ASA | SVV

Schweizerischer Versicherungsverband
Association Suisse d'Assurances
Associazione Svizzera d'Assicurazioni
Swiss Insurance Association

Documento di base

Servizio specializzato: Comitato riassicurazione

Organo: Gruppo di lavoro rischi informatici

Data: 22 febbraio 2018

Tema: **Documento di base dell'ASA sui rischi informatici**

Riassunto

Si stima che i costi annui per i rischi informatici ammontino, soltanto in Svizzera, fino a CHF 9,5 miliardi; la tendenza è in aumento. Nell'ambito della rielaborazione della strategia nazionale per la protezione della Svizzera contro i cyber-rischi, il presente documento descrive il ruolo delle assicurazioni per rafforzare la gestione dei rischi informatici. Fa inoltre riferimento ai presupposti per l'assicurabilità dei rischi informatici e discute il ruolo dello Stato e della politica nella creazione di un mercato assicurativo sostenibile per i cyber-rischi.

Gli assicuratori sostengono le aziende nella gestione dei rischi assumendosi una serie di compiti importanti dal punto di vista dell'economia nazionale. I rischi informatici presentano tuttavia alcune sfide per gli assicuratori:

- accumulazione
- mancanza di dati
- asimmetria informativa
- obblighi assicurativi

Con la crescente interconnessione dell'economia e le monoculture di hardware e software, gli attacchi informatici possono colpire contemporaneamente molte aziende e arrecare notevoli danni a tutta l'economia. Sono stati esaminati 5 scenari di accumulazione ed è stato stimato il loro danno potenziale per l'economia e il ramo assicurativo. Nel caso estremo questo danno potenziale per lo scenario «rete elettrica» si attesta a circa CHF 12 miliardi (circa il 2 percento del prodotto interno lordo (PIL) svizzero) e per gli altri scenari fino a CHF 2,5 miliardi (fino allo 0,4 percento del PIL).

Schweizerischer Versicherungsverband SVV
Conrad-Ferdinand-Meyer-Strasse 14 | Postfach | CH-8022 Zürich | Zentrale +41 44 208 28 28 | Fax +41 44 208 28 00 | www.svv.ch

Vista l'ancora piccola penetrazione del mercato per specifiche assicurazioni cyber e vista la capacità già messa sul mercato da parte degli assicuratori e dei riassicuratori, attualmente l'industria assicurativa può farsi carico anche di grandi danni informatici. Tuttavia, se la penetrazione del mercato continua a crescere sensibilmente, occorre esaminare ancora più nel dettaglio la sostenibilità dei danni da parte del settore assicurativo.

In caso di attacchi informatici a infrastrutture critiche con conseguenti danni a cose e forse anche a persone, l'industria assicurativa non offre alcuna copertura completa per i casi estremi, visto che tali gravi eventi possono superare rapidamente la capacità del ramo assicurativo. Vanno esaminate più dettagliatamente possibili soluzioni, come in caso di coperture del rischio terroristico o di pool per i danni della natura con finanziamento statale.

La mancanza di dati rende difficile all'industria assicurativa offrire prodotti adeguati a prezzi basati sul rischio. Un obbligo generale di notifica per gli attacchi informatici potrebbe fornire un aiuto, soprattutto se tali attacchi non comprendono solo violazioni della protezione dei dati, ma anche eventi di altro tipo. Tuttavia, l'esperienza mostra che, in certe situazioni, una notifica volontaria di tali attacchi è da preferire a un obbligo definito dallo Stato, perché così l'ufficio competente riceve in generale dati migliori. Dall'altra parte, i dati ricevuti non sono però rappresentativi per tutta l'economia. Bisogna chiarie se, in caso di attacchi informatici, si raggiunge il risultato auspicato (una migliore base di dati) con una notifica su base volontaria o con un obbligo di segnalazione.

Anche lo scambio dei dati ha un ruolo importante. Per lo scambio dei dati sono necessarie condizioni relative al diritto della concorrenza, sulla cui base l'industria assicurativa può organizzarsi autonomamente con altri attori attivi sul mercato.

Le asimmetrie informative tra il contraente e l'assicurazione possono far sì che l'assicurato sfrutti l'assicurazione oltre il suo scopo («moral hazard») o portare alla promozione dell'antiselezione. In entrambi i casi si tratta di fattori che limitano fortemente l'assicurabilità dei rischi. Una possibile asimmetria informativa nel settore informatico può essere affrontata con standard minimi per la sicurezza informatica.

Tali standard dovrebbero basarsi su principi e non dovrebbero oberare e gravare oltremodo sulle aziende che li implementano.

Bisogna valutare nel dettaglio come introdurre e attuare questi standard minimi:

- standard minimi stabiliti dalla legge
- una prescrizione legale per l'elaborazione di standard minimi specifici per il settore
- standard minimi specifici per il settore non stabiliti dalla legge, che sono ad esempio obbligatori per richiedere la copertura assicurativa o partecipare a determinate catene di fornitura.

Un aspetto importante che va oltre l'introduzione di standard minimi è la consapevolezza delle aziende per quanto concerne i rischi informatici. Questa consapevolezza può essere aumentata ad esempio tramite campagne e il lavoro in «Public-Private-Partnership» anche con il coinvolgimento dell'industria assicurativa.

Esistono gli obblighi assicurativi in particolare in settori dove un'attività o una struttura può arrecare danni a terzi (ad es. categorie professionali come medici, detentori di veicoli, centrali nucleari, impianti di accumulazione). Altri obblighi, come ad esempio l'assicurazione contro i pericoli naturali, concernono danni propri degli assicurati. L'obbligo costringe gli attori attivi sul mercato a trasmettere a terzi (l'assicuratore) il proprio rischio finanziario (come persona potenzialmente lesa o responsabile) e presuppone la totale assicurabilità del rischio. Visto che attualmente per i danni informatici questo aspetto è rispettato solo in parte e, in determinate situazioni, potrebbe risultare per le aziende un incentivo a ridurre gli investimenti nella sicurezza informatica perché tanto sono assicurati, tale misura è in contrapposizione al desiderio di un aumento generale della sicurezza informatica.

Secondo l'Associazione Svizzera d'Assicurazioni, la Confederazione dovrebbe - eventualmente insieme all'economia - attuare le seguenti otto misure.

1. Deve essere sensibilmente aumentata la consapevolezza delle piccole e medie imprese (PMI) circa i pericoli collegati ai rischi informatici. Vanno effettuate o sostenute le relative campagne. In generale, l'opinione pubblica deve essere sensibilizzata sui rischi informatici (awareness). A questo scopo è necessario, tra le altre misure, allestire e attuare un piano di comunicazione.
2. Bisogna promuovere la creazione di competenze e conoscenze. Di queste fa parte anche il rafforzamento della capacità di valutazione e di descrizione delle minacce informatiche.
3. Va introdotto o ampliato il resilience management a livello aziendale, in particolare al fine di evitare il rischio di accumulazione dell'economia nazionale e di permettere anche in futuro l'assicurabilità dei rischi informatici.
4. La valutazione e l'introduzione di uno standard minimo sono obbligatori e di principio sono accolti positivamente. Vanno quindi promosse la valutazione di uno (standard federale) e/o più standard (standard settoriale) e la relativa introduzione.
5. Un obbligo di notifica per gli attacchi informatici è accolto perlopiù positivamente. Gli uffici federali preposti devono perciò avviare la verifica di un concreto obbligo di notifica, nonché la decisione riguardante l'introduzione.
6. La Confederazione deve occuparsi della creazione di servizi per tutti i tipi di aziende (ad. es. consulenza, informazioni, ecc.).
7. Bisogna applicare e portare avanti, in modo coerente a livello nazionale e internazionale, l'azione penale in caso di cyber-criminalità, al fine di ridurre il numero dei sinistri futuri.
8. È assolutamente necessaria una cooperazione nazionale e internazionale (p. es. statistica comune dei sinistri, gestione delle crisi, minacce, ecc.). Ciò vale anche per il settore assicurativo.

In aggiunta alle misure sopraccitate, per le quali lo Stato deve assumere un ruolo di guida, l'industria assicurativa deve verificare le seguenti iniziative.

9. Oltre alle minacce informatiche per l'industria e il commercio, bisogna analizzare anche quelle per le istituzioni comunali, al fine di poter fornire un buon sostegno per la gestione dei cyber-rischi anche a questo livello.

10. Occorre verificare lo sviluppo dei modelli di condizioni per le assicurazioni cyber e coordinarli con i Paesi limitrofi.
11. L'industria assicurativa deve promuovere la creazione di un sapere nel settore della consulenza sulle minacce informatiche e del disbrigo dei sinistri.