INSURANCE Daily

MERCOLEDÌ 23 GIUGNO 2021 N. 1982

PRIMO PIANO

Se anche la birra ti assicura

Budweiser, uno dei principali marchi di birra, sbarca nel settore assicurativo canadese con il lancio di Budweiser Insurance. Come riportano i media locali, rivolgendosi a coloro che dubitano della serietà del progetto, Mike D'Agostini, direttore marketing di Budweiser, ha detto che la pandemia "ha aperto gli occhi dei produttori di birra" e che ora la società vuole "fornire una migliore tutela ai canadesi, consentendo loro di vivere la vita che desiderano". Citando l'aumento delle richieste di polizze vita online, la società ha specificato che Budweiser Insurance vuole essere un contratto "complementare a una copertura già esistente". Tuttavia, un secondo annuncio che descrive l'offerta di prodotti, fa rientrare le polizze più nel ramo danni che in quello vita: Budweiser vuole coprire gli imprevisti che possono rovinare il barbecue ai canadesi. Quella che Budweiser chiama Bbq Insurance è più che altro un concorso a premi. "Se succede qualcosa al tuo barbecue – si legge nella descrizione – dalla pioggia, all'esaurimento del combustibile", si può fare richiesta di risarcimento, fino a 2500 dollari, sul sito Bbqinsurance.com: ma solo pochi fortunati, settimanalmente, saranno selezionati per "il risarcimento danni". L'obiettivo di Budweiser è dare ai canadesi "un'estate senza preoccupazioni".

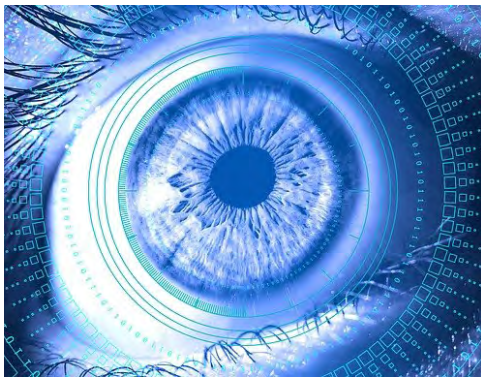
Fabrizio Aurilia

MERCATO

Difendere le istituzioni da una "guerra" cibernetica

Il dpcm 131/2020 ha posto le linee per l'implementazione dello scudo difensivo italiano contro attacchi cyber diretti a enti e aziende strategici del Paese. Questa seconda parte dell'intervento illustra i processi e le responsabilità dei 150 enti interessati

PARTE SECONDA



SOGGETTI COINVOLTI NEL PERIMETRO E LORO OBBLIGHI

Il *Perimetro di sicurezza nazionale cibernetica* si rivolge principalmente a due categorie di soggetti:

a) quelli che esercitano una funzione essenziale dello Stato, ovvero coloro che sono destinati ad assicurare la continuità dell'azione di governo e degli organi istituzionali, la sicurezza interna ed esterna, la difesa, le relazioni internazionali, l'ordine pubblico, l'amministrazione della giustizia e la funzionalità del sistema economico, finanziario e dei trasporti;

b) quelli che prestano un servizio essenziale per gli interessi dello Stato, ovvero tutti i soggetti (siano essi pubblici o privati), che assicurano il mantenimento delle attività civili, sociali ed economiche fondamentali, esercitando attività necessarie per l'esercizio e la salvaguardia dei diritti fondamentali dei cittadini (come garantire la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica, ad esempio) o esperiscono attività di ricerca che presentino particolare rilievo ai fini dello sviluppo del sistema economico nazionale.

Scopo del decreto è chiarire i criteri che guideranno l'Esecutivo nell'individuazione dei soggetti (pubblici e privati) che di tale perimetro faranno parte, nonché definire come predisporre, comunicare e aggiornare periodicamente l'elenco delle reti, dei sistemi informativi e dei servizi informatici rilevanti per la sicurezza del nostro paese, in quanto indispensabili per l'esercizio dei servizi essenziali per lo Stato.

Il provvedimento affida alle amministrazioni statali il compito di individuare le aziende operanti nei settori dell'interno, della difesa, dello spazio, dell'energia, delle telecomunicazioni, dell'economia e finanza, dei trasporti, dei servizi digitali, delle tecnologie critiche, degli enti previdenziali e del lavoro, per identificare le funzioni e i servizi essenziali, la cui interruzione o compromissione possa arrecare un pregiudizio per la sicurezza nazionale.

È anche compito delle amministrazioni graduare in una scala crescente le funzioni e i servizi per i quali, in caso di interruzione o compromissione, il pregiudizio per la sicurezza nazionale sia ritenuto massimo e le possibilità di mitigazione minime. Sarà dunque predisposta una lista di tali operatori, da sottoporre al *Comitato Interministeriale per la Sicurezza della Repubblica* (CISR).

Su proposta di quest'ultimo, l'elenco dei soggetti inclusi nel Perimetro di sicurezza nazionale cibernetica farà infine parte di un atto amministrativo, periodicamente aggiornato dalla presidenza del Consiglio dei ministri.

(continua a pag. 2)

INSURANCE Daily

MERCOLEDÌ 23 GIUGNO 2021 N. 1982

(continua da pag. 1) I soggetti inclusi nel Perimetro avranno l'obbligo di predisporre e aggiornare con cadenza annuale l'elenco dei beni ICT di rispettiva pertinenza, ovvero le reti e i servizi informatici da loro gestiti e considerati essenziali per lo Stato. Essi dovranno valutare gli effetti di un'interruzione della loro funzione, identificando i fattori di pericolo di un incidente, valutandone la probabilità e l'impatto potenziale sulla continuità ed efficacia della funzione erogata e individuando e implementando idonee misure di sicurezza.

UN RUOLO PROPOSITIVO PER LE AZIENDE RISPETTO ALLA LORO DIFESA

Il principio non è diverso da quanto previsto dalla *General Data Protection Regulation* (GDPR), entrata definitivamente in vigore il 25 maggio 2018. In base a essa, ogni azienda che tratti dati sensibili è obbligata a elaborare un sistema documentale di gestione della privacy, per soddisfare i requisiti di conformità al Regolamento stesso, individuando al suo interno i ruoli chiave destinati alla gestione e protezione dei dati trattati.

Sotto questo profilo il GDPR ha rappresentato una vera rivoluzione, perché fino alla sua promulgazione sono state le istituzioni a indicare alle aziende le modalità necessarie per la protezione dei dati trattati. Ora la questione si è letteralmente capovolta e saranno le aziende stesse, ovvero il soggetto più adatto a comprendere la portata dei dati gestiti e dei rischi legati al loro trattamento, a elaborare un piano per la protezione di questi ultimi.

Allo stesso modo, nell'ambito del Perimetro, gli enti coinvolti, una volta effettuata l'analisi del proprio rischio, dovranno individuare per ogni funzione o servizio essenziale i beni ICT necessari a svolgerli, valutando l'impatto potenziale di un incidente, sia in termini di limitazione dell'operatività del bene stesso, che relativamente alla compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da esso trattati. Il termine *compromissione* si sostanzia per il legislatore nella perdita di sicurezza o di efficacia dello svolgimento di una funzione o di un servizio essenziale dello Stato, connessa all'incidente informatico che si è verificato.

Riassumendo, il Perimetro di sicurezza nazionale cibernetica costituisce un progetto assai complesso che, oltre a stabilire i criteri secondo i quali le autorità delegate dovranno identificare i soggetti da coinvolgere, definisce le modalità con cui questi dovranno assolvere ai compiti loro assegnati e istituisce le strutture di supporto alla gestione dei processi e dei flussi operativi, per segnalare eventuali attacchi e incidenti.

RESPONSABILITÀ DA DEFINIRE, IN ATTESA DEI DECRETI ATTUATIVI

In Italia i soggetti da includere nel Perimetro dovrebbero essere circa 150 e saranno elencati in una lista che resterà segretata per garantirne la sicurezza.

Qualora uno di questi soggetti dovesse rimanere vittima di un attacco cibernetico, esso sarà obbligato a informare entro sei ore il **Csirt** (**Computer security incident response team**). In caso di grave violazione, sarà attivato l'**Nsc**, ovvero il **Nucleo per la sicurezza cibernetica**, il cui compito è quello di proporre al Presidente del Consiglio una risposta all'attacco e coordinare il ripristino del servizio.

Gli effetti del progetto non saranno certo immediati, ma andranno valutati nel tempo: si prevedeva che l'intero sistema sarebbe entrato a regime in questo periodo, ovvero entro la primavera del 2021, ma mancano alcuni decreti attuativi e ulteriori risorse che non sono state ancora individuate.

Bisognerà inoltre definire gli aspetti operativi connessi all'attuazione del Perimetro, tra cui le misure di sicurezza che gli operatori dovranno adottare per rendere affidabile la loro tecnologia.

Infine, sarà necessario determinare gli eventuali carichi di responsabilità, il che sarà molto complicato, innanzi tutto perché la lista delle società che rientreranno nel Perimetro sarà segretata, e poi perché non risulta che il provvedimento comporti sanzioni nei confronti delle aziende che non dovessero allinearsi ai criteri richiesti o che non rispettino le scadenze previste, come accade ad esempio per l'attuazione del Gdpr. I costi connessi ai cyber attacchi possono essere assai cospicui e c'è da chiedersi se si possa configurare la possibilità di richiedere un risarcimento per le eventuali vittime dell'attività svolta dai soggetti pubblici e privati che del Perimetro saranno scelti a fare parte e in che misura tale responsabilità potrà essere attribuita a essi, come verrebbe eventualmente distribuito l'onere probatorio e come verrebbe quantificato il danno che ne potrebbe derivare.

Non si tratta di questioni di poco conto, perché gli attacchi già perpetrati, soprattutto per quanto attiene alle aziende private coinvolte, potrebbero comportare risarcimenti di una certa levatura.

E dunque, se un soggetto dovesse subire un danno in seguito all'inadeguatezza dei sistemi di prevenzione o per inadempienza di un ente incluso nel Perimetro, in che termini sarebbe configurabile una sua responsabilità e in quale misura la stessa potrebbe determinare un eventuale risarcimento?

Cinzia Altomare

(La prima parte dell'articolo è stata pubblicata su Insurance Daily di martedì 22 giugno)

INSURANCE Daily

MERCOLEDÌ 23 GIUGNO 2021 N. 1982

RICERCHE

EY, cresce l'attrattività dell'Italia

Nel 2020, nonostante la pandemia, gli investimenti diretti esteri sono cresciuti del 5%

Un'Italia più attrattiva nonostante la pandemia. Nel 2020, secondo la *EY Attractiveness Survey* di **EY**, il numero di investimenti esteri diretti è cresciuto del 5% e quasi la metà dei manager intervistati (48%) si è detto pronto a espandere le proprie attività in Italia. Nello stesso periodo, giusto per avere un'idea, in Europa si è registrato un calo complessivo del 13%, con ribassi particolarmente negativi per Spagna (-27%), Russia (-26%) e Paesi Bassi (-24%).

I settori più attrattivi sono stati servizi alle imprese (13%), software e IT (12%) e logistica e wholesale (12%). Bene anche finanza (8%) e industria farmaceutica (7%), mentre per il segmento dei macchinari e delle attrezzature industriali (5%) e per quello tessile (4%) si sono registrate flessioni che possono essere almeno in parte dettate dall'incertezza legata ai mesi di lockdown. La maggior parte degli investimenti esteri è stato improntato al potenziamento della forza commerciale e del marketing (22%), ma si è assistito anche a una crescita degli impieghi volti a valorizzare il konw-how tecnico e imprenditoriale, soprattutto per quanto riguarda processi di produzione (19%), nonché ricerca e sviluppo (15%).

La maggior parte degli investimenti esteri diretti è arrivata dagli Stati Uniti (24%), seguita da Francia (16%), Germania (12%) e Regno Unito (9%). Indietro invece la potenza cinese (4%), che sopravanza di poche lunghezze il Giappone (3%). La distribuzione degli investimenti non è omogenea sul territorio nazionale e risulta concentrata sui distretti industriali più innovativi (meccatronica, lusso, design, mobile, tessile, biomedicale): in questo contesto, la parte del Leone la fa il Nord-Ovest (58%), seguito a debita distanza dal Centro.

Nonostante la crescita registrata nel 2020, la quota di mercato dell'Italia resta ancora minoritaria: nel nostro Paese arriva soltanto il 2% degli investimenti diretti totali in Europa, cosa che colloca l'Italia al 12esimo posto di questa peculiare classifica. A pesare sono criticità ben note del nostro sistema produttivo: incertezza regolamentare (58%) ed eccessivo carico burocratico (55%) costituiscono le principali aree di difficoltà per gli intervistati.

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 23 giugno di www.insurancetrade.it – Reg. presso Tribunale di Milano, n. 46, 27/01/2012 – ISSN 2385-2577

INSURANCE Daily

MERCOLEDÌ 23 GIUGNO 2021 N. 1982

INSURANCE CONNECT TV

SALUTE, LA DIREZIONE È QUELLA GIUSTA

Nicola Ronchetti, ceo di Finer, ha moderato la tavola rotonda incentrata sulla questione della salute, tema centrale del sistema italiano. Sul palco dell'Innovation Summit 2021, top manager del mercato italiano: **Giovanna Gigliotti**, amministratore delegato di UniSalute; **Cesare Lai**, amministratore delegato di Generali Welion; **Chiara Soldano**, direttore salute di Axa Italia; **Marco Vecchietti**, ad e dg di Intesa Sanpaolo Rbm Salute.

GUARDA IL VIDEO DELLA TAVOLA ROTONDA SU WWW.INSURANCECONNECT.TV