# **Catastrophic Cyber Risks** – una preoccupazione crescente

CHUBB®

*Gli incidenti informatici possono causare perdite senza confini e senza limiti nel tempo.*

In un mondo sempre più digitalizzato, aumenta la dipendenza dalla tecnologia così come la frequenza, la gravità e la sofisticazione degli incidenti informatici. Le vulnerabilità e le esposizioni si stanno moltiplicando a causa di una maggiore interconnessione, favorendo lo sviluppo di un rischio sistemico difficilmente rilevabile o controllabile. L'entità di questo rischio, unita alle relative conseguenze, potenzialmente gravi e ad impatto diffuso, aumenta la probabilità di una catastrofe informatica.

Simili alle pandemie, gli incidenti informatici possono causare perdite senza confini e senza limiti nel tempo. Non si tratta di sola teoria: i criminali informatici hanno già dimostrato la loro capacità di interrompere le catene di approvvigionamento delle imprese di tutto il mondo e paralizzare le infrastrutture critiche, come avvenuto nel recente attacco che ha costretto Colonial Pipeline a chiudere le sue linee di fornitura di carburante nella costa est degli Stati Uniti. Con i recenti incidenti cyber, che hanno causato miliardi di dollari in perdite economiche, non è difficile immaginare un attacco sistemico che potrebbe mettere alla prova la solvibilità del settore assicurativo.

A differenza dei precedenti eventi catastrofici imprevisti, stiamo assistendo alla rapida e continua espansione dei rischi cyber. Questo preavviso offre l'opportunità di agire ora per contribuire a garantire la messa in atto di adeguate difese informatiche e salvaguardie economiche in previsione di una potenziale catastrofe.

# Le assicurazioni Cyber diventano maggiorenni

*Grazie alla crescente diffusione di coperture cyber molte aziende sono protette, ma al tempo stesso aumenta l'esposizione del settore assicurativo con riferimento al rischio sistemico.*

La promessa di un'assicurazione cyber è stata pienamente realizzata negli ultimi anni, con danni liquidati dagli assicuratori a fronte di attacchi informatici significativi, fornendo protezione assicurativa a numerose aziende in tutto il mondo.

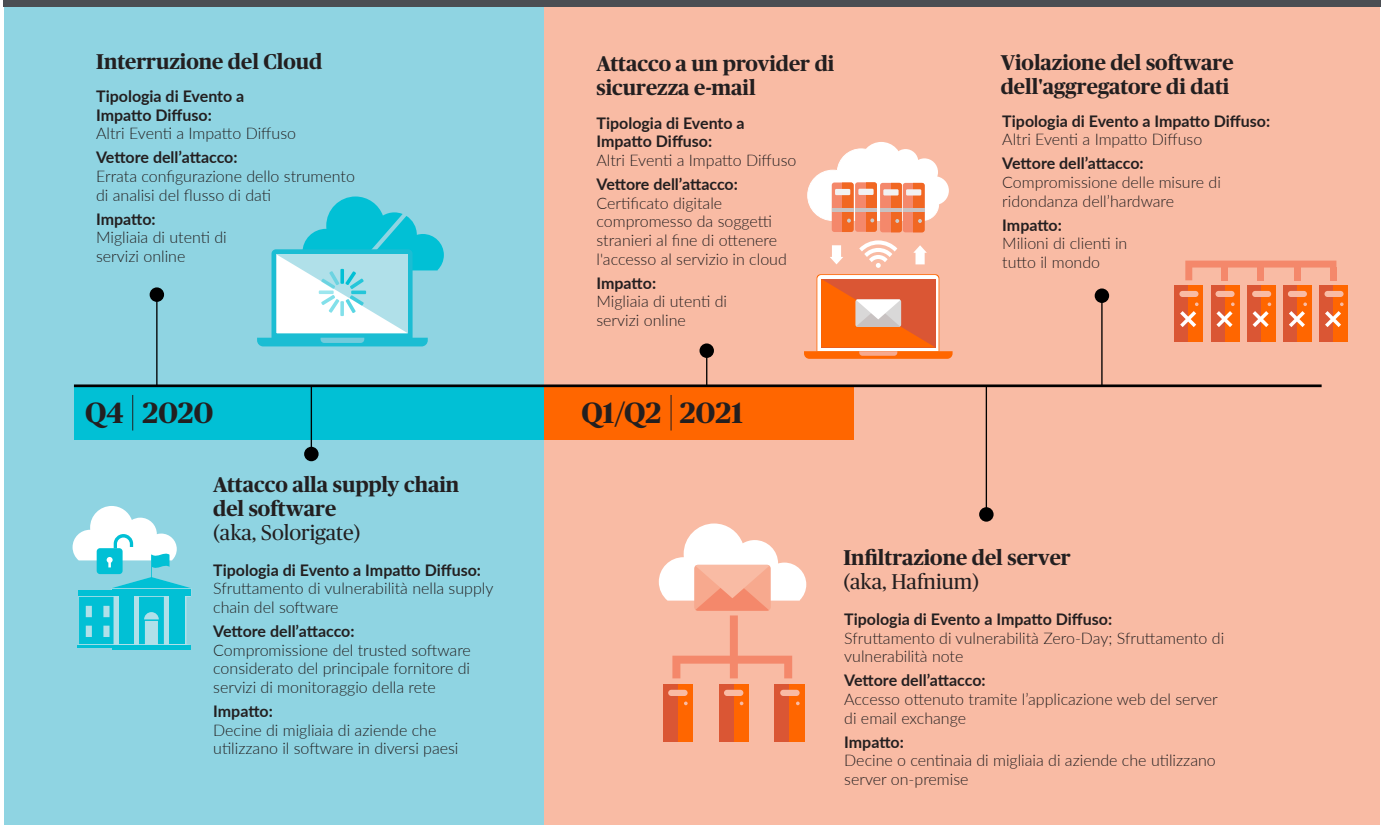
Attualmente, le garanzie principali - spese di risposta agli incidenti, danni propri da incidente informatico, Cyber liability e responsabilità professionale/errori e omissioni - forniscono importanti soluzioni di trasferimento e gestione del rischio per le aziende di ogni dimensione e settore. I servizi di gestione del rischio informatico offerti dalle compagnie assicurative sono stati preziosi nell'aiutare le aziende a mitigare il rischio e migliorare le loro difese tecnologiche sul front end, come i servizi di incident response si sono dimostrati efficaci nel riportare rapidamente le aziende alla normale operatività dopo un incidente cyber.

Grazie alla crescente diffusione delle coperture cyber - ora stimate a quasi 4 milioni di polizze (dati riferiti a compagnie assicurative domiciliate negli Stati Uniti e compagnie straniere che assicurano rischi statunitensi in forma Non-Admitted) e circa il 50% delle imprese statunitensi coperte, secondo un rapporto del Government Accountability Office del maggio 2021 - molte aziende sono protette, ma al tempo stesso aumenta l'esposizione del settore assicurativo con riferimento al rischio sistemico.

Negli ultimi anni le imprese hanno anche migliorato il loro livello di resilienza. Nel 2020 il 53% dei professionisti del settore della cyber security ha dichiarato che le loro organizzazioni hanno raggiunto un elevato livello di resilienza con riferimento al rischio cyber, rispetto al 35% del 2015.

Mentre le assicurazioni cyber stanno chiaramente assumendo un ruolo sempre più importante nel mitigare l'esposizione al rischio delle aziende, meno certa è la capacità degli assicuratori di assorbire i danni potenziali stimati a lungo termine.

## Gli eventi Cyber hanno un impatto sempre più diffuso




# Un rischio dall'evoluzione imprevedibile

*Nell'arco di 100 giorni, da dicembre 2020 a marzo 2021, svariati attacchi di grande portata hanno compromesso non soltanto software diffusi su larga scala e provider di servizi di posta elettronica, ma anche data center e infrastrutture critiche.*

Nonostante le aziende siano più consapevoli del rischio cyber e delle sue conseguenze, gli incidenti e le minacce informatiche sono in costante aumento ed evoluzione.

Oltre 18.000 nuove vulnerabilità software sono state pubblicate nel 2020, quasi il triplo rispetto al 2015 e in continua crescita. Nel frattempo, quasi 1,2 milioni di nuove minacce malware sono state identificate nel 2020, più del doppio rispetto al 2015. Tra le violazioni di sicurezza nel 2020, l'85% ha coinvolto il fattore umano, come gli schemi di ingegneria sociale.

Mentre tattiche come il ransomware sono diventate più comuni e costose, la violazione dei dati e la compromissione delle e-mail aziendali continuano a portare la frequenza degli incidenti informatici a livelli tra i più alti di sempre, specialmente durante la pandemia di COVID-19 e la conseguente diffusione di accordi di lavoro da remoto.

Anche gli attacchi informatici stanno avendo un impatto più diffuso. Nell'arco di 100 giorni, da dicembre 2020 a marzo 2021, svariati attacchi di grande portata hanno compromesso non solo software diffusi su larga scala e provider di servizi di posta elettronica, ma anche data center e infrastrutture critiche. Ben oltre 100.000 aziende di tutto il mondo sono state vittime di questi eventi.

Durante uno di questi eventi, noto come Solorigate, è stato rivelato che un massiccio attacco in cui il malware è stato incorporato in un aggiornamento di un software di monitoraggio della rete ritenuto affidabile, era passato inosservato per quasi otto mesi, colpendo circa 20.000 aziende e agenzie governative.

In un altro evento, un gruppo di hacker presumibilmente sponsorizzati dal loro governo e da organizzazioni criminali, noto come Hafnium, ha sfruttato una vulnerabilità allora sconosciuta ("zero-day") in un software comunemente utilizzato per ottenere l'accesso ai server on-premise in centinaia di migliaia di aziende.

# Gli incidenti ad alto profilo aumentano la tensione

*Quando assisteremo ad un evento cyber veramente catastrofico, diffuso e distruttivo?*

Anche se gli eventi Solorigate e Hafnium sono stati pervasivi e costosi, le conseguenze avrebbero potuto essere molto più devastanti. Sembra che lo scopo principale di ognuno di questi eventi fosse lo spionaggio; tuttavia, se l'intento fosse stato quello di rubare o distruggere dati critici o altre informazioni, le conseguenze economiche avrebbero potuto facilmente moltiplicarsi. Secondo Kevin Mandia, Amministratore Delegato di FireEye, azienda che si occupa di sicurezza di reti informatiche, durante una testimonianza depositata presso la Commissione Intelligence del Senato, se avessero davvero voluto essere distruttivi, i responsabili dell'attacco di Solorigate avrebbero avuto l'accesso e le capacità necessari.

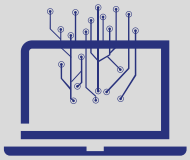
A ulteriore chiarimento, nel 2017 l'attacco NotPetya ha sfruttato uno strumento software utilizzato in ambito contabilità chiamato M.E.Doc, usato quasi esclusivamente in Ucraina, ma il malware si è poi diffuso indiscriminatamente e alla fine ha colpito molte grandi aziende con sede in Europa, negli Stati Uniti e altrove, causando perdite stimate in 10 miliardi di dollari. Alcune aziende vittime dell'attacco NotPetya hanno subito perdite superiori ai 100 milioni di dollari. Se questo tipo di malware distruttivo fosse stato utilizzato negli attacchi Solorigate o Hafnium, i danni economici complessivi avrebbero potuto essere esponenzialmente più elevati rispetto all'evento NotPetya.

Lo stesso anno l'attacco ransomware WannaCry ha colpito più di 200.000 computer in tutto il mondo. Fortunatamente è stata utilizzata una vulnerabilità nota che aveva già una patch disponibile, quindi la maggior parte degli utenti ne era immune. Come l'esempio di Hafnium fornito in precedenza, tuttavia, se si fosse sfruttata una vulnerabilità zero-day l'impatto avrebbe potuto essere molto più diffuso e grave.

Fino ad oggi abbiamo assistito a eventi di grande diffusione (ad esempio, Solorigate e Hafnium) ed eventi distruttivi (come NotPetya e WannaCry), ma finora le perdite dovute a questi eventi sono state gestibili. Con un danno potenziale così ingente, quando assisteremo a un evento cyber veramente catastrofico, diffuso e distruttivo?

# Eventi informatici potenzialmente catastrofici

*La crescente dipendenza dalla tecnologia da parte delle aziende e dei consumatori, così come l'interconnessione delle tecnologie e dei partner, hanno creato un ambiente in cui la gravità degli eventi informatici può avere una diffusione esponenziale. I seguenti tipi di eventi, soprattutto se combinati, sono stati identificati come potenzialmente catastrofici.*



### Sfruttamento di vulnerabilità note

Circa 50 nuove vulnerabilità software sono pubblicate in media ogni giorno. Se non vengono applicate patch di sicurezza, queste vulnerabilità possono essere sfruttate. Circa il 15 per cento di tali vulnerabilità sono classificate "Severe", nel senso che sono facili da sfruttare, possono essere diffuse da remoto con privilegi di accesso limitati e possono causare danni significativi. Poiché le vulnerabilità critiche sono ampiamente conosciute e possono essere identificate sulle reti delle potenziali vittime attraverso le comuni tecniche di scansione di Internet, le aziende che non riescono a porre rimedio alle vulnerabilità gravi del software sono ad alto rischio di attacchi informatici.

### Sfruttamento di vulnerabilità zero-day

Le vulnerabilità software zero-day sono conosciute dai criminali informatici, ma non ancora da tutti. Queste sono particolarmente preoccupanti perché alcune di esse sono facilmente sfruttabili, potenzialmente gravi, e spesso prive di protezione. In altre parole, anche le aziende dotate di solide politiche di patch management possono essere esposte ad attacchi zero-day.

### Sfruttamento di vulnerabilità nella supply chain del software

Gli attacchi mirati a software ampiamente diffusi sono di fatto un cavallo di Troia che permette ai malintenzionati di accedere ai sistemi attraverso un software affidabile e certificato. L'operazione Solorigate ha dimostrato un alto grado di sofisticazione da parte dei malintenzionati nello sfruttare le pratiche di sviluppo del software comunemente in uso nel settore IT. Si prevede che questi attacchi, molti dei quali sembrano essere diretti o sponsorizzati da enti governativi, siano destinati a continuare e potenzialmente ad aumentare. L'attrito geopolitico, in particolare tra l'Occidente e i suoi avversari, continuerà a esacerbare la minaccia di tali eventi in futuro.

### Interruzione di infrastrutture critiche

Attacchi e altri incidenti informatici che coinvolgono le infrastrutture critiche possono avere conseguenze devastanti. Ad esempio, nell'attacco del maggio 2021 a Colonial Pipeline, la società di fornitura di carburante che serve la costa orientale degli Stati Uniti, attraverso un attacco ransomware hacker stranieri hanno provocato il blocco dell'infrastruttura di distribuzione del carburante. Pertanto l'oleodotto è stato chiuso per diversi giorni, causando problematiche di approvvigionamento che hanno compromesso il 45% della fornitura di carburante a milioni di cittadini e imprese in diversi stati americani. Il rischio di interruzione delle infrastrutture critiche è unico nel suo genere, in quanto può verificarsi a causa di un attacco cyber ma anche attraverso guasti del sistema, errori umani, errori di programmazione o altri tipi di incidenti informatici.

### Altri eventi a impatto diffuso

Esistono alcuni tipi di attacchi cyber che possono essere condotti simultaneamente o automaticamente contro un ampio numero di vittime. Internet e alcuni servizi di telecomunicazione rappresentano oggi strumenti critici per la continuità operativa delle aziende, aumentando enormemente il rischio potenziale di compromissione delle infrastrutture stesse. In alcuni casi una società di telecomunicazioni può essere l'unico fornitore per una città grande o media. In altri casi alcune grandi aziende di cloud computing sono così ampiamente utilizzate che un'interruzione diffusa potrebbe avere un impatto sulle operazioni commerciali di migliaia o milioni di aziende diverse allo stesso tempo. Un qualsiasi attacco di questo tipo, capace di una diffusione di massa, potrebbe causare un evento cyber dalle proporzioni catastrofiche.

### Attacchi ransomware

Benché non siano necessariamente di natura catastrofica, gli attacchi ransomware, che tengono in ostaggio i dati o le informazioni delle aziende o dei singoli individui fino al pagamento di un riscatto, vengono ora eseguiti con efficienza industrializzata. Le richieste tipiche, inizialmente di migliaia di dollari, ora sono salite fino a decine di milioni di dollari, con i criminali che prendono di mira aziende di tutte le dimensioni.

## Rafforzare la resilienza informatica

*È più che mai importante per le aziende innalzare il livello delle misure di sicurezza in vista di potenziali eventi catastrofici.*

Con l'intensificarsi dei rischi informatici - sia per la natura delle attività aziendali e dei sistemi informatici, sia per la compromissione di infrastrutture comuni, sia per i malintenzionati che sfruttano le vulnerabilità - è più che mai importante per le aziende innalzare il livello delle misure di sicurezza in vista di potenziali eventi catastrofici.

Un ottimo punto di partenza è comprendere le esposizioni specifiche che ogni azienda potrebbe affrontare alla luce dei potenziali eventi informatici catastrofici delineati in questo documento, per poi impegnare le risorse necessarie a migliorare le proprie difese e la propria resilienza. Fornitori IT condivisi rappresentano un rischio sistemico significativo per le aziende, pertanto è necessario condurre un'ampia due diligence su questi fornitori e sviluppare misure di ridondanza e resilienza intorno a loro, oltre a esaminare le previsioni contrattuali per valutare come viene trasferito il rischio.

Le aziende dovrebbero anche trarre pieno vantaggio dalla competenza offerta dai loro intermediari assicurativi e dal loro assicuratore cyber. Se da un lato i team che si occupano di gestione del rischio e di continuità aziendale possono contare sulle misure di protezione adottate e le procedure di incident response, nessuna azienda potrà mai risultare completamente protetta da tutti i tipi di incidenti cyber, specialmente quelli catastrofici.

Molte compagnie assicurative offrono una gamma di servizi pre-incidente per aiutare le aziende a migliorare il livello di sicurezza informatica, come le valutazioni di prontezza della risposta, il benchmarking delle prestazioni di sicurezza, i test di vulnerabilità della rete e le simulazioni di attacco. Le aziende dovrebbero inoltre essere ben preparate a fronteggiare gli incidenti cyber. Un team di esperti nella risposta agli incidenti cyber suggerito dall'assicuratore può aiutare a contenere i danni di tali eventi e a ripristinare il prima possibile la piena operatività aziendale. Questi servizi potrebbero fare la differenza tra il semplice sopravvivere a un serio attacco informatico e l'andare avanti con fiducia.

## I prossimi passi

*Le assicurazioni cyber, come le assicurazioni del ramo danni, sono esposte ad eventi catastrofici.*

Da un punto di vista globale, gli eventi informatici catastrofici sono potenzialmente in grado di arrestare l'economia e di paralizzare le infrastrutture critiche. Proprio come nel caso della pandemia da Coronavirus, si rende necessaria una collaborazione tra governo e settore privato su argomenti importanti, come la condivisione e la segnalazione di incidenti informatici per migliorare la coerenza dei dati e l'istituzione di quadri giuridici per scoraggiare e punire i criminali informatici.

L'aumento sia della frequenza sia della gravità degli incidenti informatici sta portando le compagnie di assicurazione a rivalutare premi e condizioni. Garantire la stabilità del mercato della cyber insurance, tenendo conto della potenziale portata dei rischi catastrofici, richiederà nuove soluzioni a livello macroeconomico e aziendale, così come a livello di prodotti offerti dal settore assicurativo. La sfida diventa predisporre polizze che offrano certezza di copertura, forniscano una protezione significativa e aiutino a gestire gli eventi cyber, sia di frequenza sia di natura catastrofica, per clienti e assicuratori.

Le compagnie di assicurazione storicamente hanno assicurato le proprietà contro i rischi catastrofali, come le inondazioni e i terremoti, con coperture dedicate, per avere modo di valutare e quantificare adeguatamente tali esposizioni. Questo processo ha contribuito a mantenere la stabilità generale del mercato e la disponibilità della copertura assicurativa. Molti dei principali terremoti, inondazioni e uragani dell'ultimo mezzo secolo hanno generato profitti per il settore assicurativo nei rami danni e infortuni e raramente hanno portato all'insolvenza delle compagnie. Di conseguenza, il settore assicurativo è rimasto resiliente e stabile per gli assicurati anche in seguito a eventi catastrofici.

Le assicurazioni cyber, come le assicurazioni del ramo danni, sono esposte ad eventi catastrofici, quindi il settore assicurativo cyber potrebbe dover rispondere in maniera analoga al ramo danni. Il settore assicurativo deve essere proattivo nell'offrire una copertura per eventi catastrofici che sia separata dalle coperture base. La copertura per eventi catastrofici non sarebbe esclusa, ma sarebbe piuttosto delineata in modo più chiaro, garantendo che la copertura separata abbia un prezzo trasparente, e soggetta a un'adeguata sottoscrizione, a limiti di copertura e fidelizzazione del cliente coerenti. Questo approccio consentirà al settore delle assicurazioni cyber di continuare a fornire soluzioni innovative per gli assicurati, garantendo allo stesso tempo la sostenibilità a lungo termine del mercato.

## A proposito dell'autore

Michael Kessler è un Vicepresident del Gruppo Chubb e President della divisione Global Cyber Risk Practice di Chubb. In questo ruolo, egli supervisiona tutti gli aspetti dell'attività, tra cui la strategia, lo sviluppo dei prodotti e dell'attività aziendale, nonché le operazioni di sottoscrizione e di servizio e la performance generale di profitti e perdite. Kessler ha maturato quasi 30 anni di esperienza nel settore assicurativo e nella consulenza attuariale e in precedenza è stato Chief Reinsurance Officer di Chubb (2016-2021) e Chief Actuary per la sua attività assicurativa internazionale (2008-2016). Kessler ha conseguito una laurea in matematica presso la Cornell University. È membro dell'American Academy of Actuaries e della Casualty Actuarial Society.

# Fonti


1. Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market (2021). Retrieved from www.gao.gov/products/gao-21-477
2. Cyber Resilient Organization Report (2020). Retrieved from www.ibm.com/security/digital-assets/soar/cyber-resilient-organization-report/#/
3. National Institute of Standards and Technology's National Vulnerability Database. Accessed at https://nvd.nist.gov/vuln/search
4. AV-TEST Institute (2021). Accessed at www.av-test.org/en/statistics/malware/
5. Verizon 2021 Data Breach Investigations Report (2021). Retrieved from https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf
6. U.S. Senate Select Committee on Intelligence (2021). Accessed at www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary
7. NIST Security Vulnerability Trends in 2020: An Analysis (2021). Retrieved from www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf

## A proposito di Chubb

Chubb è la più grande compagnia assicurativa danni al mondo per capitalizzazione quotata in borsa. Opera in 54 paesi e offre, a livello globale, soluzioni assicurative a imprese di ogni dimensione, a professionisti e famiglie. Opera nel Property & Casualty (P&C) e nell'Accident & Health (A&H), con prodotti sia personalizzati sia standardizzati, attraverso una pluralità di canali. L'elevata capacità sottoscrittiva e l'attenzione al servizio ci sono riconosciuti dal mercato, soprattutto riguardo l'equità e la tempestività con cui gestiamo i sinistri. Chubb Limited, la società capogruppo di Chubb, è quotata alla borsa valori di New York (NYSE: CB) e fa parte dell'indice S&P 500. Chubb ha uffici di rappresentanza a Zurigo, New York, Londra, Parigi e in altre sedi, e impiega circa 31.000 persone nel mondo. Ulteriori informazioni su www.chubb.com/it

Per ulteriori informazioni sull'esperienza e la competenza di Chubb nella gestione dei rischi informatici è possibile visitare il sito www.chubb.com/cyber o contattare il vostro underwriter locale.



Chubb. Insured.[SM]



Chubb European Group SE, Sede legale: La Tour Carpe Diem, 31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, Francia - Capitale sociale €896.176.662 i.v.- Rappresentanza generale per l'Italia: Via Fabio Filzi n. 29 - 20124 Milano - Tel. 02 27095.1 - Fax 02 27095.333 - P.I. e C.F. 04124720964 - R.E.A. n. 1728396 - Abilitata ad operare in Italia in regime di stabilimento con numero di iscrizione all'albo IVASS I.00156. L'attività in Italia è regolamentata dall'IVASS, con regimi normativi che potrebbero discostarsi da quelli francesi. Autorizzata con numero di registrazione 450 327 374 RCS Nanterre dall'Autorité de contrôle prudentiel et de résolution (ACPR) 4, Place de Budapest, CS 92459, 75436 PARIS CEDEX 09 RCS e soggetta alle norme del Codice delle Assicurazioni francese. info.italy@chubb.com - www.chubb.com/it

IT8130-MD 11/2021