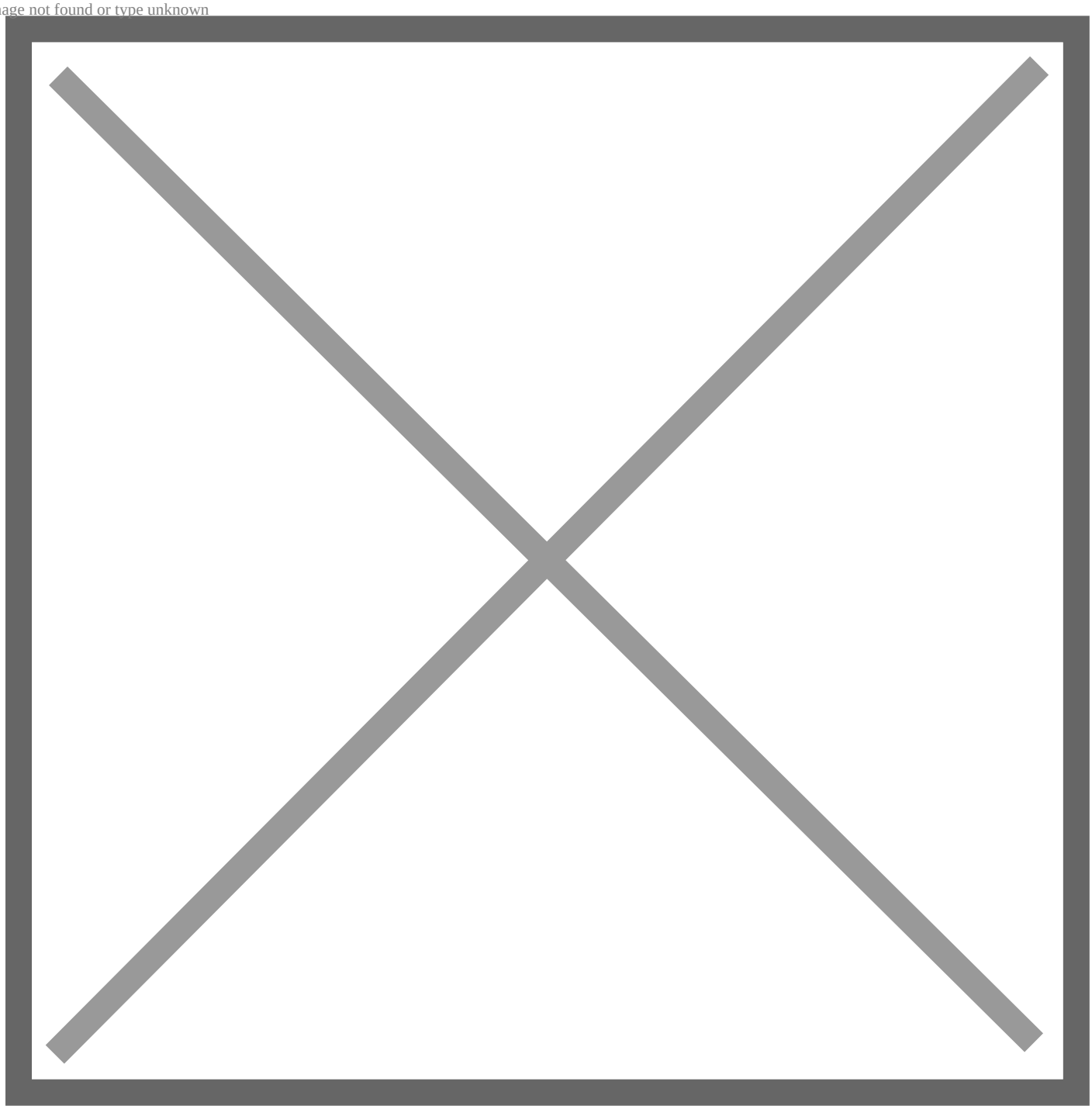
Image not found or type unknown



COREA DEL NORD

Cyberterrorismo, la nuova frontiera della guerra

ESTERI 21_12_2014

Un immagine dell'attacco informatico alla Sony

Image not found or type unknown

Il cyberattacco alla Sony Pictures "è un comportamento inaccettabile per uno Stato" afferma in una dichiarazione l'FBI puntando il dito sul regime di Pyongyang, unico sospetto nell'attacco informatico teso a sabotare la diffusione del film *The Interview* che fa il verso alla dittatura comunista asiatica e al suo leader, Kim Jong-un. Film prodotto dalla multinazionale nipponica che dagli anni '80 controlla i colossi statunitensi Columbia Pictures e Tristar Pictures, tra i più importanti produttori cinematografici del mondo.

Le indagini dell'Fbi hanno concluso che il governo della Corea del Nord è responsabile dell'attacco informatico che ha indotto Sony Pictures a ritirare il film dal mercato. Nell'affermare di aver raccolto prove sufficienti, il Federal Bureau of Investigation si è detto "molto preoccupato per la natura distruttiva di questo attacco contro un ente privato e contro i privati cittadini che hanno partecipato al lavoro". Atteso nelle sale americane a Natale, il film con James Franco e Seth Roger narra la

storia della tentata eliminazione di Kim Jong-un, leader assoluto della Corea comunista.

Per gli investigatori il cyber-attacco contro Sony sarebbe solo la punta dell'iceberg di una più vasta guerra informatica contro una serie di siti governativi. "Lo spionaggio sta accadendo a un ritmo che non abbiamo mai visto prima", riferisce alla *Cnn* Denise Zheng, vice direttrice del Center for Strategic and International Studies di Washington. Solo nell'ultimo anno i tentativi di violare i sistemi informatici delle agenzie federali statunitensi sarebbero stati 61 mila e il governo degli Stati Uniti non prende la minaccia alla leggera anche se in fatto di spionaggio elettronico il Datagate ha dimostrato come gli USA non siano certo solo vittime.

L'anno scorso Edward Snowden rivelò dal suo rifugio di Macao i dettagli del Datagate poche settimane dopo che la Casa Bianca aveva accusato direttamente la Cina di massicci attacchi informatici contro istituzioni e aziende statunitensi. Ieri il presidente Barack Obama ha definito "molto serio" l'attacco subito da Sony criticando la decisione della società giapponese di ritirare il film dalle sale definita "un errore". Sony Pictures in realtà ha dichiarato che sta cercando vie alternative per distribuire il film *The Interview*, aggiungendo di aver soltanto rinunciato a mandarlo nelle sale a Natale dopo che le principali catene di cinema lo avevano cancellato dalla programmazione.

I**ntervistato dalla *Cnn*, il presidente della società, Michael Lyndon**, ha dichiarato che la sua compagnia "non si è arresa" a Pyongyang, ma ha deciso soltanto di non distribuire la pellicola per Natale. Non c'è dubbio però che la deterrenza di nuovi attacchi cyber avrà il suo peso nelle decisioni di Sony che a causa degli hacker ha subito danni per mezzo miliardo di dollari sondo la stima di un esperto, Hemanshu Nigam, fondatore della società di consulenza per la sicurezza informatica SSP Blue.

Di fatto, tutte le sicurezze informatiche dell'azienda sono state violate e sono finiti on-line 5 film non ancora usciti sugli schermi, i dati personali di 47mila dipendenti, documenti riservati come la sceneggiatura del prossimo film di 007/ James Bond e una serie di e-mail del management di Sony.

Pyongyang però non ci sta a farsi mettere all'angolo. Nega ogni responsabilità e propone agli USA un'inchiesta congiunta sulla vicenda. "Poiché gli Usa diffondono accuse senza fondamento e ci diffamano proponiamo loro di svolgere un'inchiesta congiunta" ha sottolineato il ministero degli Esteri. "Senza arrivare a ricorrere perfino alla tortura come ha fatto la Cia - ha riferito non senza ironia l'agenzia di stampa di Stato Kcna - abbiamo i mezzi per dimostrare che non abbiamo niente a che fare con questo incidente". La vicenda va del resto inserita nei sempre più difficili rapporti tra la Corea

del Nord e la comunità internazionale dopo che l'Assemblea Generale dell'Onu ha votato per accusare il regime di Pyongyang di crimini contro l'umanità alla Corte Penale Internazionale dell'Aja. Kim Jong Un ha risposto con l'annuncio che aumenterà "gli sforzi per migliorare in ogni modo le sue capacità di auto-difesa incluse le forze nucleari".

Forse anche per le valenze militari della crisi con i nordcoreani Washington ha fatto sapere che sono in valutazione diverse opzioni di risposta al cyber-attacco alla Sony comprendenti sanzioni economiche, bancarie e l'inclusione della Corea del Nord nella lista dei paesi sponsor del terrorismo. Nella conferenza stampa di fine anno il presidente Obama ha detto che gli Usa risponderanno al cyberattacco contro Sony "in modo proporzionato, nelle modalità e nei tempi che decideremo".

Non si possono quindi escludere rappresaglie informatiche tese a minare proprio programma atomico di Pyongyang. Negli anni scorsi il virus Stuxnet. Messo a punto a quanto pare da statunitensi e israeliani, devastò le centrifughe che arricchivano l'uranio iraniano sabotando e ritardando il programma nucleare di Teheran.

Obama ha sottolineato che gli Stati Uniti hanno rinforzato l'infrastruttura della sicurezza informatica gestita dal Cyber Command di Fort Meade, in Maryland, dove operano migliaia di esperti per elaborare strategie difensive e offensive.

L'arma cibernetica è ideale per colpire avversari e rivali provocando danni devastanti ma di impatto esteriormente minore di un'azione bellica classica. La Russia paralizzò la rete informatica statale dell'Estonia nel 2007 e della Georgia durante il conflitto del 2008. Cina e Taiwan si sfidano costantemente lanciandosi reciprocamente virus e contro-virus tesi a paralizzare le rispettive reti militari mentre Pechino pare debba ai suoi hacker lo sviluppo dei nuovi aerei invisibili ai radar grazie a tecnologie rubate dalle banche dati di Pentagono e Lockheed Martin relative ai jet americani F-22 ed F-35.

La Nato si è dotata di tre strutture per la guerra informatica: Nato Computer Incident Response Capability a Bruxelles, Nato Rapid Reaction Team a Mons (Belgio) e NATO Cooperative Cyber Defence Command a Tallinn (Estonia).

Anche i singoli Paesi europei cominciano a investire in tecnologie di protezione e di attacco, specie la Gran Bretagna dove nel 2012 il 93% delle grandi società e il 76% delle piccole aziende subì intrusioni informatiche. I dati sugli attacchi sono del resto in continua crescita e nel 2013 la sola Marina degli Stati Uniti ha registrato ben 110mila attacchi contro la sua rete informatica.

Del resto l'arma cyber costa molto meno di un sistema d'arma convenzionale (aerei, portaerei, missili) ed è in grado di penetrare le difese informatiche che oggi gestiscono gli arsenali. Un virus informatico può paralizzare un'intera linea di aerei da guerra o una forza armata al completo a costi limitati allo sviluppo di un virus e al compenso degli hacker i cui eserciti al servizio degli Stati si ingrossano di anno in anno.

Per questo la cyber war è alla portata anche dei Paesi meno ricchi e che non possono permettersi strumenti militari convenzionali sofisticati. Anche per questa ragione il capo della National Security Agency americana, vice ammiraglio Michael Mc Rogers, ha detto la scorsa settimana che "la questione non è se, ma quando ci troveremo di fronte al primo attacco cibernetico di proporzioni catastrofiche", in grado cioè di paralizzare le reti informatiche che gestiscono ogni settore degli apparati pubblici dalla difesa alla sanità, dal fisco all'erogazione di energia e acqua.