CYBER INSURANCE 2024: LESSONS LEARNT

Di Cesare Burei, CEO Margas, Broker e Consulente di Assicurazioni e Debora Casalini, Cyber Risk Assistant

ESTRATTO DA

POSITION PAPER CYBERSECURITY
LA MATURITÀ DELLE AZIENDE ITALIANE NELLA RISPOSTA AL RISCHIO CYBER
by

11/2024

CYBER INSURANCE 2024: LESSONS LEARNT

Di Cesare Burei, CEO Margas, Broker e Consulente di Assicurazioni e Debora Casalini, Cyber Risk Assistant, Margas

Negli ultimi dieci anni lo strumento assicurativo ha assunto un'importanza crescente per la gestione del cyber risk e non solo per l'esistenza di una specifica certificazione nell'ambito della serie ISO 27.000 (la ISO/IEC 27102)[22]. Lo confermano i più recenti dati provenienti dai report sull'andamento del mercato

[22] https://www.isms.online/iso-27102/

assicurativo cyber a livello mondiale - 7,60 miliardi di dollari nel 2021 con una previsione di crescita fino a 20,43 miliardi di dollari entro il 2027[23]- e USA - intorno ai 4,9 miliardi di dollari nel 2023[24].

Per l'Europa, una delle poche stime esistenti, quella della Società di Riassicurazione Munich Re[25], dà il volume di premi a 2,3 miliardi di dollari alla fine del 2023, in crescita di 4 volte in cinque anni (cfr ultimi dati EIOPA, Autorità europea delle assicurazioni e delle pensioni aziendali e professionali, del 2017[26]), specialmente dopo la pandemia da Covid-19 e la crescita degli attacchi ransomware.

Ciò nonostante, l'ANIA, l'Associazione Nazionale Italiana tra le imprese Assicuratrici, fa poco più di un cenno al Cyber Risk nel rapporto annuale sulle assicurazioni in Italia 2024[27] al capitolo "Altri rami di danni" in una sottosezione sul livello assicurativo nelle PMI.

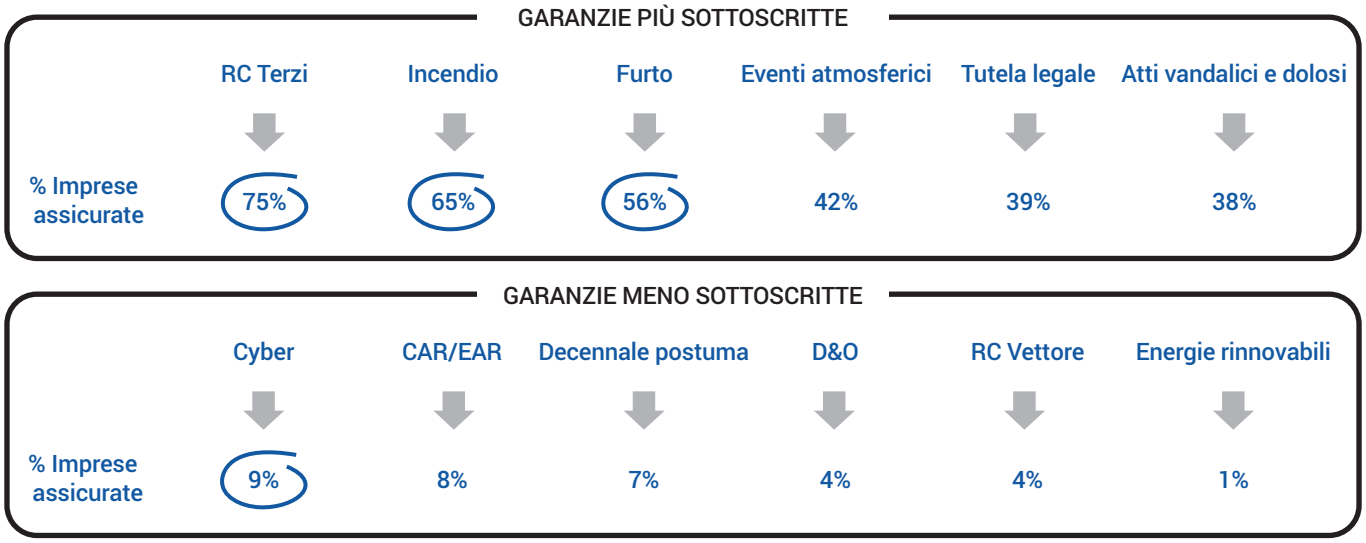
L'analisi a campione (!) rivela infatti che il 9% delle aziende PMI (!) si avvale di una garanzia cyber e di queste solo il 40% prevede la business interruption. Negli USA il livello complessivo di penetrazione nelle aziende si aggirerebbe sul 55%.

[23] https://networkassured.com/security/cybersecurity-insurance-statistics/

[24] https://networkassured.com/security/cybersecurity-insurance-statistics/

[25] https://www.ivass.it/pubblicazioni-e-statistiche/pubblicazioni/altre-pubblicazioni/2023/indagine-cyber-ris Companies https://www.eiopa.europa.eu/document/download/7cec5eef-4b6d-4cd7-ad0f-b4add0a3fe17_en?filename=Understanding%20Cyber%20Insurance%20-%20Report k/index.html?dotcache=refresh

[26] https://www.eiopa.europa.eu/document/download/7cec5eef-4b6d-4cd7-ad0f-b4add0a3fe17_en?filename=Understanding%20Cyber%20Insurance%20-%20Report



C'è molto da fare, ma, secondo la nostra esperienza e per rispondere al quesito di questa pubblicazione, una fase matura di gestione del cyber risk, non può prescindere da una soluzione assicurativa e da una consulenza che possa spiegare e motivare al cliente cosa è importante sapere e fare per assicurarsi al meglio e poi far funzionare la polizza.

[27] https://ania.it/documents/35135/439653/LAssicurazione-Italiana-2024_WEB.pdf/bf8d4d10-b3ce-45d0-62c7-76d57492be13?version=1.0&t=1719994663305

I sinistri: l'altra faccia dell'esperienza

La gestione di un incidente informatico, in presenza o in assenza di copertura assicurativa cyber, offre spunti di riflessione sulla nostra antifragilità digitale ed è, al di là dei freddi numeri statistici sulla crescita degli incidenti che diffondono panico, un buon punto di partenza. Vediamo quindi due casi verificatisi tra autunno 2023 e primavera 2024.

CASO A)

Azienda di produzione di prodotti in plastica nella filiera HORECA. Classe di fatturato 50-100 Mio, Classe dipendenti 100-200.

Impossibilità di accesso alla rete e ai sistemi aziendali. Le password non vengono più riconosciute. I backup sono compromessi. I dati dei log degli accessi al sistema sono salvati in cloud, non compromessi e disponibili. Nessun data breach.

Il fornitore IT per la gestione sistemistica interviene in 24 ore, mette la rete sotto il proprio SOC e comincia le analisi. L'incident report è pronto in un mese. L'analisi rivela un attacco ransomware.

Alla fine del terzo mese la crisi è risolta. Il bilancio è di 220.000 euro di perdite. La compagnia riconosce e risarcisce il danno per

- Costi di consulenza esterna: 40.000 euro
- Fermo d'attività: 60.000 euro
- Costi di tempo uomo dedicati alla risoluzione della crisi: 100.000 euro

Il totale degli stakeholder interni ed esterni coinvolti nel coordinamento decisionale è di 8 persone: CEO, CFO, CIO, HR interni più Legal, broker assicurativo e fornitore IT esterni.

Tempi di liquidazione: 3 mesi dalla chiusura dell'incident. Il cliente si dichiara soddisfatto della transazione.

CASO B)

Azienda di produzione nella filiera del luxury, da poco facente parte di un Gruppo gestito da un Fondo. Classe di fatturato 20-50 Mio; Classe dipendenti: 100-200.

L'azienda è supportata da un professionista IT esterno; la rete non è ancora conformata a quella dell'acquirente.

Né l'azienda colpita, né la capogruppo sono assicurate contro il cyber risk. La capogruppo prende in mano la situazione, ma è costretta ad esternalizzare un servizio di IRM (la nostra società è stata selezionata per il coordinamento dell'Incident response). I suoi fornitori IT non sono attrezzati per la messa immediata sotto SOC pretesa dal principale cliente che sospende le forniture fino a soddisfacimento della richiesta. Si scopre che l'infezione di un client per esposizione RDP ha compromesso un server in un contesto di assenza di politiche sulla gestione delle password o dei diritti di accesso. Oltre a monitorare, bisogna sanificare e denunciare preventivamente un data breach alla polizia postale, al garante privacy e ai clienti.

È necessario compilare l'asset inventory e certificare lo stato dell'arte della compromissione e le sue cause. Non c'è fermo di attività aziendale.

L'unità di crisi arriverà a contare 18 persone di 10 organizzazioni diverse, tra cui la società colpita, la capogruppo, il fondo d'investimento, il cliente principale, due studi legali, due aziende IT, il professionista IT e un esperto in brand reputation. Il caso si risolve in un mese.

Nonostante non si possa coinvolgere l'assicurazione, viene redatto un computo delle spese sostenute. A fronte di alcune voci ancora da quantificare, i costi e danni ammontano ad un minimo di 130.000 euro a cui aggiungeranno le parcelle dei professionisti. Le ore uomo totali arrivano a 800. Si attende anche un audit del cliente chiave e la risoluzione del Garante con quel che ne potrebbe conseguire.

Conclusioni

È molto evidente che a fronte di costi confrontabili - a meno ovviamente di due anni di premio assicurativo e di adeguati investimenti informatici annuali operati dalla Azienda A - i sinistri abbiano epiloghi diversi:

- Nel primo caso siamo in presenza di una azienda strutturata e organizzata nella gestione della cyber security e del risk management, di cui broker e polizza assicurativa sono un tassello. L'incident è decisamente più grave per pervasività e impatto sulla operatività aziendale, ma non pone problematiche da GDPR. L'assistenza al sinistro da parte del broker qui è compresa (entro questa soglia di danno) nel mandato ricevuto dall'azienda e ha aiutato nell'interlocuzione con periti e compagnia, pilotando una corretta e puntuale produzione documentale ai fini del risarcimento.
- Nel secondo caso possiamo parlare di una gestione della cyber security praticamente inesistente; una filiera a monte e a valle che non sembra preoccuparsi di questi aspetti. Si palesa inoltre un problema commerciale, di reputazione e comunicazione a cui nessuno ha pensato prima.

Questa azienda non sarebbe stata assicurabile, ma con un approccio diverso in prevenzione avrebbe potuto beneficiarne, come è stato nel caso A.

Lessons learnt

Per accedere alla assicurazione come strumento di finanziamento del rischio che funzioni, occorre dunque

- una postura tecnico-organizzativa adeguata e sostanzialmente compliant a GDPR, Cyber Resilience Act o DORA e ora NIS 2;
- un asset inventory sempre aggiornato, VA periodici, implementazione di MFA e VPN;
- politiche di aggiornamento dei sistemi e di backup (regola 2-3-1)
- formazione del personale.

Essere assicurati cyber implica l'onere della prova, quindi ci si deve attrezzare in "tempo di pace" per

- dimostrare cosa è successo (log management in BC, VA report, asset inventory);
- come tener conto e prova dei costi (gestionali finanziario e HR in BC);
- dotarsi di risk manager e/o costituire tavoli di lavoro permanenti e di crisi, che comprendano gli stakeholder esterni, il broker compreso.

Fare analisi e mitigazione continua, assicurarsi, essere rapidi in "tempo di guerra", con fornitori critici adeguati e correttamente assicurati, può fare la differenza fra "vivere o morire".

Fare analisi e mitigazione continua, assicurarsi, essere rapidi in "tempo di guerra", con fornitori critici adeguati e correttamente assicurati, può fare la differenza fra "vivere o morire"

PUNTI DI ATTENZIONE ED ERRORI DA EVITARE NELLA GESTIONE DEI RISCHI CYBER

Nel capitolo sono stati analizzati i punti essenziali nei percorsi verso una moderna e matura gestione del rischio cyber. Emergono, dai contributi, gli aspetti chiave su cui occorre concentrare l'attenzione.

Il primo punto è che adottare standard, framework e best practices di sicurezza, insieme alle certificazioni, è essenziale per garantire una sicurezza robusta, conformità legale e maggiore fiducia nel mercato. L'adozione di standard come ISO/IEC 27001 e 22301 oltre a migliorare la sicurezza informatica garantisce la conformità a normative come GDPR o PCI DSS. Le certificazioni non sono obbligatorie, ma utili per aumentare la fiducia di clienti e partner. Le certificazioni di cybersecurity, come CISSP e CISM, aiutano invece a formare professionisti esperti, migliorando le competenze interne e la resistenza complessiva alle minacce. In generale è poi fondamentale che la direzione aziendale e i dipendenti siano formati e sensibilizzati riguardo alla gestione dei rischi di sicurezza. La consapevolezza e la responsabilità diffusa sono chiave per una postura di sicurezza robusta.

Con riferimento a framework e best practices di sicurezza, l'adozione di molti di questi, come autenticazione multifattoriale e crittografia, riduce i rischi di attacchi. Framework come il NIST Cybersecurity Framework e il CIS Critical Security Controls forniscono approcci strutturati per gestire i rischi informatici e migliorare la resilienza. L'ISA/IEC 62443 è particolarmente rilevante per la sicurezza nei sistemi di automazione industriale. Questi percorsi di formazione sono essenziali per mantenere le organizzazioni al sicuro e competitive. Il framework Zero Trust offre maggiore protezione dei dati, visibilità della rete e flessibilità nell'adattarsi a tecnologie emergenti come il cloud e IoT. Questo approccio si basa su "mai fidarsi, sempre verificare" e mira a proteggere l'accesso a risorse sensibili attraverso il controllo continuo dell'identità e delle autorizzazioni. Gestione delle identità e degli accessi (IAM), crittografia dei dati, micro-segmentazione della rete e la sicurezza di accesso al cloud (SASE) sono tecnologie chiave per implementare il modello Zero Trust.

In ambito cloud, la raccomandazione di base è quella di considerare un Modello di Responsabilità Condivisa (SSRM), in quanto la sicurezza è una responsabilità condivisa tra il fornitore di servizi (CSP) e il cliente (CSC). Entrambi devono collaborare per garantire che i servizi cloud siano sicuri, definendo chiaramente le rispettive responsabilità. CSA offre strumenti come il CAIQ e la Cloud Control Matrix (CCM) per supportare questa collaborazione.

Altre raccomandazioni che emergono nel capitolo sono le seguenti, relative a una gestione il più possibile evoluta e "olistica" del rischio cyber.

Gestione Integrata del Rischio Multi-compliance: è cruciale adottare un approccio olistico che integri le diverse aree di rischio (cybersecurity, privacy, sicurezza fisica, continuità operativa) e monitorare dinamicamente la sicurezza tramite KPI/KRI. Questo approccio deve essere sistematico e proattivo, garantendo una visione complessiva degli impatti e permettendo una strategia di mitigazione

integrata. Il framework adottato dall'organizzazione deve assicurare la conformità a normative e standard applicabili, come il GDPR e la Direttiva NIS 2. Le recenti regolamentazioni richiedono un approccio integrato e multirischio per una gestione efficace della sicurezza.

Security by Design: serve un'integrazione della sicurezza dalla progettazione. L'approccio "Security by Design" è essenziale per prevenire vulnerabilità nei sistemi fin dalle fasi iniziali di progettazione. Ritardare l'integrazione della sicurezza può aumentare i costi e i rischi. Serve incorporare la sicurezza fin dalle prime fasi di sviluppo del prodotto per ridurre errori e costi (Shift Left Security Testing). Questo richiede una mentalità proattiva e competenze distribuite all'interno dei team di sviluppo.

Aggiornamenti e Monitoraggio. La sicurezza deve essere gestita come un processo continuo. Le vulnerabilità emergenti richiedono aggiornamenti regolari e una gestione continua dei rischi. Bisogna considerate il tema del "Debito Tecnologico", ossia, l'accumulo di sistemi obsoleti o progettati con scarsa attenzione alla sicurezza, che amplia il gap rispetto alle best practice. È necessario considerare questo aspetto soprattutto quando si introducono nuove soluzioni.

Con riferimento all'**Incident Response**, i processi IR devono essere integrati con le strategie generali di sicurezza informatica dell'organizzazione, che includono prevenzione, rilevamento e risposta agli attacchi. È essenziale, inoltre, che l'IR sia connesso a processi come l'analisi del rischio, la governance, la conformità alle policy interne e alle normative, e la gestione delle identità e dei dati. Guardando alla composizione del Team di Incident Response, dovrebbe includere esperti tecnici e di comunicazione, e potrebbe coinvolgere stakeholder a vari livelli aziendali, inclusi top management, legali e rappresentanti della comunicazione. Molto importanti le esercitazioni, come i test table-top, fondamentali per preparare il team e migliorare la risposta agli incidenti. La Guida nazionale TIBER-IT può essere utile per condurre test avanzati di cybersicurezza.

Per quanto riguarda la sicurezza degli ambienti industriali, può essere utile, soprattutto laddove le risorse sono limitate, un approccio molto pragmatico, con misure minime di sicurezza e visibilità. La protezione degli ambienti industriali è infatti oggi essenziale per prevenire danni significativi e garantire la continuità operativa. In caso di scarsa disponibilità di risorse e commitment per la sicurezza degli ICS/OT, si raccomandano le seguenti misure minime di sicurezza. Un inventario dei sistemi ICS/Scada con la relativa valutazione del rischio. L'implementazione di misure di cybersicurezza, come la configurazione del firewall e l'hardening dei prodotti hardware e software. L'utilizzo di soluzioni di sicurezza specifiche, che possono includere il monitoraggio passivo e l'implementazione di agenti per ottenere visibilità e protezione.

Va ricordato inoltre che una buona copertura assicurativa, in caso di incidente subito da un'azienda, può fare la differenza: un'azienda strutturata e

organizzata nella gestione della cyber security e del risk management ha tipicamente un broker e una polizza assicurativa come tassello del proprio cyber risk management. In caso di incidente, la copertura e l'assistenza della compagnia aiutano a riprendersi in modo più veloce e con meno danni.

Gli errori da evitare per una gestione efficace della sicurezza informatica e della compliance.

Un primo errore da evitare è l'approccio isolato ai rischi. Gestire i rischi in modo frammentato o isolato, senza considerare le interrelazioni tra i diversi ambiti, può portare a una visione incompleta delle minacce. È necessario invece adottare un approccio integrato che tenga conto della complessità e delle connessioni tra i vari tipi di rischi.

Un altro errore frequente riguarda il ritardo nell'implementazione delle misure di sicurezza. Spesso, queste misure sono posticipate a fasi successive del ciclo di sviluppo, con l'idea di risparmiare tempo o risorse. Tuttavia, questa scelta può tradursi in costi molto più elevati nel lungo periodo e in una maggiore esposizione alle minacce. È cruciale integrare le misure di sicurezza fin dalle prime fasi.

La negligenza della compliance continuativa è un altro rischio da evitare. Considerare la conformità normativa come un'attività da svolgere una sola volta può essere pericoloso. Le normative e gli standard di sicurezza sono in costante evoluzione; quindi, è fondamentale monitorare e aggiornare regolarmente le pratiche aziendali per rimanere in linea con i requisiti legali e di sicurezza.

Un ulteriore errore è la sottovalutazione della formazione, della sensibilizzazione e della creazione di una cultura della sicurezza. Non si deve trascurare l'importanza di educare continuamente dipendenti e manager riguardo alla sicurezza informatica. Una formazione costante è essenziale per aumentare la consapevolezza sui rischi e responsabilizzare tutto il personale.

Infine, ignorare il debito tecnico può avere conseguenze gravi. L'interoperabilità con sistemi obsoleti può amplificare le vulnerabilità esistenti, rendendo più difficile proteggere i nuovi sviluppi. Non affrontare il debito tecnico in modo proattivo può esporre l'organizzazione a rischi che potrebbero essere evitati con un'adeguata gestione delle risorse tecnologiche.

Evitare questi errori richiede un approccio strategico e olistico alla gestione della sicurezza e dei rischi, ma aiuta a garantire una protezione efficace dell'azienda, del suo modello di business, delle sue persone e dei suoi asset strategici a lungo termine.

Grazie dell'attenzione che ha riservato a questo documento, creato per fornirLe un utile strumento di conoscenza e consapevolezza assicurativa.

Position Paper Cybersecurity 2024

di TIG - The Innovation Group integrale

è scaricabile gratuitamente qui:

https://www.theinnovationgroup.it/position-paper-cybersecurity-2024/?lang=it

MARGAS
CONSULENTE E BROKER DI ASSICURAZIONI
Dal 1980

Via Buonarroti, 235 - 35134 Padova
Tel: 049.600271 - Fax: 049.619060
e-mail: margas@margas.it
Sito web: **www.margas.it**