Questo articolo è apparso sul Corriere del Ticino di lunedì, 28 febbraio 2005 nella sezione Primo piano

Sicurezza informatica e vita privata

Sono sempre di più le nostre informazioni personali archiviate su computer e agende elettroniche: sappiamo davvero cosa ciò significa e siamo in grado di tenerle al sicuro?

Silvano Marioni **www.marioni.org**

È di questi giorni la notizia che colossi dell'e-commerce come eBay e VISA stanno creando insieme a Microsoft un database per registrare indicazioni utili a identificare le possibili truffe su Internet. La valanga di messaggi non sollecitati sta infatti cominciando a minare la nostra fiducia di consumatori nel commercio elettronico e contemporaneamente a far temere per la sicurezza dei nostri computer.
Questa iniziativa - con altre simili - è tanto più significativa se consideriamo che è in atto un cambiamento lento e graduale ma inarrestabile nel modo di trattare le nostre informazioni personali. Lettere, fotografie, filmati, messaggi, indirizzi, fino a ieri gelosamente custodite nei nostri cassetti vengono ora archiviati sempre più spesso su computer, telefonini e agende elettroniche.
Grazie alle tecnologie digitali parte della nostra vita privata sta migrando in formato elettronico senza che ci rendiamo conto di cosa questo possa esattamente significare.
Un altro cambiamento viene da Internet che ci offre informazioni e servizi concorrenziali rispetto ai canali tradizionali ma di cui si cominciano anche a conoscere i rischi.
La combinazione di queste due situazioni ci mette di fronte a una nuova prospettiva: nella nostra vita privata possediamo sempre più beni informatici, siano essi informazioni, programmi o apparecchiature, e questi beni sono soggetti a dei potenziali rischi quando ci colleghiamo in rete. Siamo in grado di gestire la sicurezza dei nostri beni nel mondo reale, ma siamo altrettanto capaci di farlo nel mondo virtuale dell'informatica?

Dobbiamo imparare a riconoscere i rischi

Se i beni informatici non sono protetti come i nostri beni reali non è tanto per la mancanza di prodotti o di tecnologie di sicurezza, ma principalmente per la scarsa percezione dei rischi che abbiamo quando utilizziamo gli strumenti informatici oppure perché non sappiamo chiaramente come proteggerli.
Se vogliamo garantire la sicurezza dei beni informatici dobbiamo innanzitutto essere sicuri che nessuna persona o situazione ci impedisca di usare i nostri programmi e consultare i nostri dati nel momento in cui ne abbiamo bisogno.
Dobbiamo essere certi che i nostri computer, programmi e informazioni non siano soggetti a cambiamenti non autorizzati, siano essi intenzionali o accidentali. E da ultimo dobbiamo avere la garanzia che le nostre informazioni siano protette dalla consultazione da parte di persone non autorizzate e essere sicuri della riservatezza dei nostri dati personali.
In conclusione, per evitare di essere coinvolti in malversazioni o truffe informatiche, dobbiamo essere certi che quello che stiamo facendo sia veramente quello che pensiamo di fare, e avere la possibilità di verificarlo direttamente, così come facciamo nella vita reale.

Si può essere coinvolti in attività criminali

I potenziali nuovi rischi si presentano spesso in modo singolare ed inedito.
Ad esempio quando siamo collegati alla rete Internet non mettiamo a repentaglio solo la sicurezza dei nostri dati ma possiamo correre il rischio di essere coinvolti in vere e proprie attività criminali senza rendercene conto.
Contrariamente ai computer delle aziende, i computer di casa sono generalmente più vulnerabili alle aggressioni. In particolare i collegamenti permanenti ad Internet (ADSL o cable modem) danno tutto il tempo ad un intruso di scoprire i punti deboli del computer che, se non è adeguatamente protetto, può essere compromesso infettandolo direttamente e prendendone il controllo, come succede ricevendo un virus per posta elettronica.
A questo punto l'intruso può consultare o danneggiare le informazioni presenti sul computer compromesso, o lo può usare per portare attacchi verso altri siti all'insaputa del proprietario.
Attraverso il controllo di numerosi computer compromessi e la loro attivazione contemporanea, l'intruso può attaccare un sito bersaglio con richieste ostili che possono arrivare al punto di bloccarlo.
Oggi questa tecnica viene sempre meno utilizzata come «prova di bravura» da parte di chi riesce a fare questo tipo di attacco ma è diventato un vero e proprio mezzo di ricatto

utilizzato dalla criminalità informatica per estorcere denaro. In questo modo il proprietario del computer compromesso fa da paravento, nascondendo l'aggressore e diventando a sua insaputa complice nella sua attività criminale. Proteggere il proprio computer non è quindi solo una necessità per proteggere i propri dati ma anche una responsabilità per impedire la diffusione di attività criminali e garantire il corretto funzionamento di Internet.
Va detto che spesso chi ci vuole attaccare ha più successo sfruttando le nostre carenze comportamentali, che utilizzando gli strumenti tecnici più sofisticati.

Attenti alle truffe!
Il caso tipico è quello dello spam, la valanga di messaggi pubblicitari spazzatura che intasa le nostre caselle di posta elettronica, in cui c'è ampio spazio per chi cerca di mettere a segno delle vere e proprie truffe.
Sfruttando l'ingenuità delle persone, che stranamente aumenta quando si utilizza un computer, vengono proposte offerte che sembrano particolarmente allettanti quali vincite alle lotterie, programmi software a prezzi particolarmente bassi, o strane operazioni finanziarie.
In questi casi la regola principale è quella di essere sufficientemente prudenti e ragionevolmente diffidenti per tutti i messaggi di posta elettronica che provengono da sconosciuti e che fanno leva sull'avidità naturale dell'essere umano.
Un altro filone delle truffe fa leva sulla poca dimestichezza delle persone per la tecnologia. A questo ultimo caso appartiene il «phishing», termine che deriva dalla storpiatura della parola inglese fishing, pescare Questa tecnica permette infatti di pescare le informazioni finanziarie di una persona tramite l'invio di un messaggio, naturalmente falso, principalmente a nome di importanti istituti finanziari.
Questi messaggi sollecitano, ad esempio, l'accesso al sito di una banca, per una verifica dei dati oppure per controllare un addebito, e richiedono l'inserimento del nome utente e della password.
Il problema è che si è dirottati su un sito fasullo che si presenta esattamente come quello della vera banca e che permette ai malfattori di catturare tutti i dati necessari per accedere al conto del malcapitato.
Vi è anche da dire che le istituzioni finanziarie svizzere hanno adottato già da tempo una serie di misure che rendono difficile la truffa del phishing: generalmente oltre al nome utente e alla password, viene infatti richiesto un codice che cambia ad ogni sessione che è diverso per ogni cliente. Il problema si pone invece con i dati della carta di credito che, se comunicati incautamente, possono essere utilizzati dai truffatori per fare acquisti a nostre spese.
La protezione dalle truffe dipende dall'identificazione della controparte che ci contatta; se è sconosciuta dovremmo evitare di stabilire qualsiasi contatto. Nel caso di una controparte conosciuta sta a noi decidere se fornire i dati richiesti, ma attenzione a verificare che sia veramente chi dice di essere.

Cosa fare per proteggersi
Dobbiamo essere consapevoli che non basta adottare delle misure minime di sicurezza, quali ad esempio gli antivirus, i personal firewall o l'aggiornamento del software, ma è importante avere anche dei comportamenti prudenti e attenti ai possibili inganni.
Per chi volesse approfondire il tema della sicurezza informatica esistono numerosi siti di enti governativi, aziende e associazioni in cui l'argomento viene presentato in chiave comprensibile anche per il grande pubblico. Tre esempi in lingua italiana sono *www.melani.admin.ch*, il sito dell'Amministrazione Federale sulla Sicurezza dei computer e in Internet, *www.microsoft.com/italy/athome/security* il sito sulla sicurezza di Microsoft e *www.acsi.ch/sicurezza* il sito dell'Associazione delle Consumatrici della Svizzera Italiana.
In un settore in continua evoluzione come l'informatica anche le minacce cambiano continuamente. Essere coscienti che esistono dei rischi e che questi rischi possono cambiare nel tempo è un atteggiamento corretto e fondamentale per garantire la sicurezza informatica nella nostra vita privata.

Anche l'Ue si preoccupa di evitare «cyber-abusi»

intervista con Lorenzo Valeri, coordintore del progetto «e-aware»

Le tecnologie informatiche sono sempre più importanti per fornire i servizi ai cittadini e di conseguenza aumentano anche i timori di possibili «cyber-abusi».
La percezione della sicurezza informatica da parte dei cittadini è il tema del progetto eAware, una ricerca finanziata dall'Unione Europea con lo scopo di informare sui diritti e le responsabilità e promuovere un uso responsabile e sicuro degli strumenti informatici.
Ne parliamo con Lorenzo Valeri, coordinatore del progetto e responsabile per le attività di ricerca della

RAND Europe nel campo della sicurezza informatica e della privacy.

Ci può descrivere che cosa è il progetto eAware e quali sono i suoi scopi?
«L'obiettivo primario di eAware è stato quello di sensibilizzare i cittadini di 10 paesi europei al problema della sicurezza informatica. Insieme con i nostri partners, abbiamo organizzato eventi gratuiti aperti al grande pubblico dove i cittadini potevano interagire direttamente con esperti di sicurezza informatica per avere risposte ai loro dubbi, preoccupazioni, dilemmi su come proteggersi on-line. Tuttavia, il progetto è voluto andare oltre. Insieme con i miei collaboratori, abbiamo preparato una guida su come sensibilizzare il grande pubblico al problema della sicurezza informatica. In particolare, abbiamo identificato i canali da utilizzare per comunicare messaggi, come sviluppare questi messaggi e come valutare l'effettivo impatto di una simile campagna di sensibilizzazione. Per maggiori informazioni, i lettori possono consultare il documento: *http://www.clusit.it/whitepapers/eaware_practical_guide.pdf* »

La sicurezza informatica viene normalmente considerata come un problema che riguarda le aziende e non tanto i privati cittadini. Perché è importante sensibilizzare i privati su questo argomento?
«Internet fa parte della vita quotidiana di milioni di cittadini. Tuttavia, Internet non significa solo computer. Con lo sviluppo delle comunicazioni mobili e wireless, tutti oggi fanno parte del mondo Internet. In questo contesto, i cittadini sono da considerare il punto centrale per lo sviluppo della società dell'informazione. Devono aver fiducia nello strumento Internet o nel mondo wireless. Tuttavia, a differenza della aziende, i cittadini difficilmente riescono a «capire» la sicurezza informatica. Vogliono una guida che li faccia entrare in questo mondo, che li aiuti e li rassicuri».

Come fare per raccogliere l'interesse del grande pubblico sul tema della sicurezza informatica e quali sono i problemi che si incontrano?
«La questione centrale, e anche la sfida più difficile, è comunicare il problema della sicurezza informatica senza creare inutili paure. Bisogna informare bene. Purtroppo oggi i giornali parlano di sicurezza informatica mettendo insieme storie di paure, frodi on-line senza però indicare soluzione e risposte. In un prossimo futuro, bisogna ritrovare l'equilibrio nella comunicazione. Comunicare per far paura non è inutile. Comunicare per migliorare è invece quello che bisogna fare quando si parla di sicurezza informatica».

Come vede l'evoluzione dei rischi e quali misure sarebbe auspicabile prevedere per garantire una maggiore sicurezza informatica?
«Con l'arrivo del wireless, della banda larga e delle comunicazioni mobili, i rischi non potranno che crescere. Tuttavia, negli ultimi anni, la maggiore attenzione del mondo dell'Information Technology per la sicurezza ha fatto arrivare sul mercato nuove soluzioni e prodotti. Il problema, quindi, non è la mancanza di soluzioni, ma come aiutare il normale utente Internet ad utilizzarle al meglio. Ecco quindi la necessità di far pervenire al cittadino un'informazione vera e credibile sul problema della sicurezza informatica. Questo non lo devono fare solo le industrie ma in particolare strutture come centri di ricerca o università o organizzazioni "indipendenti"». S.M.