IL CICLONE CYBER RISK

di GIACOMO CORVI

UNA RICERCA DEI LLOYD'S DELINEA LE CONSEGUENZE DI UN POSSIBILE ATTACCO INFORMATICO SU LARGA SCALA: PERDITE FINO A 53,1 MILIARDI DI DOLLARI, IN LINEA CON IL COSTO ECONOMICO DEL PASSAGGIO DELL'URAGANO SANDY NEL 2012

Case intatte, infrastrutture stabili, servizi pubblici che, magari dopo un momento di stallo, tornano a funzionare regolarmente. Le conseguenze di un attacco informatico non sono immediatamente visibili. Eppure, possono rivelarsi estremamente ingenti. Al punto tale da poter essere paragonate a quelle causate da una catastrofe naturale. Il confronto arriva dal rapporto *Calcolare i costi. La decodifica delle esposizioni cyber*, realizzato dai **Lloyd's** in collaborazione con **Cyence**. Lo studio evidenzia come le perdite economiche di un attacco informatico potrebbero arrivare a 53,1 miliardi di dollari. Giusto per avere un'idea, il passaggio dell'uragano *Sandy* ha provocato perdite comprese fra 50 e 70 miliardi di dollari: le stime più affidabili spingono la cifra a oltre 65 miliardi di dollari. "I risultati di questa ricerca – spiega **Trevor Maynard**, head of innovation dei Lloyd's – evidenziano come le perdite economiche legate a eventi cyber abbiano il potenziale di provocare danni estremi, come quelli causati dai maggiori uragani".

DUE SCENARI DI PERDITA

Il rapporto si basa sull'elaborazione di due scenari, entrambi sviluppati in caso di *grande evento* o *evento estremo*. Il primo, quello a più alto impatto, prevede un attacco a un fornitore di servizi cloud da parte di un gruppo di *hacktivists*: in questo caso, le perdite vanno da un minimo di 4,6 miliardi a un massimo di 53,1 miliardi di dollari. Dati che, tuttavia, costituiscono soltanto una media di valori ben più variabili, che possono essere influenzati dall'entità e dalla durata dell'attacco: lo scenario peggiore stima perdite fino a 121 miliardi di dollari, persino superiori ai 108 miliardi di dollari di danni provocati dal passaggio del devastante uragano *Katrina* nel 2005.

Più contenute, ma comunque rilevanti, le perdite nel caso di un attacco simultaneo a una serie di aziende che usufruiscono di un software vulnerabile: in questo secondo scenario, le perdite variano fra 9,7 e 28,7 miliardi di dollari.

PERDITE PIÙ INGENTI

Le perdite sarebbero, insomma, ingenti. E diventano ancor più elevate se si considera che, come precisa il rapporto, la stima dei costi tiene conto delle sole perdite dirette: le conseguenze in termini di danni alla proprietà, lesioni fisiche, perdite di clienti e danni reputazionali non sono state infatti prese in considerazione nell'elaborazione degli scenari. "È necessario – avverte Maynard – che le imprese siano preparate a fronteggiare non soltanto i costi diretti, ma anche le spese a lungo termine che possano derivare dall'attacco". Anche perché, aggiunge, "l'introduzione del *General data protection regulation* imporrà nuove regole e controlli, con multe fino al 4% del fatturato annuo globale o, nel caso in cui sia più alto, a 20 milioni di euro".

CRESCE LA CONSAPEVOLEZZA...

Il rischio per le imprese è elevatissimo. E cresce all'aumentare della digitalizzazione e, di conseguenza, del numero di oggetti connessi alla rete. Secondo la **Financial Conduct Authority**, gli attacchi informatici sono cresciuti del 1.700% negli ultimi tre anni. E, più in generale, un recente studio ha evidenziato come i *cyber attack* siano costati alle aziende fino a 450 miliardi di dollari ogni anno. "Ormai è una questione di *quando*, e non di *se*, un'azienda verrà attaccata", osserva Maynard.

In questo contesto, complici anche i recenti casi dei malware *WannaCry* e *Petya*, non stupisce che la consapevolezza in materia sia cresciuta. "La *cyber security* è oggi una delle principali preoccupazioni delle aziende", commenta Maynard. "Il nostro rapporto *Fronteggiare la sfida del cyber risk* – aggiunge – ha evidenziato come la sicurezza informatica sia ormai un argomento centrale delle aziende, con il 54% dei ceo di società europee che hanno assunto il controllo del settore".

***Trevor Maynard**, head of innovation dei Lloyd's*

... MA NON ABBASTANZA

La strada da percorrere resta, tuttavia, ancora lunga. E, in particolare, proprio sul fronte della *cyber insurance*. "Sebbene la domanda di coperture stia crescendo, la maggior parte delle perdite non sono assicurate", osserva Maynard.

Il gap assicurativo risulta evidente se si torna agli scenari elaborati nel rapporto. Nel primo caso, il livello di copertura si attesta infatti fra il 13% e il 17%, con perdite assicurative comprese fra 620 milioni e 8,1 miliardi di dollari. Livelli ancor più bassi nel secondo scenario, dove la penetrazione delle coperture sprofonda al 7% e le perdite per le compagnie si attestano fra 762 milioni e 8,1 miliardi di dollari. L'eventualità di un attacco su larga scala potrebbe, inoltre, avere effetti sistemici sull'intero comparto. Un grande evento, per esempio, porterebbe a un incremento del 19% nel *loss ratio* dell'industria assicurativa: in caso di evento estremo, il dato schizzerebbe del 250%.

MIGLIORARE IL PORTAFOGLIO

La minaccia è evidente. Quello che ancora manca è una consapevolezza diffusa, in grado di gestire il rischio anche in momenti di presunta tranquillità. Un fronte, quello del cyber risk, dove pesa la mancanza di dati provenienti da fonti istituzionali, che sappiano tener conto dell'accumulo e della modellizzazione del rischio. Obiettivo del rapporto è proprio quello tentare di colmare la lacuna, fornendo una rappresentazione realistica dei danni che un attacco potrebbe provocare all'economia globale. "Abbiamo fornito questi scenari – conclude Maynard – per far comprendere alle compagnie il livello di esposizione al cyber risk, in modo tale che possano così migliorare la gestione del portafoglio e proseguire nella crescita del settore con maggior serenità".