Crisi di Stato

Come farsi rubare i data-base della Polizia e vivere felici.

Nella notte tra il 24 ed il 25 luglio 2011, il gruppo di hackers internazionale denominato Anonymous – già agli onori della cronaca per l'attacco contro i siti di Scientology, rivendicato in nome dello spirito libertario del web e contro i metodi massimalisti e di censura praticati da quell'organizzazione (1), e per i più celebri interventi in difesa di Wikileaks – hanno forzato i server della Polizia italiana, e per la precisione del CNAIPIC, il Centro Nazionale Italiano per la Protezione delle Infrastrutture Critiche, la sezione della Polizia di Stato preposta alla difesa di tutti i "nodi" informatici cruciali delle istituzioni della penisola. Come dire: un gruppo di ragazzi sorvegliati a vista svaligia la casa superprotetta del Giudice preposto a controllarli mentre sono agli arresti domiciliari.
Questo discusso gruppo di hackers aveva già forzato in una precedente occasione, a inizi 2011, le piattaforme web del Governo Italiano, per protesta "politica" contro lo stile di governance del Premier Berlusconi, mandando in tilt nel corso della cosiddetta Operazione Italia i siti di Palazzo Chigi e di vari Ministeri. All'epoca un Dirigente della Polizia Postale, il corpo di vigilanza italiano contro gli abusi informatici, da cui dipende anche il CNAIPIC, aveva dichiarato: "Questo genere di azioni difficilmente si può contrastare perché provengono da più computer sparsi non solo in Italia, ma anche all'estero". Gli Anonymous avevano risposto con un breve ma per certi versi fascinoso comunicato stampa: "Noi non amiamo la violenza, noi non vogliamo la guerra, noi non cerchiamo di creare disordini. Noi siamo i protettori umili e innumerevoli e della libertà di parola. Noi siamo la massa critica".
Ma la beffa appare ancor più clamorosa di quella di inizi anno, se consideriamo che non più di un mese prima, i cyber-

detective del Ministero degli Interni avevano effettuato alcuni arresti, dichiarando pomposamente alla stampa: “Decapitati i vertici italiani di Anonymous”. Gli stessi hackers formalmente “decapitati” che poche settimane dopo hanno inferto un durissimo colpo di credibilità al CNAIPIC, il corpo scelto della Polizia Postale, i guardiani della sicurezza informatica di tutti noi. Peraltro, come fosse possibile “decapitare” un’organizzazione non verticistica e che ha in una struttura “a rete” il suo stesso DNA, era poco chiaro a qualunque addetto ai lavori del settore, ma si sa: la comunicazione si muove sui binari dello “scoop” e raramente su quelli dell’autenticità.
L’esperto informatico Roberto Preatoni ha dichiarato in un’intervista al cliccatissimo quotidiano on-line Affari Italiani: “…Non ho idea di come abbiano fatto, non mi serve saperlo: c’è sempre stato un modo e sempre ci sarà. E’ inutile: da un lato ci sono decine di tecnici che si arrovellano per cercare di mettere in sicurezza le infrastrutture critiche, dall’altro c’è sempre un singolo creativo che ragionando in maniera non lineare riesce a trovare un modo per metterli nel sacco. E se il modo non c’è, lo inventa, non c’è verso. Il creativo che ragiona in maniera non lineare si chiama hacker, per l’appunto. Non esiste definizione migliore”.
Gli Anonymous hanno dichiarato su uno dei loro blog ufficiali: “Questa corrotta organizzazione (il CNAIPIC, ndr.) ha raccolto del materiale sequestrato dai computer di professionisti della sicurezza e lo ha utilizzato negli anni per condurre operazioni illegali in accordo con servizi segreti stranieri, invece che utilizzarlo per condurre investigazioni lecite”. Poco importa che gli stessi Anonymous due giorni dopo i fatti abbiano preso le distanze dall’accaduto, attribuendo la forzatura dei data-base della Polizia ad un altro gruppo di hackers, i Nkwt Load: ciò che conta è che ben 8 Giga di file riservati siano stati sottratti da depositi informatici considerati super-sicuri e con scioltezza pubblicati in rete, su tre distinti siti, disponibili alla lettura da parte di

chiunque si sia preso la briga in quelle ore di downlodarne con sollecitudine il contenuto. Se non è crisi questa…
Come ha risposto il Ministero dell'Interno alla crisi? Sollecitato da Daniele Tigli, un collega di Faenza particolarmente attento a tutto ciò che è oltre i confini del web tradizionalmente inteso, ho preso contatto con l'Ufficio stampa della Polizia poche ore dopo la pubblicazione della notizia on-line. Mi hanno rassicurato che "un comunicato stampa stava per essere diramato" (2), e in effetti l'ho trovato nella mia casella di posta poche ore dopo. Lo sconcerto è stato però grande quando ho aperto il file, che recitava (riporto verbatim): "In relazione alla divulgazione in Rete di documenti sottratti dai suoi sistemi informatici, la Polizia delle Comunicazioni ha in corso attente verifiche tecniche mirate ad accertare la reale portata degli eventi. Di fatto, risultano pubblicati online contenuti apparentemente riconducibili al CNAIPIC della stessa Polizia delle Comunicazioni sulla cui autenticità sono in corso accertamenti". Fine del comunicato. Due frasi. Nessun dettaglio. Nessun virgolettato. Nessuna analisi nel merito della tipologia di file trafugati. Nessuna dichiarazione del Ministro su quella che appare la più eclatante violazione informatica mai avvenuta in Italia da quando esiste la rete internet.
Mentre realizzavo un servizio sull'accaduto (3) per la SBS (4), con la quale collaboro, ho chiesto all'Ufficio Stampa del Ministero di tenermi sollecitamente al corrente sugli sviluppi della questione. A parte una bulimica e imbarazzante quantità di comunicati stampa sulla situazione del traffico sulle autostrade italiane prese d'assalto dai vacanzieri, non è pervenuta nei giorni successivi nella mia casella e-mail alcuna news di aggiornamento su questo delicato dossier, e alla data di chiusura di questo articolo sul sito ufficiale della Polizia di Stato non risulta pubblicato alcunché al riguardo. Anzi, con mio stupore, ho anche verificato che anche il laconico – e ben poco utile – comunicato del 25 luglio il cui testo vi ho riportato sopra, non risulta pubblicato sulla

media room della Polizia (5): o non vi è mai stato, o è stato rimosso…
È appena utile evidenziare che – con tutto il rispetto per la necessaria riservatezza delle indagini – sono state violate dagli addetti alla comunicazione della Polizia le più elementari regole della gestione di casi di crisi:

- non è stata diramata un'informazione immediata, costante e completa;
  non sono state individuate e rese note – pur nel rispetto delle procedure di sicurezza necessarie in questi casi – le criticità che hanno portato alla crisi;
  non sono stati individuati e resi noti eventuali profili di responsabilità;
  non sono state illustrate anche sommariamente le innovazioni alle procedure che impediranno il ripetersi di episodi del genere in futuro, aspetti che riguardano – anche – la sicurezza di tutti noi;
  nessun portavoce ufficiale (il Ministro o un suo autorevole delegato) ha preso la parola per rassicurare tutti i pubblici coinvolti circa il buon esito della crisi.

A oltre 15 giorni dall'evento, da un corpo altamente specializzato come la Polizia Postale ci si aspettava certamente di più, se non altro sotto l'aspetto del flusso informativo. Ma più ancora, stupisce l'assoluta assenza d'iniziativa politica dei vertici del dicastero degli Interni e del Governo, una volta ancora apparentemente "distante" dai problemi concreti della vita dei cittadini. Con decine di milioni di connessioni web attive in Italia, il profilo della sicurezza dei data-base informatici non mi sembra affatto una issue da trascurare o sottostimare.
(1) Vedasi il mio articolo "Scientology: critiche ragionate alla strategia di comunicazione" pubblicato su Ferpi News all'indirizzo internet http://www.ferpi.it/ferpi/novita/notizie_rp/internazionale/sci

entology-critiche-ragionate-alle-strategie-di-comunicazione/notizia_rp/43153/7
(2) Il mio contatto con il Ministero risale al 25/07/11, h 16:00 circa
(3) Downlodabile su http://www.sbs.com.au/yourlanguage/italian/highlight/page/id/179547/t/Hackers-at-work
(4) La radio di Stato Australiana, il più importante network nazionale che trasmette – in più lingue – anche in tutta l'Oceania
(5) http://www.poliziadistato.it/articolo/183-Ufficio_stampa/

Affrontare le voci di corridoio in azienda

La comunicazione interna e le situazioni di crisi.
Affrontare le voci di corridoio in azienda.pdf

Diffamazione, se l'omeopata minaccia il blog

Boiron chiede ad un blogger italiano la rimozione di opinioni ritenute diffamanti.
Diffamazione se l omeopata minaccia il blog.pdf

Dai campi energia per sostituire tre centrali

Dalle campagne italiane è possibile ottenere nei prossimi dieci anni energia rinnovabile in grado di sostituire tre centrali nucleari con il diretto coinvolgimento delle imprese agricole e senza causare danni al territorio.
Dai campi energia per sostituire tre centrali.pdf

Il Pentagono svela la nuova strategia anti hackerDopo terra, cielo e mare è l' ora della guerra in rete

Dopo terra, cielo e mare è l’ ora della guerra in rete.
Il Pentagono svela la nuova strategia anti hacker.pdf