Le inchieste del Mattino

L'Italia è «Cyberdebole» record di attacchi hacker

▶L'ultimo colpo all'Archivio di Stato sottratte cinquemila password

▶Lo stesso gruppo aveva colpito il ministero Ambiente, Juve ed Eni

IL CASO

Valentino Di Giacomo

«Ops Beni Culturali pensiamo ci sia un problema, date un occhiata a questi 5465 utenti con password in chiaro». Ancora un attacco hacker ad un sito della pubblica amministrazione, stavolta nel mirino dei cyber-criminali ci è finito il portale web dell'Archivio di Stato. Il furto di dati è stato rivendicato dal proprio account Twitter dagli hacktivisti di LulzSec Italia. I criminali informatici, sfruttando le vulnerabilità nella programmazione del sito web che collega gli archivi per i beni culturali di tutte le province italiane, sono riusciti ad impossessarsi di oltre 5mila user e password costituendo, per ironico contrappasso, un proprio archivio dei dati rubati poi subito diffusi in rete. L'elenco violato, che circola ancora sui social, vede anche account di manager di Eni e Juventus.

GLI HACKER

Non sono nuovi ad imprese di questo genere gli hacktivisti di LulzSec. Lo scorso mese furono già protagonisti di un'incursione nei sistemi della Motorizzazione civile di Roma e provocatoriamente minacciarono il sindaco Virginia Raggi di toglierle la patente. Ancor più massiccio fu l'attacco al sito del ministero dell'Ambiente messo knock-out per oltre cinque giorni e sottraendo dagli archivi le valutazioni di impatto ambientale e le relazioni tecniche sia dell'aeroporto di Firenze che della Tap, il gasdotto che dalla Turchia arriva in Puglia. LulzSec è un gruppo hacker attivo da qualche anno anche in Italia. A livello mondiale, soprattutto negli Usa, la sigla si è dichiarata responsabile di diversi attacchi come la compromissione degli account degli utenti della Sony Pictures nel 2011 e la messa in offline del sito della CIA, l'intelligence statunitense. Dopo che il sito del dipartimento di pubblica sicurezza dell'Arizona venne compromesso furono additati come gruppo cyber-terroristico. Lo stile di questi hacker è diventato celebre soprattutto per i messaggi sarcastici che pubblicano dopo aver compiuto le irruzioni, dicono di non compierle per fini di lucro, ma per creare caos. Durante l'ultima campagna elettorale delle politiche italiane hanno piratato i siti della Lega di Matteo Salvini pubblicando oltre 76mila mail di esponenti del partito.

IL 47 PER CENTO DEI SITI ISTITUZIONALI CONTINUA A UTILIZZARE CONNESSIONI SENZA PROTEZIONI

GLI ATTACCHI

Se i membri di LulzSec si definiscono hacker etici, in Italia gli attacchi informatici a istituzioni o aziende sono più che quintuplicati rispetto allo scorso anno e non solo per mano loro. Secondo l'ultima relazione annuale dell'intelligence le azioni ostili hanno riguardato prevalentemente i sistemi di pubbliche amministrazioni centrali e locali (72%). Nel corso dello scorso anno – secondo i dati diffusi dai nostri Servizi segreti - è stato individuato un sensibile aumento di attacchi contro reti ministeriali (24%) e di enti locali (39%). Gli autori di queste attività sono in larga parte (61%) attribuibili alla galassia degli hacker attivisti, ma uno su quattro giungono da Paesi esteri, in una guerra cyber che perdura da anni e che vede l'Italia molto spesso nel mirino di altre potenze straniere. Altri tentativi di intrusione informatica sono poi riferibili a gruppi terroristici (5%). Ma la minaccia maggiore è probabilmente quella sferrata al nostro tessuto economico con l'obiettivo di carpire informazioni alle imprese con alta specializzazione. Il comparto intelligence ha spiegato che da parte di operatori esteri si sono registrate «iniziative tese ad esfiltrare tecnologia e know-how e iniziative di spionaggio industriale». Siti costruiti in maniera poco sicura mettono a repentaglio non solo le istituzioni, ma soprattutto il nostro tessuto economico con tentativi sempre più diffusi di rubare i progetti made in Italy.

I COMUNI

Eppure le regole per prevenire questo genere di attacchi ci sarebbero, come ad esempio il Gdpr (il General data protection regulation) approvato un anno fa. Ma portali istituzionali di ministeri, forze dell'ordine, regioni e partiti politici non sono ancora attrezzati. Secondo una recente ricerca molti di questi siti non hanno un'informativa privacy aggiornata al nuovo Regolamento Europeo, ma fanno riferimento ancora alle vecchie normative. Uno studio condotto dall'Osservatorio di Federprivacy, su ben 3mila siti dei comuni italiani, 1.435 di essi (47%) continuano ad utilizzare connessioni non sicure basate sul vecchio protocollo «http» e per questo etichettati come «non sicuri» dai principali browser. Inoltre, 1.079 siti di comuni (36%) non rendono disponibili i dati di contatto del Responsabile della Protezione dei dati, figura obbligatoria.

LE CONTROMOSSE

Una sottovalutazione che mette in pericolo la sicurezza nazionale su tutti i fronti, anche in campo militare. «L'Italia – spiega il sottosegretario alla Difesa con delega alla cybersecurity, Angelo Tofalo - è ancora indietro rispetto alla consapevolezza della minaccia. Noi per la prima volta abbiamo messo al centro dell'agenda questa tematica, come ministero abbiamo costituito un gruppo di progetto per creare un nuovo Comando sulla cyber con alla guida un Generale a tre stelle. Tutti gli uffici della Difesa saranno messi insieme per migliorare lo scambio informativo tra i vari apparati». Da oltre un anno il Cisr (Comitato interministeriale per la sicurezza della Repubblica) ha dato la delega alla cybersecurity al vicedirettore del Dis, Roberto Baldoni. Ma la strada per difendersi sembra ancora lunga.

RIVENDICAZIONE Il tweet degli hacker che annuncia la violazione del database con le password dell'Archivio di Stato

Intervista Raoul Chiesa

«Troppe gare al risparmio i migliori fuggono all'estero»

«Sicuramente gli hacktivisti di LulzSec hanno una credibilità internazionale di un certo livello, si farebbe male a credere che si tratti di ragazzini appassionati di informatica che giocano a smanettare sul pc, già in passato hanno fatto azioni di grande rilievo». Raoul Chiesa è uno dei primi hacker etici italiani, celebre con lo pseudonimo di «Nobody», da anni l'informatico torinese ha messo le proprie competenze al servizio della cybersecurity di cui è tra i massimi esperti internazionali.

Oltre 5mila password rubate. Che fine faranno?

«Purtroppo chi è in quella lista diffusa dal gruppo LulzSec è molto probabile subirà qualche attacco. La statistica ci indica che almeno la metà degli utenti usa la stessa password su diverse piattaforme, da Facebook a Linkedin, da Twitter ai portali di e-commerce. Non mi sorprenderebbe se qualche male intenzionato usasse quelle password per entrare su altre piattaforme. Tra l'altro questo attacco è avvenuto in giorni in cui molti sono in vacanza e magari sono meno attenti nel verificare intrusioni».

Tra gli user diffusi ci sono anche manager di Eni e Juventus.

«Stavolta è toccato a loro, ma quante volte è accaduto che attacchi pirata abbiano diffuso user e password di ministri, dipendenti e funzionari di alto livello della pubblica amministrazione, poi da lì ci vuole poco, facendo quella che viene tecnicamente definita "ingegneria sociale", far partire altre incursioni verso altre piattaforme istituzionali o aziendali».

HACKER Raoul Chiesa di definisce hacker etico

Com'è possibile dopo tutti questi anni che i cyber-criminali abbiano ancora vita facile?

«Anche questa incursione dimostra l'inadeguatezza dei sistemi delle pubbliche amministrazioni che spesso hanno la cattiva abitudine di avere dei database con user e password non cifrate. Il problema è che quando lo Stato fa delle gare di appalto per la creazione di questi portali si cerca sempre di rivolgersi a chi fa il prezzo più basso. Dopodiché chi si è aggiudicato la gara fa partire una serie di subappalti a catena: poi alla fine chi realmente opera per costruire il sito magari è un ragazzo che prende 30 euro al giorno e non si può pretendere che oltre ad essere un esperto di grafica possa essere pure capace ad impostare determinati sistemi di sicurezza per rendere meno vulnerabile il sistema».

Come si risolve il problema?

«Se prendiamo tutti i bandi di gara fatti negli ultimi anni dagli enti istituzionali difficilmente troveremo una ricerca indirizzata ad aziende e persone preposte a risolvere i problemi della cybersecurity. Non esiste la consapevolezza della minaccia a tutti i livelli: dallo Stato, alle imprese, fino ai semplici cittadini. Eppure in Italia siamo molto bravi, ma i migliori programmatori fuggono all'estero proprio perché qui non abbiamo un'adeguata cultura della sicurezza informatica».

Che tipo di attacco è quello compiuto all'Archivio di Stato?

«Banalmente mi sembra di tipo "Sql injection". In due parole significa che se il programmatore scrive male il codice software anche se non hai una password ti puoi accreditare e accedere al sito come amministratore. Ormai è un tipo di attacco così semplice, diffuso da più di 10 anni, ci sono persino dei programmini sul web che riescono automaticamente a compiere queste incursioni. È incredibile che nel 2019 possano esserci ancora queste vulnerabilità strutturali su siti dello Stato dove transitano dati e informazioni che impattano non solo sulla sicurezza nazionale, ma anche su quella delle nostre imprese e dei cittadini in generale. Bisognerebbe investire di più, ma non c'è la volontà di farlo».

v.d.g.