msn

Faggioli (Polimi): “Gli hacker non sono samurai invincibili”

“La falla di sicurezza dei processori Intel è un fatto gravissimo, soprattutto nel metodo: come è possibile immettere sul mercato prodotti così vulnerabili?”. A spiegare i fenomeni **cybercrime** e della **cybersecurity**, partendo dall’ultimo clamoroso caso dopo un 2017 in cui solo nel primo semestre (e solo conteggiando i casi acclarati) gli attacchi informatici sono cresciuti dell’8,35% a livello globale, è **Gabriele Faggioli**, responsabile scientifico dell’Osservatorio Information Security & Privacy del **Politecnico di Milano**, presidente del Clusit (Associazione italiana per la sicurezza informatica) e CEO di P4I, società di advisory del gruppo Digital360. “Come tutelarci? Scaricando sempre gli aggiornamenti disponibili e informandoci di più. Per dirla alla Tobagi, gli hacker non sono samurai invincibili”.

Partiamo dal caso più recente: quello dei processori “fallati” di tre colossi dell’informatica come Intel, Amd e Arm, che potrebbero esporre miliardi di pc ad attacchi hacker. Che cosa è realmente successo?

“Innanzitutto mettiamo subito in chiaro una cosa: in questo caso non si è trattato di attacchi, ma di vulnerabilità del sistema tecnologico. Una falla di sicurezza importante ha coinvolto miliardi di apparecchiature in tutto il mondo, peraltro tutte di produzione recente, mettendo a rischio i dati di aziende e privati contenuti nelle strumentazioni informatiche. Potenzialmente potrebbe non succedere nulla, se non ci fossero persone disoneste nel mondo, ma purtroppo non è così e quindi non sono da escludere pericoli importanti e diffusi. L’aspetto più grave comunque non è tecnologico ma di metodo: immettere sul mercato prodotti con vulnerabilità così gravi equivale a vendere automobili che non frenano anche in caso di una normale pioggia. Come può essere sfuggito il problema in sede di ricerca, progettazione e sviluppo?”.

Chi sono i bersagli più sensibili e come possono tutelarsi?

“Chiunque, perché le operazioni di cybercrime, dai *malware* al *phishing* che sono le più diffuse, giocano sui grandi numeri. Si colpiscono miliardi di persone magari senza mirare qualcuno in particolare, sperando che qualcuno ci caschi. Sono ovviamente a rischio le persone anziane, ma paradossalmente anche i

giovani che utilizzano molto di più gli strumenti elettronici e, pur essendo più esperti nell'utilizzo pratico, spesso prestano poca attenzione perché sono meno portati alla diffidenza e alla riflessione prima dell'azione. Il consiglio è quello di scaricare sempre tutti gli aggiornamenti disponibili, dal sistema operativo al browser, e poi di informarsi di più. Questo deve essere anche un compito del pubblico: è ora che l'educazione informatica entri nelle scuole in pianta stabile".

Il rapporto del Clusit (Associazione italiana per la sicurezza informatica) evidenzia che i rischi del cybercrime sono ancora prevalentemente collegati ai danni economici che possono provocare nelle vittime. Quali sono i vari tipi di rischi?

"Nel 75% dei casi i cybercriminali colpiscono le loro vittime con l'obiettivo di estorcere denaro. Solo in piccola parte però questo avviene attraverso l'intrusione nei sistemi di pagamento elettronici, che oggi sono sempre più sicuri, mentre per lo più si tratta di truffe perpetrate via email, giocando sull'inganno. Ricordo ad esempio il caso della truffa nigeriana, ma anche altre che sono andate di moda nel 2017. Ecco perché insisto sulla necessità di una maggiore informazione. Poi ci sono il cyberbullismo, i danni d'immagine, il furto di dati personali, il furto d'identità. E lo spionaggio".

Ecco, nel 2017 il cyberspionaggio è cresciuto molto, salendo alla ribalta delle cronache con casi come quello del Russiagate: può diventare la nuova frontiera del crimine informatico?

"Difficile dire se sarà un nuovo trend preponderante. Di sicuro i casi conosciuti sono cresciuti del 126% in un anno, anche se sono ancora numericamente pochi sul totale, per quanto molto importanti come quello del Russiagate. Sono tuttavia convinto che la pratica possa continuare a diffondersi, non solo in ambito geopolitico ma anche in quello aziendale, come strumento di concorrenza sleale".

Chi c'è di solito dietro l'hackeraggio?

"Le organizzazioni criminali, di tutto il mondo, che ne fanno ormai una sicura e sostanziosa fonte di guadagni. Poi i lupi solitari, e persino alcuni Stati, come per esempio Russia e Cina, anche se loro naturalmente negano".

Tornando alle falle tecnologiche, che sono quelle che possono poi favorire il cybercrime: in molti accusano i big della Silicon Valley di assumere un atteggiamento troppo superficiale sulla questione. E' d'accordo?

“Non direi che c’è trascuratezza in assoluto, ma approcci un po’ leggeri talvolta sembrano esserci anche se la diffusione massiva delle apparecchiature connesse porta il problema in casa non solo dei big della Silicon Valley ma anche di tutte le aziende che realizzano o chiedono la realizzazione di prodotti e servizi informatici e telematici. Potrebbero fare di più? Sicuramente sì, ma credo che lo faranno: c’è una presa di coscienza sempre maggiore, grazie anche all’attenzione mediatica che i continui casi emersi di recente stanno ricevendo”.

I dati Clusit dicono invece che è proprio l’Europa ad essere vulnerabile agli attacchi informatici. Perché, e come sta cercando di risolvere il problema?

“In Europa ci sono più vittime ma è normale, perché alcuni Paesi, tra cui anche l’Italia, soffrono di un ritardo storico nell’informatizzazione, rispetto al Nord America ma non solo. Informatizzazione significa anche cultura informatica, e in questo siamo indietro, anche se si stanno muovendo passi importanti. La normativa in discussione al Parlamento Europeo (denominata cybersecurity act) dovrebbe rafforzare l’Enisa, l’Agenzia europea per la sicurezza delle reti e dell’informazione, e dovrebbe portare a un quadro organico delle certificazioni di sicurezza informatica di prodotti e servizi. E’ un buon passo”.

© Fornito da Firstonline Gabriele Faggioli Politecnico di Milano

E l’Italia?

“Sta migliorando. Innanzitutto è cresciuta l’attenzione del pubblico: il Governo uscente ha approvato il nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica. Bene anche le Misure minime di sicurezza ICT per le pubbliche amministrazioni che AGID (Agenzia per l’Italia digitale) ha adottato negli scorsi mesi. Ritengo da sempre che la Pubblica amministrazione italiana sia troppo frammentata a livello di organizzazione delle infrastrutture e delle

applicazioni informatiche con conseguente aumento dei costi e dei rischi informatici. Credo che sarebbe invece opportuno accentrare la gestione delle infrastrutture e delle applicazioni per permettere razionalizzazione, risparmi di costi e maggiore sicurezza. Non c'è dubbio infatti che solo i player che possono contare su importanti economie di scala sono in grado di investire adeguatamente: basti pensare alle più importanti piattaforme di cloud computing del mondo, come Dropbox. Nessun privato, libero professionista ma neanche nessuna Pmi o large enterprise può permettersi investimenti così massicci e continui per la sicurezza. L'esternalizzazione e l'aggregazione rendono i sistemi più sicuri ed efficienti. Comunque la strada è giusta, anche se temo che potrebbero venire a mancare le risorse: per mettere in sicurezza la Pa servono miliardi".

A livello di imprese invece?

"Nella fascia alta, cioè tra le imprese più grandi, ritengo che il tema della sicurezza informatica sia ormai all'ordine del giorno. Sono invece in ritardo le Pmi. Il tema è che gli investimenti in sicurezza informatica sono troppo bassi: la spesa ICT (Information and Communication Technologies) in Italia è stata di 66 miliardi nel 2016. Il Politecnico di Milano ha stimato che di questi 66 miliardi meno di 1 miliardo è stato destinato alla sicurezza, cioè l'1,5% (lo 0,05% del Pil): troppo poco. Del resto chi di noi si fiderebbe di acquistare un'automobile sapendo che il costruttore ha dedicato solo una risorsa su 100 alla sua affidabilità?".

Infine una provocazione: abbiamo parlato di ritardo tecnologico, anche dell'Italia, ma a volte è proprio la diffusione della tecnologia in ambiti sempre più ampi a determinare un rischio maggiore. Il rapporto Clusit infatti inserisce anche smart working, Internet delle cose e Industria 4.0 tra i fattori di pericolo…

"E' fisiologico, perché aumenta la superficie di attacco, ma la tecnologia non va demonizzata. E' come se per evitare gli incidenti in automobile, tornassimo a muoverci in carrozza. Sicuramente sta alle aziende rendere i prodotti sempre più sicuri e al pubblico determinare regole e contribuire alla formazione dei cittadini. Ma problemi purtroppo ce ne saranno sempre, come in tutte le cose: per incuria, ignoranza, disinformazione. Serve cultura e comprensione dei rischi e quindi capacità di capire dove è bene fermarsi per il proprio bene, ma anche per quello altrui".