più di 4000 dipendenti della stessa società
- Errore umano: 250 clienti di un rivenditore online hanno ricevuto un'email erroneamente inviata a tutti gli indirizzi che risultavano visibili, senza nascondere i destinatari della mailing list
- Errore umano: uno studio di commercialisti invia per errore documentazione ad un terzo. La corrispondenza inviata conteneva informazioni confidenziali.
- Errore umano: il responsabile delle risorse umane di un società invia per errore, alla mail di alcuni candidati, la documentazione relativa alle schede di tutti i dipendenti aziendali. La società ha dovuto affrontare spese legali per il procedimento innanzi l'autorità di vigilanza, nonché i costi per le transazioni con i dipendenti che avevano subito il furto di identità

ITAS MUTUA

ESEMPI DI SINISTRO / 5

- Una università scopre un attacco SQLi contro il proprio sito web. Il rettore riceve una mail dall' hacker, che dichiara di avere accesso a dati personali di studenti. La compagnia mette in contatto l'assicurato con esperti legali e informatici. A seguito di analisi informatica, si apprende che la violazione è modesta e che l'hacker ha accesso a una piccola base dati di circa 250 dipendenti. Seguito parere legale, l'università decide di non notificare l'incidente. *Costo gestione sinistro: Legali € 10.000 – Esperti informatici € 15.000*
- Azienda manufatturiera multinazionale soffre attacco phishing. Account email di oltre 30 dipendenti sono compromessi. Servizi legali necessari in USA, UK e Spagna. Notifica a tre Enti Regolatori in USA e in UK. *Costo gestione sinistro: Legali € 35.000 – Esperti informatici € 65.000 – Pubbliche Relazioni € 10.000*

ITAS MUTUA

Il Rischio Cyber si gestisce attuando un **Piano di Sicurezza Informatica** (strumenti di cyber-sicurezza, formazione dipendenti, penetration test)

L'incertezza di ritenere in proprio il **rischio residuo** si elimina con una **polizza assicurativa**.

ITAS MUTUA

Con la polizza i **costi diventano certi**:

- Premio di polizza
- Franchigie
- Massimali

ITAS MUTUA

PERCHÉ COMPRARE LA POLIZZA

- Nelle polizze di RCT tradizionali il rischio non è coperto
- Le polizze Elettronica coprono solo il danno fisico ai beni e hanno esclusioni specifiche su cyber, virus, attacchi informatici
- Con i Servizi si ha consulenza anche senza sinistro
- Per la gestione dei sinistri ho un unico interlocutore: ITAS
- Servizio Legale e informatico a disposizione
- Servizio per la gestione della crisi
- Perché se ho un danno cyber, potrei anche chiudere l'attività!

ITAS MUTUA

Per stipulare la polizza è necessario avere:

1. Installato l'Antivirus + Firewall

(è come mettere la cintura di sicurezza o il casco)

2. Fare il Back-up dei dati

(senza non si possono recuperare)

ITAS MUTUA

3. in base a quanto stabilito all'art.32, paragrafo 1, comma c) del Reg. EU 679/2016 (GDPR)
   a. un piano di disaster recovery?
   b. un piano di continuità aziendale?
   c. un piano di reazione a seguito di intrusioni nella rete e di incidenti dovuti a virus

Questi 3 controlli sono necessari per la Aziende Manifatturiere

Nel caso non ci fossero, è necessario conoscere quali misure alternative sono previste

ITAS MUTUA

COSA COPRE LA POLIZZA

1. Responsabilità Civile verso Terzi

2. Danni diretti

ITAS MUTUA

SEZIONE RCT

1. Responsabilità per la sicurezza delle informazioni e Privacy

Danni e Spese di Difesa in conseguenza di qualsivoglia richiesta di risarcimento derivante da:

1. violazione dei dati personali;
2. violazione della sicurezza dei sistemi informatici;
3. inosservanza di un obbligo di notifica;
4. Inadempimento colposo della Politica Privacy (il documento operativo e procedurale adottato dall'Assicurato per l'adeguamento alla vigente normativa sulla privacy)

ITAS MUTUA

SEZIONE RCT

2. Responsabilità per l'attività multimediale e pubblicitaria

Danni e Spese di Difesa in conseguenza di richiesta di risarcimento derivante da atti commessi dall'Assicurato nell'attività di creazione, pubblicazione, riproduzione, diffusione o realizzazione materiale media per il pubblico.

ITAS MUTUA

SEZIONE RCT

3. Costi, oneri e Sanzioni PCI

le penalità contrattuali previste dalle società emittenti carte di credito o altri fornitori di servizi finanziari a carico dell'Assicurato per Costi, oneri e Sanzioni PCI in conseguenza di sospetta Violazione di Dati.

SEZIONE DANNI DIRETTI

1. Danni relativi all'interruzione della propria attività

che siano diretta conseguenza di una Violazione della Sicurezza, ovvero:

1. l'Accesso o Utilizzo Non Autorizzato di Sistemi Informatici, compresi l'Accesso o Utilizzo Non Autorizzato derivante dal furto di una password da un Sistema Informatico o da un Assicurato;
2. un Denial of Service Attack nei confronti dei Sistemi Informatici;
3. con riferimento alla copertura di cui alla Sezione di Responsabilità Civile, un Denial of Service Attack che riguardi sistemi informatici che non siano di proprietà, posseduti, gestiti o controllati dall'Assicurato; o
4. il danneggiamento di Sistemi Informatici attraverso un Codice Maligno o la trasmissione di un Codice Maligno dai Sistemi Informatici.

SEZIONE DANNI DIRETTI

Danni relativi all'interruzione della propria attività

- ✓ Profitto netto al lordo delle imposte che l'Assicurato avrebbe incassato o guadagnato durante il Periodo di Ripristino (massimo 180 giorni)
- ✓ Spese fisse di gestione sostenute dall'Assicurato (inclusi i compensi e gli stipendi) durante il Periodo di Ripristino (massimo 180 giorni)
- ✓ Spese per un esperto informatico
- ✓ Spese Straordinarie

ITAS MUTUA

SEZIONE DANNI DIRETTI

2. Costi per recupero dati

quale conseguenza diretta di una Violazione della Sicurezza dei sistemi informatici.

SEZIONE DANNI DIRETTI

3. Danni da Cyber estorsione

quali perdite conseguenti ad una Minaccia di Estorsione cibernetica.

ITAS MUTUA

SEZIONE DANNI DIRETTI

4. Costi di istruttoria

connessi ad uno dei procedimenti elencati nelle condizioni di assicurazione (es. procedimento avviato dal Garante per la Protezione dei dati personali, dall'Autorità per le Garanzie nelle Comunicazioni o da altra pubblica autorità etc..);

ITAS MUTUA

SEZIONE DANNI DIRETTI

5. Spese per investigazione

le spese ragionevoli sostenute dall'Assicurato - previo assenso dell'Assicuratore - per assumere un investigatore - abilitato all'esercizio di tale attività - per la ricerca di prove per l'individuazione dell'autore dell'atto illecito che abbia causato un evento coperto dalla Polizza

ITAS MUTUA

SEZIONE DANNI DIRETTI

6. Danni da E-Crime (garanzia opzionale)

derivanti da:

1. istruzioni fraudolente;
2. trasferimento fraudolento di fondi;
3. frodi telefoniche.

SEZIONE DANNI DIRETTI

7. Servizi per la gestione di una violazione dei dati

sono forniti senza ausilio di altre Compagnie

1. **assistenza legale**;
2. **assistenza da parte di un esperto di sicurezza informatica**;
3. **assistenza da parte di un PCI Forensic Investigator**;
4. **notifica ai Soggetti Titolari**;
5. **messa a disposizione di un call center per fornire informazioni ai Soggetti Titolari**;
6. **il monitoraggio del credito, il monitoraggio dell'identità o altra soluzione ai Soggetti Titolari** coinvolti a causa della Violazione dei Dati;
7. **i costi per pubbliche relazioni o gestione della crisi.**

ITAS MUTUA

ATTIVITÀ ASSICURABILI

La polizza è rivolta a favore di piccole medie imprese quali:

- Artigiani, Aziende di produzione e manifatturiere
- Aziende Edili, Aziende di produzione di energia elettrica
- Aziende di Ricerca di Marketing, Agenzie di pubblicità, Agenzie Immobiliare, Agenzie organizzazione eventi, Agenzie viaggio
- Istruzione Privata: Scuole, Asili, Nidi, Collegi, E-learning
- Professioni Tecniche (ad es. Architetti, Geometri, Ingegneri, Periti, ecc.), Professionisti (ad es. Avvocati, Commercialisti, Consulenti del lavoro e fiscali, Amministratori di Condominio, ecc.), ONLUS, Agenzie di Assicurazione
- Hotel (Alberghi, B&B, Ostelli, altre strutture ricettive), Ristorazione
- Sanità privata: Ambulatori, Centri diagnostici, Cliniche private, Laboratori Analisi, Medici in attività privata, Residenze Anziani
- Vendita al dettaglio e ingrosso (compreso e-commerce)
- Concessionari auto, Società di trasporto private, Logistica

ITAS MUTUA

ATTIVITÀ NON ASSICURABILI

- Istituzioni finanziarie / Criptovalute / Agenzie di cambio
- Società che elaborano pagamenti
- Pubbliche amministrazioni, Trasporti Pubblici, Ospedali Pubblici
- Aziende coinvolte con la Sicurezza Nazionale, Telecomunicazioni
- Compagnie aeree / aeronautiche / aerospaziali, Terminal portuali, Aeroporti, Stazioni
- Servizi informatici, servizi di hosting e gestione di siti Web, provider Internet, provider cloud, provider di sicurezza informatica, creatori di siti Web
- Software house, sviluppatori di software, app di riconoscimento facciale
- Giochi in linea, videogiochi, Social networks, Aggregatori
- Controlli in background / società di controllo in remoto / elaborazione dati, verifica informazioni
- Società di distruzione / archiviazione di dati
- Siti web

Sottolimiti del Massimale Aggregato per singola garanzia

	Sottolimiti
SEZIONE 1 - RESPONSABILITÀ CIVILE VERSO TERZI	
1.3: Responsabilità per la sicurezza delle informazioni e privacy	100%
1.4: Responsabilità per l'attività multimediale e pubblicitaria	100%
1.5: Costi, oneri e sanzioni PCI	10%
SEZIONE 2 - DANNI DIRETTI	
2.2: Danni relativi all'interruzione della propria attività	30%
2.3: Costi per recupero dati	10%
2.4: Cyber estorsione	10%
2.5: Costi di istruttoria	30%
2.6: Spese per investigazione	10%
E-Crime	10%
2.7: Massimali per Servizi per la gestione di una Violazione dei Dati	
Numero di Soggetti Titolari da Notificare	10%
Massimale	50%

ITAS MUTUA

GRAZIE

ITAS MUTUA