La Cyber Security Istituzionale

Date : 27 febbraio 2017

A molti non sarà sfuggito lo scandalo provocato dalla vicenda Occhionero, i fratelli che hanno rubato dati e informazioni sensibili a politici e uomini di potere del panorama italiano. Allo stesso tempo, a circa metà gennaio, si sono rincorse alcune notizie circa l'intenzione del presidente degli Stati Uniti Donald Trump, di non utilizzare un cellulare dedicato per le comunicazioni istituzionali. Il punto in comune di queste due situazioni è anche il nucleo di questo articolo: la cyber security nelle istituzioni. Riguardo la vicenda Occhionero, sono stati veramente molti i commenti circa la carenza di protezione tecnica dei nostri politici. Protezione che, fin troppo spesso, viene delegata a software, hardware e soluzioni commerciali. Il vero fulcro della questione però è un altro: *perché mai un politico dovrebbe svolgere la sua funzione istituzionale, utilizzando mezzi privati e non dedicati*?

Prima di addentrarci nelle problematiche squisitamente tecniche, è opportuno notare che tra l'elenco degli spiati non compare, ad esempio, il Ministro della Difesa Pinotti. Il motivo è che la regolamentazione delle procedure riguardante il materiale classificato, è sufficientemente severa da ridurre drasticamente gli incidenti. Diviene quindi chiaro che il nodo della questione è più organizzativo che tecnico. Fatta questa precisazione è possibile iniziare a scandagliare anche gli aspetti tecnici della faccenda. Uno tra tutti riguarda EyePyramid, il malware con il quale è stato perpetrato l'attacco. Il malware utilizzato per infettare politici ed economisti è stato ricavato da una variante di EyePyramid ed è stata proprio questa variazione a renderlo invisibile agli occhi degli antivirus.

Tecnicamente l'attacco lanciato contro gli spiati è stato confezionato sotto forma di un banale allegato di posta elettronica. Gli addetti ai lavori avranno imparato a temere le mail di finta fatturazione o rimborso che, al loro interno, contengono ransomware come il Cryptolocker. Eppure, parallelamente ai dettagli tecnici, c'è un aspetto più importante da sottolineare. L'intera vicenda è venuta fuori grazie ad una segnalazione dell'ENAV: un operatore si è insospettito dalla mail e ha richiesto ad una società specializzata di effettuare controlli approfonditi sul file, svelando l'arcano. Ancora una volta non è stata un'azione di qualche software a difendere la struttura ma una procedura applicata in modo eticamente e deontologicamente puntuale. La società incaricata di effettuare le verifiche ha, successivamente, riconosciuto il malware nell'allegato alla mail ma è stata la professionalità di quell'operatore a proteggere l'intera infrastruttura dell'ENAV.

La complessità di questo attacco è inoltre dato da un duplice aspetto: l'architettura informatica utilizzata, costituita da una serie di scatole cinesi sparse oltre i confini nazionali e un gran lavoro di ingegneria sociale. Il pregevole lavoro del CNAIPIC ha permesso di risalire alla fonte del problema in pochissimo tempo, con la preziosa collaborazione del Federal Bureau of Investigation. I giorni successivi sono stati un susseguirsi di congetture e sentenze anche se pochi hanno detto l'unica cosa veramente importante: la causa alla base della propagazione del malware non è stata tanto di natura tecnologica, quanto di natura deontologica. Non è possibile, infatti, affidare comunicazioni istituzionali a persone e sistemi non preparati per gestirle. Lo stesso Donald Trump è stato messo alle strette per evitare che le comunicazioni ufficiali viaggiassero sul suo smartphone personale e, qui in Italia, la prassi è la medesima. Bisogna capire che coloro che ricoprono ruoli istituzionali hanno, come primo dovere, quello di salvaguardare la sicurezza delle istituzioni. Esistono procedure, norme e anche tecnologie ma non si può pensare che tutto possa essere risolto dall'adozione di un comune antivirus.

Proviamo, quindi, a parlare di buone prassi e cominciamo con l'affermare che gli affari istituzionali e quelli privati non possono risiedere sul medesimo dispositivo. Il rischio è troppo elevato, considerato a maggior ragione che, normalmente, i dispositivi utilizzati dai nostri politici non sono opportunamente configurati. Qualche giorno fa l'esercito britannico ha reso noto che utilizzerà dei dispositivi iPhone per i suoi ufficiali. La particolare architettura li ha fatti prevalere ai concorrenti ma, nonostante tutto, British Telecom apporterà comunque delle modifiche per renderli ulteriormente sicuri. Questo a dimostrazione che non basta procedere all'acquisto di un comune smartphone ma è necessario assicurarsi che esso sia correttamente sicuro. Un secondo elemento di attenzione è sulle modalità di comunicazione: avere un cellulare protetto e lasciarlo nelle mani di terzi è una prassi che si verifica fin troppo spesso e che, come sappiamo, in passato è stato origine di infiltrazioni. Pensiamo al caso di Hacking Team: gli operatori potevano installare la minaccia sui dispositivi in pochi minuti. Bisogna quindi comprendere che cellulari, tablet, computer, sono oggetti sensibili, importanti come cassette di sicurezza. Non possono essere lasciati incustoditi, né consegnati con leggerezza nelle mani di una persona non autorizzata e da questo elemento discende l'ultimo punto: la deontologia. Non mi stancherò mai di scrivere che, soprattutto per i ruoli istituzionali, la deontologia è fondamentale. Non è possibile anteporre le proprie comodità davanti al rischio di rendere meno sicure infrastrutture e informazioni. Quanti scandali provengono dalle intercettazioni di chat, immagini, email? Ce lo insegnano gli Stati Uniti con quelli emersi durante le presidenziali ma possiamo anche concentrarci su quelli italiani.

Esiste, infine, anche l'aspetto più tecnico al problema, a cui avevamo accennato ad inizio articolo. Bisogna comprendere che alcune soluzioni sono più sicure di altre. Le architetture Unix sono, senza alcun dubbio, molto più adeguate ad essere utilizzate in ambienti sensibili. Questo perché il cuore dell'architettura (il kernel) è protetto dalla comunicazione diretta con le applicazioni di terze parti, impedendo l'esecuzione di codice malevolo. Ovviamente anche le architetture Unix possono essere attaccare ma risulta più difficile perpetrare tale attacco e questo le rende preferibili dai tecnici durante l'uso in ambienti di produzione. Ciò detto le architetture Unix spesso risultano meno intuitive, meno versatili e quindi apparentemente più ostili ad un uso quotidiano. In realtà negli ultimi cinque anni, queste soluzioni sono diventate sicuramente più alla portata di tutti. Lo stesso sistema operativo iOS degli iPhone è basato su un'architettura Unix (per la verità è un'architettura mista tra Unix e FreeBSD). Il panorama

Android è più variegato perchè, benchè Android sia basato su un kernel Linux, universalmente riconosciuto come molto sicuro, il sistema operativo subisce molte modifiche a seconda del produttore dello smartphone. Queste modifiche possono incidere tanto sull'interfaccia grafica, quanto sugli aspetti più endogeni dell'architettura. Ogni modifica può rappresentare una potenziale breccia alla sicurezza del dispositivo. In altri casi Android è stato utilizzato per creare smartphone altamente sicuri, come ad esempio il Blackphone. Tutto dipende dalla configurazione del produttore che, in modo più o meno sicuro, modifica l'equilibrio del sistema operativo.

A questo punto è opportuno fare alcune riflessioni in merito all'eziologia dell'attacco utilizzato nel caso degli Occhionero. Come molti avranno letto, tra le persone spiate con la variante di EyePyramid c'era anche una loggia massonica. Forse non tutti sanno che nella sua versione originale *EyePyramid* fu utilizzato anche nel caso Bisignani esponente della P4. La vicenda è stata affrontata dettagliatamente dal sito della società di sicurezza TrendMicro che, al proposito, ha pubblicato:

"*In 2012, a high-profile Italian businessman and ex-journalist named Luigi Bisignani was prosecuted as part of the "P4 secret society," (short for Propaganda 4). The P4 was the fourth of the masonic lodges in Italy, which was supposedly influencing political decisions.*

The malware used in those attacks used several Gmail addresses as dropzones. Investigators at CNAIPIC (an Italian cybercrime body) found that these same addresses were used by recent EyePyramid variants as well. Independently, we found that older (2012) variants of EyePyramid were doing the same thing. One more interesting link that we found is the use of the mail.hospenta.com mailserver, which is similar to the one used by the recent versions of EyePyramid. Curiously, only the 2010 version—and not the 2012 version—used mail.hostpenta.com."

Le informazioni possono essere trovate sul sito ufficiale TrendMicro alla pagina: https://goo.gl/42iDlt

C'è un altro elemento che unisce la vicenda Occhionero a quella di Bisignani: è la presenza del CNAIPIC che, anche con Bisignani, fu in grado di verificare l'impiego diEyePyramid (all'epoca in versione originale). Queste affermazioni hanno uno scopo, attirare l'attenzione su un aspetto procedurale che non è a carico dell'utente ma dell'amministrazione. Di fatto il personale tecnico dell'amministrazione è spesso osteggiato quando prova ad imporre soluzioni tecnicamente più adeguate al ruolo. Si entra in un conflitto di competenze e ruoli non indifferente. Non a caso, riprendendo l'esempio riportato all'inizio dell'articolo, Donald Trump ha rifiutato l'utilizzo di un cellulare dedicato proposto dal Ministero della Difesa americano. In Italia la situazione è la medesima se non più complicata perché non vi è una reale consapevolezza dei rischi e delle minacce a cui siamo esposti. Il nostro Paese non ha, per fortuna, ricevuto attentati davvero rilevanti dal punto di vista cyber e questo ha impedito la formazione di una coscienza in merito. Per essere più chiari, è come se il parlamentare italiano ricevesse un ordine preciso del Ministero dell'Interno ad utilizzare uno speciale smartphone/tablet/computer per le sue attività professionali. Non sarebbe poi così assurdo se questo servisse a tutelare i dati nazionali, ma sappiamo che per le autorità di polizia spesso è

persino difficile eseguire delle intercettazioni.

Le soluzioni quindi si slanciano su due percorsi paralleli ma collegati. Il primo, di natura squisitamente tecnica, potrebbe riguardare la fornitura di un kit di lavoro standard composto da smartphone, tablet, notebook con configurazione specifica e autorizzazioni di accesso limitate e ben calibrate. Se pensate che questo sia un futuro remoto sappiate che la RAI, tanto per citare un'azienda nota a tutti, dispone di una sicurezza identica a quella appena descritta. Il dipendente che deve accedere a determinati sistemi può farlo solo se munito dello specifico portatile aziendale che, oltre ad un token hardware, è stato registrato all'interno dell'architettura di sistema come *autorizzato ad operare*. Già solo con questa soluzione si potrebbero eliminare gran parte dei rischi di cui abbiamo fatto menzione. L'applicazione pratica sarebbe di basso impatto considerando che un'infrastruttura aziendale dovrebbe già avere attive delle regole di filtraggio del traffico. Inoltre esistono diverse modalità per mantenere in sicurezza le informazioni, a seconda del tipo di dato che s'intende proteggere. Negli ultimi anni, soprattutto legato alla e-Economy, si sente parlare della *blockchain*. Si tratta di una decentralizzazione delle autorizzazioni a compiere determinate azioni che non sono più a carico di un unico sistema ma vengono distribuite a più apparati/persone in grado di verificare la veridicità del comando. Ovviamente questo sistema può funzionare solo in determinate occasioni ma la filosofia di decentramento si sta espandendo molto velocemente anche nei produttori di hardware. Una forma di decentramento molto elementare è disponibile su quei sistemi dove, l'autorizzazione ad utilizzare una particolare applicazione del computer, viene inviata allo smartphone del proprietario e, se disponibile, contemporaneamente anche al tablet. Ovviamente, dal punto di vista tecnico, il decentramento comporta una riduzione sensibile dei rischi ma anche una maggiore complessità architetturale ed è alla base di concetti noti e fondamentali come la clusterizzazione, la virtualizzazione, ecc..

Il secondo fronte è di tipo procedurale e consiste nella normazione di prassi sicure ed affidabili per la regolamentazione di consegna, utilizzo, e gestione di guasti degli apparati dedicati all'impiego istituzionale. Sicuramente questa regolamentazione esiste a livello di singolo ufficio ma non è detto che esista a livello intra-istituzionale. La mancata applicazione di queste regole, inoltre, rischia di compromettere l'intero apparato di sicurezza dedicato all'utente. Ecco quindi che l'impianto procedurale, benché definito, deve essere assolutamente rispettato per mantenere il giusto equilibrio operativo. Torniamo nuovamente al concetto deontologico di rispetto della norma che, in Italia, trova purtroppo molta difficoltà ad attecchire anche a causa dell'incertezza della sanzione per chi trasgredisce le regole. Nel portare un esempio, è opportuno scegliere un attore istituzionale di tutto rispetto: l'Unione Europea, infatti, possiede un portale di progetto nel quale è assolutamente vietato implementare direttamente plug-in di terze parti che eseguono script interattive con siti esterni. In sostanza la regola impone di non aprire il perimetro del portale all'esterno tramite plug-in che, per quanto certificati, potrebbero rappresentare un rischio alla sicurezza interna.

L'auspicio finale è quello di avere, in un futuro prossimo, maggior rigore nella scelta di apparati e tecnologie che siano veramente orientate ad un uso esclusivamente istituzionale. In tal senso l'Europa ce lo insegna con un comparto di norme e buone prassi che possano essere veramente rispettate al fine di mantenere il giusto livello di sicurezza. Lo scopo di queste regole, infatti, non è di limitare l'iniziativa di comunicazione del politico, ma è quella di proteggere in

modo serio le informazioni da lui trattate. È una questione importante, ed è una questione dovuta allo Stato e quindi ai cittadini.

A cura di: **Edoardo Limone**