INSURANCE Daily

GIOVEDÌ 18 FEBBRAIO 2021 N. 1895

PRIMO PIANO

Rc sanitaria, l'indagine di Ivass

L'Ivass ha avviato una nuova indagine sulla Rc sanitaria, che fa seguito alla rilevazione condotta nel corso del 2020. "L'emergenza sanitaria causata dal Covid – spiega l'Autorità nella lettera inviata alle compagnie – ha suggerito di rilevare alcune informazioni integrative, senza alterare la struttura del resto della rilevazione".

Nella precedente indagine le compagnie hanno dovuto segnalare, tra le altre cose, i premi lordi contabilizzati, i sinistri gravi denunciati tra il 2010 e il 2020, e le caratteristiche delle coperture. Ora l'Ivass integra le richieste di informazioni, chiedendo dettagli relativi ai sinistri denunciati nel 2020 connessi al Covid e la presenza "di condizioni di esclusione specifiche e di eventuali condizioni aggravanti nei contratti a causa dei rischi da Covid, e segnalazione di eventuali ostacoli per l'operatività nel settore della Rc sanitaria dovuti all'emergenza Covid".

"I dati da trasmettere – precisa l'Ivass – saranno acquisiti tramite l'applicazione Infostat esclusivamente in formato xml. La trasmissione dei dati dovrà essere effettuata nel periodo compreso tra il 15 marzo e il 23 aprile 2021".

Anche le società che operano in Italia nel ramo Rc Generale che non hanno assunto rischi di Rc sanitaria "dovranno comunque segnalare alcune semplici informazioni".

B.M.

RICERCHE

Sistemi di controllo industriale, ecco i rischi cyber emergenti

Un report realizzato dai Lloyd's assieme a CyberCube e Guy Carpenter descrive nel dettaglio tre scenari che rappresentano i percorsi più plausibili attraverso cui un attacco informatico contro i sistemi di controllo industriale (Ics) potrebbe generare gravi perdite assicurate

Il rischio informatico è in continua evoluzione, il che significa che gli assicuratori devono comprendere i rischi emergenti per stare al passo con le esposizioni dei loro clienti. Per questo i **Lloyd's**, assieme a **CyberCube** e **Guy Carpenter,** hanno condotto un'analisi che descrive nel dettaglio tre scenari che rappresentano i percorsi più plausibili attraverso i quali un attacco informatico contro i sistemi di controllo industriale (Ics) potrebbe generare gravi perdite assicurate. Tutti e tre gli scenari analizzati, sottolineano gli autori dello studio, hanno precedenti storici, e il report descrive come potrebbero verificarsi gli eventi più gravi. Lo studio, in particolare, ha preso in considerazione quattro settori chiave dipendenti dai sistemi Ics: produzione, spedizioni, energia e trasporti. Relativamente a ciascuno di essi sono stati esaminati i precedenti storici e i potenziali impatti futuri.

UN CAMBIO DI PROSPETTIVA

"Il potenziale di pericoli fisici – si legge nello studio – rappresenta un importante punto di svolta per il più ampio ecosistema (ri)assicurativo cyber. In precedenza era stato ritenuto improbabile che questo rischio potesse avere un impatto significativo sul mercato, visto che le minacce informatiche tradizionalmente emergono sotto forma di perdite non fisiche". Tuttavia il divario tra *information technology* (IT) e *operational technology* (OT, tecnologia operativa), insieme alla crescente diffusione dell'automazione e alla sofisticazione di coloro che mettono in atto gli attacchi. Sottolinea lo studio, rendono fondamentale che i (ri) assicuratori considerino attentamente come possono verificarsi le maggiori perdite e i potenziali impatti.

(continua a pag. 2)

INSURANCE Daily

GIOVEDÌ 18 FEBBRAIO 2021 N. 1895

(continua da pag. 1)

I PERCORSI PLAUSIBILI E QUELLI PREFERITI

Come accennato, Lloyd's, CyberCube e Guy Carpenter hanno collaborato per sviluppare una visione dei sinistri assicurati del settore informatico a partire da una serie di diversi scenari informatici. Gli scenari proposti si basano su attacchi contro Ics cyber e fisici. Utilizzando uno schema, il report illustra i percorsi di attacco "plausibili" e quelli "preferiti" che costituiscono la spina dorsale di quella che originariamente era la ricerca per sviluppare uno scenario realistico di disastro (realistic disaster scenario, Rds). Sono stati inclusi diversi scenari illustrativi che possono essere utilizzati dai sindacati dei Lloyd's per comprendere e misurare i rischi informatici operativi emergenti.

I tre scenari plausibili considerano: *(1)* un attacco malware mirato alla catena di approvvigionamento, in cui i malintenzionati violano un produttore di dispositivi e compromettono i prodotti di quel produttore prima della distribuzione; *(2)* un attacco mirato alla vulnerabilità dell'Internet of Things (IoT), in cui gli aggressori sfruttano una vulnerabilità in dispositivi IoT ampiamente utilizzati che si trovano in ambienti industriali; *(3)* l'infiltrazione di reti IT industriali per attraversare l'*air-gap* di OT.

"Un evento OT – si legge nello studio – potrebbe plausibilmente innescare una perdita che porta a danni alla proprietà e alla perdita di vite umane in una struttura, e portare a estese indagini forensi, operazioni di ripristino e, se necessario, a richiami di prodotti per limitare ulteriori danni". Tuttavia, rassicura il report, al momento è poco probabile che si verifichino presso più siti eventi capaci di generare danni property molto diffusi, interruzione dell'attività e risvolti in termini di costi umani.

GLI ASPETTI CHIAVE

"Lo studio – scrivono gli autori – fa luce su un ambiente in cui, fino a oggi, la stragrande maggioranza delle istanze si è basata sull'IT e non su processi fisici. Crediamo di essere a un punto di svolta in cui il potenziale per le minacce informatiche di colmare il divario tra IT e OT sta diventando sempre più evidente".

Il report mette in evidenza una serie di aspetti chiave emersi dall'analisi. In primis, c'è il fatto che "il rischio di un incidente cyber-fisico Ics è in aumento, soprattutto per le singole entità". È inoltre probabile che "un singolo attore affiliato a uno Stato nazionale o uno stesso Stato nazionale dispongano delle risorse e del livello di sofisticazione tecnica necessari per un attacco dannoso orientato agli Ics". Un attacco mirato contro un sito industriale in un settore di importanza strategica, o di straordinaria rilevanza economica o sociale (o una qualsiasi combinazione di questi fattori) sarebbe estremamente significativo: si tratta, ad esempio, dei settori chiave citati all'inizio: produzione, energia, trasporti e spedizioni.

Le continue tendenze di maggiore adozione del cloud nelle operazioni industriali, la convergenza di IT e OT e la proliferazione dell'IoT e della cosiddetta *smart manifacturing* "possono aggravare i problemi di sicurezza e aumentare i profili di esposizione".

AMBITI ANCORA NON DEL TUTTO CONOSCIUTI

Il report si conclude formulando una serie di raccomandazioni e suggerendo potenziali aree di interesse per il mercato dei Lloyd's, ma anche per chiunque sia interessato alla gestione o alla sottoscrizione dell'esposizione informatica.

"Si consiglia – si legge – di continuare la ricerca e di concentrarsi sullo sviluppo e sul miglioramento della gestione dell'esposizione e degli standard di sottoscrizione in un'area emergente del rischio informatico i cui confini devono ancora essere definiti". Il mercato assicurativo ha una ricca legacy nell'adattamento ai rischi emergenti e alle tendenze in evoluzione. "Man mano che il rischio di perdite cyber-fisiche cresce – conclude il report – è essenziale che il mercato sviluppi prodotti e le expertise per servirlo".

Beniamino Musto

INSURANCE Daily

GIOVEDÌ 18 FEBBRAIO 2021 N. 1895

NORMATIVA

La clausola di regolazione del premio

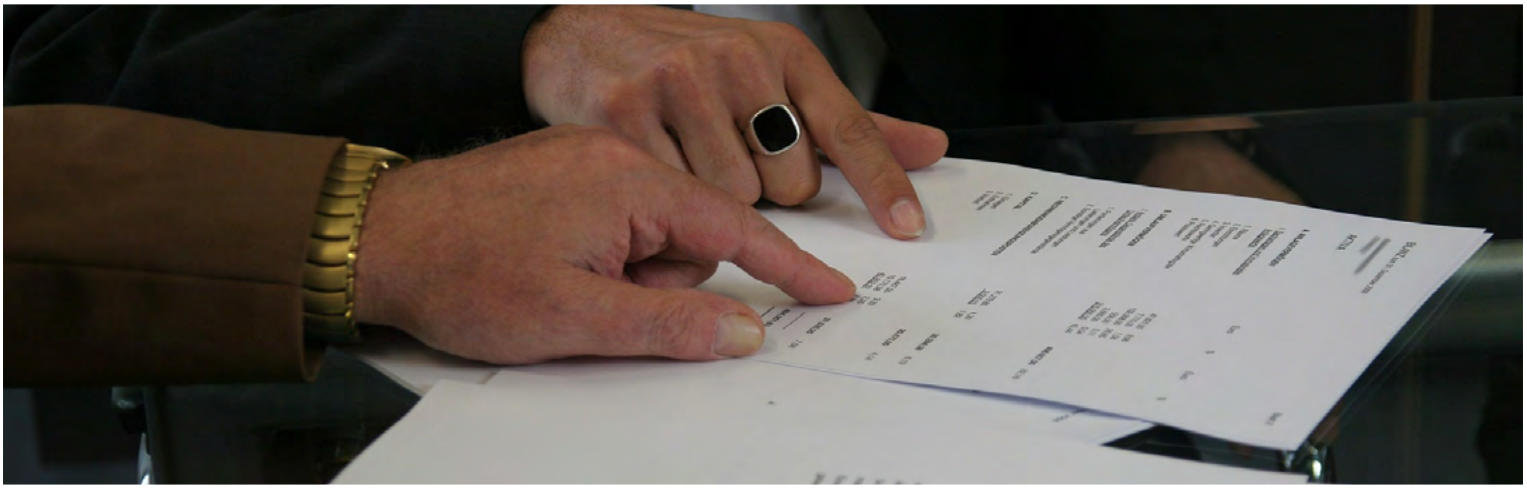
Questo tipo di postilla è impiegata soprattutto nell'assicurazione per il trasporto merci e nel credito commerciale. Ma cosa succede se l'assicurato non versa il conguaglio?

Tra le pattuizioni di polizza più diffuse nel mercato assicurativo vi è sicuramente la clausola di regolazione del premio.

Si tratta della clausola con cui il premio assicurativo viene assoggettato a elementi di rischio variabili: nella polizza è indicato un premio minimo, fissato in via provvisoria e anticipata in un determinato importo, e un premio eventualmente dovuto a conguaglio, in considerazione dei dati variabili che l'assicurato si obbliga a comunicare all'assicuratore alla fine del periodo assicurativo.

La clausola di regolazione del premio è impiegata soprattutto nell'assicurazione per il trasporto merci e nell'assicurazione del credito commerciale, poiché il suo meccanismo consente di adeguare il premio all'effettivo rischio assicurato, che l'assicuratore non era in grado di stabilire al momento della sottoscrizione del contratto o dell'inizio del periodo assicurativo.

Il premio minimo a importo fisso, dunque, deve essere pagato anticipatamente, mentre all'esito della comunicazione dei dati variabili sarà possibile accertare se l'assicurato deve versare un ulteriore premio a conguaglio in ragione del maggior rischio emerso.



Diverso dal versamento di un premio

Ma cosa succede nel caso in cui l'assicurato non versa il conguaglio del premio, oppure omette addirittura di comunicare i dati variabili all'assicuratore impedendo l'accertamento?

La Cassazione ha da tempo chiarito che l'adempimento di tali obblighi da parte dell'assicurato è adempimento di una obbligazione diversa da quella di versamento del premio ai sensi dell'articolo 1901 del codice civile (cfr. ad esempio Cassazione Civile Sezioni Unite 28 febbraio 2007, n. 4631).

Di regola, quindi, in tali ipotesi non si verifica automaticamente la sospensione della garanzia assicurativa, ma le conseguenze dell'inadempimento vanno valutate *case by case* in base a buona fede nell'esecuzione del contratto, tempo di esecuzione della prestazione e importanza dell'inadempimento.

Secondo una recente sentenza del tribunale di Roma, tuttavia, una pattuizione *ad hoc* inserita nella polizza può prevedere la sospensione della garanzia assicurativa come conseguenza del mancato versamento del premio aggiuntivo o della mancata comunicazione dei dati variabili: tale pattuizione determina validamente la sospensione derogando alla regola generale, purché sia stata oggetto di specifica sottoscrizione ex articolo 1341 del codice civile.

Alla luce delle evoluzioni giurisprudenziali, dunque, risulta fondamentale dotarsi di testi di polizza che siano adeguatamente specifici al fine di regolare le conseguenze dell'inadempimento dell'assicurato agli obblighi relativi al premio variabile.

Daniele D'Antonio,
Studio RP Legal & Tax

INSURANCE Daily

GIOVEDÌ 18 FEBBRAIO 2021 N. 1895

COMPAGNIE

Zurich Italia si allea con Viasat

I clienti della società specializzata in servizi telematici potranno sottoscrivere la polizza ZurichGò a condizioni agevolate

Zurich Italia ha annunciato l'avvio di una nuova partneship con **Viasat**. L'accordo, nello specifico, prevede che i clienti di Viasat che scelgono uno dei tre pacchetti *Sicuri & Protetti (basic, safety o security)* potranno assicurare a prezzi vantaggiosi il proprio veicolo con la polizza ZuriGò con uno sconto del 10% sulla garanzia obbligatoria, uno del 60% sulle garanzie opzionali *furto* e del 50% contro gli infortuni del conducente.

"Zurich è da sempre attenta all'evolversi degli stili di vita, dei bisogni e dei trend di consumo, in particolare all'evoluzione della mobilità", ha commentato **Elena Rasa**, chief underwriting officer della compagnia. "Viasat – ha proseguito – è una realtà italiana vicina ai valori della nostra compagnia, che ha contribuito nel tempo a importanti miglioramenti nell'ambito della sicurezza alla guida, e questo accordo conferma l'impegno di Zurich per la protezione delle persone in un momento delicato di ripresa della mobilità con nuove abitudini e con un maggiore bisogno di sicurezza".

Giacomo Corvi

Insurance Daily
Direttore responsabile: Maria Rosa Alaggio alaggio@insuranceconnect.it
Editore e Redazione: Insurance Connect Srl – Via Montepulciano 21 – 20124 Milano
T: 02.36768000 **E-mail:** redazione@insuranceconnect.it
Per inserzioni pubblicitarie contattare info@insuranceconnect.it
Supplemento al 18 febbraio di www.insurancetrade.it – Reg. presso Tribunale di Milano, n. 46, 27/01/2012 – ISSN 2385-2577