Dedichiamo anche le pagine di Cittadini & Computer di questo numero al problema della sicurezza informatica. Abbiamo sottolineato molte volte quanto la nostra vita sia ormai legata al buon funzionamento dei grandi sistemi informatici, dagli archivi del fisco ai sistemi di prenotazione delle linee aeree, tanto per restare su argomenti che abbiamo trattato negli ultimi mesi. È chiaro che la protezione di questi centri non riguarda soltanto gli addetti ai lavori, ma ci interessa tutti in quanto cittadini-utenti. E dobbiamo occuparcene, perché anche la sicurezza fa parte di quella cultura informatica di base della quale ormai nessuno può fare a meno

La sicurezza dei sistemi informativi

di Manlio Cammarata

Il discorso sulla sicurezza dei sistemi informativi presenta diversi aspetti. Si va dalla protezione fisica degli impianti alla protezione logica degli archivi (perché un sistema può essere distrutto dal fuoco o da un crollo dell'edificio in cui si trova, ma anche dall'intrusione di pirati informatici), per arrivare alla prevenzione delle intercettazioni degli scambi di dati sulle reti, dell'accesso fraudolento a informazioni riservate o dell'alterazione dolosa o fortuita delle informazioni. C'è poi il problema dei virus, che per fortuna riguarda solo i personal computer, ma che può avere comunque ricadute dannose sull'efficienza dei sistemi più grandi, quando i PC che fungono da terminali dei sistemi stessi vanno fuori uso a causa di un'infezione.

Il poliziotto...

La prima giornata del Securicom, il convegno sulla sicurezza dei sistemi informativi che si è tenuto a Bologna in maggio, ha visto due interventi molto interessanti: quello del vicequestore Alessandro Pansa, dirigente del Nucleo Centrale Criminalità Informatica della Polizia di Stato, e quello del dottor Antonio Di Pietro, il magistrato che ha scoperchiato la pentola della tangentocrazia milanese.

Il dottor Pansa ha tracciato un bilancio di poco più di due anni di attività del Nucleo, attività che si è spesso scontrata con due ordini di problemi: la quasi totale mancanza di denunce di computer crime da parte di privati e la difficoltà di individuare comportamenti penalmente perseguibili. Il primo problema è legato alla convinzione che la pubblicità del reato sia più dannosa del reato stesso, il secondo dalla mancanza in Italia di una legislazione specifica sui reati informatici.

«Il livello di sicurezza dei sistemi informativi nel nostro Paese è piuttosto basso» si legge nella relazione di Pansa «sia per quanto concerne le reti di trasmissione dati, che i centri di elaborazione. Le reti telematiche sono sicuramente poco affidabili. Il controllo degli accessi, attraverso parole-chiave, è concepito per garantire una comoda e precisa contabilizzazione delle spese da parte del gestore della rete. Così sarà agevole riscuotere dagli utenti il pagamento del servizio, ma tutto ciò non è sufficiente a garantire accessi non au-

Riconoscimento biometrico: il disegno tridimensionale della mano può essere letto dal computer. Però manca il programma per predire il futuro...

torizzati. Per quanto concerne, poi, il mondo delle aziende che utilizzano sistemi informativi, è possibile fornire un giudizio attendibile sul grado di sicurezza delle aziende che forniscono servizi bancari e finanziari in genere, mentre scarsissimi sono gli elementi di valutazione in ordine alla sicurezza delle aziende industriali. Infatti in tali aziende la sicurezza funziona adeguatamente solo se inserita in un contesto strategico definito e condiviso dall'alta direzione».

Per quanto riguarda le intrusioni nei sistemi informativi, secondo Pansa in Italia il problema più grave non è quello degli «hacker», che operano dall'esterno dei sistemi informativi, ma quello degli «insider», operatori che attaccano i sistemi dall'interno, utilizzando per scopi illeciti l'accesso di cui dispongono per i loro compiti istituzionali. Bisogna poi notare che i danni prodotti dagli insider vengono sempre denunciati quando riguardano il settore pubblico, mentre sono pochissimi i casi di denunce provenienti dal settore privato.

Ma l'aspetto più preoccupante, secondo il vicequestore, è che la criminalità organizzata sfrutta sempre più a fondo le tecnologie avanzate, per gestire non solo i profitti illeciti, ma anche le attività criminali che producono tali profitti. «La mafia oggi usa estensivamente strumenti informatici», ha detto Pansa, citando alcune recenti indagini. Si è poi occupato del problema dei virus, sottolineando l'importanza di creare una «cultura della sicurezza», resa ancor più necessaria dalla presenza in Italia di un numero elevato di criminali informatici, alla quale non fa ancora riscontro una legislazione penale adeguata.

... e il magistrato

Eventi come il Securicom di solito non arrivano sulle prime pagine dei giornali. Ma questa volta c'è stata un'eccezione, perché nella prima giornata del convegno era previsto un intervento del giudice Antonio Di Pietro, quello che ha scoperchiato la pentola della tangentocrazia milanese. Ovvio quindi l'interesse della grande stampa di informazione, con titoli e foto in grande evidenza. L'intervento era stato concordato prima che il magistrato arrivasse agli onori delle cronache, in considerazione del fatto

Sicurezza e diritti sindacali

Duplicazione dell'hardware e dei dati, protezione delle linee di comunicazione, algoritmi di controllo delle transazioni, procedure di Disaster Recovery, crittografia... le invenzioni destinate alla sicurezza sembrano ancora più numerose dei rischi, ma c'è una categoria di misure di protezione che può attentare ai diritti dei lavoratori e provoca conflitti sindacali. Sono i sistemi che consentono di indentificare l'operatore che accede a un sistema e effettua determinate transazioni.

È una materia molto delicata. Le norme di sicurezza in molti casi impongono che un lavoratore — poniamo l'esempio di un impiegato di banca — debba inserire il suo badge magnetico nel terminale per avere accesso al sistema e compiere un'operazione di movimento di denaro. Oltre al consenso per l'operazione, il sistema si preoccupa di conservare una registrazione, che consenta di risalire a chi ha svolto quella determinata transazione, nel caso che vi sia una successiva contestazione. È chiaro che non si può fare a meno di questa procedura di sicurezza, altrimenti sarebbe facilissimo per chiunque spostare somme su un certo conto e poi dissolversi senza lasciare tracce. Ma a questo punto è possibile che, con appositi algoritmi, si ricavino informazioni sull'attività del dipendente: quante transazioni compie, quanto tempo impiega e così via. Questo contrasterebbe con le disposizioni dello Statuto dei lavoratori, che vietano all'imprenditore di svolgere controlli continui sulle prestazioni dei dipendenti.

E ci sono anche altri problemi. Le telecamere, per esempio, che spesso sorvegliano aree delicate, sono un altro strumento di controllo che contrasta con i diritti del lavoratore. In alcuni istituti finanziari si devono conservare le registrazioni delle telefonate, per poter eventualmente fornire la prova di transazioni disposte con questo mezzo. Ancora, il calcolo dei costi delle telecomunicazioni può rendere necessaria la memorizzazione di tutti i numeri esterni che vengono chiamati dai telefoni di un'azienda, e così via.

C'è quindi da risolvere un contrasto tra le esigenze della sicurezza e il diritto alla riservatezza del singolo dipendente. Questo problema è stato trattato al Securicom da Roberto Pietrobelli, che ha preso in considerazione sia le norme italiane, contenute appunto nello Statuto dei Lavoratori, sia le recenti proposte europee. Ma la soluzione difficilmente può essere trovata ricorrendo a disposizioni di uso generale, data la grande varietà di casi che si possono verificare. Dalla relazione di Pietrobelli sono emersi però alcuni esempi molto interessanti di accordi aziendali, che hanno permesso di conciliare le contrapposte esigenze. Nel caso dell'impiego di badge, per esempio, si è stabilito che le registrazioni devono essere crittografate e aggregate per gruppi di dipendenti; per la sorveglianza con telecamere si è trovata la soluzione di non collegare i monitor in permanenza, ma di custodire le registrazioni in archivi a doppia chiave, una per l'azienda e una per la rappresentanza sindacale. Per la registrazione dei numeri telefonici chiamati possono essere cancellate le ultime cifre, e quando ci sono apparecchi di registrazione collegati in permanenza ai telefoni i dipendenti devono disporre anche di telefoni non controllati per le loro chiamate personali.

Insomma, deve vincere il buon senso. Lo ha detto anche il giudice Di Pietro, interrogato sull'argomento alla fine del suo discorso. Bisogna cercare di capire caso per caso, ha detto il magistrato, se il comportamento del datore di lavoro sia motivato solo da esigenze di sicurezza, o se i controlli possono inutilmente limitare i diritti del dipendente.

Aschieri: occorre formare alla sicurezza

Alessandro Aschieri, una lunga esperienza all'IBM in diversi ruoli, fra i quali la direzione programmi di sicurezza, ora opera come consulente proprio in questo settore. Al Securicom ha svolto un'interessante relazione su «Metodologie e tecniche di sensibilizzazione e di addestramento aziendale in tema di sicurezza informatica».

Il problema della sicurezza informatica nelle aziende, ha detto Aschieri, è oggi complicato dal decentramento delle attività di elaborazione, conseguente sia all'avanzata dell'informatica distribuita, sia alla nuova struttura delle organizzazioni, non più verticale e accentrata, ma sempre più orizzontale e con una accentuata dispersione dei centri di responsabilità. I due fattori si combinano tra loro e comportano un significativo cambiamento nell'impostazione dei sistemi di protezione: prima l'informatica era controllata esclusivamente dagli specialisti dell'EDP, che avevano quindi anche l'intera responsabilità della sicurezza. Oggi le attività di elaborazione sono scese a livello dipartimentale e a livello individuale, attraverso i mini e i PC, e i problemi di prevenzione si pongono anche se questi non sono collegati in rete. Le reti stesse hanno poi problemi di sicurezza particolari. Insomma, la diffusione dell'informatica comporta la diffusione del rischio.

La conseguenza è preoccupante: mentre prima le responsabilità di controllo erano nelle mani di personale specializzato in informatica, e quindi culturalmente e psicologicamente preparato, oggi esse si spostano su persone che non hanno una preparazione specifica e che spesso tendono a sottovalutare, se non a ignorare, il problema. Si pone quindi l'esigenza di addestrare queste persone, superando anche una serie di problemi psicologici.

E proprio su questo punto abbiamo voluto porre alcune domande ad Aschieri alla fine della conferenza.

* * *

Ingegner Aschieri, nella sua relazione, e alla fine rispondendo a una domanda, lei ha sottolineato un problema psicologico molto importante: il fatto che molte persone trascurano di occuparsi degli aspetti della sicurezza delle attività informatiche. Ora noi sappiamo, ce lo ha spiegato per primo il dottor Freud circa un secolo fa, che quando un individuo trascura un problema che pure dovrebbe interessarlo, vuol dire che lo ha rimosso, perché evidentemente provoca in lui uno stato di ansia al quale vuole inconsciamente sottrarsi. Il paradosso è aumentato dal fatto che se noi cerchiamo di attirare l'attenzione di una persona su un problema rimosso, otteniamo un rifiuto ancora più violento, come sa, per esempio, chi ha cercato di convincere un claustrofobico a prendere l'ascensore. Come si fa, in una fase di addestramento, a superare questa difficoltà?

La mia risposta nasce dall'esperienza di almeno dodici anni di attività di consulenza nel campo della sicurezza informatica. In pratica ho fatto il predicatore, anche con seminari ad altissimo livello. Poi l'altissimo livello mandava quello più in basso, però intanto era stato toccato. In questo arco di tempo ho potuto capire che l'elemento di risposta che scavalca queste situazioni di rifiuto di solito ha un'origine storica: sono successe cose che ci costringono a occuparci di questo argomento. E qui gioca a favore del discorso sulla sicurezza l'estensione e l'infittimento della materia, cioè la cosiddetta pervasività dell'informatica.

Ma è ormai un fatto pacificamente riconosciuto, e lo ha sottolineato anche lei, che la diffusione crescente dell'informatica determina un aumento dei rischi. Come può una maggiore pervasività diventare un elemento favorevole?

L'informatica sempre più pervasiva crea sempre più problemi, per cui se non è fatta con buona qualità si creano dei pasticci, i danni diventano tanti. Diventa un po' forzante l'esperienza, non l'amore per la cultura, perché io penso che oggi un management che non sia particolarmente dotato, un management normale, ha una tale serie di problemi per poter campare tutti i giorni, problemi di vari tipi, politici, sindacali, finanziari, di scenario, che è costretto a stratificarli. E l'informatica più ancora che utilizzarla, secondo me continua a subirla. In pratica il discorso è generazionale, bisogna che un certo strato di persone esca dalla scena perché va in pensione, e arrivino quelli della generazione successiva, che avendo vissuto l'informatica fin da quando è comparsa, la trovano come un fattore naturale, un elemento di cultura generale. Come i nostri figli, che manovrano il televisore con il telecomando, e non lo hanno imparato da nessuno, mentre le nonne dicono: cambiami il canale, perché con quel coso lì... È la stessa storia.

A proposito di cultura informatica, vi sono alcune realtà, come la LUISS, che è tesa alla formazione dei manager della nuova generazione, che fanno della cultura informatica un pilastro della formazione generale. Ma per il resto, dal suo punto di osservazione, come può essere valutata la situazione in Italia?

Siamo ancora a un livello insufficiente. Abbiamo bisogno di una cultura informatica superiore a quella che la scuola oggi fornisce.

Escludendo le lauree in Informatica, o alcuni casi in Ingegneria o in Economia e Commercio, saranno sì o no l'otto o il nove per cento dei laureati, considerando le materie che interessano l'azienda, ad avere una preparazione adeguata. Tutti gli altri ne sanno ancora troppo poco.

Purtroppo è un discorso che richiede tempi lunghi.

Dunque il futuro dovrebbe portarci a un miglioramento della situazione per quanto riguarda la cultura della sicurezza. Ma a breve e medio termine, come vede le condizioni di sicurezza dei grandi sistemi informativi? Mi riferisco naturalmente sia alle grandi aziende, che forse sono più attente e preparate, sia alle strutture pubbliche. La relazione del dottor Pansa ha messo in luce un livello di sicurezza piuttosto basso. Secondo lei esistono seri rischi di gravi intrusioni, o di cadute rovinose e prolungate dell'attività di qualche organizzazione importante? Non parliamo, è ovvio, dei vari venerdì 13 e Michelangelo, che forse sono rischi più... giornalistici che reali.

Io direi questo: che in tutto il mondo gli hacker hanno dimostrato che si va praticamente dove si vuole. Quindi ciò che trattiene dell'andare a curiosare, a rompere le scatole nei grandi archivi dei nostri ministeri o in altre organizzazioni, io credo che sia il fatto che non gliene importa niente a nessuno! Ma non perché ci siano nell'informatica di oggi, se non in casi particolari, delle grandi difese, perché come si va negli schedari della NASA, o del Ministero della Guerra francese, si può andare nei sistemi del Ministero dei Lavori Pubblici italiano.

Le difese ci sono, naturalmente, ma davanti al grande esperto le difese cadono. Praticamente oggi si considera che la difesa assoluta è l'isolamento assoluto, ma un sistema isolato non comunica. Se un sistema è interconnesso ha dei rischi che si possono ridurre, ma non si possono cancellare. Quindi l'intrusione nei grandi sistemi è una cosa possibile, ed infatti avviene, e può capitare a noi come ad altri.

E potrebbe essere un'intrusione distruttiva, un'intrusione con conseguenze catastrofiche?

Questo è difficile. Perché le intrusioni sono sempre state conoscitive, perché lo scopo è mettere in pubblico delle cose che qualcuno ritiene che debbano essere segrete. C'è un po' quella mentalità da Robin Hood, che procura molte grane, ma la cosa finisce lì.

che è un grande appassionato, oltre che esperto, di informatica. «Mi atterrò al tema concordato a suo tempo», ha dichiarato Di Pietro all'inizio, facendo intendere che non intendeva trattare i fatti di Milano, ma poi ha parlato a braccio, in un discorso dal tono spesso appassionato, che ha suscitato applausi. Soltanto al momento di andare via, ha detto qualcosa sull'importanza degli strumenti informatici nelle indagini in corso a Milano.

Ci sono due aspetti del problema, ha detto il magistrato nel suo intervento. Il primo è l'impiego dei mezzi informatici per le indagini su reati tradizionali, il secondo sono le indagini, svolte con mezzi normali o informatici, sui fatti commessi con il computer o contro il computer, che sono moralmente, socialmente, e solo qualche volta penalmente rilevanti, date le carenze della legislazione attuale. I problemi sono molti e complicati: ha fatto l'esempio di una recen-

Fulvio Berghella: i virus come "moda sociale"

Direttore centrale Istinform, dopo essere stato per anni all'IPACRI (l'Istituto Per l'Automazione delle Casse di Risparmio Italiane), Fulvio Berghella è uno dei massimi esperti italiani di virus, e allo stesso tempo consulente a tempo pieno per la sicurezza dei sistemi informativi negli istituti di credito verso cui si rivolge l'attività di Istinform.

Al Securicom Berghella ha tenuto, oltre alla relazione di cui abbiamo riferito in altra parte, anche un tutorial specifico sui virus del computer, insieme al prof. Mezzalama del Politecnico di Torino.

Il quadro che esce dalle parole di Berghella non consente molto ottimismo sul fenomeno dei virus, almeno a breve periodo, ma nel medio termine le cose dovrebbero cambiare. Vediamo perché.

Stiamo assistendo a una sorta di gioco di guardie e ladri tra chi cerca di prevenire i danni da virus e chi si impegna a trovare metodi sempre nuovi per aggirare le protezioni. Per quanto tempo si potrà andare avanti in questo modo?

Ritengo che ci troviamo di fronte a un fenomeno che ha tutte le caratteristiche della moda sociale.

L'esperienza storica dimostra che questi fatti hanno un periodo di sette-otto anni, diciamo un decennio per semplicità.

Se consideriamo iniziato il fenomeno nel periodo 1987-89, credo che ne avremo agli stessi ritmi di oggi per almeno altri due anni; anche in seguito il problema rimarrà a livelli significativi ma certamente fino al '94-95 rimarranno gli odierni ritmi di crescita esponenziale.

Dal lato dei fornitori non ci sembra di poter prevedere grosse novità in nessun ambiente di sistema operativo.

Piuttosto è prevedibile una ripartizione e una specializzazione delle tipologie di virus: da un lato un aumento di virus generici fatti da chiunque, dall'altro pochissimi virus mirati a situazioni specifiche.

Sembra prendere corpo quindi l'ipotesi

secondo cui alcuni virus siano costruiti con un obiettivo preciso.

Le prove a disposizione finora sono poche. Ci sono stati finora soltanto quattro arresti di creatori di virus, e in tutti e quattro i casi il capo d'accusa è stata l'estorsione.

A questa tipologia si possono aggiungere i casi di ricatto verso aziende infettate da un dipendente o da un esterno, per ottenere denaro in cambio della disinfezione.

Sono noti già da tempo invece diversi casi di sabotaggio a mezzo di virus, per danneggiare l'immagine di un'azienda o per determinare un danno diretto mediante distruzione di dati.

Abbiamo avuto poi dei casi con motivazioni politico-sociali, le piste bulgare o italiane (il Crackerjack), e infine c'è il gruppo di virus di origine spontanea, nati spesso per spirito goliardico o per ricerca.

Resta comunque la possibilità che esistano altri fenomeni alla base dell'origine di gruppi di virus, fenomeni di cui non siamo ancora a conoscenza.

Rimangono fuori da questa classificazione i casi di virus scritti appositamente da un dipendente per danneggiare la propria azienda.

Esistono dati certi su casi di questo genere?

Ne siamo direttamente a conoscenza.

Passiamo a un altro argomento. Prima il Club Computer Crime, oggi Istinform e SecurityNet. Qual è il ruolo di queste organizzazioni nel panorama della sicurezza e in particolare dei virus?

L'esperienza del Club Computer Crime fu molto positiva, perché fummo i primi in Italia ad attivare dei meccanismi di sicurezza di questo genere, unitamente a un'attività di ricerca specifica. Ma nel frattempo sta cambiando il sistema bancario (si pensi al 1993, alla legge Amato); era necessaria una revisione del sistema.

È in quest'ottica che mi trovo ora in Istinform. Inizialmente su 280 banche che aderiscono al consorzio soltanto tre o quattro avevano sviluppato una sensibilità alla problematica della sicurezza informatica. Per questa ragione ideammo il meccanismo di SecurityNet, come servizio interbancario capace di costituire luogo di dibattito ma anche un polo di consulenza specifica, informatica e organizzativa. A questo scopo la nostra funzione è anche di mediare le esigenze di fornitori e utenti, per realizzare delle soluzioni realmente utili al sistema bancario.

Abbiamo scelto appositamente di separare il problema virus dal resto, poiché si rendeva necessario un intervento immediato e inoltre i livelli di impatto di questo problema sull'organizzazione rispetto ad altri problemi (un esempio: il Disaster Recovery) sono enormemente differenti. Nel caso dei virus il problema si risolve spesso installando dei prodotti antivirus e creando un minimo di sensibilità.

Il punto di forza di SecurityNet consiste soprattutto nell'informazione imme-

te indagine svolta con la collaborazione del Nucleo Centrale Criminalità informatica, sulla base della denuncia di una banca dati inglese violata da un hacker milanese. Ma gli investigatori hanno scoperto che in realtà si trattava di un giapponese, che si faceva passare per milanese saltando da un computer all'altro. Di chi è la competenza? Il danno chi l'ha subito? «Nel momento in cui scopro il colpevole, io magistrato d'Italia ho il diritto di perseguirlo?» ha chiesto Di Pietro. «E poi, se non possiamo fargli nulla, quello ci deride pure...», e nel caso dell'indagine dell'anno scorso sulla grande truffa al Videotel, il giudice ha posto il problema della liceità dell'intercettazione, non di conversazioni telefoniche, previste dal codice, ma di collegamenti telematici.

Ma per Di Pietro, se è comunque urgente che il Parlamento legiferi il più presto possibile sui crimini commessi con sistemi informatici o contro sitemi informatici, le norme attuali possono in molti casi essere sufficienti per punire comportamenti di questo tipo. Ma il problema principale, ha sottolineato il magistrato, non è intercettare qualche giovanotto che si intrufola in una banca dati solo per dimostrare di essere capace di farlo, ma di prevenire, prima ancora che reprimere, comportamenti che possono determinare danni molto più gravi.

Perché l'esperienza di recenti indagini ha dimostrato che in molti casi di gravi reati informatici c'è un «basista» all'in-

diata. Noi gestiamo una banca dati, un BBS a cui tutti contribuiscono con segnalazioni di software infetto o sospetto.

L'iniziativa di SecurityNet ha dimostrato la propria validità in occasione di determinati eventi precisi, come nel caso di alcune grosse infezioni nel periodo tra novembre e Natale dello scorso anno in cui siamo giunti all'identificazione di un nuovo virus, ora noto come 855, che abbiamo provveduto a segnalare al circuito di ricerca.

***T**orniamo a un tema tecnico. Si comincia a sentir parlare di controllo dell'integrità in alternativa alla scansione delle firme dei virus. È una tecnologia promettente?*

Penso che si debba distinguere tra la teoria e la pratica. In teoria è un sistema ottimo, ben superiore alla scansione. Ma in pratica è adottabile soltanto in ambienti molto stabili, perché una minima variazione della composizione del sistema porterebbe a segnalazioni di modifiche che possono facilmente scatenare meccanismi di falso allarme.

***C**he evoluzione si prevede per l'Italia?*

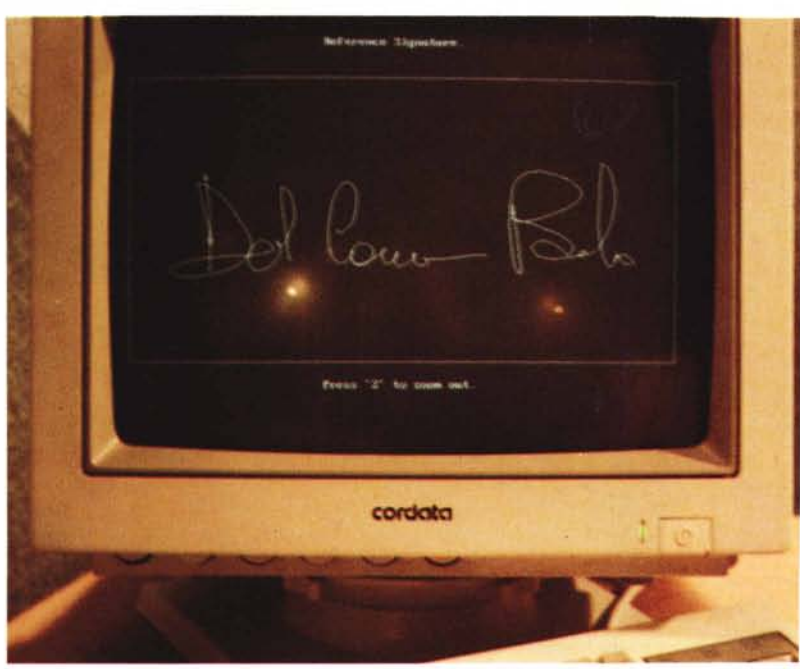
In Italia esiste una notevole attenzione sia per la prevenzione che per il contrasto significativo.

Abbiamo un interesse specifico nella Polizia di Stato, abbiamo il ruolo determinante delle riviste (tra cui la vostra), abbiamo una presenza sulla stampa e in televisione.

Non importa se spesso i messaggi sono enfatizzati, l'importante è che si parli del problema, e le aziende stanno rispondendo molto bene.

Dall'altro lato assistiamo al fenomeno preoccupante della crescita del numero di virus italiani, e parallelamente al lancio nel nostro Paese di virus sviluppati altrove, in un meccanismo di scambio che stiamo cercando di chiarire.

Stefano Toria

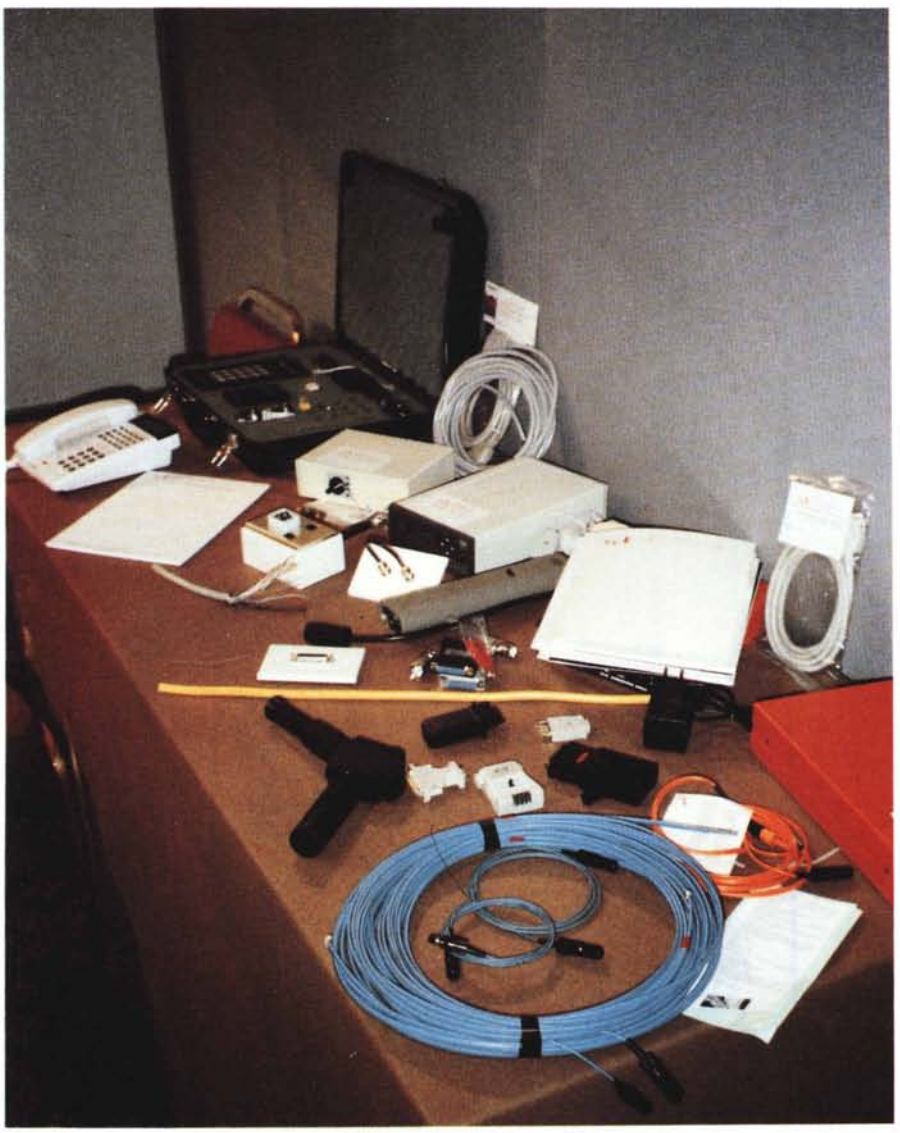


Ci sono anche sistemi per il riconoscimento della firma, ma la loro affidabilità non è ancora molto elevata.

terno dell'organizzazione colpita, altro che ragazzini-hacker...

Informazioni riservate

Quando si parla di sicurezza informatica si pensa prima di tutto a terribili disastri o a rovinose incursioni di hacker in importanti archivi. Ma ci sono aspetti assai meno spettacolari e, purtroppo, molto più diffusi: le intrusioni «conoscitive», cioè l'accesso non autorizzato a memorie che contengono dati riservati. Queste violazioni della privacy possono riguardare basi di dati pubbliche (si pensi alla giusta riservatezza che dovrebbe riguardare i dati sanitari di ciascuno di noi), o piccoli archivi personali. A questo proposito è stata molto interessante la relazione presentata al Securicom da Rosanna Santonocito del «Sole 24 Ore», che ha messo in rilievo il conflitto che può sorgere tra la riservatezza delle informazioni e la necessità, per motivi di organizzazione, che le stesse informazioni possano essere lette da più persone.



La sicurezza delle reti richiede anche complessi controlli sull'hardware.

Gli aspetti più importanti della sicurezza di un'azienda editoriale sono due, ha detto Santonocito: il primo riguarda il giornale stesso, le cui fasi di produzione sono tutte governate da computer, dalla stesura degli articoli all'impaginazione, fino alla stampa. «L'integrità dei dati, le misure di ripristino nel caso di un blackout o di un'interruzione del sistema o delle comunicazioni sono l'integrità del giornale stesso. La sicurezza del sistema editoriale è la sicurezza che il giornale arrivi l'indomani in edicola. Ma è anche fondamentale l'aspetto della riservatezza e della protezione delle informazioni che sono alla base dell'attività del giornalista, nel momento della raccolta delle informazioni, della stesura del pezzo e della lavorazione della pagina, come pure la tutela del suo archivio di informazioni e fonti».

Al «Sole 24 Ore» è in corso il passaggio dal vecchio sistema centralizzato a un'architettura client-server. Il server supporta le gestione delle basi di dati, gli archivi di produzione, il funzionamento della rete e, naturalmente, il governo dell'intero sistema. Il giornale nasce invece nelle stazioni «client». Qui si concentrano tutte le attività editoriali e i relativi problemi, fra i quali uno è particolarmente importante ai fini della sicurezza: la possibilità che a determinati archivi possano accedere utenti diversi dal giornalista che ha preparato o sta preparando un determinato pezzo. Infatti il testo deve essere visionato da caposervizio o da altre funzioni gerarchicamente superiori, deve passare all'impaginazione e alla tipografia. C'è anche la questione relativa alla discontinuità della presenza del giornalista in redazione, e quindi questi accessi devono essere possibili anche in sua assenza, per non parlare dei casi non infrequenti in cui più giornalisti lavorano sullo stesso argomento e devono quindi avere la possibilità di scambiarsi informazioni.

Tutti questi problemi vengono gestiti dal sistema in modo automatico (anche i flussi sulla rete sono crittografati con algoritmi variabili), con una stratificazione che prevede l'uso di password e chiavi gerarchiche. In pratica è previsto il flusso operativo di un testo, con il consenso per i diversi accessi previsti. All'inizio, nel quotidiano milanese, come in altre aziende editoriali, il sistema era molto rigido, e questo comportava difficoltà nelle situazioni di emergenza, al-

l'ordine del giorno nel lavoro giornalistico. Il sistema dei livelli è stato quindi azzerato e chiunque può dare l'approvazione per il rilascio di un pezzo.

Addio riservatezza! Ma il sistema mantiene una traccia degli accessi che sono stati operati su ogni articolo, e così è possibile risalire all'autore di eventuali azioni non consentite. La lezione che si ricava da questa esperienza è chiara: le regole di sicurezza devono essere stabilite in modo di non provocare difficoltà nella gestione del sistema, e per questo spesso è necessario ricorrere a compromessi. Lo aveva detto, il giorno prima, il vicequestore Antonio Pansa: se non siamo sicuri di poter impedire che qualcuno apra la nostra cassaforte, almeno spargiamo intorno un po' di farina, così potremo trovare le tracce del malfattore. Ma la sicurezza deve essere anche una preoccupazione fondamentale dell'utente: sta a lui non lasciare «in giro», cioè in archivi accessibili ad altri, le informazioni che vuole mantenere riservate, e inventare e custodire con attenzione le sue password.

Carte intelligenti e riconoscimento biometrico

Uno dei problemi fondamentali della sicurezza informatica, e non solo informatica, è l'identificazione delle persone che accedono a un sistema o a un'area determinata. Oggi il metodo più diffuso è quello dei «badge» magnetici, cioè dei tesserini di plastica, simili alle carte di credito, che attivano il consenso all'accesso a un sistema o a un'area fisicamente protetta, e nello stesso tempo comunicano i dati del possessore al sistema di controllo, che li conserva in memoria. Ma è chiaro che sottrarre un tesserino è troppo facile, e anche la produzione di badge falsi non è un grosso problema. Un maggiore livello di sicurezza è dato dal controllo incrociato dei dati del tesserino con una password (il PIN, Personal Identification Number del Bancomat, per esempio), ma anche questo può essere sottratto al legittimo titolare.

È necessario un controllo «intelligente», che può essere ottenuto con le carte a microprocessore, come ha spiegato a Bologna Giovanni Gurrieri, responsabile marketing nella Direzione Commerciale di Olivetti Italia (che ha introdotto la C-LESS, il tesserino senza contatti del quale abbiamo parlato sel numero 117 di MC). La carta intelligente consente un'elaborazione locale e quindi il riconoscimento dell'utente anche off-line, cioè senza la necessità di collegamento con un elaboratore centrale (come avviene nel Bancomat), e quindi si presta particolarmente alla sicurezza degli ambienti ad architettura distribuita, oggi sempre più diffusi.

Però anche la carta intelligente non può garantire un sicuro riconoscimento

Disaster Recovery: l'esperienza della FIAT

Intrusioni, virus, guasti a singoli elementi hardware: le procedure di sicurezza di un sistema informativo devono prevedere tutte le possibili azioni per la protezione degli archivi e la continuità delle elaborazioni. Per questo vengono duplicati gli archivi e molto spesso si prevede la sostituzione di un elaboratore con un altro di riserva, spesso in modo automatico. Ma se l'intero sistema, per un motivo o per l'altro, va fuori servizio? Pensiamo a un incendio, un terremoto, un attentato: gli scongiuri di rito possono non essere sufficienti ad allontanare un'eventualità di questo tipo, e anche la prevenzione può fallire. È necessario quindi prevedere e predisporre i mezzi per riprendere l'attività nel più breve tempo possibile, insomma si deve fare un piano di «Disaster Recovery».

La risposta della FIAT a questo problema è stata illustrata al Securicom da Walter Castellazzi, che ha parlato della Sersis, una società nata espressamente per fornire tutti i servizi necessari ad assicurare la continuità delle attività di elaborazione al tutte le società del Gruppo, in presenza di emergenze o sinistri che rendano indisponibili le risorse dei rispettivi centri.

Gli elementi fondamentali del progetto sono due: il centro di continuità e il piano di ripristino.

Il «centro di continuità» è situato in uno stabilimento provvisto di tutti i possibili sistemi di protezione anti-intrusione e di collegamenti con l'esterno, fra i quali una centrale telefonica gestita dalla SIP. Non mancano i gruppi elettrogeni ad avviamento automatico e poderosi sistemi di batterie per assicurare la continuità dell'alimentazione elettrica. Il centro è diviso in due aree, ciascuna della quali comprende sala macchine, sala regia e uffici: la prima (area calda) è completamente attrezzata con eleboratori, memorie e sistemi di trasmissione dati. Serve per emergenze della durata massima di trenta giorni ed è in grado di entrare in funzione entro ventiquattr'ore dalla notifica dell'emergenza. Il sistema è stato dimensionato in modo di supportare le attività del centro più importante del gruppo, quello della FIAT Auto.

Per emergenze più lunghe, fino a un anno (il tempo presumibilmente necessario a ricostruire un centro distrutto) c'è una seconda area (area fredda), completa di tutte le infrastrutture, ma priva di macchine. I fornitori si sono impegnati a installare entro un mese tutto l'hardware che possa essere necessario. In questo modo, in caso di un'emergenza prolungata, le elaborazioni passano alla seconda area nel giro di un mese e la prima resta disponibile per altre, non augurabili, necessità di intervento. E se anche questo non basta? Statisticamente, ha detto Castellazzi, è un'eventualità quasi impossibile. In ogni caso il centro può servire contemporaneamente fino a quattro utenti, suddividendo le risorse di elaborazione fino a dove è possibile in funzione dei MIPS e dei Gigabyte di memoria disponibili.

Ma la disponibilità fisica del centro di continuità non basta. Occorre stabilire le procedure per il suo impiego e addestrare il personale. Ecco dunque l'importanza del «piano di rispristino», che prevede tutte le azioni necessarie a spostare le eleborazioni nel centro di continuità al verificarsi dell'emergenza e il ritorno al centro primario a emergenza finita. Il centro in realtà è sempre in funzione con simulazioni di ripristino, e in esso si alterna il personale dei centri primari, che in caso di necessità deve sapere esattamente tutto quello che deve fare. È stabilito in partenza il compito di ciascuno, e l'hardware e le procedure sono continuamente aggiornati. «Il piano di ripristino è, quindi, la descrizione delle azioni di tipo operativo e logistico che devono essere svolte prima, durante e dopo il verificarsi dell'emergenza e la descrizione nel minimo dettaglio di "chi fa che cosa" per non lasciare nulla al caso o alla libera iniziativa».

E ora vediamo alcuni dati del centro della Sersis, che, fra l'altro, è a disposizione anche di società esterne al Gruppo FIAT:

— la sala macchine e telecomunicazioni dell'area «calda» ha una superficie di 800 mq, mentre l'area «fredda» misura 1.200 mq.

— Ciascuna delle due aree dispone di 380 mq di uffici; nella prima questi sono attrezzati con scrivanie e terminali, nella seconda sono solo predisposti.

— 240 mq sono occupati da nastroteche operative.

— Nell'area «calda» è installato un IBM 3090 con una potenza di 44 MIPS; le unità a dischi hanno una capacità di 150 GB, oltre alle unità a nastri e a cartucce.

— Infine la potenza elettrica: una sottostazione da 4.000 kVA e 2.850 kVA di gruppi elettrogeni automatici, oltre ai gruppi di batterie, assicurano la continuità dell'alimentazione.

È superfluo a questo punto parlare della centrale di raffreddamento e di quella per il trattamento dell'aria, o della centrale termica: questa è sicurezza «chiavi in mano», come comperare un'automobile...

del soggetto che la usa. In molti casi è indispensabile che il computer possa controllare l'identità di una persona, operazione possibile digitalizzando e archiviando alcune caratteristiche fisiche di un soggetto. Ne ha parlato Attilio Colombo in una relazione sulle tecniche di riconoscimento biometrico densa di dati tecnici e rilevazioni statistiche. Bisogna distinguere, ha detto Colombo, tra «riconoscimento» e «identificazione» di un soggetto. Nel primo caso la digitazione di alcuni dati o l'introduzione di un badge richiamano le caratteristiche biometriche del soggetto da un archivio, e

Virus: prevenzione e difesa

Dopo i clamori giornalistici che si sono verificati intorno alle date di venerdì 13 ottobre 1989 e del 6 marzo di quest'anno per il pubblico i virus sono divenuti una realtà nota, anche se non compresa a fondo. Due interventi che si sono succeduti nel corso della prima mattinata hanno contribuito a gettare maggiore luce, oltre che sul fenomeno in sé, su ciò che si sta facendo in Italia per prevenire i maggiori rischi.

Il prof. Marco Mezzalama del Politecnico di Torino ha illustrato le modalità con cui può verificarsi l'attacco di un virus a un sistema, con particolare riguardo alle configurazioni di rete. Negli ambienti distribuiti infatti risiedono i maggiori rischi connessi alle infezioni virali poiché l'integrazione dei sistemi, finalizzata alla rapida diffusione delle informazioni, costituisce un fattore accelerante anche per la diffusione dei virus.

Quale il rimedio? Innanzitutto una particolare attenzione alla problematica della sicurezza sin dalle prime fasi della progettazione delle reti, adottando configurazioni restrittive e attivando tutti i possibili filtri. Occorrerà prevedere delle funzioni di controllo degli accessi e una raccolta di informazioni che consenta agli amministratori di mantenere traccia di ciò che accade nel sistema.

Il successivo intervento è stato curato da Fulvio Berghella, direttore centrale di Istinform che è l'istituto di consulenza informatica e organizzativa delle aziende ordinarie di credito e delle Banche Popolari. Prendendo l'avvio dall'attività di SecurityNet, l'iniziativa attivata lo scorso anno da Istinform per la prevenzione delle infezioni virali (v. intervista nel riquadro), Berghella ha tracciato un quadro della situazione nel nostro Paese e nel mondo per quanto attiene alla diffusione dei virus.

Una breve storia dei virus dal 1986 a oggi vede sostanzialmente tre fasi nello sviluppo dei virus: un primo periodo caratterizzato da azioni spontanee di impronta goliardica o di sfida intellettuale, seguito da una fase in cui si affermano nuove tecnologie nello sforzo di mimetizzare l'attività dei virus e renderli invisibili ai programmi antivirus, fino all'attuale situazione in cui si è potuta identificare l'attività di numerosi gruppi che curano la realizzazione e la diffusione di intere famiglie di virus.

Dal lato della difesa, molte aziende produttrici di software si sono dedicate allo sviluppo di programmi antivirus, per un mercato che negli ultimi anni è cresciuto del 30% l'anno.

D'altra parte nemmeno i creatori di virus sono stati fermi: nel mese di aprile 1992 i virus noti ammontavano a 1263 nel solo ambiente MS-DOS, ma si stima che circa altri 300 virus siano in attesa di essere classificati ed analizzati nei laboratori di ricerca antivirus. I dati disponibili, raccolti ed elaborati da Istinform in un'apposita ricerca, mostrano una crescita esponenziale nel periodo luglio '89-marzo '92.

Le proiezioni per i prossimi due anni non sono rosee: gli esperti concordano sul fatto che anche la crescita del numero di virus non possa essere inferiore al 30% annuo nei prossimi tempi.

Berghella è passato quindi ad illustrare la provenienza dei virus, per quelli di cui è stato possibile tracciarne l'origine: l'Italia è al quarto posto nella classifica, con 26 virus, dopo la Bulgaria con 51, gli USA con 48 e la CSI (ex URSS) con 40. L'Italia ha conquistato il proprio primato negativo in pochi mesi, tra l'agosto del 1991 e il gennaio del 1992.

La ricerca realizzata da Istinform prosegue poi con alcuni interrogativi: a quanto ammonta il danno medio causato da un virus? Chi porta i virus in azienda? Come reagisce l'organizzazione?

Si è osservato che nella maggior parte dei casi il danno diretto causato dai virus consiste nella perdita di un determinato quantitativo di tempo alla ricerca di tutti i possibili ricettacoli di infezione e per il ripristino del sistema allo stato originario. I tempi totali dichiarati dagli interessati portano a una media di 21 ore per ciascun ambiente isolato dell'azienda. Ma nei casi in cui i computer coinvolti siano più di uno, e si verifichi la presenza combinata di più virus, la stima sale a 39,5 ore necessarie per il ripristino dei sistemi.

Si è cercato poi di determinare da dove provenissero i virus in azienda; molti ritengono che la fonte principale di infezione stia nei videogiochi e negli applicativi introdotti illecitamente, ma la ricerca ha consentito di individuare altre cause: ad esempio il personale di società esterne che frequenta l'azienda per manutenzione del software o dell'hardware è stato responsabile di infezioni nel 35,5% dei casi. Nel 10,52% dei casi esaminati i virus sono pervenuti attraverso dischetti arrivati ufficialmente da altre aziende (versioni dimostrative, etc.).

Nelle aziende colpite da virus si è cercato di adottare soluzioni organizzative adeguate. Le misure poste in atto sono state diverse: da un controllo generalizzato su tutto il software che entra in azienda a controlli parziali e differenziati, alla installazione di software antivirus. La disposizione più frequente consiste nel divieto di utilizzare software diverso da quello distribuito ufficialmente dall'azienda. È stata adottata dall'84% delle aziende, ma sempre a seguito di brutte esperienze con qualche virus.

Il controllo di configurazione nel software

Un tentativo di risolvere il problema della sicurezza alla radice si riscontra nell'ITSEC (Information Technology Security Evaluation Criteria). Nato da un gruppo di lavoro a cui parteciparono esperti francesi, tedeschi, olandesi e inglesi, è stato coordinato dal Senior Officials Group - Information Security della Commissione delle Comunità Europee.

Un lavoro analogo era stato svolto dal Dipartimento della Difesa U.S.A., che in precedenza aveva pubblicato il TCSEC (Trusted Computer System Evaluation Criteria), noto anche come «Orange Book». Analoghi corpi normativi esistono anche nel Regno Unito, in Germania e in Francia.

L'obiettivo di ITSEC è di valutare la sicurezza insita in un sistema o in un prodotto hardware o software. Parlando di sicurezza si fa riferimento a tre caratteristiche: la riservatezza intesa come prevenzione di rivelazioni non au-

il sistema procede a un confronto tra questi dati e quelli rilevati al momento. Nel secondo il computer identifica il soggetto sulla base di questi dati, confrontandoli con tutti quelli che ha in memoria: si tratta di sistemi particolarmente interessanti per le indagini di polizia.

I sistemi oggi disponibili, per lo più ancora in fase di sperimentazione o di messa a punto, sono basati su elementi fisici diversi: l'immagine della retina, la classica impronta digitale, il disegno tridimensionale della mano, l'analisi delle caratteristiche della voce. La definizione del livello di sicurezza di questi sistemi viene ricavata dall'incrocio di due dati: la percentuale di riconoscimenti errati, quelli in cui l'accesso viene erroneamente consentito a un soggetto non autorizzato, e la percentuale di rifiuti opposti, al contrario, a soggetti autorizzati. Inoltre è importante che l'operazione avvenga in tempi ragionevoli, al più una decina di secondi.

Altri sistemi in fase di studio riguardano l'analisi facciale, ottenuta con sistemi impostati su reti neurali, e l'analisi della dattilografia, molto utile per l'identificazione degli operatori autorizzati ad agire su determinati terminali. Questo sistema analizza le caratteristiche della digitazione sulla tastiera e comprende anche un algoritmo di crittografazione e una protezione antivirus.

Conclusioni

Al di là dei sistemi più o meno sofisticati che possono essere impiegati per la protezione dei sistemi informatici, o per impedire che i sistemi stessi vengono impiegati per scopi non leciti, un dato emerge chiaramente dal convegno di Bologna: il discorso sulla sicurezza va impostato in un'ottica globale, che comprende sia la protezione fisica delle installazioni, sia la prevenzione di intercettazioni, intrusioni logiche e contaminazioni da virus, sia i guasti dell'hardware o i malfunzionamenti del software che possono causare perdite o alterazioni di dati. E in più la prevenzione dei reati che possono essere commessi attraverso sistemi informatici e telematici, anche con sistemi che consentano, mediante la registrazione degli accessi, l'identificazione a posteriori degli autori di interventi illeciti. Una materia estremamente complessa, anche perché nell'eterno gioco a guardie e ladri sono quasi sempre questi ultimi a fare la prima mossa, e tocca alle guardie inseguire i malfattori. E nel campo dell'informatica la prima mossa consiste spesso nell'impiegare metodi e tecnologie sempre più avanzati.

Prevedere e prevenire, dunque, e anche scoraggiare. Soprattutto bisogna far sì che la sicurezza sia un elemento intrinseco non solo dei sistemi, ma anche del comportamento degli addetti. Questo significa creare una «cultura della sicurezza». Insegnare l'informatica non deve ridursi a spiegare il bit e il byte o il funzionamento di una macchina, ma anche informare e persuadere sui rischi insiti nell'esistenza stessa delle nuove tecnologie. MC

torizzate di dati, l'integrità come prevenzione di modifiche non autorizzate, e la disponibilità come prevenzione di rifiuti non legittimi di fornire informazioni o risorse.

Sette livelli crescenti, da E0 a E6, descrivono situazioni in cui si passa da una affidabilità del tutto inadeguata a livelli via via crescenti, fino ai livelli massimi. È interessante notare come si sia introdotto il concetto di «obiettivo di sicurezza» (Target Of Evaluation o TOE): lo scopo di ITSEC non è di definire livelli crescenti di sicurezza bensì livelli crescenti di controllo sul raggiungimento dell'obiettivo di sicurezza.

Gli strumenti adottati infatti sono quelli già noti negli ambienti di sviluppo rigorosamente controllati: descrizioni formali del disegno del progetto, controllo di configurazione, analisi del progetto e/o del codice sorgente, modellizzazione formale della politica di sicurezza, controllo di congruità delle funzioni di imposizione della sicurezza e disegno architetturale con gli obiettivi politici. In sintesi al fine di ottenere un accettabile livello di affidabilità dei sistemi è necessario porre la giusta enfasi sul processo di sviluppo e sulle modalità di attivazione in esercizio del prodotto/sistema.

La sicurezza di un supercomputer

L'esperienza del CINECA, il Consorzio Interuniversitario per il Calcolo Automatico presso il quale è installato tra l'altro un supercomputer Cray, mostra come i problemi in un ambiente di questo genere non siano particolarmente dissimili da quelli di qualsiasi altro ambiente di tipo universitario o accademico. Le esigenze di condivisione di programmi e dati fanno risultare spesso restrittive le misure di sicurezza necessarie in un sistema di grandi dimensioni.

Il problema è stato risolto in fasi differenziate. All'inizio l'obiettivo è consistito nel garantire due elementi principali: il controllo sull'identità dell'utente e la protezione delle basi di dati.

È noto che gli attentati alla sicurezza di un elaboratore possono rientrare in tre tipologie: azione irresponsabile occasionale, curiosità e sfida intellettuale, vera e propria azione dolosa.

I primi due tipi di rischi sono i più frequenti in ambiente universitario, ma per difendersi da essi sono sufficienti dei semplici meccanismi di difesa come quelli accennati, integrati da alcuni accorgimenti più precisi quali il limite di vita per le password e una regola precisa per la costituzione delle stesse password, per impedire l'uso di parole banali (es. la password uguale al nome di login).

Associato a queste misure di prevenzione si è adottato il criterio del cosiddetto «least privilege», consistente nel garantire a ciascun utente esclusivamente quei privilegi che gli consentano di portare a termine specifiche operazioni.

Con lo sviluppo del modello di elaborazione distribuita si sono acquisiti gli strumenti per consentire all'utenza di lavorare sfruttando appieno le caratteristiche di un sistema di questo genere. Si sono adottate tutte le misure di sicurezza previste da UNICOS, l'ambiente Unix del Cray, imponendo regole per la definizione della password, vita limitata della stessa, definizione rigorosa dei privilegi accordati a ciascun utente, e severa limitazione delle interazioni con i file system remoti.

L'adozione di misure restrittive non ha tuttavia intralciato la fornitura dei servizi fondamentali: trasferimento di file, utilizzo di X-Windows e posta elettronica.

È in corso il progressivo adeguamento ad alcuni obiettivi minimali di sicurezza, sostanzialmente nei confronti di eventuali attacchi provenienti dalla rete a cui il Cray è connesso. Saranno valutate le possibilità di attivare un sistema di sicurezza contenuto in UNICOS, che implementa alcune delle indicazioni contenute nell'«Orange Book» a cui si faceva riferimento più sopra, sebbene sarà difficile che tali raccomandazioni vengano integralmente applicate per la poca realisticità e la intrinseca difficoltà di applicazione di misure così restrittive in un ambiente universitario.

Stefano Toria

Professionalità ed

Assistenza Qualificata

EGiS COMPUTER

Prodotti di Alta Qualità

Convenienza nei Prezzi

VENDITA AL MINUTO E PER CORRISPONDENZA
COMPETENZA E CORTESIA A VOSTRA DISPOSIZIONE PER CONSIGLIARVI NELLE VOSTRE SCELTE

I punti vendita di EGiS COMPUTER sono a :

Sede ROMA : Via Castro Dei Volsci, 40/42 (M ColliAlbani) - 00179 - Tel. 06/7810593 - 7803856
Filiale UDINE - Zona Tre Venezie - S. Daniele del Friuli - Via Kennedy, 31 Cso Riviera, 1 - Tel. 0432/941078

Orario 9:30-13:00 / 16:30-19:30 - Giovedì chiuso - Sabato Aperto

CONTATTATECI ! IL VANTAGGIO PIU' GROSSO SARA' IL VOSTRO !

TUTTI I SISTEMI PC-COMPATIBILI

> > Anche IN PROVA nella vostra sede per 10 gg EFFETTIVI !!* < <
Pagamento RATEIZZATO in TUTTA ITALIA - Pratica in 1 giorno

286 /16	**286 / 27**	**386sx / 16**	**386sx / 25**
415	**579**	**605**	**699**
386 / 25	**386 / 33**	**386 / 40**	**486sx**
899	**999**	**1.115**	**1.450**
486 / 25	**486 / 33**	**486 / 33**	**Notebook 2Mb**
1.550	**64K Cache**	**256K Cache**	**386sx HD60Mb**
	1.696	**1.875**	**2.390**

Ogni computer è da ritenersi funzionante, collaudato e così configurato :
Piastra Madre - 1 MegaByte RAM - Scheda Grafica VGA 800x600
Drive 1,44 - 2 Seriali - 1 Parallela - Cabinet DeskTop - Tastiera 101 Tasti

PIASTRE MADRI

286 / 16	130
286 / 27	170
386sx / 16	270
386sx / 25 SMT	300
386 / 25	499
386 / 33 Cache	599
386 / 40 Cache	669
486sx	950
486/33 64 K Cache SMT	1.190
486/33 256K Cache SMT	1.330

Schede VGA

800x600 256 KByte	75
1024x768 512 KByte	119
1024x768 1 MByte	175
1280x1024 1Mb 32000 Col.	220
1280x1024 700000 Colori	269

AMIGA

Amiga 500	565
Amiga 500 Plus	667
Amiga 2000	1.200
Drive Esterno	129
Espans. 512K A500	69
Monitor 1084/S CBM	395
Monitor D-Top Stereo	360
Mouse Amiga	50
Scanner Amiga	380
Videon 3.0	462
MIDI Amiga	60
AT ONCE	396
HD 500 GVP 50 M	820
HD 2000 GVP 80 M	990
Controller GVP	370

I prezzi sono in migliaia di lire (IVA escl.)

(*) restituzione dell'anticipo se non soddisfatti con addebito solamente del 12% quale avvenuto noleggio

DRIVE & Floppy

1,2 MByte	105
1,44 MByte	95
3,5 DSDD	700 £
3,5 HD	1400 £

CABINET

Desk Top	140
Mini Tower	220
Tower Medio	290
Alimentatore	90

> > > > > > STAMPANTI < < < < < <

9 AGHI 259 **24 AGHI 375** **LASER 1.175**

Citizen - OKI - Star - NEC - Epson - HP - Fujistu

GARANZIA 12 MESI
Riparazioni con sostituzione del pezzo in 24 ore lavorative !

Rinnovamento del Vostro vecchio sistema con manodopera gratuita !

ACCESSORI

Sound Blaster	210
Sound Blaster Pro	330
Gruppo Continuità 250W	370
Gruppo Continuità 500W	490
Gruppo Continuità 700W	650
Scanner + OCR	280
Scanner 256 toni + OCR	420
Scanner a Colori	699
Scanner da tavolo	980
Fax Murata M15	750
Videon 3.0	650

ANCHE A RATE IN TUTTA ITALIA !
Potete ora avere in mano la certezza di ogni Vostro acquisto : rate da £52000 per 12 mesi senza cambiali
Evasione della pratica in 1gg su territorio nazionale
Un'occasione in più , una comodità in più...

GROSSA POTENZA VIDEO
A BASSO COSTO
Aggiornate la vostra VGA !
Max 1280x1024 - Max 32000 Colori **£ 49.000**
Idem + Anti-Aliasing 750000 Col. **£ 79.000**
... e senza cambiare Monitor !!!

MONITOR

VGA Monocromatico	160
VGA Mono 1024	199
VGA Color a partire da	390
VGA Color 1024 da	425
MultiSync Color	650
VGA 19" Color 1024	1.700
NEC 3FG	990

HARD DISK

45 Fujitsu	340
105 Fujitsu	600
350 Fujitsu	1.495
135 Segate	660
210 Segate	980
52 Quantum	450
80 Quantum	550
400 Western Digital	1.600
CD ROM + Audio	600
CD ROM esterna	950
Syquest	1.250
Streaming Tape - - Colorado 120	599

ADD ON

Tastiera 101 tasti	59
Contr. FD-HD AT Bus	40
Contr. FD-HD MFM	120
Seriale	25
Parallela	20
Game Doppia	22
Multi I/O	50
Joystick	22
Controller + 2 Ser/2 Paral	75
Mouse a partire da	19
MS DOS 5.0	150
MS DOS + Windows 3.1	299
Windows 3.1 (agg.)	99