IL QUOTIDIANO ON LINE DELL'ECONOMIA DIGITALE E DELL'INNOVAZIONE

http://www.corrierecomunicazioni.it/digital/47613_london-bridge-snell-grazie-al-digitale-solo-8-minuti-per-fermare-l-attacco.htm

London Bridge, Snell: "Grazie al digitale solo 8 minuti per fermare l'attacco"

07/06/16

In occasione del summit NetEvents il punto sulle nuove cyberminacce ma anche sul ruolo che l'informatica può e deve avere sempre di più nel gestire e prevenire gli eventi terroristici. L'ex capo del Prevent programme del Foreign office britannico: "Dieci anni fa sarebbe occorsa almeno mezz'ora per coordinare un intervento e sventare l'attacco. E' un aspetto da non sottovalutare"

di Domenico Aliperto

Il prezzo da pagare per una sempre più stretta interconnessione tra mondo fisico e realtà digitale è l'**aumento esponenziale delle conseguenze che gli attacchi informatici** hanno sulla vita di tutti giorni d i imprese e pubbliche amministrazioni. Sicuramente l'attenzione mediatica monterà ulteriormente quando a pagare lo scotto del cyber crime saranno anche i comuni cittadini. E a quel punto aziende e istituzioni non potranno più mantenere la condotta che contraddistingue oggi molte organizzazioni: far finta di nulla fino a quando – inevitabilmente – non accade qualcosa di spiacevole. Oggi tra l'altro subire un attacco informatico – che sia chiaro: dal **ramsomware** al **data breach** ha la stessa dignità di qualsiasi altro crimine – è vissuto ancora come un'onta, un fatto da mantenere nascosto non solo al mercato, per ovvie

questioni legate a percezione di affidabilità e rapporti con la concorrenza, ma anche alle autorità.

Deve cambiare in primo luogo questo atteggiamento se si vuole arrivare alla definizione di una società digitale in cui i confini tra lecito e illecito nella conservazione e nel trattamento dei dati siano ben netti al di là di quanto prescritto dalla legge. E va necessariamente adottata una nuova mentalità se si vuole combattere ad armi pari i cyber criminali: la prevenzione non è più sufficiente, bisogna intervenire in maniera proattiva, assumendo la prospettiva degli attaccanti e collaborando con le altre imprese del proprio settore, scavalcando le tradizionali barriere della competizione. Sono questi i principali messaggi lanciati in occasione del **NetEvents European Media Spotlight 'Innovators in Cloud, IoT, AI & Security'**, convention internazionale che si è tenuta a Londra in questi giorni e che ha per l'appunto visto convergere vendor tecnologici e analisti specializzati in cyber security.

Parlando prima di tutto di aziende, in che modo si può bilanciare l'introduzione di policy di data protection e sicurezza informatica con le performance operazionali e con la privacy dei collaboratori? Come detto, bisogna prima di tutto fare uno sforzo di immedesimazione e provare a entrare nella mente degli hacker. “Chi sono? Nel 70-80% dei casi si tratta di criminali con competenze informatiche di base che cercano di sfruttare le falle evidenti di un mercato ricco e in espansione per sottrarre dati”, ha spiegato **Brian Lord, analista con una carriera ventennale all'interno del CGHQ** (Government Communications Headquarters), l'agenzia governativa che si occupa della sicurezza, dello spionaggio e del controspionaggio in ambito ICT. “La fetta restante è composta da specialisti che rischiano tempo, denaro e libertà personale per portare attacchi mirati, che possono anche impiegare anni per raggiungere il proprio obiettivo. Nel primo caso difendersi è relativamente semplice: bastano strumenti e cultura di base per prevenire o respingere gli attacchi indiscriminati. Ma il fenomeno non va assolutamente sottovalutato, visto che nel complesso il ramsomware e in generale la perdita di dati possono generare danni equivalenti al 4% del PIL mondiale. Quando invece si è, come per esempio nel caso delle banche, nel mirino di professionisti, diventa imprescindibile lavorare anche a livello di industry e coinvolgere il governo”.

Il problema è che il settore dell'IT non dispone ancora delle professionalità giuste. E se a dirlo è **Guy Franco, ex hacker e fondatore oltre che CTO di 7 Javelin** (azienda specializzata in cyber security), meglio crederci. “Non dobbiamo poi dimenticare la capacità che esercitano i cyber criminali di influenzare utenti e mercati attraverso la disinformazione”, ha continuato Franco. “Il ruolo dei social media qui è cruciale, e occorre avviare una cooperazione tra governi e piattaforme, anche se queste ultime sembrerebbero piuttosto riluttanti. Ma quella di Facebook & co. è una posizione insostenibile nel medio termine e penso che prima o poi assisteremo a un cambiamento in questo senso. Anche perché – non dimentichiamolo – parliamo di società grandi e globali, ma ancora molto giovani”.

In questo senso anche il pubblico è ancora immaturo, e per questo vulnerabile al modo in cui i media trattano l'argomento, spesso accusando l'intelligence non solo di non saper prevenire attacchi informatici, ma anche gli attentati terroristici che minano la tranquillità delle grandi città europee. Inevitabile il riferimento ai **fatti del London Bridge**: si sarebbe potuto evitare?

“Secondo me il dato più rilevante è che ci sono voluti solo otto minuti per fermare l'attacco, in un'area urbana incontrollata, ovvero non sottoposta a particolare attenzione delle forze dell'ordine”, ha detto **Arthur Snell, già capo del Prevent programme del Foreign office britannico**. “Dieci anni fa sarebbe occorsa almeno mezz'ora per coordinare un intervento e sventare l'attacco. Questo è un aspetto che non va sottovalutato”.

In ogni caso, che si parli di pubblica sicurezza o di proprietà intellettuali di un'impresa, oggi proteggere il valore attravero l'IT significa adottare un **approccio SysSecOps (Systems Security Operations)**, ennesima parola d'ordine del marketing di settore che sottintende la totale integrazione delle operazioni con i sistemi e gli strumenti di security, specialmente per quanto riguarda l'esperienza dell'utente finale sui terminali. Terminali che con l'Internet of Things potranno essere qualsiasi cosa: un'automobile, uno smart watch, una maglietta, un tostapane. “Il punto è questo”, è intervenuto l'**analista Alan Zeichick**: “non è più possibile limitarsi a dire sì o no quando si tratta di erogare un servizio su cui è stato riscontrato un attacco: il rischio di perdere clienti è troppo alto. L'intelligenza artificiale può venirci in soccorso, valutando quali sono effettivamente gli accessi e gli utilizzi consentiti in situazioni pericolose e quali no, definendo per area geografica, tipologia di utente e applicativo il margine d'azione consentito. Le telco e i carrier sono in tal senso gli operatori giusti al posto giusto per affrontare la sfida”.

Una sfida che parte innanzitutto dalla visibilità. Secondo **Roark Pollock, SVP Solutions Marketing di Ziften**, non è l'endpoint l'elemento che va preservato. “La questione fondamentale è riuscire ad avere una buona visibilità di quello che succede quando il dispositivo comunica con il network aziendale. Questo permette alla divisione IT di gestirne la sicurezza”. **Paul Ferron, Director Solutions Sales di CA Technologies**, rilancia la tesi di un approccio olistico: “Dobbiamo osservare lo user journey e riuscire a diventare agili nel fornire applicazioni sicure”. Per **Rik Turner, analista di Ovum**, questo significa cambiare completamente tattica: “Bisogna passare dal prevenire gli attacchi all'identificare, mitigare e risolvere gli attacchi”.

 07 Giugno 2017

TAG: london bridge, cybersecurity