VareseNews

Sicurezza in Internet, la truffa è in agguato

Pubblicato: Martedì 26 Aprile 2005

Nel mare magnum di Internet si intensificano le minacce alla sicurezza dei dati personali: la colpa non è solo di software e sistemi vulnerabili, o dell'astuzia dei truffatori, ma spesso dell'utente stesso. Questo è il giudizio, in verità un po' disarmante, che emerge dalla prima mattinata di incontri al Lugano Communication Forum, denominata "**Security Day**" e dedicata alla discussione di tutte quelle fondamentali problematiche dell'Information and Communication technology (ICT) che si riferiscono alla tutela dei dati e dei sistemi da attacchi e violazioni di ogni genere. Nutrito il gruppo dei relatori che si sono succeduti sul palco, offrendo i loro punti di vista e le loro esperienze sulla situazione attuale in questo campo. Ad organizzare l'incontro erano **Clusis e Clusit**, **associazioni no-profit** (rispettivamente svizzera e italiana) che promuovono la sicurezza informatica in cooperazione con enti pubblici e aziende.

Dopo il saluto iniziale di **Walter Gianotti**, rappresentante Clusis per il Canton Ticino, il direttore sviluppo e piattaforma di Microsoft Svizzera **Stefano Santinelli** ha messo sul piatto i primi problemi. «Vi è sempre un tradeoff reciproco tra sicurezza, economicità e usabilità di un sistema" ha detto Santinelli. Con le ultime uscite di Microsoft, Windows 2003 Server e il Service Pack 2 per Windows XP, abbiamo dovuto privilegiare la sicurezza a scapito dell'usabilità. La sicurezza è diventata un problema industriale». Ormai gli attacchi da parte di abili **creatori di virus** si succedono a ritmo impressionante, e la finestra di vulnerabilità di ogni nuova release (edizione) di un software o di un sistema si amplia a dismisura: «Gli attacchi avvengono nel 99% dei casi quando il problema che li consente è già stato individuato e divulgato. Oggi, però, vengono sfruttati in pochi giorni, non dopo settimane come in passato. Poi ci si mettono anche gli utenti: le password vengono craccate con troppa facilità, in quanto brevi o prevedibili. Per testare l'attenzione degli utenti abbiamo anche provato a diffondere un finto virus con scritto: attenzione, questo è un virus! Ebbene, non ci crederete ma il 20% degli utenti l'ha aperto…». Il problema maggiore, oggi, non sono comunque i virus, ma lo **spamming** e il **phishing**, cioè il furto dei dati personali, quali ad esempio i codici di accesso ai conti bancari e simili.

In seguito **Donato Piffaretti** di BossLab ha portato l'esempio di una società che gestisce in outsourcing le problematiche della sicurezza e del **back office**, insistendo sulla triade confidenzialità, integrità e disponibilità dei dati come chiave di una buona gestione.

Gigi Tagliapietra del Clusit, invece, ha messo in luce in un intervento brioso e non privo di humor la necessità della convivenza e dell'integrazione tra l'information technology e l'amministrazione, e soprattutto del nesso strettissimo fra sicurezza e infrastrutture base come quelle elettriche, idriche o di trasporto. «Oggi i dati ***sono*** l'azienda – ha detto Tagliapietra -. Tutto è parte di un sistema integrato, in cui un attacco informatico tipo *denial of service* è altrettanto grave di un blocco totale della produzione: a volte, anzi, l'uno causa l'altro».

Servono dunque regole, e serve soprattutto che chi opera su dati e attività "sensibili" conosca

l'importanza di essi, per tenere alta la guardia. Sempre per il Clusit, **Stefano Quintarelli** ha esposto le meraviglie dell'**RFID tag**, una teconologia che sfrutta le onde radio per identificare con preicisione prodotti, ma anche persone. L'RFID tag funziona in base al principio dei transponder passivi, ormai miniaturizzati a dimensioni microscopiche e a costi irrisori, e tali da potere essere comodamente alloggiati in una banale tessera che si attiva al passaggio in un campo elettromagnetico. Questo, ovviamente, pone seri problemi di *privacy*, perché in teoria si potrebbe essere "tracciati" in permanenza con un sistema del genere. Va anche detto, però, che l'RFID è facilmente schermabile, volendo.
Terzo relatore del Clusit è stato il fisico **Andrea Pasquinucci**, che ha spiegato come in futuro le comunicazioni criptate saranno assolutamente sicure grazie alla **crittografia quantistica**. Questa, teorizzata già dal 1970, sfrutta le proprietà delle singole particelle elementari della materia (i fotoni, ad esempio) "traducendo" il loro stato in differenti valori di un singolo bit; e siccome **è impossibile osservare una singola particella senza modificarla**, per i principi della fisica submicroscopica, ogni intercettazione verrebbe subito notata. L'informatica, con la continua miniaturizzazione dei componenti, sta per cozzare contro questo **muro di indeterminazione quantistica**: la soluzione del futuro saranno i computer ottici, che utilizzeranno i singoli fotoni anziché i segnali elettrici su piste di rame, come ora. La combinazione pc ottico-crittografia quantistica dovrebbe cominciare a prendere piede tra **una decina d'anni** con i primi prototipi funzionali.
Dopo **Michele Albertini**, che ha esposto la legge sulla protezione dei dati personali (LPDP) vigente nel Canton Ticino, il consulente informatico del CISPP **Silvano Marioni** ha esposto i pericoli delle truffe online note **con** i nomi di **phishing** e **pharming**. Il phishing è una truffa tipica: con una falsa e-mail si invita l'utente a reimmettere i propri dati in una pagina Internet **falsificata**, in apparenza assolutamente **identica** a quella della propria banca, per esempio, con il rischio di vedersi rubare i codici d'accesso al conto. Per difendersi bisogna esercitare la massima vigilanza e **non usare mai i link contenuti nelle e-mail,** ma se del caso scrivere a mano l'indirizzo nell'apposita barra del programma di navigazione. Il pharming è una maligna evoluzione del phishing, che opera una redirezione dell'accesso a siti "normali", **"dirottando"** l'utente su un sito pirata (copiato dall'altro) e facendosene dare i dati personali. Per sfuggire a questa autentica **pirateria informatica** si possono utilizzare programmi che monitorano quanto avviene nel sistema, come ad esempio il nuovo **anti-spyware** di Microsoft, ma anche rendere di sola lettura il file **hosts** (presente in ogni pc) che contiene la "rubrica" degli indirizzi DNS, quelli che, dietro gli indirizzi "alfabetici" che conosciamo, costituisce il vero "indirizzario" pubblico di Internet. In conclusione **Edilberto Bottini**, per la **Symantec svizzera**, ha esposto le nuove prospettive dell'integrazione tra gli **antivirus** e lo **stoccaggio dati** (Symantec sta per unirsi a Veritas, leader del settore), con la quale non si dovrà più scegliere tra sicurezza e rapida disponibilità dei dati.
Redazione VareseNews
redazione@varesenews.it