Questo articolo è apparso sul Corriere del Ticino di martedì, 13 febbraio 2001 nella sezione Informatica e Sicurezza

Internet: gli attacchi informatici

Attualmente ne sono vittime sia i grandi siti web sia i singoli utenti

Silvano Marioni **www.marioni.org**

Le possibilità di comunicazione di Internet hanno favorito la nascita di nuove opportunità commerciali, come ad esempio il commercio elettronico, ma sono anche state utilizzate da malintenzionati che hanno potuto mettere a segno una serie di crimini impensabili fino a pochi anni fa. In particolare nel corso dell'anno 2000 abbiamo assistito ad una serie di attacchi emblematici che hanno fatto sorgere numerosi interrogativi sulla sicurezza della grande Rete. Durante il mese di febbraio sono venuti alla ribalta gli attacchi di Denial of Service, una forma di attacco non particolarmente sofisticato ma in grado di bloccare un sito Web. Questo attacco ha colpito siti importanti quali eBay, Amazon, CNN, e Yahoo, causando danni finanziari importanti. Nel mese di maggio il virus I LOVE YOU ha colpito decine di milioni di computer in tutto il mondo, presentandosi come un curioso messaggio di amore proveniente da una persona conosciuta. Anche in questo caso la rimozione del virus da tutti i computer infettati ha avuto costi difficilmente calcolabili. Questi esempi sono rappresentativi delle due principali tipologie di attacchi presenti attualmente su Internet. Gli attacchi contro i siti Web e gli attacchi contro gli utenti della rete. Nel caso degli attacchi contro siti Web le tipologie vanno dal vandalismo con motivazioni ideologiche, come nel caso degli attacchi di Denial of Service contro i siti emblematici della New Economy, a più tradizionali forme di crimine come il furto di oltre 55'000 numeri di carte di credito dal sito Creditcard.com o lo spionaggio industriale, come nel caso dell'attacco al sito di Microsoft. Gli attacchi contro utenti della rete sono finalizzati ad istallare dei virus o altri software "maligni", che prendono il controllo del computer. Questi programmi spesso non creano danni apparenti ma presentano il rischio di distruzione o spionaggio dei dati personali. Il caso del virus I LOVE YOU è stata una grande seccatura ma in sé non ha creato danni irreparabili. Diverso è stato il caso dei clienti di una grande banca svizzera costretti a modificare in tutta fretta le loro modalità operative di home banking per evitare che un software "maligno" catturasse le password dei loro conti bancari e le inviasse, tramite Internet, a qualche malintenzionato in qualche parte del mondo. Ma come reagire a queste minacce? La protezione di un sito Web è sicuramente un'attività molto sofisticata che richiede competenze professionali specifiche e che difficilmente potrebbe essere descritta in queste poche righe. Per quanto riguarda la protezione dei computer degli utenti collegati alla rete Internet sono possibili alcune contromisure. Innanzitutto è necessario istallare sul computer un programma antivirus ed è importante aggiornarlo regolarmente. Questa precauzione permette di proteggere da virus o da programmi "maligni" che dovessero arrivare dall'esterno, ad esempio tramite posta elettronica. Un altro tipo di programma che si sta rivelando sempre più importante è il Personal Firewall, utile soprattutto se si effettuano dei collegamenti a Internet particolarmente lunghi. Durante questi periodi il computer può essere intercettato e subire degli attacchi. Il Personal Firewall crea uno schermo di protezione e impedisce che qualcuno possa entrare sul computer per spiare o istallare software "malizioso". Ma la protezione del proprio computer non deve basarsi solo sull'acquisto di programmi ma soprattutto sull'acquisizione di buone abitudini. Ad esempio è importante utilizzare delle password che siano facili da ricordare ma difficili da indovinare. Per la protezione dei dati personali è utile avere password differenti da quelle che genericamente vengono richieste da numerosi siti Internet. Per quanto riguarda la posta elettronica, è importante valutare con prudenza i messaggi che ci sembrano dubbi o sospetti e non aprire i files allegati. Su Internet siamo di fronte a nuovi crimini che si manifestano in modo non sempre comprensibile al grande pubblico. Da un lato le notizie che ci giungono dai media sono spesso superficiali e rischiano di creare dei falsi allarmismi e far sorgere timori ingiustificati. Dall'altro le società attive nelle nuove tecnologie non amano pubblicizzare i problemi della Rete, semplificando e minimizzando i rischi che sono presenti e reali. In una società sempre più basata sull'informazione e la comunicazione, è necessaria più oggettività e più attenzione per un problema come quello della sicurezza. Solo con la fiducia e la trasparenza sulla sicurezza dei dati personali sarà possibile convincere le persone ad utilizzare appieno le nuove opportunità offerte dalla Rete.

La complessità dei sistemi informatici è causa della loro insicurezza

Intervista con il guru mondiale della sicurezza informatica Bruce Schneier

Bruce Schneier è sicuramente una delle persone più rappresentative nel modo della sicurezza informatica a livello mondiale. Fondatore e direttore tecnico della società Counterpane, è stato consulente di grosse aziende quali Microsoft, Citibank o di enti governetivi quali la Casa Bianca o la National Security Agency. Ha consolidato la sua fama anche grazie ai numerosi libri. Tra questi possiamo citare "Applied Cryptography", una vera e propria bibbia sul tema della sicurezza informatica pubblicata in oltre 130'000 copie, e il suo ultimo libro "Secrets & Lies" in cui esamina in modo critico come è gestita oggi la sicurezza su Internet. Abbiamo chiesto a Bruce Schneier il suo punto di vista sulla sicurezza informatica e cosa prevede per il futuro.

Anche se i media trattano ormai con regolarità i problemi di sicurezza di Internet e delle altre tecnologie che utilizziamo quotidianamente, sono poche le persone che pensano che questi problemi li riguardino direttamente. Non pensa che sia utile dare maggiore importanza agli aspetti di sicurezza della tecnologia? Come pensa si possa aumentare la consapevolezza di questi problemi.

La sicurezza è una componente fondamentale di ogni società e la sicurezza di una tecnologia è estremamente importante se si vuole che questa tecnologia sia accettata e utilizzata.
La produzione tecnologica è spinta dalle caratteristiche, dalle prestazioni, dalla velocità. Non ci sono standard per la qualità o per la sicurezza e non ci sono responsabilità nel caso di software non sicuro. Per questo non esiste un incentivo economico per creare prodotti di alta qualità. C'è invece un incentivo economico per creare il livello di qualità più basso che il mercato riesce ad accettare.
E fintanto che non ci sarà la domanda dei clienti per una qualità più alta e una migliore sicurezza questo non cambierà. Personalmente vedo due scelte per il futuro. La prima alternativa consiste nell'accettare consapevolmente la situazione attuale e imparare a gestire la sicurezza. L'altra possibilità consiste nel ridurre le esigenze, semplificare e cercare di aggiungere delle procedure di sicurezza. I clienti non arriveranno a chiedere questo – l'argomento della sicurezza è troppo complesso per essere recepito direttamente – ma potrebbero arrivarci dei gruppi di opinione, delle organizzazioni di difesa dei consumatori. Non credo comunque che questa ipotesi possa realizzarsi tanto presto perché le persone non vorranno privarsi delle prestazioni e dei modi d'uso a cui si sono abituati e non vorranno essere limitate nelle loro scelte.

Nel suo libro "Applied Cryptography" lei presenta un mondo in cui le informazioni sono mantenute sicure per sempre, grazie alle regole matematiche della crittografia.

Nel suo ultimo libro "Secrets & Lies" lei contraddice queste tesi, criticando certezze che sono ormai considerate fondamentali nella nostra società tecnologica

Ho cambiato il mio messaggio perché oggi la maggior parte delle insicurezze su Internet non hanno niente a che vedere con la crittografia. Se pensiamo ad attacchi quali Buffer Overflows, vulnerabilità degli script CGI, Denial of Service, cavalli di Troia e virus, ci rendiamo conto che hanno poco a che vedere e non possono essere risolti con un uso corretto della crittografia.
La sicurezza globale di un sistema è determinata dall'anello più debole della catena e questo non è in genere la crittografia. Per esempio non importa che tipo di algoritmo crittografico si utilizza se poi ci lasciamo convincere a comunicare la nostra password al primo sconosciuto che ci chiama al telefono. Il punto fondamentale da comprendere è che la sicurezza non è un prodotto ma un processo. Non è qualcosa che si può aggiungere al termine dello sviluppo di un sistema. Per avere un sistema sicuro è fondamentale comprendere le minacce reali e progettare le opportune contromisure fin dall'inizio. Non sono necessarie soluzioni perfette ma nemmeno sistemi che possono essere scardinati al primo attacco.

La crittografia è uno strumento fondamentale per garantire la riservatezza dei dati personali o per tutelare i diritti umani nei regimi non democratici. Che cosa pensa dell'utilizzo emergente della crittografia da parte di organizzazioni criminali, terroristi, pedofili e delle nuove sfide che questo crea per gli organismi di tutela della legge?

Nel mio libro "Applied Cryptography" ho scritto 'La crittografia è troppo importante per essere lasciata ai governi. Sono ancora di questa opinione, anche se in un senso più generale. La sicurezza è troppo importante perché sia lasciata semplicemente a qualsiasi organizzazione. Ed è troppo personale perché sia lasciata ad una sola organizzazione che ne diventi arbitro.

Penso che l'utilizzo criminale della crittografia sia un problema, ma siamo di fronte ad un problema universale. Tutte le tecnologie possono essere utilizzate in modo onesto o disonesto e la crittografia non fa eccezione. Personalmente io credo che il valore sociale della crittografia e la sicurezza informatica saranno in grado di tenere alla larga i disonesti.

Oggi la tecnologia ci offre più opportunità e più scelte ma sta diventando sempre più complessa. Lei pensa che questo possa creare maggiori problemi di sicurezza e che cosa prevede per il futuro?

La complessità dei nostri sistemi informatici è la causa diretta della loro insicurezza. Le tecnologie digitali sono state caratterizzate da una serie infinita di innovazioni, conseguenze non previste e attese, e non c'è ragione di pensare che non sarà così anche in futuro.
Come consumatore penso che questa complessità sia molto bella. Ci sono più scelte, più possibilità, più cose che posso fare. Come professionista della sicurezza penso che tutto ciò sia terrificante. La complessità è la peggior nemica della sicurezza. Questo è stato vero fin dall'avvento dei primi computer e penso continuerà ad esserlo anche in futuro. E fintanto che il cyberspazio continuerà ad essere sempre più complesso sarà sempre meno sicuro.