ASA | SVV

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

RELAZIONE

Di Severin Moser, membro del comitato direttivo dell'ASA
Evento **Conferenza stampa annuale dell'ASA 2018**
Data 18 gennaio 2018
Luogo Zurigo

Rischi informatici – Il punto di vista degli assicuratori

Fa stato la versione orale.

Gentili signore, egregi signori

Il mondo è sempre più connesso … Entro il 2020 50 miliardi di apparecchi saranno collegati all'«Internet of Things»: dal frigorifero alla radio e al televisore, fino ai chip per la salute impiantati nel corpo umano. Sulle strade circoleranno 250 milioni di veicoli, che registreranno ed elaboreranno costantemente dati, si allineeranno con satelliti e innumerevoli applicazioni e in parte viaggeranno già autonomamente.

Si tratta di grandi opportunità. Tuttavia, dove ci sono opportunità si celano anche dei rischi: cyber attacchi, furti di dati, frodi informatiche e guasti al sistema sono solo alcuni esempi di minacce reali della digitalizzazione. I costi medi annui per i danni informatici sono stimati a 450 miliardi di dollari statunitensi in tutto il mondo. Questa cifra è più del doppio rispetto a quella per le catastrofi naturali a livello mondiale che, secondo Swiss Re, ammonta a circa 200 miliardi di dollari statunitensi sulla media pluriennale. Secondo uno studio McAfee, soltanto nel nostro Paese i costi annui causati dai danni informatici raggiungono i 9,5 miliardi di franchi svizzeri.

Riconoscere i rischi acuti

Sono costi enormi. E rischi enormi. Le persone vogliono tutelarsi dai rischi. Per proteggersi bisogna però essere consapevoli della loro esistenza. La consapevolezza dei rischi e in particolare dei rischi informatici che nasconde la digitalizzazione sembra essere poco sviluppata nel nostro Paese, soprattutto anche nelle PMI. È quanto emerso dal sondaggio «Cyberrisiken in Schweizer KMU» (rischi informatici nelle PMI svizzere) condotto da gfs e commissionato anche dall'ASA.

Secondo lo studio, il 56 percento dei direttori delle PMI svizzere intervistati si sente da ben a ottimamente protetto dagli attacchi informatici. Il rischio di essere vittima di un attacco informatico è

ritenuto basso: solo il 10 percento considera un grande pericolo l'essere messo fuori gioco per un giorno intero. Soltanto il 4 percento ritiene un grande o un enorme pericolo il fatto che un rischio informatico possa compromettere perfino l'esistenza dell'attività. Ciò mostra chiaramente quanto sia ancora bassa la consapevolezza dei rischi in questo segmento a livello decisionale (e non a livello informatico).

Le soluzioni specifiche sono sempre precedute da un'analisi mirata dei rischi. Secondo l'Allianz Risk Barometer 2018, per il quale sono stati interpellati circa 2'000 esperti del rischio in tutto il mondo, quest'anno l'interruzione d'esercizio rappresenta il maggior rischio aziendale a livello mondiale. Anche in Svizzera questo rischio continua a occupare la prima posizione. Le conseguenze di un'interruzione d'esercizio possono mettere in pericolo l'esistenza di un'azienda.

Possono portare a un'interruzione d'esercizio attacchi informatici come furto di dati, attacchi hacker o ransomware. I rischi informatici sono in crescita a livello mondiale e nel 2018 in Svizzera si trovano in 3ª posizione nella classifica dei rischi.

Cyber assicurazioni – sviluppo del mercato
Il mercato delle cyber assicurazioni è ancora piccolo, ma in crescita. Esperti di Swiss Re stimano attualmente un incasso annuo per i premi delle assicurazioni cyber pari ad appena 400 milioni di dollari statunitensi per il mercato europeo. A titolo di paragone: i premi incassati per i veicoli si attestano presumibilmente a 161 miliardi di dollari statunitensi in Europa. Uno studio attuale di KPMG prevede entro il 2036 un volume di premi per le assicurazioni cyber in Svizzera di circa 2,2 miliardi di euro. Tre quarti di questo volume proverrebbero da piccole aziende e da privati.

Attualmente il calcolo dei premi rappresenta una grande sfida. È difficile calcolare i rischi perché non sono disponibili dati di riferimento per il modello di calcolo, soprattutto a causa del rapido progresso tecnologico che fa costantemente emergere nuovi rischi informatici. Così i prodotti informatici diventano più complessi. Ciò ci mostra che la sicurezza informatica va oltre la copertura assicurativa. La copertura va di pari passo con un maggiore fabbisogno di consulenza e con servizi volti a chiarire e riconoscere gli attacchi.

Oltre ad Allianz, altri membri dell'ASA come Zurich, La Mobiliare o Generali – per citarne solo alcuni – offrono già soluzioni assicurative «state of the art» per aziende e privati, al fine di rispondere in maniera adeguata alle esigenze del mercato.

Agire insieme contro i pericoli
Ma gli assicuratori da soli possono offrire protezione? In qualità di associazione liberale siamo prudenti nel richiedere regolamentazioni o addirittura interventi statali. Tuttavia, alla luce di questo

aspetto ambivalente – in particolare per noi assicuratori – della trasformazione digitale, siamo dell'opinione che valga la pena confrontarsi con le domande se e come lo Stato deve intervenire e dove l'economia può collocare le proprie linee guida.

Vanno chiarite nel dettaglio la suddivisione dei ruoli e l'estensione dei campi d'azione di Stato ed economia. Per quanto riguarda tali questioni l'ASA ha coordinato le richieste dell'intero settore in un gruppo di lavoro con specialisti delle aziende affiliate. Il comitato direttivo sta elaborando i presupposti necessari che si basano sull'attività del gruppo di lavoro. Anche per questo tema il contatto con altre associazioni professionali, l'amministrazione e la politica è centrale. Dal nostro punto di vista, in particolare nel caso dei rischi informatici, non basta più procedere in modo isolato.

Misure di protezione

La gestione comune dei rischi informatici si basa su due misure centrali: sensibilizzazione dell'opinione pubblica e cooperazione internazionale a tutti i livelli. La consapevolezza dei rischi informatici deve essere notevolmente aumentata. L'opinione pubblica, e mi riferisco in particolare alle PMI, va sensibilizzata di conseguenza. La lotta contro la criminalità informatica non può avvenire separatamente. I rischi informatici non si fermano ai confini. L'azione penale contro la criminalità informatica deve essere promossa in modo coerente e a livello internazionale. Noi assicuratori siamo chiamati a sviluppare ulteriormente la cooperazione internazionale tra di noi e con le autorità. Penso in particolare a statistiche comuni sui sinistri e a una gestione organizzata delle crisi.
Inoltre, bisognerebbe esaminare l'implementazione di un ufficio di segnalazione centrale per attacchi informatici.