CYBER CRIME, NESSUNO SI SENTA ESCLUSO

di BENIAMINO MUSTO

I RECENTI CASI DI PETYA E WANNACRY MOSTRANO UNA PREOCCUPANTE ESCALATION DEGLI ATTACCHI CIBERNETICI. MA LE IMPRESE ITALIANE STANNO GESTENDO QUESTA MINACCIA SPINTE PIÙ DAGLI INCENTIVI PUBBLICI CHE DA UNA REALE SENSIBILITÀ SUL TEMA. IL TUTTO MENTRE SUL MERCATO ARRIVERANNO MILIONI DI OGGETTI, CONNESSI ALLA RETE, NON DOTATI DI ADEGUATI SISTEMI DI PROTEZIONE. SE NE È PARLATO NEL CORSO DELLA TAVOLA ROTONDA DEDICATA AI RISCHI INFORMATICI

Il 27 giugno scorso il virus informatico *Petya*, partito dalla Russia, si è diffuso a macchia d'olio in tutta Europa. Petya ha disattivato centinaia di computer, rendendo inaccessibili i file, e chiedendo un riscatto di 300 dollari in Bitcoin per liberarli. Una richiesta simile a quella del ransomware *Wannacry* che lo scorso maggio aveva infettato migliaia di computer in oltre 150 Paesi. Dalla pubblica amministrazione alla piccola impresa, fino ad arrivare alle grandi multinazionali, nessuno sembra essere indenne da una minaccia che, in questo momento, più che un rischio che si sta gestendo assomiglia a una *spada di Damocle* pronta a colpire. Perché, come è stato osservato nel corso della tavola rotonda dedicata al cyber risk, "c'è una enorme impreparazione culturale e organizzativa nei confronti di questa minaccia". Ad affermarlo è stato **Umberto Rapetto**, già generale della Guardia di Finanza, oggi cyber security advisor. "Spesso si parla di questo tema con una visione quasi mistica. Eppure – ha ammonito – dovremmo riflettere sul fatto che probabilmente servirebbe una Rc obbligatoria anche per questa tipologia di rischi. Non si tratta solo di una prospettiva di risarcimento danni: per essere assicurabili bisogna innanzitutto dimostrare di aver adottato determinate procedure di sicurezza". Lo ha ribadito anche **Tomaso Mansutti**, amministratore delegato della **Mansutti**: "nell'intero processo di risk management l'assicurazione affronta solo la parte finale. Sarebbe un errore guardare alla polizza come l'unico elemento di cui

UNA MINACCIA CHE RIGUARDA TUTTI

Durante la tavola rotonda, Tomaso Mansutti, ad dell'omonima società di intermediazione, ha citato alcuni numeri riguardanti i crimini informatici. A partire da una ricerca di Cisco, da cui è emerso che il 65% delle email che ognuno riceve sono classificabili come spam: l'8/10% di queste sono dannose. Relativamente al cloud, invece, il 27% degli strumenti adottati sono ritenuti altamente pericolosi per la sicurezza dei dati. Per quanto riguarda il fishing, Mansutti ha spiegato che nell'ultimo anno il fenomeno è incrementato del 1166%. "Il 23% delle persone che ricevono email di fishing aprono la mail. L'11% di queste clicca sull'allegato che non dovrebbero aprire e il 60% di coloro che lo aprono subiscono un danno – ha detto – e si tenga conto che le coperture assicurative coprono solo le responsabilità da eventi dolosi, sebbene il 60% dei danni sui dati arrivino da problemi interni all'azienda. In Italia si spende circa 1 miliardo di euro in sicurezza informatica: circa il 30% delle aziende investe per adeguarsi, e circa il 40% investe solo dopo aver subito un danno.

Da sinistra: ***Tomaso Mansutti****, amministratore delegato della Mansutti;* ***Alvise Biffi****, coordinatore advisory board cyber security di Assolombarda e vicepresidente di Piccola industria – Confindustria nazionale;* ***Maria Rosa Alaggio****, direttore di Insurance Review e* ***Umberto Rapetto****, ex generale della Guardia di Finanza*

l'azienda deve dotarsi per risolvere il problema". Per Mansutti, compito degli assicuratori è quello di accompagnare l'impresa in tutto il processo di analisi dei rischi".

AZIENDE, LA CORSA AGLI INCENTIVI

Secondo Rapetto "in Italia siamo scampati ai recenti attacchi ransomware per via della nostra arretratezza tecnologica, che ci separa da altri contesti dove istituzioni e imprese sono molto più connesse". E i casi Petya e Wannacry non sembrano aver gettato le aziende italiane nel panico, né aver generato in loro una particolare frenesia per dotarsi di più efficaci misure di sicurezza. "Al momento le imprese sono più che altro impegnate ad accaparrarsi, entro la fine di quest'anno, gli incentivi pubblici, iperammortamento e superammortamento, concessi a chi realizza un impianto connesso 4.0", ha spiegato **Alvise Biffi**, coordinatore advisory board cyber security di **Assolombarda** e vicepresidente di *Piccola industria* – **Confindustria nazionale**. Biffi ha lamentato il fatto che il legislatore abbia dato una finestra di tempo molto stretta tra produzione e consegna del prodotto per l'ottenimento dei benefici fiscali. "È evidente – ha precisato – che l'aspetto della cyber security va pensato *by design"*.

HACKERARE IL TOSTAPANE

"Quando si progetta un oggetto connesso – ha detto Biffi – bisogna tener conto del fatto che si espone ad attacchi di malintenzionati. La sicurezza informatica può riguardare anche un semplice elettrodomestico". Biffi cita il caso, divenuto celebre, avvenuto lo scorso anno sulla costa orientale degli Usa, che ha messo fuori uso i siti web di colossi come **Amazon** e **PayPal**. "Quell'attacco, che si è tradotto in un intasamento del traffico informatico, era partito proprio da frigoriferi, tostapane e telecamere di sorveglianza: oggetti per i quali non erano state pensate alcune misure di sicurezza". Come ha osservato Rapetto, "è come aver costruito dei veicoli per circolare in autostrada e poi non averli dotati di freni per poterli fermare". Ragione per cui, secondo Rapetto, "dovremo iniziare a pensare a delle responsabilità oggettive per degli oggetti che si affacciano sulla rete, perché ciascuno di essi può essere governato dall'esterno. Tutti coloro che parlano con grande serenità dell'*IoT* spesso dimostrano di non aver capito di cosa parlano. Noi – ha ammonito – non siamo ancora preparati all'internet delle cose. Non siamo capaci di gestire un sistema vero, figuriamoci di gestire una rete affollata di oggetti connessi che ci danno come risposta sapere se il latte è scaduto".

PRIVACY, LA MANNAIA DELLE SANZIONI

Oltre ai risvolti per i prodotti, il rischio cyber coinvolge anche l'ambito della tutela dei dati. Le nuove normative in materia, cosa porteranno concretamente in termini di protezione? Secondo Mansutti, le nuove regole "ci obbligano a ripensare la privacy. Non più come mero adeguamento alla normativa, ma stimolando una nuova visione della responsabilità dell'azienda per curare i dati al proprio interno". Per Mansutti, emergeranno "nuovi profili di responsabilità per gli amministratori, che in futuro saranno molto impattanti, e di cui ancora non ci si rende conto". Anche Biffi è dello stesso parere: "pochissime realtà stanno affrontando nel modo corretto questo tema. E l'approccio sanzionatorio funziona poco, perché le multe, in caso di inottemperanza, sono talmente elevate da sembrare irreali".