CYBER, UNO SCENARIO ANCORA TUTTO DA CAPIRE

di LAURA SERVIDIO

DI RISCHIO INFORMATICO SI PARLA MOLTO, MA SI AGISCE POCO: SERVE UN APPROCCIO PRAGMATICO AL PROBLEMA, CON LA CREAZIONE DI UNA CASISTICA, E UN'OPERA DI SENSIBILIZZAZIONE E FORMAZIONE DI TUTTI GLI ATTORI. MA, SOPRATTUTTO, OCCORRE UN'OFFERTA CHE SIA DAVVERO EFFICACE

Cyber è il termine più abusato del decennio. Un fenomeno che ha implicazioni e impatti ancora poco immaginabili e su cui il Governo è pronto a spendere 150 milioni di euro. Lo scenario, infatti, non è così roseo né facilmente prevedibile: oggi, anche il dispositivo più banale, come un Gps, può essere messo sotto attacco, innescando una serie di problemi in grado di paralizzare la nostra quotidianità.
"In Giappone, nel 1998 – spiega **Umberto Rapetto**, ex generale della **Guardia di Finanza**, attualmente cyber security advisor – quando si verificò il black out del sistema Gps, gli automobilisti dovettero attendere l'aggiornamento del software prima di ritrovare la via di casa. Un altro esempio emblematico, è quello di una nave mercantile assicurata che può essere sottoposta a dirottamento informatico (*hi-jacking*), comodamente da remoto, e senza particolari difficoltà".

***Umberto Rapetto**, generale (R) della Guardia di Finanza, cyber security advisor*

Riconoscere le tante insidie, dunque, non è facile. A ciò si aggiunge la scarsa percezione che ancora aleggia nel nostro Paese sulla minaccia informatica e sull'importanza delle operazioni di ripristino, altro tema sottovalutato: "se l'Europa vede la risorsa cybernetica come una potenzialità, in Italia, questa tematica non è mai stata approfondita – osserva Rapetto – e nessuno degli oltre 50 player che offrono una copertura sul rischio cibernetico è ancora riuscito a mettere a punto una polizza davvero efficace".

POCHE LE INFORMAZIONI SUGLI ATTACCHI

È difficile potersi cimentare in un settore dove, tra le altre cose, non esiste una casistica: quando si parla di rischio informatico, infatti, siamo di fronte a una generale mancanza di informazioni. "Mentre sulle nostre auto siamo invasi dai dati, grazie all'ausilio delle scatole nere, sui sistemi informatici non si sa nulla. E chi è sotto attacco, non ne parla per due motivi: uno di immagine, l'altro giudiziario. Il primo è legato alla reputazione dell'azienda, mentre il secondo si riferisce alla normativa, sia italiana che europea, che prevede sanzioni penali per chi non adotta misure di sicurezza informatica, costituendo per le vittime *non protette* un grosso deterrente a uscire allo scoperto".
L'assenza di denunce rende difficile creare una casisti-

LA NORMA A TUTELA DEL DATO

Secondo l'articolo 615 ter del Codice Penale, chiunque si introduca illecitamente in un sistema informatico è punibile con la reclusione fino a tre anni, che diventano cinque in caso di intrusione in un sistema pubblico.
Il nostro Paese ha poi elaborato una normativa ad hoc sul cyber crime: la legge 547/93 regola le fattispecie dei reati informatici, prevedendo sanzioni sia per chi si introduca in un sistema protetto, sia per chi non ricorra alle necessarie *misure di sicurezza*, a tutela dei dati.
A supporto di ciò, anche il regolamento europeo (recentemente pubblicato in Gazzetta) e il decreto legislativo 196/2003 (in materia di privacy), in cui si afferma che, se la violazione avviene in un sistema non protetto da strumenti di sicurezza, il reato non esiste e non è possibile far valere gli strumenti giuridici: chi non si tutela, dunque, è sanzionabile penalmente in quanto le conseguenze si riverberano sulle persone i cui dati avrebbero dovuto essere protetti.

ca da cui poter trarre quali sono state le metodologie, le tecniche, le opportunità sfruttate, la gravità delle conseguenze e le misure di sicurezza più opportune ed efficaci.

SE LA MINACCIA È SEMANTICA

La conoscenza di ciò che si è già verificato aiuta a guidare l'operatività di chi è attaccato: ad esempio, arrestando ogni attività per evitare che il sistema contaminato si propaghi agli altri soggetti coinvolti. Altra eventualità, ancora più pericolosa, è l'attacco semantico, che avviene quando si è convinti, erroneamente, di essere ancora in possesso delle informazioni. "Emblematico – racconta Rapetto – è il caso dell'ospedale *Gradenigo* di Torino, che ha subìto un rimescolamento progressivo dei dati sensibili dei pazienti, con conseguenze molto pesanti sull'operatività della struttura".
Per affrontare il tema, serve parlare di meno e fare di più, in modo pragmatico. Agendo sull'accrescimento delle competenze e delle esperienze, e sulla sensibilizzazione di tutti gli attori. "Bisogna partire da un adeguato percorso formativo, magari organizzato a livello consortile, che coinvolga innanzitutto i periti"; oltre a questo, secondo l'esperto, urge una seria valutazione dei rischi, per garantire l'esistenza di controlli adeguati, in grado di evitare ogni tipo di attacco, anche quello semantico. "Il tutto coinvolgendo e sensibilizzando l'insieme dei soggetti interessati sulla pericolosità della minaccia informatica".
Ultimo punto, l'offerta: nel cyber si cerca spesso di proporre soluzioni accattivanti, "viceversa – conclude Rapetto – bisogna essere più previdenti, mettendo a punto un *syllabus* che definisca ogni singolo rischio in modo uniforme, condiviso, e adeguato alla realtà informatizzata, e che dia una maggiore consapevolezza di tutte le minacce a cui può essere sottoposta un'azienda".