Computer Underground

Ai virus informatici è intitolata questa rubrica, che ormai da oltre due anni segue il fenomeno cercando di fornire ai lettori informazioni utili e aggiornate al tempo stesso. Ma i virus non sono che uno degli aspetti di un problema ben più ampio, quello della sicurezza informatica, a sua volta parte di un discorso ancora più vasto e configurabile come un problema di volta in volta aziendale, infrastrutturale, sociale, etc. Iniziamo il 1993 tracciando un breve profilo di un problema scottante: quello della penetrazione non autorizzata nei sistemi informatici altrui, meglio nota (anche se impropriamente) come «hacking»

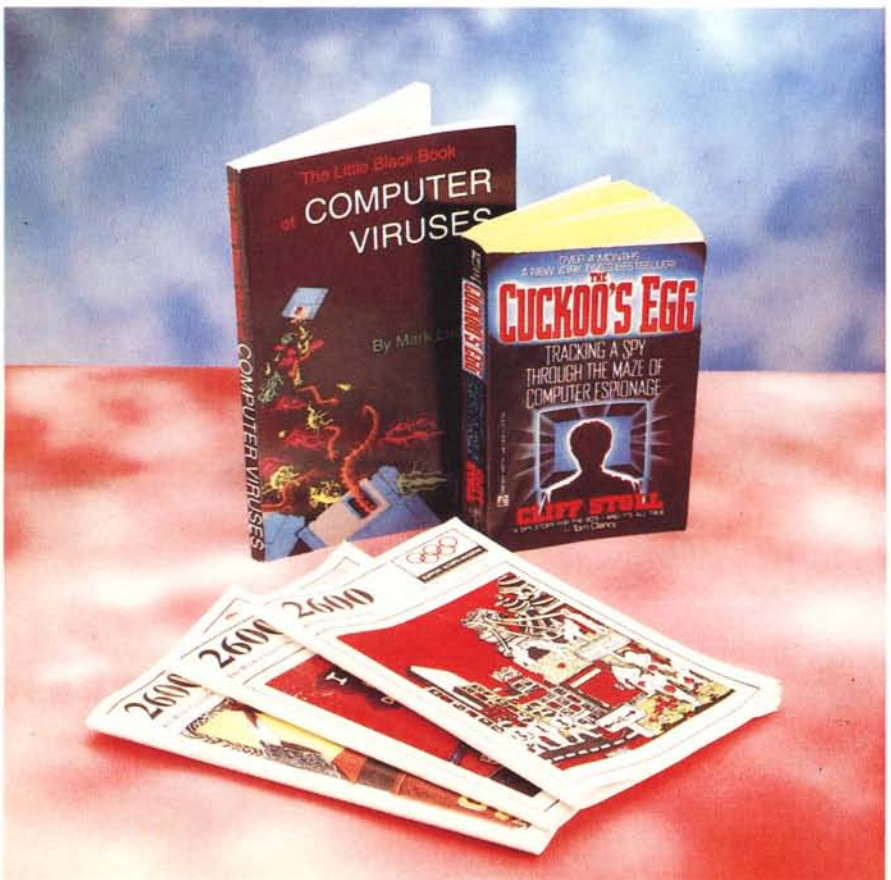
di Stefano Toria

Introduzione

Nato durante la seconda guerra mondiale per far fronte alle esigenze del calcolo balistico, il computer ben presto uscì dal ristretto campo di applicazione militare e si configurò come quello che è tuttora: uno strumento potente e flessibile per gestire ed elaborare masse di informazioni.

Tralasciando le considerazioni tecnologiche o comunque strettamente informatiche, se si guarda la storia del computer da questo punto di vista è necessario ragionare in termini di risorse e del relativo valore. La possibilità di concentrare e gestire economicamente grandi quantità di informazioni ha dato luogo a realtà economiche rilevanti e a fenomeni del tutto nuovi nella storia dell'umanità.

Sin dai primi tempi è risultato indispensabile pianificare, controllare e contabilizzare l'accesso e l'uso delle risorse di elaborazione e degli archivi; ragioni di riservatezza, di convenienza economica o politica hanno imposto la necessità di garantire la disponibilità delle risorse a taluni soggetti precludendola ad altri.



Si sono quindi sviluppati i sistemi di controllo degli accessi; controllo fisico nei primi tempi, che si è rapidamente trasformato in controllo logico, deputando allo stesso elaboratore la funzione di verificare il diritto all'accesso di ciascun soggetto che lo richiedesse.

La barriera all'accesso ai sistemi di elaborazione dovette essere rinforzata man mano che, con il progresso dei sistemi e con la loro diffusione, cresceva il numero delle persone in grado di servirsi degli elaboratori e interessati a farlo. Se in un primo tempo non erano necessarie particolari difese perché la difficoltà dell'uso degli elaboratori e la ridottissima diffusione della cultura informatica non ne determinavano il bisogno, in tempi successivi si dovette procedere alla costruzione di sbarramenti via via più sofisticati man mano che cresceva la potenza degli elaboratori, il quantitativo di informazioni strategiche consegnate al loro controllo, e il numero di persone in grado di servirsi degli elaboratori per accedere a queste informazioni.

L'evoluzione della tecnologia ha comportato da un lato l'aumento delle applicazioni degli elaboratori, dall'altro la maggiore diffusione degli strumenti e della cultura informatica. I grandi sistemi bancari, che gestiscono e movimentano quotidianamente enormi quantità di denaro, gli elaboratori scientifici che controllano processi impossibili da ge-

stire manualmente, per non parlare delle applicazioni militari, comportano livelli di riservatezza e di sicurezza molto avanzati. Ecco quindi che si definisce meglio il tema della sicurezza informatica: si tratta della necessità di garantire la disponibilità di risorse e informazioni a chi ne ha il diritto, per funzione o per contratto, e di precluderla agli altri.

Curiosità più o meno legittima

Qualsiasi problema di sicurezza si definisce in funzione di due elementi: della definizione di un evento dannoso e della probabilità che si verifichi. Se la Luna cadesse sulla Terra sarebbe una notevole catastrofe, ma la probabilità che questo accada secondo le leggi della meccanica celeste così come le conosciamo è talmente trascurabile da non destare preoccupazione. La probabilità che un vaso cada dal mio terrazzo sulla testa di un passante è ben più elevata, anche se il danno di per sé è più ristretto (perdita di una sola vita umana contro i diversi milioni nel caso della caduta della Luna); quindi ha senso che io prenda precauzioni per evitare che accada.

Al crescere della diffusione degli elaboratori e della cultura informatica è cresciuto parallelamente il numero di persone interessate a vario titolo ad accedere alle risorse di calcolo pur non avendone a rigore il diritto: dallo studente che ha esaurito la quota di tempo macchina concessa dal suo professore senza peraltro aver concluso il proprio lavoro, al curioso, al criminale che cerca di spostare importi di denaro o di prelevare segreti da vendere.

Particolarmente rilevante, per la diffusione del fenomeno, la schiera dei semplici curiosi.

Hacker

Se per molti l'elaboratore è uno strumento, per alcune persone è stato ed è un oggetto di passione, di un interesse particolare che prescinde dalle finalità per le quali esso viene impiegato e si concentra sulla macchina, sulle sue funzioni, sul suo uso. Alcuni sono divenuti talmente abili nell'uso e nella programmazione del proprio elaboratore da essere in grado di fargli svolgere compiti molto complessi senza particolari difficoltà, talvolta creando programmi che sono al tempo stesso brevi, complessi, e di grande eleganza formale. A queste persone negli Stati Uniti è stato dato il nome di «hacker», un tributo alla loro abilità.

Gli anni '80 sono stati il massimo momento di gloria degli hacker. Il personal computer ha portato grandi potenze di calcolo sul tavolo di chiunque, e gli appassionati hanno potuto sbizzarrirsi a far fare le cose più strane ai propri computer. Nello stesso tempo si stava consumando la rivoluzione telematica, e il mondo si stava silenziosamente rivestendo di una rete di cavi, fibre ottiche e canali satellitari che oggi collegano centinaia di migliaia di sistemi e mettono milioni di persone in condizione di lavorare con qualsiasi elaboratore al mondo senza doversi spostare dalla propria sede. Queste infrastrutture, indispensabili a chi lavora, sono anche affascinanti di per sé e hanno destato la curiosità di numerosissimi hacker: molti di essi hanno acquistato un modem, e hanno cominciato ad esplorare fuori della porta di casa propria.

Alcuni non si sono limitati a curiosare ma hanno lasciato un segno tangibile della propria presenza, vuoi per sbadataggine, vuoi deliberatamente. Finché il fenomeno era limitato a pochi esperti in buona fede il fatto più che un danno ha costituito un fastidio; ma con il tempo è aumentato il numero di persone che si dedicavano a questo nuovo hobby, e il fenomeno ha assunto dimensioni preoccupanti. Alcuni dei nuovi hacker non erano più animati soltanto dal desiderio di conoscere. Presto sono venuti fuori goliardia, vandalismo e varie forme di criminalità, e il problema è divenuto serio. Fino al punto in cui il termine «hacker» ha perso il suo originario significato ed è passato a indicare colui che penetra illegittimamente i sistemi informatici altrui.

Guardie e ladri

Da un lato quindi abbiamo i gestori dei sistemi informatici, dall'altro gli hacker. (Anche se a taluni può non piacere, per chiarezza continueremo a utilizzare questo termine per indicare i «pirati informatici» piuttosto che i «superesperti»). Per un certo tempo la situazione è risultata nettamente a favore di questi ultimi: impreparati a un assalto determinato, i gestori dei sistemi in molti casi non avevano messo in atto alcun sistema di difesa perché non lo ritenevano necessario: questo significava lasciare campo libero agli hacker.

Ma vediamo più in dettaglio cosa ciò significa. La barriera all'accesso a un elaboratore può essere realizzata in diversi modi, il più utilizzato è quello di verificare la conoscenza di un elemento segreto, o più frequentemente dell'associazione tra un elemento pubblico e uno segreto. Ad esempio, l'utente dovrà scrivere il proprio nome e cognome, poi dietro specifica richiesta inserire una parola chiave univocamente associata al proprio nome: l'associazione tra nome e parola chiave è nota soltanto all'elaboratore e all'utente. Se l'utente che afferma di chiamarsi Rossi non conosce la parola chiave associata al nome di Rossi, vuol dire che non si tratta di Rossi in persona. Potrebbe trattarsi di un'altra persona, Bianchi supponiamo, autorizzata anch'essa ad accedere all'elaboratore e quindi a conoscenza di una diversa parola chiave. Ma Bianchi dovrà presentarsi con il proprio nome, fornire la propria parola chiave e soltanto allora sarà riconosciuto e autorizzato a entrare; se tenta di farsi passare per Rossi dovrà essere respinto. Questo è particolarmente rilevante quando Rossi e Bianchi sono autorizzati a fare cose diverse sull'elaboratore, ed è importante che Rossi non metta le mani tra le cose di Bianchi e viceversa.

I sistemi di controllo di accesso attualmente utilizzati sugli elaboratori sono variazioni di questa semplice struttura, e ciascun gestore di sistema deve curare la messa in opera della sicurezza, modificando opportunamente lo schema di sistema di sicurezza fornito dal costruttore dell'elaboratore o del sistema operativo. Tutti i sistemi di una certa dimensione vengono venduti con uno schema di sicurezza predisposto in modo standard; il gestore dovrà partire da questo schema per costruire il proprio.

Purtroppo accade spesso che il gestore si limiti ad aggiungere alcune parole di accesso per il proprio personale, lasciando invariato lo schema previsto dal costruttore. Questo accadeva soprattutto alcuni anni fa, prima che si sviluppasse la consapevolezza del problema. In questo caso qualsiasi hacker, resosi conto del tipo di elaboratore su cui si trovava, era in grado di accedere servendosi delle parole chiave standard.

Molti gestori sono corsi ai ripari, sia per brutte esperienze personali sia perché opportunamente avvertiti da consulenti o fornitori. Ma gli hacker hanno sviluppato tecniche di assalto più sofisticate e il gioco continua.

L'uovo del cuculo

Ciò che lascia sconcertato il grande pubblico è il fatto che gli hacker possano avere campo libero senza che nessuno possa fare nulla per identificarli e bloccarli. Quello che il pubblico ignora è che quasi sempre gli hacker si servono di

linee telefoniche commutate, cioè quelle che vengono utilizzate per le normali conversazioni telefoniche. Fino a poco tempo fa chi riceveva una chiamata telefonica non aveva alcun modo per determinare il numero telefonico del chiamante. I sistemi telefonici a tecnologia elettromeccanica, come quelli utilizzati tuttora in parte dalla Sip e da altri gestori europei, non forniscono questa informazione e per determinare da dove proviene una chiamata è necessario «ribattere» il collegamento, selettore per selettore, seguendo fisicamente il percorso dei cavi fino a risalire all'armadio stradale da cui parte la coppia di fili che va all'apparecchio telefonico del chiamante.

Le centrali elettroniche sotto questo punto di vista sono migliori, ma l'informazione sull'identità del chiamante è disponibile soltanto a livello di sistema. In entrambi i casi quindi solo la società telefonica è in grado di identificare da chi proviene una chiamata; e praticamente in tutti gli Stati democratici dotati di un sistema telefonico l'identificazione della provenienza di una chiamata viene effettuata soltanto su richiesta dell'Autorità giudiziaria.

I gestori dei sistemi informatici quindi sono sfavoriti: se ricevono una chiamata indesiderata non possono sapere chi li sta chiamando. Potrebbero staccare tutte le linee per evitare le chiamate indesiderate, ma in questo modo impedirebbero anche quelle legittime, e in un mondo dipendente da un rapido scambio di informazioni molti sistemi informatici tagliati fuori dal flusso di scambio sono condannati a morire in breve tempo.

La situazione promette di migliorare sensibilmente: a breve scadenza sarà disponibile in molti sistemi telefonici il servizio di «Caller ID», che consente al chiamato di richiedere allo stesso sistema telefonico l'identificativo (prefisso e numero) del chiamante. Questo porrà fine alle chiamate fastidiose (scherzi, maniaci, etc.) e nel nostro caso renderà più rischiosa l'attività degli hacker: un conto è nascondersi dietro a un facile anonimato, certi del fatto che sarà difficile che il gestore del sistema-bersaglio vada a chiedere alla Magistratura l'intercettazione delle proprie linee; un conto sarà quando lo stesso gestore potrà presentarsi dallo hacker a chiedergli conto del proprio operato.

Ma spesso gli hacker non chiamano direttamente il sistema-bersaglio: un interessantissimo esempio di una intrusione perpetrata con criteri scientifici è raccontata dallo stesso gestore del sistema che l'ha subita, nel libro «The Cuckoo's Egg» di Cliff Stoll (it. «L'uovo del cuculo», Sperling-Kupfer).

Nel 1986 Stoll, astronomo, venne dimesso dal laboratorio di ricerca presso il quale lavorava perché i fondi erano finiti. Il suo stesso capo gli procurò un posto presso uno dei centri di informatica dell'università di Berkeley, dove il suo primo incarico consistette nel trovare la ragione di uno sbilancio di 75 centesimi nella contabilità del centro. La ricerca della causa dell'errore portò Stoll a scoprire un intruso nel sistema, a seguirlo giorno dopo giorno nelle sue pazzesche escursioni per sistemi militari, alla ricerca di informazioni classificate, escursioni che vennero meticolosamente intercettate e registrate da Stoll senza che lo hacker se ne accorgesse, senza che nessuno intervenisse per fare nulla, né l'FBI, né la CIA, né la NSA.

Stoll riuscirà comunque a rintracciare questo hacker, seguendo il filo dell'incredibile connessione che entrava nel sistema di Berkeley passando per la rete Tymnet acceduta chiamando un numero di Oakland, che a sua volta veniva raggiunto passando per un «outdial» privato (un modem collegato a un elaboratore per fare chiamate uscenti anziché ricevere quelle entranti) in Virginia. Lo hacker entrava nel sistema in Virginia passando per una connessione via satellite originata dall'università di Brema, a sua volta chiamata direttamente per telefono. Per districare questa matassa sono occorsi diversi mesi di intercettazioni, durante i quali lo hacker ha avuto modo di fare man bassa di informazioni riservate senza che Stoll potesse fare nulla per impedirglielo.

Lo scopo di Stoll era infatti quello di identificare e bloccare questa persona che si serviva del sistema di Berkeley come di un punto di passaggio per confondere ulteriormente le acque, garantendosi il diritto di accedere alle risorse vitali del sistema con una tecnica molto simile a quella utilizzata dal cuculo per assicurare un nido alla sua prole: depositare un oggetto estraneo (in questo caso un programma) fatto in modo tale da ingannare il sistema che lo avrebbe ritenuto legittimo.

Se Stoll si fosse limitato a bloccare l'accesso al proprio computer, l'ignoto hacker avrebbe trovato una diversa strada per le proprie scorrerie, passando per un altro delle decine di migliaia di elaboratori collegati alla rete Internet negli Stati Uniti, e nessuno sarebbe mai riuscito a rintracciarlo. Lasciandogli aperte le porte Stoll riuscì invece a identificarlo e a segnalare il fatto all'autorità competente. Markus Hess di Hannover fu quindi condannato da un tribunale tedesco per spionaggio, insieme ai suoi complici Dirk Brezinski e Peter Carl.

Il «verme» della Internet

Poco dopo il fatto raccontato da Stoll un nuovo episodio di intrusione informatica scosse gli Stati Uniti. Stavolta non si trattava di una singola penetrazione: all'improvviso, nella notte fra il 2 e il 3 novembre 1988, migliaia di elaboratori in tutto il paese subirono forti e inspiegabili rallentamenti. Un'analisi dei lavori attivi sul sistema mostrò che un programma, arrivato apparentemente dal nulla, si era installato e a sua volta si riproduceva trasferendo copie di se stesso su altri sistemi collegati alla rete. Migliaia di sistemisti in centinaia di centri lavorarono freneticamente per tutta la notte per frenare l'invasione. Alla fine il programma fu bloccato, analizzato e studiato e si potè riscontrare che ciò che aveva dato luogo alla sua diffusione incontrollata era un banale errore di programmazione.

La struttura del programma era semplice: una volta installatosi su un elaboratore andava alla ricerca delle tabelle in cui sono descritti i collegamenti in rete con altri elaboratori; quindi sfruttando alcuni «bachi» del sistema operativo Unix si trasferiva su tutti i sistemi collegati e si installava, ricominciando il proprio lavoro. Il meccanismo previsto dal programmatore per evitare che il programma si installasse più volte sullo stesso elaboratore non aveva funzionato, per cui lo stesso programma si trovò a girare in più copie sulle stesse macchine.

L'identificazione del responsabile del fatto non fu semplice, ma alla fine si riuscì a centrare l'attenzione su Robert T. Morris, uno studente della Cornell University. Particolare curioso: Robert Morris è figlio di Robert Morris Sr., direttore scientifico del National Computer Security Center e inventore dello schema di protezione mediante password utilizzato nello Unix.

Anche Morris Jr. fu condannato, come i tre tedeschi, ma nel suo caso vennero applicate le norme specifiche sui crimini informatici recentemente varate negli Stati Uniti. La sentenza fu relativamente mite: nel maggio 1990 gli furono comminati tre anni con la condizionale, una ammenda di $10.000 e 400 ore di lavoro in favore della comunità.

La vicenda di Morris ha avuto uno strascico importante. Poiché la sua vicenda ebbe una eco enorme nei mezzi di informazione molte aziende lo contattarono per assumerlo come specialista in sicurezza (un ladro è un ottimo collaudatore di antifurti); questo fatto poteva costituire un pericolosissimo precedente, perché qualcuno avrebbe senz'altro pensato: «Morris ha bloccato seimila computer e lo hanno assunto con uno stipendio di $50.000 l'anno, io adesso provo a bloccarne ventimila e chissà con che stipendio mi assumeranno». Per scongiurare questo rischio un gruppo di circa 500 esperti di informatica, tra cui docenti universitari e specialisti di aziende e enti pubblici e privati scrisse quindi una lettera aperta alle aziende che potevano essere interessa-

te all'assunzione di Morris invitandole a non farlo nell'interesse della collettività.

L'anarchia organizzata

Anche in Europa gli hacker si sono dati molto da fare. Particolarmente rilevante, soprattutto per il gran parlare che se n'è fatto, il Chaos Computer Club tedesco, costituito nel 1981 con finalità vagamente politiche riprese in parte dall'ideologia cyberpunk: soprattutto la difesa della libertà delle informazioni, che sono patrimonio di tutti, e del diritto di venirne a conoscenza superando, se necessario, ogni barriera.

Nel gennaio 1989 Fulvio Berghella e Roberto Cena dell'IPACRI intervistarono Steffen Wernery, leader del Chaos Computer Club. Dall'intervista emerge la figura di un giovane attirato dalle nuove tecnologie ma anche preoccupato da taluni risvolti sociali a cui non viene prestata, secondo lui e secondo il gruppo a cui appartiene, sufficiente attenzione. Toccando temi come la sicurezza delle carte di credito, la tutela delle informazioni riservate e la disponibilità delle informazioni pubbliche Wernery dimostra di essere sensibile alle problematiche della sicurezza sebbene dal punto di vista di un cittadino, estraneo alla gestione dei sistemi informativi ma fortemente critico dei metodi con cui viene condotta.

I membri del Club vedono quasi sempre la sfida intellettuale insita nell'attività di uno hacker. Con le parole di Wernery, «è difficile proibire alle persone di essere migliori di quelli che hanno costruito le macchine, perché io con un piccolo computer da 600 DM posso annientare una macchina che costa 6 milioni di DM. Ed è difficile proibirlo dato che io lo faccio azionando alcuni tasti ed essendo più intelligente».

Oltre al Chaos Computer Club, che emerge nel panorama mondiale come l'unico caso di associazione pubblicamente costituita e registrata presso un Tribunale, operano nel mondo numerose altre associazioni, più o meno clandestine e pressoché sconosciute a chi non ne fa parte. Tracciarne una mappa è estremamente difficile per la mancanza di informazioni dettagliate e per l'estremo dinamismo con cui tali associazioni nascono, si trasformano e scompaiono senza lasciare traccia.

In alcuni casi l'organizzazione è più stabile e pubblica anche un proprio organo informativo. È il caso della rivista «2600», vera miniera di informazioni sulle tecniche di penetrazione dei diversi sistemi. E non solo di sistemi informatici: un'ampia parte della rivista è dedicata alle informazioni sul «phreaking», un neologismo coniato dalla unione delle parole «phone» e «freak» e che sta a indicare la penetrazione illecita delle reti telefoniche allo scopo di utilizzarne gratuitamente i servizi. Lo stesso nome della rivista trae origine dalla telefonia: un segnale di servizio utilizzato in particolari circostanze sulle reti telefoniche ha appunto la frequenza di 2600 Hz *(Questa tecnica fu usata per la prima volta da John Draper, soprannominato Captain Crunch, che usava appunto il «fischietto» contenuto nelle omonime confezioni di cereali, per frodare la compagnia dei telefoni N.d.R.).*

La fiducia perduta

Ma che danno può fare uno hacker? Molti di essi rispettano un «codice d'onore», piuttosto indefinito per la verità, che tra l'altro impone di non lasciare tracce della propria penetrazione, di operare in modo da non causare danni, di astenersi dalla penetrazione dei sistemi bancari per evitare che l'eventuale pubblicità data al fatto possa determinare una perdita di fiducia nel sistema bancario.

Non tutti sono così «galantuomini». Molti entrano per distruggere, e talvolta ci riescono. Spesso il danno che causano risulta molto più grande di quello che avevano previsto: è stato il caso di Morris, che al momento del rilascio del suo programma-verme si proponeva di installarne una copia in ciascuno degli elaboratori di un certo tipo collegati alla rete, e si ritrovò invece con migliaia di questi programmi impazziti che circolavano indisturbati mettendo in ginocchio la rete stessa.

In alcuni casi il danno può essere più subdolo. Uno degli elaboratori in cui si introdusse Markus Hess era il sistema di controllo del Bevatron. Si tratta di un acceleratore di particelle che si serve di magneti enormi per sparare particelle subatomiche su bersagli prestabiliti, normalmente ioni pesanti accelerati fino quasi alla velocità della luce.

I fisici di Berkeley talvolta debbono restare in coda per mesi prima di potersi servire del Bevatron. Ma non sono i soli a stare in coda: ci sono anche numerosi pazienti ammalati di cancro. Il Bevatron infatti è in grado di accelerare ioni di elio a una velocità alla quale acquistano un'energia di circa 160 milioni di elettronvolt. A questa velocità viaggiano per pochi centimetri e quindi scaricano tutta l'energia accumulata. Posizionando opportunamente un tumore alla distanza giusta gli ioni lo penetrano e distruggono le cellule tumorali. Questo metodo di cura viene utilizzato soprattutto per il cancro dell'encefalo, che sovente è inoperabile.

Il sistema di controllo del Bevatron si incarica appunto di determinare la distanza e la velocità giuste. Un errore di una frazione di millimetro o di una frazione di secondo può significare la distruzione di cellule cerebrali anziché tumorali. Uno hacker che si mette a giocare con un sistema di questo genere potrebbe giocare con il cervello altrui.

Anche senza raggiungere estremi così drammatici tuttavia il danno provocato dagli hacker può essere grave. Ne abbiamo fatto esperienza personalmente su MC-link, la nostra rivista telematica. La comunicazione telematica è una forma di comunicazione nella quale non c'è possibilità diretta di controllo della identità della persona con cui si comunica. Ricevo un messaggio da una persona che si firma Mario_Rossi@cnr.it: chi mi garantisce che si tratta del vero Mario Rossi? Teoricamente nessuno; debbo fidarmi. Su questa fiducia si è basata per lungo tempo la comunicazione telematica. Ma a un certo punto ci si è dovuti rendere conto che alcune persone deliberatamente assumevano una identità falsa su alcuni sistemi telematici, vuoi perché si registravano con nominativi falsi, vuoi perché si trattava di hacker che avevano ottenuto illegalmente accesso servendosi del codice di persone realmente esistenti, più o meno a loro insaputa.

Nel primo periodo della sua esistenza MC-link era un sistema completamente aperto. Era in corso di sviluppo e di sperimentazione, e la procedura di «abilitazione» (cioè di autorizzazione all'accesso previa verifica dell'identità) era poco più che una formalità automatica. In questo modo molte persone ottennero un accesso con dati falsi. Successivamente il fenomeno assunse dimensioni più rilevanti al crescere della notorietà del sistema, fino al punto in cui si dovettero prendere precise misure. Attualmente MC-link è l'unico sistema del suo genere che garantisce formalmente l'identità delle persone che lo utilizzano. È un bene? Da un punto di vista aziendale lo è senz'altro. Ma per la collettività telematica è un grave danno il fatto che sia stato necessario adoperarsi esplicitamente, e con strumenti poco simpatici come contratti e autentiche notarili, per essere certi che chi si firma Mario Rossi sia effettivamente il vero Mario Rossi e non qualcuno che si fa passare per lui.

La diffusione dell'informatica e della telematica richiede sistemi semplici da utilizzare, facili da raggiungere e affidabili. E richiede molta fiducia. La sicurezza ha requisiti diametralmente opposti: complessi sistemi di protezione e password, elaboratori possibilmente isolati e la massima diffidenza possibile. Sono obiettivi apparentemente inconciliabili.

MC

Stefano Toria è raggiungibile tramite MC-link alla casella MC0170 e tramite Internet all'indirizzo MC0170@mclink.it.