convegno
"STRATEGIA DI DIFESA CONTRO LA MINACCIA CIBERNETICA"
organizzato dal Centro Studi Difesa e Sicurezza
Camera dei Deputati, Sala dei Gruppi Parlamentari
Roma, Via Campo Marzio 72
12.03.2013

La cyber security è legge anche in Italia e possiamo quindi entrare nel novero dei Paesi che hanno deciso di affrontare in maniera ortodossa il problema della difesa digitale.

L'ultimo articolo del provvedimento, però, spegne l'entusiasmo, laddove si dice **"Dal presente decreto non derivano nuovi oneri per il bilancio dello Stato"**. E lo stupore è amplificato se si confronta la situazione italiana con il ben più agguerrito piano di intervento britannico.

105 milioni di sterline due anni fa, 155 l'anno scorso, 180 per questo esercizio e 210 per quello 2014-15: è questa la progressione degli **stanziamenti aggiuntivi per complessivi 650 milioni di sterline che alimentano strategia e programma del Regno Unito**.

E' la forza della consapevolezza del rischio. La relazione del National Audit Office (NAO) parla chiaro. **Solo nel 2011 la Gran Bretagna ha contabilizzato 44 milioni di attacchi informatici**, l'80% dei quali poteva essere evitato con semplici operazioni di "igiene" di computer e reti. Nel mirino chiunque: istituzioni, aziende, professionisti. Il "cyber-attack" già nel 2010 era diventato uno dei quattro rischi nazionali. E non c'è da rimaner sorpresi visto che lo **specifico danno annuo stimato per il Regno Unito oscilla secondo il NAO tra i 18 e i 27 miliardi di sterline**.

Sono cifre impressionanti che però scompaiono dinanzi a quel trilione di dollari di perdite indicati già nel 2009 da Obama e rammentati l'estate scorsa dal generale Keith B. Alexander, direttore della National Security Agency (NSA) e comandante dell'US Cyber Command.

Qualunque sia il costo derivato dagli attacchi cibernetici, è fin troppo ovvio che si debba esser pronti ad impiegare denaro per arginare e contrastare il problema.

Proprio in tale ottica Telecom Italia ha investito nella sfera culturale, ha puntato sulla modernità della propria struttura e ha individuato gli strumenti per non duellare a mani nude.

L'azione di contrasto è assicurata dalla disponibilità di due Security Operations Center, dislocati uno a Roma e l'altro a Milano. Poli di eccellenza di livello internazione, non si limitano a dar corso ad attività di ricerca e studio ma sono costantemente impegnati in prima linea per monitorare la situazione, identificare possibili minacce, ipotizzarne il possibile impatto, individuare le soluzioni maggiormente tempestive, fronteggiare eventuali attacchi, puntare sul più sollecito ripristino delle condizioni di normalità.

I Security Operations Center di Telecom Italia – nel solo mese di gennaio 2013 - hanno rilevato e risolto 359 incidenti di sicurezza. La solidità dell'assetto di protezione ha fatto sì che non ci siano mai state situazioni ad alta criticità e soltanto 3 volte si sia dovuto riconoscere un rischio di livello medio.

L'adeguatezza dei SOC è comprovata dal brillante superamento di una recente grave emergenza a livello internazionale. Qualche mese fa si è assistito, infatti, al più imponente tentativo di dirottamento

collettivo degli utenti Internet: una micidiale contaminazione di milioni di computer aveva destabilizzato la capacità di orientamento degli strumenti di navigazione online. Poche righe di codice maligno erano riusciti a modificare il percorso di instradamento degli apparati in Rete: nel mirino del crimine tecnologico erano finiti i DNS (i Domain Name Systems) ovvero quei computer che – convertendo i nomi dei siti digitati alla tastiera in numeri IP – permettono a persone, aziende ed enti di spostarsi su Internet. La modifica fraudolenta dell'indicazione del server DNS sulle macchine degli utilizzatori finali avrebbe portato al caos e in molti Paesi si sono vissuti momenti di estrema difficoltà. Il SOC di Telecom Italia ha pensato di mettere subito a disposizione di tutti una procedura che era in grado di allertare chi sfortunatamente era incappato nel micidiale "DNS Changer", evitando conseguenze nefaste a chi era rimasto infettato dallo specifico malware.

L'oculata gestione di migliaia segnalazioni di sicurezza e l'idonea soluzione di centinaia di incidenti segnano in maniera inequivocabile il totale controllo della situazione, pur nella consapevolezza che l'inarrestabile sviluppo di iniziative offensive non permette soste. Per migliorare le performance in termini qualitativi e quantitativi abbiamo implementato una rete di "honeypot", che consente di recepire lo sviluppo di software maligni capaci di contaminare sistemi informatici di qualsiasi "taglia", e di conoscere anzitempo ogni nuove modalità di aggressione e prevedere anche le più impensate dinamiche di attacco. Gli honeypots sono sistemi che vengono esposti per esaminare il comportamento di malintenzionati che tentano di accedere indebitamente o di fare danno senza sapere di trovarsi alle prese con una sorta di trappola che registra ogni dettaglio e contribuisce ad incrementare i modelli di sicurezza già predisposti.

Analogamente a quanto si rivela all'estero, Telecom Italia ha riconosciuto una costante crescita dei tentativi di "denial of service", ossia di operazioni offensive volte a determinare la paralisi dei sistemi informatici e delle reti di trasmissioni dati: il mandare fuori servizio, magari per un banale "overload", il cervello di una organizzazione può avere effetti devastanti anche quando ci si trovi dinanzi ad un semplice pur pesante rallentamento delle funzioni. Nel 2012 I SOC di Telecom Italia hanno affrontato con successo 1378 attacchi DDOS e hanno respinto 1009 attacchi a sistemi informatici esposti su Internet.

L'analisi del fenomeno del Distributed Denial of Service e la progettazione di rimedi ad hoc di accertata validità hanno permesso a Telecom Italia di generare un'apposita offerta: il Servizio di DDOS Mitigation, che non ha tardato a farsi apprezzare dalle Istituzioni e dai gestori di infrastrutture critiche, si sta rivelando in grado di drenare la rete a dispetto delle più massicce operazioni di intasamento e saturazione.

Altro spettro è quello dei "data breach": le incursioni sempre più spesso mirano a sottrarre dati e il cyber spionaggio ha incentivato intere Nazioni a militarizzare il contesto e a schierare battaglioni di hacker inquadrati in reparti speciali al fianco di quelli convenzionali.

Uno studio condotto dal Verizon RISK Team in collaborazione con la Australian Federal Police, la Dutch National High Tech Crime Unit, il CERT irlandese, la Police Central e-Crime Unit londinese e lo United States Secret Service ha riconosciuto ben 855 casi di intrusione fraudolenta in database sensibili e la gravissima compromissione di oltre 174 milioni di record personali nel 2012.

Si tratta di un fenomeno in crescita che mette a repentaglio la riservatezza di informazioni industriali, commerciali, istituzionali e dei singoli cittadini. A correre simili gravi rischi non sono soltanto le aziende ma anche e soprattutto gli enti pubblici che gestiscono imponenti moli di dati di estrema criticità.

Il continuo variare – nei modi e nell'intensità – degli attacchi rende difficile una adeguata difesa per le piccole realtà e un **cloud computing certificato** può essere la prima soluzione, addirittura "ambientale", al problema della cyber war. **L'idea di Nuvola Italiana** è nata proprio per garantire l'offerta di un servizio che offrisse non solo vantaggi tecnologici, ma fosse in grado di assicurare la serenità operativa di chi vuole sfruttare le più moderne soluzioni di automazione senza dover temere un pericoloso arrembaggio digitale.

La migrazione di dati e applicazioni su una piattaforma blindata in maniera professionale equivale al ricorso ad una specie di moderno castello. Se il fossato è presidiato da specialisti e il ponte levatoio è solido quanto basta, la partita con chi attacca si può ancora giocare.

La cronaca parla fin troppo chiaro. Anche Società ritenute inviolabili possono cadere vittima di cyber-attacchi. Microsoft, Facebook, Twitter, Apple. New York Times, Wall Street Journal, Federal Reserve sono stati i bersagli degli ultimi mesi, ma **la vulnerabilità di chi si espone sul web potrebbe essere marginale rispetto la criticità dei sistemi nevralgici isolati da Internet e considerati al sicuro**. Spesso si dimentica che il nemico può celarsi in seno alla medesima organizzazione destinataria di un attacco o di un sabotaggio: **le rilevazioni dei SOC di Telecom Italia consentono di**

riconoscere che almeno il 12% degli incidenti ha origine all'interno della stessa realtà che costituisce il target.

Un modello di difesa di Stato non può quindi prescindere dalla realizzazione di condizioni di base adeguatamente protette, come non può non avvalersi della competenza, dell'esperienza e dei mezzi di un player che queste trincee conosce a perfezione.

C'è molto da fare. E bisogna farlo subito.