

In Usa è guerra ma solo telematica

SAN JOSÉ (CALIFORNIA) – Si chiama Cyberstorm ed è un'esercitazione che riproduce gli effetti di un cyber-conflitto. Il progetto è frutto della collaborazione tra pubblico e privato sul fronte della e-sicurezza. Di cui si è parlato alla Rsa 2006, l'evento di settore più importante al mondo **DI GIANLUCA GRECHI**



Il successo per presenza di aziende e per numero di visitatori di Rsa 2006, la più importante fiera sulla sicurezza nella tecnologia che si è tenuta a San José in California, dimostra come il tema della security sia tra i più sentiti tra le aziende e tra gli operatori della Pa americana, che hanno approfittato della presenza dei massimi esperti del settore, tra

cui Bill Gates, per fare il punto della situazione e conoscere le nuove soluzioni di difesa disponibili. Dai dati presentati è emerso come il governo federale americano abbia compiuto passi da gigante in particolare nella raccolta di informazioni che sono alla base delle scelte di sicurezza. La collaborazione tra settore pubblico e privato è culminata in Cyberstorm, un'e-

sercitazione che riproduce gli effetti di una guerra telematica dove operatori pubblici e privati si sono affiancati in stretta alleanza per sconfiggere una serie di attacchi informatici e reali. Uno scenario da guerre stellari che ha permesso di testare sul campo la preparazione delle strutture federali e il loro coordinamento con le diverse agenzie preposte alla difesa delle infrastrutture strategiche e le più grandi società americane. L'esercitazione, che si è



www.iss.net/rsa_2006

svolta lo scorso febbraio, è stata



www.dhs.gov

organizzata dalla neonata Ncsd (National cyber security division) che fa parte del Department of Homeland Security, il dipartimento creato dall'amministrazione Bush all'indomani dell'attacco terroristico dell'undici settembre e ha visto il debutto del

National cyber response coordination group, il gruppo di coordinamento nazionale il cui compito è quello coordinare con prontezza la risposta agli attacchi informatici. Uno dei problemi che l'Ncsd ha contribuito a risolvere è quello della circolazione delle informazioni tra pubblico e privato. Infatti, la maggiore lamentela sollevata a oggi dalle aziende private era che le informazioni raccolte e trasmesse all'Ncsd non erano poi condivise con gli operatori con la giustificazione di voler mantenere riservati dati che, se im-

propriamente diffusi, avrebbero potuto mettere a repentaglio la sicurezza nazionale. L'esercitazione digitale Cyberstorm ha per la prima volta cercato di dare soluzione a questo problema, coinvolgendo 115 agenzie pubbliche, private e internazionali, tra cui la Croce Rossa, che hanno dovuto coordinarsi per rispondere a ottocento "eventi" che richiedevano una reazione tempestiva. Nessuno dei partecipanti ha voluto esprimere commenti conclusivi sull'effettivo stato di preparazione della nazione a simili tipologie di attacchi anche perché nel test non erano stati coinvolti i provider di servizi di comunicazione via internet, che dovrebbero costituire le prime linee di difesa nella risposta a eventuali attacchi informatici.

Le aziende nel mirino

Rsa 2006 è stata anche la sede ideale per commentare una recente inchiesta su un campione di oltre duemila organizzazioni pubbliche e private realizzata dall'Fbi dalla quale è emerso che il 90% delle realtà intervistate ha subito lo scorso anno incidenti che hanno compromesso la sicurezza dei propri computer. L'indagine ha rivelato una diffusa evidenza di attività criminali online aventi per obiettivo organizzazioni americane, e nonostante una generale maggior attenzione e vigilanza solo il



Bill Gates

che essi provenivano dall'interno della propria organizzazione.

Più pericoli online

Se la diffusione degli attacchi informatici crea crescenti problemi alle aziende americane, anche l'utenza privata vive un momento difficile. Sempre a Rsa è stata resa pubblica un'altra indagine, sponsorizzata da Ibm su un campione di settecento persone, dove emerge che il numero di persone che teme di restare vittima di un attacco informatico sia il triplo (26%) di coloro che temono di subire un crimine nel mondo reale (8%). La "paura cibernetica" sta

"furto d'identità" citato dal 43% del campione, seguito dalla "perdita di denaro" (24%). Per difendersi il 70% ha dichiarato di cercare sui siti visitati simboli e anche marchi che siano in qualche modo garanzie di sicurezza.

Le soluzioni di Rsa

Per rispondere alle istanze di sicurezza del pubblico e risolvere i problemi evidenziati da organizzazioni pubbliche e private, le aziende presenti a Rsa 2006 sembrano orientate verso due soluzioni: l'uso di "chiavi" sicure e la realizzazione di nuovi processi di autenticazione che superino il concetto tradizionale di password. Le aziende leader del settore, tra cui Microsoft, Verisign e Ibm, stanno investendo fortemente in tecnologie che siano in grado di individuare con tempestività o addirittura



prevenire attività fraudolente sulla rete. Ibm ha annunciato un servizio per le organizzazioni pubbliche e per le aziende che analizza il comportamento di utenti individuali e di gruppi di utenti per evidenziare comportamenti sospetti o inusuali quali per esempio come, dove e quando un utente si collega a un network e a che tipo di applicazioni accede. L'interesse verso queste soluzioni è testimoniata da una serie di recenti acquisizioni

Un'inchiesta dell'Fbi ha evidenziato che il 90% delle oltre duemila organizzazioni intervistate ha subito lo scorso anno incidenti che hanno compromesso la sicurezza dei propri computer

9% delle realtà colpite da attacchi informatici li ha poi riportati all'agenzia di investigazione federale. Tra i più comuni incidenti denunciati primeggiano i virus, di cui è rimasto vittima l'83% degli intervistati, seguiti dallo spyware (programmi software che si nascondono nel computer e spiano l'attività che viene effettuata sul pc) che ha colpito il 79% del campione, mentre il 20% ha denunciato azioni di sabotaggio del proprio network. Le perdite totali stimate dal 64% delle società oggetto dello studio ammontano a 32 milioni di dollari, di cui ben 12 causati da virus. Il fatto più sconcertante è l'origine degli attacchi, visto che il 44% ha dichiarato

già influenzando il comportamento della popolazione visto che il 37% degli intervistati ha ammesso di non essere disposto a fornire il proprio numero di carta di credito durante una transazione online, la stessa percentuale che ammette di non fidarsi a usare servizi di online banking o le reti wireless disponibili nei locali pubblici o negli aeroporti. Il reddito sembra essere un fattore discriminante se si considera che il 34% delle persone che ammette di temere più un crimine virtuale di uno reale ha un reddito superiore ai cinquantamila dollari, contro il 12% di chi si colloca al di sotto di tale soglia. Ciò che la gente teme di più è il



che ha investito il settore: la società Rsa ha rilevato per 145 milioni di dollari la Cyota, leader nella segnalazione di attività fraudolente nel settore dei servizi bancari e finanziari, mentre Verisign ha comprato per 12 milioni di dollari Snapcentric, operante nello stesso settore e focalizzata sul settore delle carte di credito. Nel dibattito è intervenuto anche Bill Gates che ha evidenziato l'obsolescenza del concetto di password che saranno sostituite da nuovi dispositivi come le chiavi Usb o le security card che consentono all'utente di essere univocamente riconosciuto dal sistema. ■

GIANLUCA GRECHI