Executive Summary

445 miliardi di $

Costo annuale previsto per l'economia globale a causa dei crimini informatici [3]

200 miliardi di $

Costo annuale previsto per le 4 principali potenze economiche mondiali - USA, Cina, Giappone e Germania

50%

Le principali 10 economie rappresentano circa il 50% dei costi per i crimini informatici

Il panorama odierno sui rischi informatici

L'aumento dell'interconnettività, la globalizzazione e la **"commercializzazione"** del crimine informatico provocano incidenti informatici sempre più gravi e frequenti, incluse le violazioni dei dati.

Uno dei principali rischi informatici riguarda la protezione e riservatezza dei dati.

La relativa legislazione si rafforzerà a livello mondiale. Si prevede che aumenteranno le denunce e le multe per violazione dei dati. Le leggi si sono già inasprite negli USA, ad Hong Kong, Singapore e Australia. L'Unione Europea sta cercando di trovare un accordo per trovare delle regole comuni di protezione dei dati. Si prevede che i vari Paesi intraprenderanno linee guida più dure.

L'interruzione delle attività (Business interruption, BI), il furto della proprietà intellettuale e l'estorsione informatica - sia per guadagni finanziari che non finanziari - rischiano di aumentare. I costi dovuti alla BI possono essere della stessa entità - o anche superiori - ai danni diretti dovuti ad una violazione dei dati.

Gli attacchi degli hacker occupano i titoli dei giornali, ma esistono molti altri **"ingressi"** tramite i quali un'azienda può essere colpita da attacchi informatici. L'impatto dell'interruzione delle attività (BI) provocato da un guasto tecnico è spesso sottovalutato rispetto agli attacchi informatici.

La vulnerabilità dei sistemi di controllo industriale (industrial control systems, ICS) agli attacchi, rappresenta una minaccia importante. Fino ad oggi si è verificata spesso la manipolazione di account di turbine e centrali elettriche. Tuttavia, il danno potrebbe essere ancora superiore nelle strutture sensibili alla sicurezza, come le centrali nucleari, i laboratori, i fornitori d'acqua o i grandi ospedali.

Best practice di sicurezza e protezione informatica

Secondo il **Barometro dei Rischi di Allianz**[1], quello informatico è il rischio più sottovalutato dalle aziende, ma non esiste una **"soluzione magica"** per la sicurezza informatica.

In aggiunta ai danni pagati a seguito della perdita di dati dei clienti e dell'impatto della BI, la perdita di reputazione può essere un'importante causa di danno economico per le aziende.

Strumenti di monitoraggio, una migliore elaborazione e una maggiore consapevolezza da parte dei dipendenti possono rendere le aziende più preparate ai rischi.

Le aziende devono identificare i beni più sottoposti a rischi e debolezze, come il "fattore umano" o un'eccessiva fiducia nei riguardi dei terzi. I dipendenti possono, inavvertitamente o deliberatamente, provocare episodi che coinvolgono la sicurezza IT o la perdita di privacy.

Le aziende devono creare una cultura della sicurezza informatica e un approccio **"think-tank"** per affrontare meglio i rischi. Le diverse strutture dell'azienda devono condividere le conoscenze, provare a scatenare una crisi o violare un piano di reazione, effettuando dei test.

Il rischio informatico è in costante evoluzione, e possono emergere **"rischi nascosti"**. Ad esempio, le aziende devono considerare come le attività di fusione e acquisizione (merger and acquisition, M&A) e le modifiche nelle strutture aziendali, possano influire sulla sicurezza informatica e in particolare sul possesso dei dati di terzi.

Le aziende devono, infine, decidere quali rischi evitare, accettare, controllare o trasferire.

1 *Il Barometro dei Rischi di Allianz conduce indagini su più di 500 risk manager ed esperti di oltre 40 Paesi.*

Rischio informatico e assicurazioni - crescita e tendenze

Il mercato assicurativo informatico continuerà ad evolversi; questo sviluppo porterà con sé nuove sfide e la necessità di testare concetti e normativi di polizza, con la possibilità che sorgano dei contenziosi.

Non è raro che tale evoluzione si verifichi con i nuovi prodotti, e potrà farci conoscere meglio i rischi.

La consapevolezza - sia per quanto riguarda la comprensione aziendale delle esposizioni che la preparazione degli assicuratori - deve migliorare in caso di domanda crescente. Altre sfide sono rappresentate dal costo della polizza, dai modelli di rischio oltre ad incidenti che possono dare luogo a danni fisici.

Si stima che attualmente il mercato assicurativo informatico valga circa **2 miliardi di $** in premi a livello mondiale, e che le aziende statunitensi rappresentino circa il 90% del totale.

Meno del 10% delle aziende oggi acquistano un'assicurazione informatica. Tuttavia, si prevede che il mercato assicurativo informatico avrà un tasso di crescita a due cifre, anno su anno, per raggiungere **+20 miliardi di $** nel prossimo decennio.

La crescita negli USA è già in atto, provocata dalle leggi sulla protezione dei dati. Gli sviluppi legislativi e gli aumentati livelli di responsabilità, accelereranno la distribuzione di questa copertura anche in altri Paesi, così come la presenza di sempre più piccole e medie imprese **(PMI)** che cercano copertura per questo rischio.

Attualmente, i settori che potrebbero tendere ad acquistare un'assicurazione informatica sono quelli che detengono grandi volumi di dati personali – settore medico e delle vendite al dettaglio - o che si affidano a processi di tecnologia digitale, come produzione e telecomunicazioni. Tuttavia, l'interesse è in aumento tra servizi finanziari, settore energetico, utenze, trasporti, a causa dei crescenti pericoli dovuti all'interconnettività.

I rischi di responsabilità e di protezione dei dati oggi dominano il panorama informatico. Nel corso del prossimo decennio, l'impatto di una BI dovuta ad incidenti informatici e il continuo sviluppo di un mondo tecnologicamente interconnesso, causeranno una preoccupazione sempre maggiore per le aziende, provocando una crescita della richiesta di coperture.

Le aziende sono anche esposte al rischio informatico tramite le catene di fornitura, ed è sempre più necessario considerare l'impatto di un incidente in questo campo, come le responsabilità da affrontare in caso di impossibilità di consegnare i prodotti o di perdita dei dati dei clienti, per non parlare dei costi per la risoluzione di questi problemi. Le aziende cercheranno sempre di più di estendere la protezione anche alle loro catene della fornitura.

Rischi emergenti: l'impatto della tecnologia

L'"Internet delle cose" avrà un'influenza sempre maggiore nel mondo in cui viviamo e sul nostro business. Le stime prevedono che entro il 2020 un trilione di dispositivi saranno in connessione. Nuove tecnologie creano nuove vulnerabilità, e i criminali informatici possono sfruttare questo aumento di interconnettività.

Le aziende si basano sui dati aggiornati in tempo reale. Qualsiasi sospensione della catena di elaborazione - anche per un minuto - può provocare gravi interruzioni aziendali che influiscono sul bilancio.

Mano a mano che la tecnologia si evolve, i vecchi dispositivi ancora in uso possono creare vulnerabilità, soprattutto quando si basano su sistemi operativi non più supportati.

L'uso di servizi e di strumenti di archiviazione esterni - come il cloud - comporta dei rischi. I problemi potenziali sono l' interruzione dell'attività aziendale ad ampia scala e le perdite per la violazione dei dati.

La prospettiva di un' ingente perdita informatica è sempre più probabile. Un attacco o un incidente che provochino enormi danni da interruzione di attività o di reputazione, potrebbero mettere a repentaglio l'attività di aziende di grandi dimensioni.

Un attacco riuscito al cuore delle infrastrutture di Internet, come ad esempio ai protocolli principali come il Border Gateway Protocol (BGP) o il Domain Name System (DNS) avrebbero conseguenze inimmaginabili[2].

Un importante attacco o incidente informatico che coinvolga aziende elettriche o di erogazione di servizi può dar luogo ad interruzioni significative, danni fisici o persino – in futuro - mortali, mentre una cyber-guerra tra due Paesi potrebbe danneggiare i servizi Internet a livello globale.

Il tema della protezione di infrastrutture critiche, farà si che i governi siano sempre più interessati alla sicurezza informatica, dando luogo a gradi sempre maggiori di monitoraggio e attribuzione di responsabilità.

2 *Cyber Security In An Interconnected World: Recent Critical Events In A Nutshell, Allianz Group Economic Research*
3 *Net Losses: Estimating the Global Cost of Cyber Crime, CSIS/McAfee*