Metti al SICURO il tuo ISTITUTO SCOLASTICO

Linee guida per la SICUREZZA informatica e la tutela della PRIVACY

Microsoft®

SOMMARIO

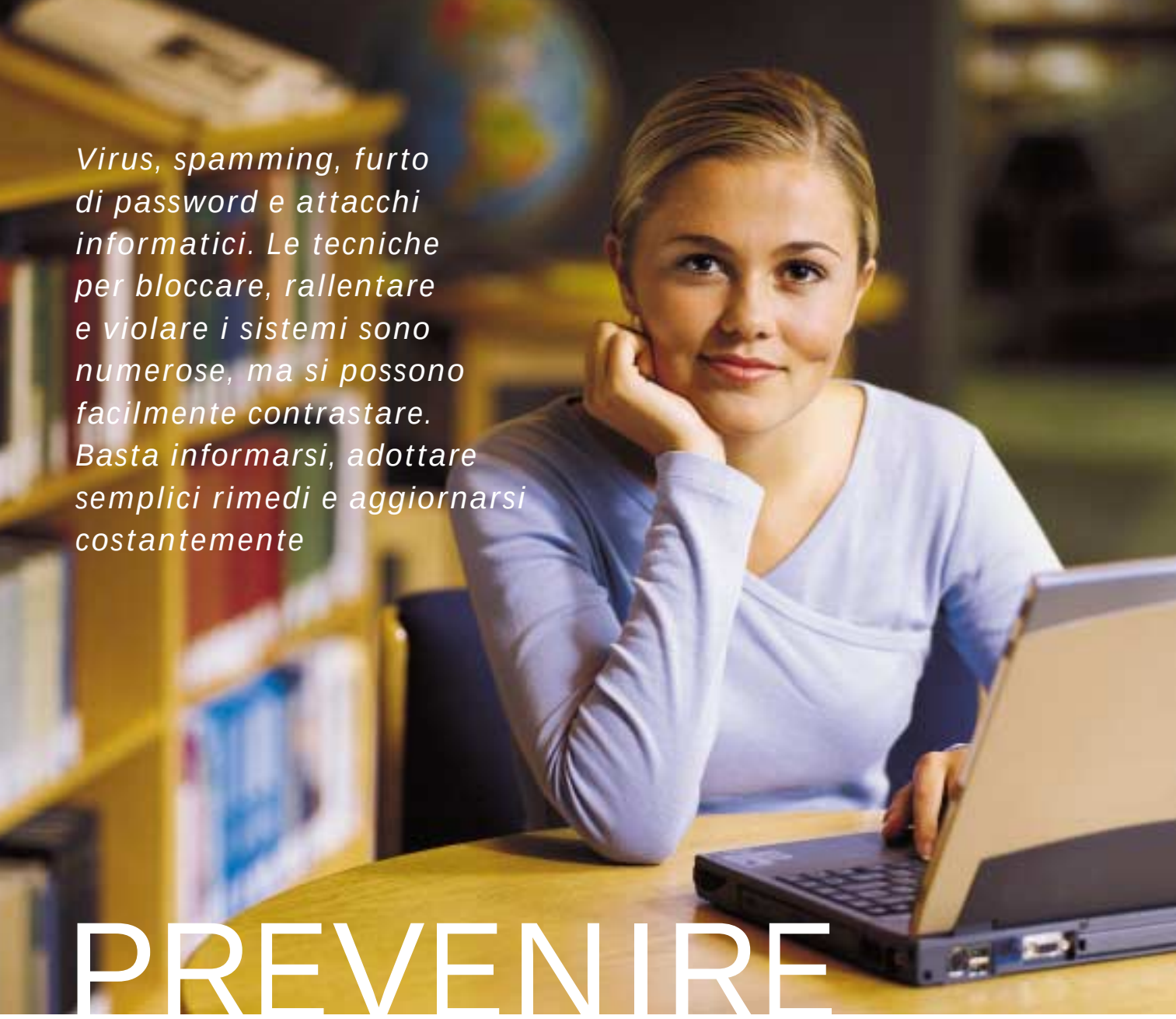
Metti al SICURO il tuo ISTITUTO SCOLASTICO

Si dice che quando un problema assilla in maniera grave è meglio agire con decisione. Si interviene, si rimuove la causa, spendendo energie (e spesso denaro) e con il senno di poi - alla fine - si ricorda al malcapitato sottoposto alla cura che era meglio prevenire. Lo stesso accade agli studenti che non superano gli esami o accumulano debiti formativi. Era meglio che studiassero a tempo debito, si ricorda loro.

In maniera analoga, quando si prende in considerazione il tema della sicurezza informatica esistono due approcci differenti con cui valutare impegni, implicazioni, conseguenze. C'è chi corre ai ripari una volta subiti i danni e chi, invece, più intelligentemente, cerca di stare al passo con i tempi e affronta le dovute precauzioni con il giusto anticipo.

Per chi usa i computer a fini didattici, la sicurezza è uno dei valori a cui prestare maggiore attenzione, insieme certamente alle finalità di studio, all'appropriatezza degli strumenti e al loro corretto impiego. Posizionare un computer in un'aula è come adottare un libro di testo: deve garantire una reale crescita degli studenti, favorire la collaborazione e l'approfondimento, ma anche proteggere chi non ha ancora acquisito il giusto spirito critico, mettendo al sicuro ogni aspetto didattico. Un computer deve proteggere i dati personali, le informazioni. Più in generale, le attività svolte. Deve garantire, cioè, che tutto quanto elaborato attraverso i sistemi informatici sia mantenuto in funzione, senza manomissioni, ritardi, cancellazioni. Sia in aula sia nelle segreterie o nelle amministrazioni è necessario che il software resista agli attacchi esterni, preveda e annulli l'impatto negativo di eventi straordinari o attività illegali. Crei, cioè, un effetto "cassaforte" intorno ai dati, mantenendoli e garantendo continuità al lavoro dei dipendenti degli istituti scolastici, dei docenti e degli studenti. Tutto questo in un contesto in cui le insidie sono imprevedibili: oggi si va dall'infezione di nuovi e sempre più pericolosi virus informatici all'uso illecito dei PC da parte di hacker, all'attacco di malintenzionati che intendono disturbare e manomettere i sistemi. Ma non solo. I problemi possono essere anche di altro tipo: l'errato trattamento dei dati personali come previsto dalla nuova Legge sulla Privacy, comporta sanzioni che vanno dalla multa fino alla reclusione. Non si tratta cioè di semplici e costosi malfunzionamenti, ma di reati.

Come Microsoft abbiamo deciso da tempo di sostenere non solo una campagna di sensibilizzazione sui temi della sicurezza, di cui questa guida è un'ulteriore espressione, ma anche un'intensa attività di ricerca e supporto in favore degli istituti scolastici che lavorano quotidianamente utilizzando le tecnologie informatiche. A fianco delle migliorie nel nostro software, ai servizi di aggiornamento e informazione che forniamo anche online, abbiamo puntato sulla professionalità di partner e consulenti certificati (Microsoft Certified Partners) - che sappiano tradurre le nostre attenzioni verso gli istituti, le esigenze di docenti e studenti. La nostra convinzione è semplice: informare e informarsi è meglio che curare. Costa meno, contribuisce alla formazione, mantiene sicuri gli istituti scolastici. Non accumulate "debiti formativi" in questa materia. ■



Virus, spamming, furto di password e attacchi informatici. Le tecniche per bloccare, rallentare e violare i sistemi sono numerose, ma si possono facilmente contrastare. Basta informarsi, adottare semplici rimedi e aggiornarsi costantemente

PREVENIRE le INSIDIE informatiche

Il 29 giugno 2004 John Bambenek, ricercatore informatico, ha annunciato di avere scoperto una delle più sofisticate forme di truffa degli ultimi anni ai danni degli utenti Internet. Si trattava del caso di un nuovo programma malevolo progettato per rubare numeri di carte di credito, password e altri dati usati dagli utenti.
Grazie a una finta immagine inserita in un pop up pubblicitario il programma riusciva a penetrare sul PC della vittima e installarvi un programma per registrare i tasti battuti dall'utente.
Questo sofisticatissimo sistema era, però, del tutto inoffensivo nel caso fosse stato installato il software in grado di cancellare ogni vulnerabilità, reso disponibile gratuitamente da Microsoft già tre mesi prima.

Che cosa si rischia?

Con la sicurezza non si scherza, dunque. A parte il furto di password, esistono numerose altre tecniche elaborate dai pirati informatici. Indipendentemente dai meccanismi adottati la posta in gioco è comunque sempre molto elevata. Vediamo i casi più comuni. In primo luogo si può incorrere nel blocco dei sistemi, resi inutilizzabili da virus, danni fisici o attacchi di pirati informatici. In altri casi si verifica soltanto un rallentamento delle attività, meno pericoloso, ma altrettanto deleterio dal punto di vista economico. Provate a immaginare che cosa significhi fermare, per esempio, il lavoro di tutti i dipendenti di un istituto, le lezioni e le attività didattiche a causa di un malfunzionamento

della rete. C'è poi una questione di immagine. Subire una violazione dei propri sistemi di sicurezza, un sabotaggio o un'intrusione significa perdere credibilità e fiducia, in primo luogo da parte degli studenti: un danno difficilmente quantificabile che crea forte imbarazzo. Infine, i dati. I danni possono riguardare la modifica, il furto o addirittura la perdita totale di informazioni importanti, elemento fondamentale per l'erogazione dei servizi. In ultimo - anche se si tratta di un caso meno frequente - si rischia la corresponsabilità nei reati informatici. Se malintenzionati prendono il possesso del vostro PC potrebbero usarlo per arrecare danni a terzi, a vostra insaputa, coinvolgendovi in attività illegali.

"GLI ATTACCHI INFORMATICI CRESCONO DEL 50% OGNI ANNO"
(FONTE: ASSINFORM)

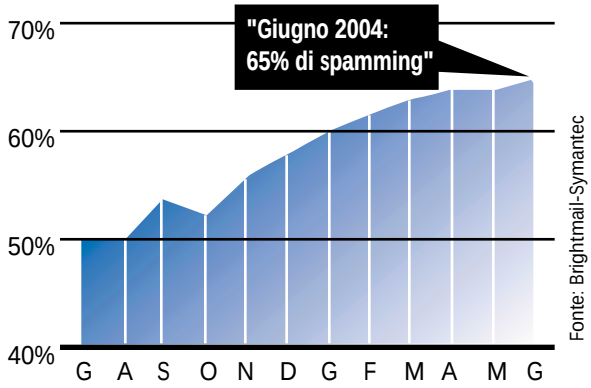
Le minacce più diffuse

Le più diffuse tecniche degli hacker sono note da molti anni, ma continuano a rappresentare una minaccia. I pirati informatici, infatti, raffinano sempre più sistemi e strumenti. Di conseguenza è necessario aggiornare periodicamente il modo con cui difendersi.
Ma quali sono le minacce più diffuse? Certamente il più noto degli inconvenienti è il cosiddetto spamming, ovvero la posta elettronica "spazzatura", la cui ricezione non è stata autorizzata. Oltre alla perdita di tempo che comporta è veicolo di virus e worm, piccole applicazioni dalle mille sfaccettature (che si trasmettono anche tramite semplice copia di un file da un dischetto) e che creano danni di ogni tipo: dal blocco del PC alla replica non autorizzata di messaggi o file, dalla trasmissione di informazioni alla modifica nascosta delle caratteristiche di un sistema. Altri pericoli sono gli attacchi informatici. Sono perpetrati dai pirati ai sistemi di rete e tendono a bloccare l'uso dei PC o sfruttare illegalmente le vulnerabilità delle reti. Talvolta sono pensati soltanto per isolare e bloccare un sito Internet, subissandolo di richieste e fermando le attività online. Un altro pericoloso e silenzioso sistema di sfruttamento è l'uso non autorizzato di identità digitali, ovvero di login e password altrui. Questo è un pericolo frequente quando si usano PC condivisi. Attraverso di esso si possono controllare le reti private, accedere a informazioni, rubare dati, modificare siti Internet per arrivare talvolta a sfregiare l'immagine stessa di un'istituzione, una scuola o un'università. Infine c'è l'abuso di accesso a Internet, realizzato sia ai danni delle reti fisse sia mobili; meno frequente, arreca comunque un notevole danno economico. In ultimo, c'è il furto vero e proprio: di computer, di informazioni estrapolate sulla base della buona fede degli utenti, di capacità di calcolo. Prendendo il possesso di un PC in maniera illegale, se ne possono sfruttare le caratteristiche, sia hardware sia software. Un inconveniente oneroso quanto pericoloso dal punto di vista legale.

Aggiornare, conoscere, prevenire

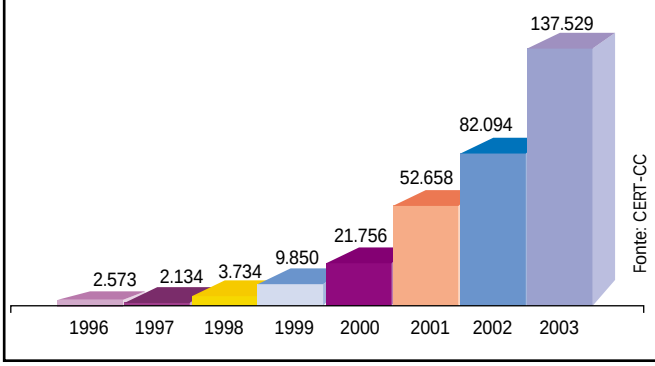
Per tornare alla vicenda scoperta da Bambenek si comprende ora come si tratti certamente di un caso estremo che mostra, però, due importanti verità. Primo: i pericoli informatici sono molti, difficilmente identificabili senza una costante attenzione o informazione, si moltiplicano in numero e virulenza, possono arrecare danni sia a livello economico, anche soltanto facendo perdere tempo, sia a livello di privacy, sottraendo e distribuendo informazioni importanti. Secondo: le insidie informatiche si possono contrastare in maniera efficace, soprattutto adottando politiche preventive e prendendo in considerazione la reale portata dei pericoli. Perché - ci si chiede spesso - dovrebbe riguardare proprio la mia scuola? Ebbene, taluni virus o lo spamming, per esempio, non fanno distinzione. Colpiscono in maniera indifferenziata, grandi e piccoli istituti scolastici, università, scuole di specializzazioni, aule isolate con poche postazioni. Il rimedio da adottare è, però, lo stesso: aggiornamento, prevenzione, conoscenza. Questa guida vi porterà passo passo a comprendere quali accorgimenti e comportamenti adottare per rendere sicuro il vostro PC o la vostra Rete. Nessun panico, dunque. La sicurezza si può migliorare, basta sapere come e soprattutto che cosa fare. ■

PERCENTUALE DEI MESSAGGI DI POSTA ELETTRONICA IDENTIFICATI COME SPAMMING



Oltre 104 miliardi di e-mail filtrati da Brightmail nel mese di giugno 2004

ATTACCHI ALLA SICUREZZA INFORMATICA



La sicurezza informatica è al centro del nuovo Codice in materia di protezione dei dati personali. Secondo la normativa ogni istituto scolastico dovrà dotarsi di adeguati sistemi di accesso ai dati, di credenziali per il trattamento degli stessi e aggiornare costantemente i sistemi di protezione

IL RISPETTO della PRIVACY

Cambia la privacy, cambiano le regole informatiche per la gestione dei dati personali. Dal 1 gennaio 2004 è in vigore in Italia il Codice in materia di protezione dei dati personali (Decreto legislativo n. 196 del 30/6/2003) che riforma interamente la disciplina sulla privacy, riaffermando il diritto di ognuno alla protezione delle informazioni personali che lo riguardano. Tutti gli istituti scolastici di ogni ordine e grado, ogni categoria privata o pubblica che abbia a che fare con il trattamento di dati personali o sensibili devono prestare attenzione alla nuova normativa, calibrando le proprie scelte e politiche sul nuovo disposto normativo. Devono attenersi, cioè, a precise regole di tipo tecnico, informatico, logistico e organizzativo per garantire l'integrità e la riservatezza delle informazioni trattate e limitare al minimo le fonti di rischio. È un impegno da prendere seriamente. Il dirigente scolastico rischia, infatti, di incorrere in sanzioni penali. Ma che cosa si deve fare in concreto? Entro il 30 giugno 2005 le istituzioni scolastiche dovranno stendere un Documento Programmatico sulla Sicurezza (DPS), ovvero un manuale in cui descrivere la situazione attuale - e trattare l'analisi dei rischi, la distribuzione dei compiti, le misure approntate, la distribuzione delle responsabilità, le procedure per il ripristino dei dati, i piani di formazione interna ecc. - e gli interventi che scuole, Atenei, centri di formazione intendono realizzare per adeguarsi alla nuova normativa. Se per certificate ragioni il DPS non può essere steso entro giugno, gli istituti scolastici hanno tempo al massimo entro la fine di settembre 2005.

IL REQUISITO MINIMO: LA SICUREZZA

Le misure minime

Ci sono alcuni provvedimenti considerati "minimi" da adottare, misure di sicurezza stabilite dal Garante della Privacy (cfr. www.garanteprivacy.it) che consentono ai direttori scolastici di evitare la responsabilità penale. Innanzitutto l'obbligo di ridurre quanto più possibile il rischio che i dati personali vengano distrutti o dispersi anche accidentalmente, che siano accessibili a persone non autorizzate, che possano essere trattati in maniera illecita. Questo significa che le istituzioni scolastiche devono applicare opportuni interventi che tengano conto anche del progresso tecnologico e dell'utilizzo sempre più frequente, per esempio nelle segreterie scolastiche, di PC per l'archivio e la custodia dei dati. Gli archivi digitali in cui sono memorizzate le informazioni devono, di fatto, essere custoditi e resi sicuri, protetti sia da possibili minacce esterne (virus, attacchi hacker, ecc.) sia da un uso improprio all'interno dell'istituto. In altre parole, il requisito minimo è la sicurezza.

Accesso, credenziali, aggiornamenti

In primo luogo è necessario proteggere l'accesso ai dati, che deve avvenire soltanto da parte di persone autorizzate. Il nuovo Codice prevede l'utilizzo di una serie di strumenti affinché, attraverso specifici criteri di autenticazione, i sistemi di sorveglianza e di sicurezza

COSA DEVONO FARE I DIRIGENTI SCOLASTICI

- Nominare uno o più responsabili della sicurezza e del trattamento dei dati (ove disponibile il docente che ha seguito la formazione C2 del progetto FORTIC);
- Nominare gli incaricati;
- Fare il censimento dei trattamenti nell'organizzazione per potere effettuare le notificazioni;
- Emanare un regolamento sul trattamento, la comunicazione e la diffusione dei dati (DPS);
- Predisporre l'informativa;
- Adottare un piano per aumentare le misure di sicurezza e predisporre il Documento Programmatico per la Sicurezza.

installati per la protezione dei locali dove risiedono archivi fisici e i sistemi informatici siano in grado di riconoscere in maniera univoca le persone autorizzate. Questi strumenti possono essere sistemi di rilevazione biometrica, di videosorveglianza, localizzatori di persone, password, certificati digitali, carte a microprocessore, codici identificativi. Non importa la "chiave" usata, ciò che conta per la protezione generale dei dati è che la serratura impiegata sia resistente e a prova di scasso.
La legge definisce, inoltre, i criteri con cui queste credenziali devono essere scelte. Per esempio nel caso di una password, questa deve essere composta da almeno otto caratteri, non deve contenere alcun riferimento che possa ricondurre facilmente al proprietario e deve essere modificata dalla persona autorizzata la prima volta che viene utilizzata e, successivamente, ogni sei mesi; ogni tre mesi nel caso di trattamento di dati sensibili o giudiziari. Le altre misure minime prevedono: l'aggiornamento periodico dei sistemi informativi con programmi forniti dai produttori per eliminare alcune vulnerabilità individuate (patch di sicurezza, aggiornamenti del software, ecc.); l'utilizzo di strumenti informatici, come software antivirus e firewall, per proteggere i dati dal rischio di intrusione da parte di personale non autorizzato, di perdite dovute all'azione di virus e worm; la realizzazione periodica di copie di riserva dei dati su supporti elettronici (back up) per garantire la custodia e il salvataggio sicuro delle informazioni trattate. Gran parte cioè di ciò che descriveremo nel decalogo della sicurezza di questa guida.

LA TECNOLOGIA MICROSOFT DI ULTIMA GENERAZIONE È IN LINEA CON LE DIRETTIVE DEL NUOVO CODICE DELLA PRIVACY

Disposizioni da attuare

Per adeguarsi alle disposizioni richieste dal nuovo Codice, gli istituti scolastici dovranno effettuare nuovi investimenti in materia di sicurezza. Esistono sul mercato soluzioni informatiche di recente rilascio che permettono già di attuare in maniera semplice e senza costi aggiuntivi tutte le misure minime di sicurezza richieste, come le credenziali di autenticazione, la protezione dei sistemi da programmi maligni, la prevenzione di vulnerabilità attraverso il continuo aggiornamento del software, copia di sicurezza e ripristino dei dati. Microsoft, come illustreremo in seguito, è già in linea con le direttive del Codice. Le sue tecnologie e i suoi programmi garantiscono già alle scuole di ogni ordine e grado i massimi livelli di sicurezza e la possibilità di essere in regola con le misure richieste dalla nuova normativa sulla privacy. ■

LE NUOVE MISURE RICHIESTE DAL CODICE DI PROTEZIONE DEI DATI PERSONALI (DLGS N° 196/2003)

1. Censimento e aggiornamento dei trattamenti;
2. Lista degli incaricati;
3. Gestione delle credenziali di autenticazione;
4. Password, token o dispositivi biometrici;
5. Protezione della sessione di lavoro;
6. Profilazione dei privilegi per l'accesso;
7. Aggiornamento dei programmi per prevenire vulnerabilità e correggere difetti del software;
8. Protezione dei supporti rimuovibili;
9. Adozione di misure idonee per assicurare l'integrità e disponibilità dei dati;
10. Salvataggio e ripristino dei dati;
11. Ripristino dei dati e sistemi salvati;
12. Difesa degli accessi abusivi;
13. Analisi dei rischi informatici;
14. Relazione di conformità dell'installatore per adozione di misure minime;
15. Formazione specifica degli incaricati.

Per affrontare la sfida della sicurezza è necessario affidarsi a soluzioni complete, in grado di garantire stabilità al sistema e durante il lavoro quotidiano con i programmi di produttività individuale

PROTEZIONE e AFFIDABILITÀ per PC e reti degli ISTITUTI

Provate a pensare alle innumerevoli attività che oggi si possono svolgere attraverso un personal computer: dalle lezioni a distanza, all'invio di messaggi, dalla scrittura di testo all'elaborazione di complessi calcoli di tipo matematico. Quale altro strumento rappresenta meglio l'unità minima e più importante per chi lavora nelle aree amministrativo-logistiche di un ente scolastico? Lo strumento più funzionale per svolgere lezioni multimediali o calcoli di laboratorio? Attorno a questo nucleo ruota gran parte delle lezioni più innovative, del lavoro quotidiano di dipendenti scolastici, delle attività di un istituto o delle previsioni di ricercatori. È ovvio, però, che quanto più ci si affida a esso, tanto più deve essere sicuro e protetto dalle minacce esterne, sia che si tratti di un singolo PC sia di una rete di computer collegati fra loro. L'utilizzo sempre più frequente di Internet e dalla posta elettronica espone, infatti, i computer e la rete degli istituti alla pericolosa azione di virus e worm e di pirati informatici. La scelta di un sistema operativo all'avanguardia, progettato tenendo conto dell'uso crescente della connettività, e di una soluzione affidabile capace di aumentare il livello di produttività possono fare la differenza.

RIDURRE I RISCHI DOVUTI ALLE MINACCE ESTERNE O AI BLOCCHI DI SISTEMA MIGLIORA LE ATTIVITÀ DIDATTICHE E LA SICUREZZA DEGLI ISTITUTI

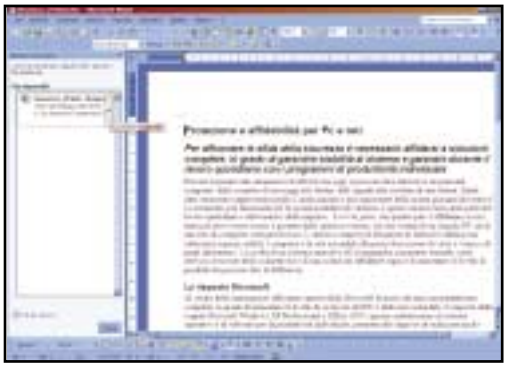
La risposta Microsoft

Al centro della strategia per affrontare questa sfida Microsoft ha posto da anni una piattaforma completa, in grado di aumentare il livello di sicurezza del PC o della rete informatica. Composta dalla coppia Microsoft Windows XP Professional e Microsoft Office 2003, questa combinazione di sistema operativo e di software per la produttività individuale permette agli istituti scolastici di realizzare anche piccole reti di tre o quattro PC, rendendo il lavoro più collaborativo e favorendo l'utilizzo di tutte le periferiche (stampanti, fax e connessione Internet) in maniera più efficiente. Il recente rilascio del nuovo Windows XP Service Pack 2 (SP2) assicura, inoltre, anche grande sicurezza. Unita a Office 2003 risolve la maggior parte delle problematiche relative alla protezione del PC. I due software integrano una serie di funzionalità che contribuiscono ad aumentare il livello di sicurezza delle applicazioni e dei documenti, dal controllo all'accesso alle informazioni, come richiesto dal nuovo codice sulla privacy, alla prevenzione della perdita di dati e informazioni, alla protezione di virus e worm inviati via posta elettronica

o inseriti all'interno di macro, fino a nuovi filtri in grado di contrastare il fastidioso fenomeno dello spamming.

Produttività sicura

Quando si scrive una lettera o si riceve un messaggio è rassicurante sapere di non andare incontro a sorprese. Perdere i dati già elaborati o ricevere posta indesiderata, però, quante volte succede! Con il nuovo Office 2003, Microsoft ha puntato proprio a questi piccoli importanti elementi per la sicurezza e la stabilità dei dati. Oggi con Office 2003 i sistemi sono protetti dai virus che si possono propagare al momento dell'apertura di documenti contenenti delle macro, impedendone l'esecuzione, e sono in grado di bloccare file allegati ai messaggi di posta elettronica dai contenuti pericolosi. In maniera automatica evita che gli utenti aprano inavvertitamente dei file che contengono dei virus, inclusi quelli che si presentano come innocui file di immagine o di testo. Nel caso poi di problemi relativi a programmi, all'hardware o interruzioni dovuti a un blocco del sistema l'applicazione effettua in automatico un back up e il ripristino dei file su cui si stava lavorando, evitando la perdita, anche parziale, dei documenti non ancora salvati e ripristinando automaticamente le applicazioni in caso di malfunzionamenti. Questo assicura agli utenti la massima produttività anche nelle circostanze meno prevedibili. Pensate cosa potrebbe accadere se dopo aver lavorato per ore alla stesura di un capitolo della propria tesi un malfunzionamento arrestasse il sistema di un laureando. Con Office 2003 il lavoro è sempre al sicuro, senza perdite inutili di tempo e soprattutto di informazioni.



Con Microsoft Office 2003 il vostro lavoro è sempre al sicuro: anche dopo un improvviso blocco del sistema potete recuperare i testi originali.

Windows messo a nuovo

Anche la riduzione dei più comuni rischi dovuti alle minacce esterne o ai blocchi di sistema migliora la produttività e l'efficienza. Per questo motivo, Microsoft ha progettato l'aggiornamento Windows XP Service Pack 2, pensato per garantire la massima sicurezza e affidabilità a livello client. Aggiornamento gratuito per tutti gli utenti Windows XP, Service Pack 2 è, infatti, molto di più di una raccolta di programmi di protezione che risolvono alcune vulnerabilità del sistema operativo. Rappresenta una nuova versione di Windows, capace di incrementare il livello di sicurezza del PC senza rinunciare alla facilità di utilizzo.

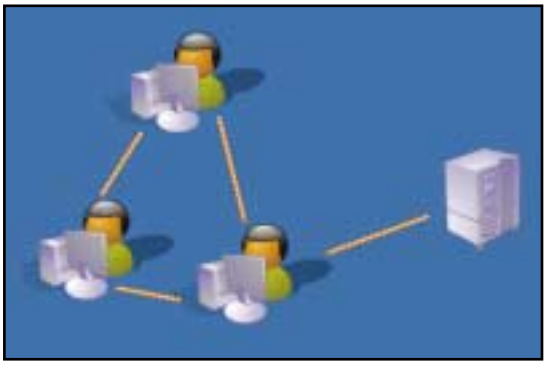
Innanzitutto, attiva in modalità predefinita (ovvero, non è necessario da parte dell'utente intervenire sulla configurazione del PC) un potente firewall che protegge il sistema già durante le prime fasi di avvio, impedendo intrusioni indesiderate o la diffusione di particolari tipi di worm attraverso una connessione Internet. Un rimedio utile nel caso di PC condivisi, magari in un'aula multimediale. Apporta poi altre migliorie, che riguardano il livello di protezione della rete e della memoria del PC. Inoltre, Windows XP SP2 contiene nuove funzionalità per gestire in maniera più efficace i messaggi di posta elettronica e rendere più sicura la navigazione sul Web, bloccando, per esempio, l'azione di pop up o di messaggi pubblicitari e impedendo di scaricare dalla rete programmi e codici pericolosi, proteggendo così l'attività di studenti poco attenti alla sicurezza durante l'accesso su Internet. Tra le novità annovera anche un Centro per la sicurezza, sorta di plancia di comando all'interno del PC in cui stabilire facilmente tutti i parametri di sicurezza per la propria macchina.

VUOI OTTENERE WINDOWS XP SP2? VISITA IL SITO

WWW.MICROSOFT.COM/ITALY/SECURITY

Dal singolo PC alla rete

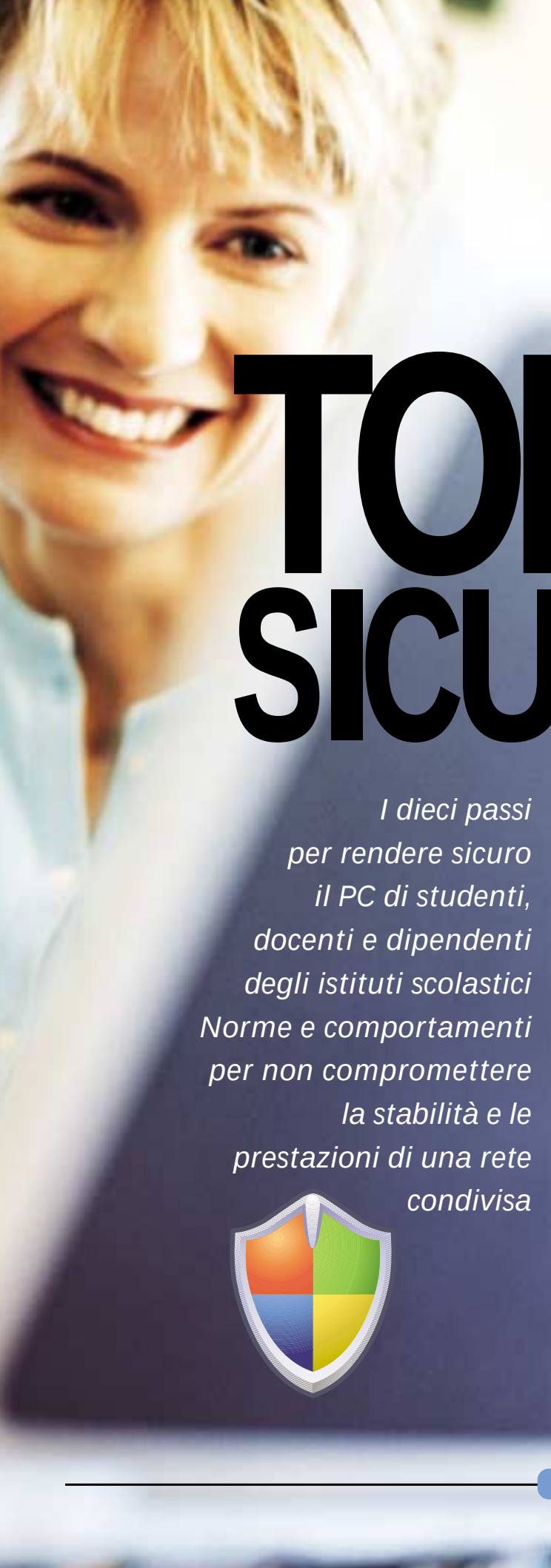
L'abbinata di Windows XP SP2 e Office 2003 rappresenta il massimo livello di sicurezza del PC a livello client, ma esistono anche soluzioni per la protezione delle reti degli istituti scolastici a livello centrale. Dal singolo PC alle reti più articolate, Microsoft garantisce a ogni livello di complessità delle reti i sistemi necessari per affrontare la sfida della sicurezza.



Windows Small Business Server 2003 è particolarmente adatto alle esigenze degli istituti scolastici di medio-grandi dimensioni (fino a 75 PC)

La presenza di un server semplifica molte operazioni in un istituto. Centralizza le attività, gli archivi, i programmi e soprattutto rende più facile anche il controllo dei livelli di sicurezza di una rete. Per esempio, Windows Small Business Server 2003 è particolarmente adatto alle esigenze degli istituti di medie dimensioni.

Collega in rete fino a 75 PC e offre, in un'unica piattaforma, tutte le funzionalità per la gestione delle attività di un istituto: connessione a Internet sicura, gestione della posta elettronica, supporto per eventuali dispositivi mobili, accesso remoto, condivisione di file e stampanti, invio fax dalla postazione di ogni utente, strumenti per il back up e ripristino di dati, applicativi per la creazione di una Intranet per condividere dati e informazioni in maniera semplice ed efficace. ■



TOP 10 SICUREZZA

I dieci passi per rendere sicuro il PC di studenti, docenti e dipendenti degli istituti scolastici Norme e comportamenti per non compromettere la stabilità e le prestazioni di una rete condivisa

L'ABC della sicurezza si riassume facilmente: rispetto di regole elementari e corretti comportamenti nell'uso del PC. Bastano, infatti, pochi accorgimenti e un preciso impiego del computer per evitare spiacevoli inconvenienti, esporre il proprio computer a virus o attacchi. Per gli utenti più esperti si tratta di attitudini acquisite, ma per molti, in particolare per chi usa il computer per esempio in un'aula scolastica senza prestare troppa attenzione agli aspetti tecnologici, non è tutto così scontato. In queste pagine cercheremo di illustrare in maniera semplice i 10 passi da seguire per rendere veramente sicuro il computer, proteggendo attività didattiche, privacy e lavoro. Partendo da soluzioni legate alla sicurezza fisica e all'uso individuale del PC arriveremo all'uso di strumenti e soluzioni per reti più complesse. Iniziamo.

1. La sicurezza fisica

Primo: assicurate il vostro PC dal punto di vista fisico. Potrà sembrare scontato, ma anche la protezione da pericoli reali o dalla possibilità di furti e danni esterni è un aspetto da non sottovalutare. In particolare, occorre prestare attenzione agli allarmi, alle chiusure dei cabinet o dei luoghi in cui si conservano i PC: aule, laboratori, uffici, segreterie. Questa lista di 10 promemoria può aiutare ad assicurare meglio i propri computer:

1.1 posizionate i computer in aree che possano essere chiuse a chiave o in cui si possano installare allarmi;

1.2 assicuratevi che l'accesso alla stanza con i PC sia controllato visivamente da qualcuno;

1.3 per computer di maggior valore o server dedicati, restringete l'accesso o mettete un sistema di identificazione;
1.4 considerate sempre anche il rischio di un incendio: adottate i sistemi di prevenzione;
1.5 fate in modo che un responsabile chiuda a chiave i locali quando non c'è nessuno;
1.6 controllate gli allarmi regolarmente;
1.7 marchiate i computer dell'istituto con informazioni per identificare il proprietario, la scuola, il luogo;
1.8 conservate i numeri seriali dei PC nel caso di furto;
1.9 stabilite regole chiare per gli utenti che utilizzano dispositivi mobili o apparecchiature di valore e rendeteli responsabili della restituzione;
1.10 fate installare gruppi di continuità utili nel caso di black out, in particolare per portare corrente ai server o ai computer che non devono subire interruzioni o fermi macchina.

La sicurezza fisica inizia dalla identificazione univoca del proprio PC

2. Antivirus su misura

Seconda regola: utilizzate un antivirus aggiornato. Non ci sono altre precauzioni così importanti come l'adozione di un software antivirus. La sua azione è preventiva, lavorando a monte delle infezioni. Permette la scansione dei file che vengono trasferiti sul PC via e-mail, via rete o semplicemente come copia da memorie esterne (floppy, ecc.) e pulisce quelli che presentano programmi maligni. Gli antivirus più evoluti mettono anche in quarantena i file incriminati, permettendo agli utenti di analizzare anche contenuti infetti e capire di quale pericolo si tratta. Per un uso corretto di questi applicativi è consigliabile seguire questi principi:

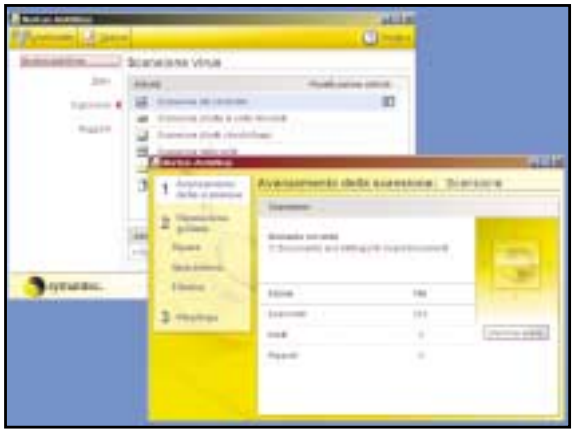
A. occorre installare un antivirus su ogni macchina di una rete;
B. l'antivirus deve essere adeguato alle proprie esigenze e all'esposizione al pericolo;
C. il software va aggiornato frequentemente, anche più volte al giorno, in caso di notizia di attacchi particolarmente virulenti sulla rete Internet, ricevendo informazioni e aggiornamenti dai produttori del software;
D. è necessario adottare qualsiasi meccanismo di autoprotezione disponibile, in particolare l'avvio automatico dell'antivirus;

LE 10 REGOLE DELLA SICUREZZA

1. Assicurate il vostro PC dal punto di vista fisico;
2. Utilizzate un antivirus aggiornato;
3. Eseguite regolari backup del PC;
4. Utilizzate password forti e cambiatele regolarmente;
5. Adottate il sistema di cifratura per le informazioni più importanti;
6. Navigate in Rete in modo prudente;
7. Installate un firewall;
8. Usate la posta elettronica in maniera sicura;
9. Aggiornate il sistema periodicamente;
10. Proteggete le vostre connessioni.

E. non disattivare mai le protezioni antivirus sulla posta in entrata, in uscita, sugli script e sulle macro, se disponibili;
F. lanciare periodicamente un controllo completo del proprio PC, come se fosse un malato su cui fare un check up per valutare lo stato di salute. Per questa analisi è possibile utilizzare gli strumenti di pianificazione dell'antivirus, che permettono di eseguire in automatico, secondo un periodo prefissato, la scansione dei dischi e delle periferiche;
G. per i più esperti, è consigliabile anche tenere dei dischi di installazione del sistema a portata di mano e un set di dischetti di emergenza, di sola lettura, con i file di base per il ripristino di un sistema compromesso.

L'elenco riportato vale come guida per un comportamento responsabile, ma è ovvio che a monte di un antivirus deve esserci la precisa consapevolezza che ogni file, la cui provenienza non è accertata, è potenzialmente pericoloso e che non si devono aprire tutti i file ricevuti. Di questo devono essere consapevoli tutti gli utenti di PC, dagli studenti fino al direttore scolastico. Gli espedienti con cui malintenzionati trasmettono contenuti infetti è sempre più raffinato: si va dai file nascosti in pagine Web alle macro inserite in file Word. L'esecuzione di qualche appli-


Un buon antivirus è indispensabile per combattere la diffusione di virus, worm e script maligni e salvaguardare la propria attività quotidiana

GLI ANTIVIRUS PIÙ NOTI

Symantec [www.symantec.com]
McAfee [www.mcafee.com]
Sophos [www.sophos.com]
Trendmicro [www.trendmicro.com]
Computer Associates [www.ca.com]
I link alle principali società produttrici di antivirus sono disponibili all'indirizzo:
http://www.microsoft.com/italy/security/articles/software_antivirus.mspx

cazione non richiesta è di conseguenza sempre da verificare con le dovute cautele. Prima di dare un ok è meglio pensarci tre volte. Nel caso malaugurato questo avvenisse, gli antivirus aiutano gli utenti ad affrontare l'azione pericolosa dei virus e a debellarli. La precauzione, si può dire, non è comunque mai troppa. Allo stesso modo è assolutamente indispensabile mantenere aggiornato l'antivirus. Avere un software che non è al passo con il database dei virus in circolazione è sinonimo di esposizione alla contaminazione. Nella scelta di un antivirus, dunque, è preferibile adottare quelli che permettono il downolad da Internet degli aggiornamenti rilasciati in tempo reale. Un ultimo accorgimento: se non avete grandi competenze in materia di prevenzione di virus scegliete quei produttori che offrono maggiori garanzie, che hanno una storia, uomini e conoscenze che rendono i software da loro creati estremamente affidabili.

3. Archiviare le informazioni utili

Si chiama "back up", tecnicamente. Più semplicemente significa creare un "archivio delle informazioni che potrebbero tornare utili nel tempo". Un po' come fare delle fotocopie da inserire in un faldone distinto da quello originale per evitare, in caso di incendio, di perdere preziosi documenti. Anche con il PC è necessario predisporre copie da archiviare per prevenire gravi danni ai sistemi o alle apparecchiature hardware. È una prassi necessaria, soprattutto per salvaguardare la propria attività didattica o la conservazione di informazioni privilegiate, magari di tipo amministrativo. La stessa nuova legge sulla privacy, di cui abbiamo parlato nelle pagine precedenti, impone agli istituti che conservano dati di studenti, famiglie o fornitori, svolgendo il ruolo di responsabili del trattamento, di fare la copia settimanale dei database che contengono le informazioni. In generale dunque, **come terza regola della sicurezza eseguite regolarmente il back up della macchina su cui è svolta un'attività.**
In pratica come si fa? Tenuto conto che fare un back up significa spostare determinati dati da un supporto informatico a uno differente, esistono back up completi e parziali, in base alla volontà di conservare tutto o solo una parte delle informazioni. Sta all'utente (oppure, nel caso specifico di un istituto che ha adottato un DPS, un incaricato preciso) scegliere che cosa è più utile ai fini della conservazione dei dati, quanti ne vuole conservare e con quale frequenza desidera aggiornare il proprio archivio. Allo stesso modo esistono sistemi per eseguire copie una tantum o in maniera pianificata. Il primo fa capo al semplice trasferimento di dati su floppy, Cd-Rom, Dvd o cassette DAT. Il secondo all'impiego di sistemi software e hardware per regolarizzare la copia di dati sui supporti esterni o rendere più facile un eventuale ripristino delle informazioni perse. Microsoft, per esempio, ha predisposto per Windows XP Professional l'utilità di sistema denominata BackUp, richiamabile dal Pannello di Controllo. Questa permette non soltanto l'archiviazione ragionata dei documenti, in base alla collocazione precisa, ma anche una successiva ricostruzione della struttura delle informazioni salvate.
Se poi si utilizza un server l'operazione è ancora più semplice poiché, accentrando i dati, è possibile eseguire un unico back up valido per numerosi utenti. Con Windows Server 2003, inoltre, si può recuperare la versione precedente di ogni file elaborato con Word o Excel, direttamente dalla macchina dell'utente, richiamando le proprietà del file.

I SUPPORTI PIÙ COMUNI PER ESEGUIRE I BACK UP

Quantità di dati	Supporto
Sotto i 1,4 MB	Floppy disk
Fino a 256 MB	Chiavi USB
Sotto i 700 MB	Cd-Rom
700 MB - 4,7 GB	Dvd
2 GB - 12 GB	DAT (Digital Audio Tape)

4. Questione di password

La password è il modo più comune per autenticare un'identità. È la chiave da inserire nella "serratura digitale" di un PC per accedere ogni giorno ai programmi e alle risorse utili. Come tutte le serrature, però, deve funzionare e la chiave deve avere determinate caratteristiche che rendono difficile ogni tentativo di scasso. In primo luogo, perché questo si verifichi, è necessario impiegare termini difficilmente indovinabili. Un esempio classico di parole da evitare, per esempio, è la login uguale al nome e la password al cognome, oppure al nome dell'istituto e alla città che lo ospita. Oppure al luogo di nascita o di residenza, oppure informazioni e dati facilmente riconducibili agli utenti o agli amministratori. **La regola più indicata è: utilizzate password forti e cambiatele regolarmente.** Ma che cosa significa in concreto una password "forte"? Partiamo, inizialmente, da alcuni esempi di segno opposto, ovvero dalle password deboli, per focalizzare la questione:

A. l'assenza di password è un grave errore. Così come la login uguale alla password. Permettono un accesso nel sistema senza alcuna difficoltà;
B. il nome reale del proprietario del PC, come già accennato, o il nome dell'istituto di appartenenza è sconsigliabile. Troppo immediato;
C. parole dal significato compiuto, sebbene meno immediate, sono comunque facilmente attaccabili attraverso sistemi automatici di scasso basati sui dizionari;
D. vanno evitate, inoltre, parole comuni, come "password" o formule del

tipo "1234", tipica per esempio delle segreterie telefoniche.

Al contrario, invece, si possono definire queste regole per aumentare la forza di una password:

1. ogni password deve avere almeno 8 caratteri. Ma più è lunga meglio è.
2. è utile inserire una combinazione di maiuscole e minuscole, lettere, numeri e simboli (compreso lo spazio), come potrebbe essere a titolo di esempio questa stringa: "JFk7!<e02". Ovviamente la difficoltà è quella di ricordarla;
3. rende forte una password la sua durata limitata nel tempo. Buona norma sarebbe quella di cambiarla ogni 3 mesi, meglio ancora ogni 45 giorni. Nel momento in cui si cambia, è necessario anche produrre significative variazioni dalle password precedenti.

Microsoft Windows Xp è in grado di imporre da solo queste regole a ciascun PC sul quale viene installato, in conformità anche alla nuova normativa sul trattamento dei dati personali, che stabilisce una forte regolamentazione anche sull'uso di sistemi di autenticazione e protezione delle informazioni. Per esempio, al primo accesso dopo la configurazione sarà richiesto all'utente di cambiare la sua password oppure sono rifiutate password troppo corte o che non rispettano la regola 2). Con Windows Server 2003, addirittura, si possono determinare una volta sola tutte le configurazioni dei PC di rete, senza perdere tempo.

In ultimo qualche regola aggiuntiva. Come ricordare le password? È possibile per esempio affidarsi a piccoli trucchi, anche se è meglio stare attenti che non rendano riconoscibile le parole nascoste.

In Windows 2000 e XP le password possono essere frasi, come "Domani studio algebra!" oppure si possono creare frasi simili a rebus, come "AT=Archimede+Talete!". In ultimo, si possono usare acronimi, come per esempio"Su1inM" che sta per "sono un asso in matematica". Attenzione, però, a non usare formule che abbiano un senso noto, perché se lo hanno per voi, potrebbero averlo anche per chi cerca di scassinare la vostra autenticazione. Infine, è giusto ricordare che esistono programmi e meccanismi automatici per trovare un password. Talvolta è soltanto una questione di tempo, per cui ogni password va custodita come la chiave di casa. Non va mai ceduta a nessuno. Se qualcuno viene a conoscenza della vostra password, il PC è potenzialmente vulnerabile! Scontato poi di non scriverla vicino al PC.

Grazie a Windows XP Service Pack 2 i download automatici da Internet e l'esecuzione di programmi potenzialmente dannosi sono bloccati. La navigazione è più sicura e sotto controllo

Per gli utenti che lavorano in una rete e condividono file con Windows Server 2003 è possibile crittografare i file in modo veloce e senza l'uso di applicazioni esterne

5. File cifrati

Così come le password proteggono l'accesso all'intero sistema, anche a livello più basso, per i singoli file che contengono informazioni riservate, esistono sistemi di difesa che impediscono l'accesso indesiderato da parte di persone indiscrete, ladri o hacker. In entrambi i casi se rubano il PC avete la certezza che hacker e curiosi faranno veramente fatica a trovare una via di accesso ai vostri dati. Per proteggerli, dunque, potete applicare la **quinta regola: adottate il sistema di cifratura per le informazioni più importanti**. Come fare? Sul mercato esistono software dedicati per crittografare le informazioni, ma spesso si tratta di applicativi complessi, che vincolano in maniera troppo forte l'uso e lo scambio di informazioni cifrate. Windows XP, invece, permette di cifrare i dati in modo davvero semplice. Quando si condividono file di lavoro su un server con sistema Windows Server 2003, scegliendo le proprietà di un file con il tasto destro e la voce Crittografia nelle opzioni avanzate si può cifrare un file, facendo in modo che l'unica persona autorizzata a modificarlo risulti il proprietario stesso del file. Alla vista questo file assumerà la colorazione verde nelle cartelle di sistema.

6. Sul Web senza paura

Internet è una minaccia o una risorsa? Certamente la seconda, ma non si deve dimenticare, in chiave di sicurezza informatica, che un canale così vasto è anche fonte di numerosi quanto sofisticati pericoli in cui spesso incappano studenti o docenti poco esperti. **Come sesta regola si può dunque dire: navigate in modo prudente.** In sostanza significa ancora una volta stabilire alcune regole e attenervisi. Sia per quanto riguarda la navigazione individuale sia se si consulta Internet in un contesto di gruppo, per cercare informazioni, svolgere ricerche o approfondire temi legati ai propri interessi. Ecco alcuni principi chiave, ovviamente da interpretare secondo le esigenze individuali:

1. non accedete a siti che non considerate affidabili;
2. non eseguite transazioni, acquisti di materiale didattico o pagamenti di servizi utilizzando circuiti bancari sconosciuti;

Le funzionalità di sicurezza presenti in Windows XP Service Pack 2 garantiscono la rimozione automatica di allegati pericolosi inseriti nei messaggi di posta elettronica

3. non navigate sul Web direttamente dal server di una rete. Questo perché nel caso si incappasse in un elemento compromettente per la sicurezza, il danno sarebbe ovviamente più elevato;
4. accedete a Internet con un firewall (di questo parleremo tra breve in dettaglio);
5. stabilite una politica condivisa per la navigazione e rendetela nota a chi usa i PC. In particolare, stabilite quali comportamenti sono considerati illeciti (per esempio, la navigazione su siti pornografici, violenti, illegali ecc.). È ovvio che non riguarda soltanto la sicurezza, ma l'etica del navigatore Web. È giusto ricordare a studenti, docenti e utenti in generale che le implicazioni sui livelli di sicurezza delle reti sono dirette.

Alla maggiore protezione durante la navigazione ha pensato anche Microsoft. Windows XP Service Pack 2 ha reso più sicuro l'accesso a Internet. In particolare, ha aumentato i controlli sulle applicazioni che dal Web cercano di eseguire automaticamente operazioni potenzialmente dannose per i PC. Oltre a bloccare i cosiddetti controlli Active X, impedisce alle finestre pop up di aprirsi, fermando ogni tentativo di attivazione automatica. Sarà lasciata all'utente la scelta su questi elementi della navigazione Web. Spesso e volentieri, infatti, nascondono programmi maligni, come per esempio i dialer, o confondono eccessivamente i navigatori. I pop up si potranno vedere così soltanto su richiesta dell'utente, che potrà anche stabilire una lista di siti a cui è permessa questa funzione. Fine delle finestre a sorpresa, dunque, durante la consultazione del Web! Tutto sarà sotto il diretto controllo del navigatore, che potrà decidere se farsi "disturbare" da informazioni aggiuntive, spesso pubblicitarie. Allo stesso modo la Service Pack 2 per Windows XP permette un altro grande passo in avanti per la sicurezza, facendo in modo che i download automatici siano interrotti. Questo evita le installazioni accidentali di download indesiderati, proteggendo soprattutto i navigatori inesperti. Dialer e applicazioni intrusive, spyware e programmi simili avranno vita sempre più difficile. Infine, con le migliorie studiate da Microsoft con la Service Pack 2 si impedisce l'attività di particolari comandi e plug-in che cercano di sfruttare il browser Internet per eseguire funzioni non standard. Questi cosiddetti add-on sono monitorati in un apposito nuovo pannello di gestione.

7. Una barriera chiamata firewall

Settima regola: installate un firewall. Questo principio non ha deroghe. Il firewall, infatti, è uno degli strumenti più utili per contrastare i tentativi di intrusione su un PC e in una rete. Di che cosa si tratta? Un firewall, con buona approssimazione, è un sistema in grado di decidere quali informazioni e dati far passare e quali fermare in una rete. Ispeziona, cioè, il flusso di dati che passa sulla rete locale, intervenendo nel momento in cui identificasse qualcosa di non permesso dalle regole che l'amministratore del firewall ha deciso.

ALTRI FIREWALL CONSIGLIATI

Symantec [www.symantec.com]
McAfee [www.mcafee.com]
ZoneLabs [www.zonelabs.com]

Un firewall può essere sia un dispositivo fisico esterno al PC sia una componente software che collabora con il sistema operativo e i programmi installati. Microsoft Windows XP, per esempio, ha in dotazione un firewall, denominato Windows Firewall, a protezione dei dati personali e contro le intrusioni non autorizzate. Semplice e flessibile, permette di bloccare le connessione alla rete da parte di programmi. Con la nuova Service Pack 2 sono state migliorate tre aree strategiche nell'uso delle reti, tra cui lo stesso Windows Firewall, reso più facile da usare e potenziato. Il nuovo Windows Firewall è installato di default, per aumentare ancora di più i livelli di sicurezza. Questo significa che senza dovere intervenire nella definizione di particolari caratteristiche, il PC di studenti, docenti e impiegati degli istituti è già pronto a combattere i tentativi di intrusione. Il software, inoltre, consente il flusso normale del traffico in uscita e filtra sessione per sessione tutte le attività

UN CENTRO DI CONTROLLO SULLA SICUREZZA

Il Centro Sicurezza PC è una nuova funzionalità di Windows XP Service Pack 2 che offre agli utenti un punto centrale per cercare informazioni relative alla sicurezza ed eseguire qualsiasi operazione legata alla protezione. Il Centro Sicurezza PC controlla lo stato delle tre funzionalità principali di protezione: il firewall, gli aggiornamenti automatici e la protezione antivirus. Se il Centro Sicurezza PC rileva un problema in una di queste aree, di solito in fase di avvio, visualizza un'icona e un fumetto nell'area di notifica sulla barra delle applicazioni di Windows; riconosce Windows Firewall e numerosi firewall di terze parti, oltre alle più comuni soluzioni antivirus.

Il Centro Sicurezza PC è una nuova funzionalità per la gestione completa delle applicazioni dedicate alla sicurezza del computer

da e verso reti esterne. Questo agevola il normale accesso a Internet, per esempio per esplorare il Web e recuperare la posta elettronica, impedendo qualsiasi flusso di dati non richiesti. Per chi dispone di una piccola rete, magari in una scuola con pochi PC, è possibile anche configurare una sola volta le caratteristiche di sicurezza desiderate e poi adattare i computer collegati senza perdite di tempo.

Due ultimi dettagli prima di passare alla posta elettronica. Tra i vantaggi di un firewall è giusto annoverare anche la capacità di nascondere i singoli PC di una rete all'esterno. In altre parole un firewall rende la vita difficile agli hacker che desiderano raggiungere una determinata macchina, poiché le identità sono coperte e protette in maniera specifica. Infine, è necessario ricordare ciò che un firewall non può fare. È giusto sapere anche questo, per evitare spiacevoli sorprese. Per esempio, non protegge da attacchi iniziati quando una rete è già stata compromessa, oppure da alcuni virus che non transitano dalla rete (per esempio presenti in file su floppy disk). Non protegge, in ultimo, da intrusioni interne, cioè da hacker che hanno iniziato a danneggiare la rete dall'interno di un istituto.

8. Posta elettronica sotto controllo

Ottavo: usate la posta elettronica in maniera sicura. Possedere un sistema di posta elettronica sicuro non è più un optional, ma un reale vantaggio. Considerato il crescente bisogno di utilizzare la rete per comunicare e condurre attività amministrative, tenere sotto controllo i sistemi di e-mail è infatti fondamentale per dare continuità, sicurezza e protezione al lavoro e alle attività didattiche. La posta elettronica tuttavia, essendo il più usato servizio basato su Internet, è anche il più sfruttato sistema per portare attacchi alla sicurezza dei PC. Virus, spam, script maligni, macro: le minacce più sofisticate oggi arrivano proprio via e-mail. Per questo motivo è opportuno adottare le dovute cautele, seguendo regole di comportamento semplici quanto efficaci. Eccone alcune di base:

1. tenete aggiornato il software per la posta elettronica. Per questo visitate spesso il sito dei produttori del vostro software, scaricate e installate le patch indicate;
2. installate un antivirus che controlli la posta in entrata e quella in uscita;
3. filtrate lo spamming, creando regole o scegliendo i produttori che permettono di impostare filtri automatici;
4. non aprite gli attachment considerati pericolosi;
5. non rispondete allo spamming, perché confermereste di avere un account di posta attivo. Semplicemente cancellate le e-mail indesiderate;
6. non fornite mai dati sensibili via e-mail. Per esempio non trasmettete mai password, numeri di carta di credito, informazioni personali.

Anche in questo caso si tratta di regole di comportamento. Esistono poi software che agevolano l'esecuzione di tutto ciò in maniera automatica. Per esempio con Microsoft Office Outlook 2003 è possibile combattere attivamente lo spamming. Si possono definire, infatti, una serie di variabili per ottimizzare i messaggi in entrata, come per esempio i mittenti considerati attendibili e quelli visti come "spammer", ecc. Allo

Windows Firewall presenta tre stati principali: "Attivato", "Non consentire eccezioni" e "Disattivato". Il primo protegge il computer, ma consente di impostare specifiche eccezioni al criterio di protezione. Il secondo può essere utilizzato quando il computer si trova in un ambiente non sicuro, come una rete wireless pubblica non protetta o una rete locale colpita da un virus. L'ultima possibilità è utile per brevi periodi, per esempio, per diagnosticare eventuali problemi relativi al firewall, ma è consigliabile evitarne l'utilizzo per periodi prolungati.

PER GLI ISTITUTI DI GRANDI DIMENSIONI

Tra le offerte Microsoft per il mercato education c'è una soluzione studiata per la protezione totale delle reti di medie dimensioni e complesse, tipiche di grandi istituti, Università, centri di ricerca. Il nuovo firewall Microsoft ISA SERVER 2004 (Internet Security Acceleration Server), facile da gestire e da configurare, consente di gestire in modo sicuro la rete scolastica. Oltre alla sicurezza a livello perimetrale, include funzionalità avanzate di protezione a livello di applicazioni, per l'accesso al Web - bloccando la navigazione da parte degli utenti a siti dai contenuti non appropriati - e per le connessioni tra due reti (Virtual Private Network), limitandone l'ingresso se i computer non hanno installato aggiornamenti software e programmi antivirus

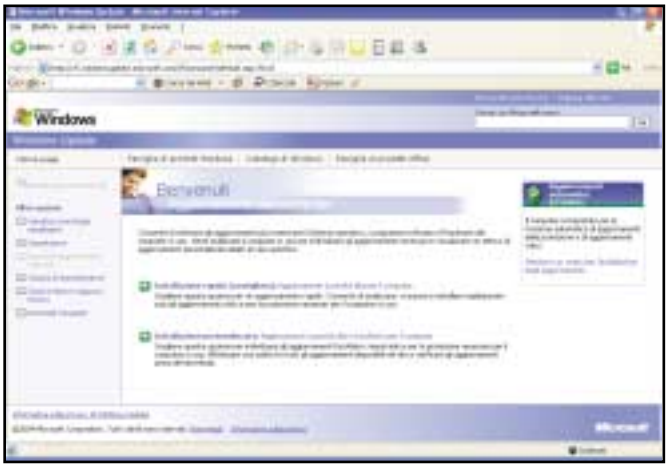
Il nuovo Windows Firewall garantisce maggiore controllo sugli allegati di posta elettronica e la possibilità di stabilire i contenuti considerati attendibili

stesso modo è aumentato il livello di protezione della Rubrica, per impedire ai virus di replicarsi sfruttando gli indirizzi presenti. Un altro fronte su cui è possibile aumentare la sicurezza delle e-mail è quello del blocco automatico degli allegati considerati non sicuri. Microsoft, inoltre, rende disponibile un servizio (Office Update) che esegue il rilevamento automatico per individuare gli aggiornamenti gratuiti che possono migliorare la stabilità e la protezione di tutte le applicazioni di Office 2003 e Microsoft Office Outlook 2003. Grazie alla Service Pack 2 per Windows XP questo meccanismo è stato integrato nel sistema: ogni allegato a rischio ricevuto tramite Internet Explorer, Outlook Express o Instant Messenger viene bloccato. L'utente non sarà in grado di aprirlo, ma vedrà un messaggio relativo al blocco o un'anteprima non dannosa relativa al contenuto "congelato" dal sistema. Ma non solo. Per gli istituti di medio-grandi dimensioni, enti di ricerca, Università, Microsoft ha pensato anche a un passo ulteriore. Grazie ai filtri antispam che si possono installare su Microsoft Exchange Server 2003 (piattaforma per la gestione della posta elettronica già inclusa in Microsoft Small Business Server 2003) l'intera rete è al riparo dalla posta indesiderata. Ogni singolo PC è al sicuro, anche nel caso di accessi al proprio account tramite l'interfaccia Web. L'obiettivo di queste migliorie, come ha dichiarato lo stesso Bill Gates, è quello di pensare e progressivamente avvicinarsi a un "futuro senza spamming!".

9. Aggiornare il sistema

Nona regola: aggiornate il sistema periodicamente. Ogni accorgimento rischia di non essere sufficiente per una protezione completa se i sistemi operativi o le applicazioni non sono aggiornate con regolarità ed efficacia. Microsoft rilascia gratuitamente una volta al mese aggiornamenti e patch proprio per proteggere e migliorare i propri prodotti nel corso del tempo. Per chi dispone di un PC con sistema operativo Microsoft o di prodotti della famiglia Office esistono due semplici sistemi per verificare i livelli di sicurezza e di aggiornamento del software impiegato. Il primo è Microsoft Windows update.

Un meccanismo immediato che grazie al collegamento Internet al sito http://windowsupdate.microsoft.com effettua una scansione del sistema e suggerisce quali componenti aggiuntive scaricare gratuitamente e installare. Il secondo, invece, è specifico per chi usa il software per la produttività individuale Microsoft Office 2000, Microsoft Office XP e prodotti della piattaforma Office System. Anche in questo caso, collegandosi al sito http://office.microsoft.com/italy/ProductUpdates/ vengono suggerite agli utenti le ultime migliorie realizzate da Microsoft per rendere più efficiente e sicuro il software. Con un download e l'installazione delle componenti aggiuntive si eliminano rischi e nuove minacce. Per gli istituti con un server e una rete di medio-grandi dimensioni, invece, Microsoft ha predisposto una soluzione a più ampio raggio. Tali enti hanno la possibilità di aggiornare i propri PC grazie a Microsoft Software Update Services (SUS). Componente aggiuntivo gratuito per Windows 2000 Server e Windows Server 2003, è stato progettato appositamente per gestire l'applicazione dei più recenti aggiornamenti e garantire un livello di protezione uniforme a tutta la rete scolastica. Come funziona? Semplice: con SUS viene installata su Windows Server un'applicazione che consente agli amministratori di ricevere automaticamente gli aggiornamenti e distribuirli in modo rapido e affidabile a tutti i computer desktop e server sui quali sono installati Windows 2000, Windows XP e Windows Server 2003.
L'amministratore può valutare gli aggiornamenti, testarli e decidere quali distribuire ai PC della rete dell'istituto. In SUS sono incluse tutte le patch associate ai bollettini sulla sicurezza per Windows. In pratica, ogni allarme relativo alla sicurezza di Windows trova una risposta adeguata negli aggiornamenti rilevati automaticamente da SUS. I vantaggi più evidenti dell'uso di un software come questo sono intuibili: un aggiornamento del sistema rapido, costante e a basso costo. Inoltre, ciò che rende efficace tutto il meccanismo di aggiornamento è la tempestività: il sito web Windows Update viene aggiornato contemporaneamente al rilascio dei bollettini sulla sicurezza e, grazie alla funzione automatica



Microsoft Windows Update, Office Update e Software Update Services sono i tre servizi di aggiornamento dei sistemi e delle applicazioni che permettono di scaricare gratuitamente e aggiornare i PC client e server per garantire massima sicurezza

NETIQUETTE E NAVIGAZIONE SICURA

Oltre alle dieci regole qui elencate, è opportuno ricordare che la sicurezza informatica è anche una questione di comportamenti e che gli istituti scolastici hanno responsabilità nei confronti degli studenti in Rete. In particolare, le criticità legate all'uso scorretto del PC emergono durante l'uso della posta elettronica, la navigazione sul Web, la partecipazione a forum o chat di discussione.

Tutte le regole elencate sono volte alla riduzione dei pericoli e dell'esposizione degli studenti alle insidie della Rete.

È, tuttavia, indicato adottare nelle aule e nei laboratori telematici alcune policy condivise di utilizzo, se non addirittura sottoscrivere il Codice di autoregolamentazione Internet e Minori del ministero dell'Innovazione e delle Tecnologie (www.mininnovazione.gov.it).

Oltre a essere evidente la necessità della presenza dell'insegnante come guida durante le sessioni, si rende indispensabile l'adozione di una "netiquette". Con questo termine si indicano le regole di base per l'uso del PC e del Web. Si specifica cioè un'etica (etiquette) valida per la rete (net). Tali regole vanno scritte, rese note e apposte in ogni aula. Esistono numerosi esempi di netiquette in Internet, in particolare a corredo di noti servizi di Chat o Forum. Si possono prendere come esempio e adattati alle singole realtà degli istituti scolastici. Una seconda importante soluzione a cui pensare, per esempio nel caso di scuole elementari e medie, sono i browser che filtrano la navigazione per bloccare contenuti non adatti all'età dei giovani navigatori.

Per informazioni più approfondite si può consultare il sito dell'Osservatorio Tecnologico per la scuola del Miur (www.osservatoriotecnologico.it/internet/bambini_rete.htm).

di sincronizzazione, anche SUS è informato in tempo reale. La distribuzione automatica degli aggiornamenti sui PC consente di risparmiare tempo, assicurando la copertura da possibili attacchi. Inoltre, tutti i computer di una rete o di un'aula multimediale in questo modo presentano lo stesso grado di aggiornamento e di sicurezza, diminuendo l'esposizione ai pericoli informatici. In sostanza, SUS permette di tenere il passo delle più recenti protezioni e, al tempo stesso, abbatte i costi e i tempi relativi alle operazioni d'aggiornamento.

10. Connessioni protette

Decima regola: proteggete le vostre connessioni. Lavorare da casa, collegarsi alla rete dell'Università in viaggio, connettersi dall'esterno alla rete di un istituto scolastico sono situazioni sempre più frequenti nelle scuole, in particolare in quelle di grado superiore o negli Atenei. Consentire i collegamenti da remoto e mettere a disposizione l'e-mail anche a distanza permettono una flessibilità mai conosciuta in precedenza. Sono soluzioni che rappresentano una risorsa importante per gli istituti, per flessibilizzare le attività didattiche, la collaborazione e lo scambio di informazioni. Al tempo stesso, però, sono elementi di grande esposizione al rischio. Lascereste, infatti, le chiavi dell'aula multimediale in mano a uno sconosciuto? Lo stesso deve valere per il sistema di trasmissione dei dati o i dispositivi mobili. Se la connessione avviene sulla rete pubblica di Internet, chiunque potrebbe insinuarsi e utilizzarla per i più disparati scopi. Allora è bene ricorrere alle contromisure adeguate. Crittazione dei dati e severe procedure d'autenticazione sono tra gli strumenti a disposizione per re-impossessarsi del nostro bene. A questi requisiti corrisponde la descrizione della Virtual Private Network (VPN), che rappresenta un canale di comunicazione sicuro in mezzo al mare magnum di Internet: una specie di tunnel nel quale i dati trasmessi sono al riparo dalle possibili interferenze esterne.

Anche per i collegamenti wireless il discorso è analogo. Altrettanto diffusi sono, infatti, i collegamenti, da notebook o palmari: è il cosiddetto wireless networking, di cui regina indiscussa è la tecnologia Wi-Fi. Sebbene lo standard Wi-Fi stabilisca dei criteri di protezione dei dati e di controllo degli accessi, la sicurezza non è mai troppa. Il pericolo è evidente: chiunque, senza bisogno di un collegamento fisico, è potenzialmente in grado di intromettersi nella comunicazione, se questa non è adeguatamente protetta. L'intruso potrebbe intercettare e "ascoltare" le comunicazioni, entrare e sottrarre parte dei dati. Per questo è bene assicurarsi di volta in volta, eventualmente ricorrendo a dei consulenti esperti, perché siano attivate tutte le caratteristiche di sicurezza per le reti wireless: limitazioni d'uso negli orari d'ufficio e di lezione, utilizzo di card certificate e di password a combinazione alfanumerica, restrizioni sul numero di utenti e degli accessi, accesso tramite server dedicati. Non dimenticatelo: proteggere le connessioni significa proteggere gli istituti scolastici e più in generale l'attività didattica. ■

La tecnologia Microsoft garantisce costanti aggiornamenti per la sicurezza informatica a costi limitati, aiutando gli istituti a mantenere nel tempo il possesso di software e l'uso di sistemi affidabili

La MANUTENZIONE ha un COSTO

Quando si acquista un'automobile o uno strumento di lavoro si prendono in considerazione sempre alcune variabili per ottimizzare i costi nel tempo: l'affidabilità, la solidità, la presenza sul territorio di rivenditori e meccanici specializzati, la notorietà di una marca, garanzia di assistenza e facilità nel trovare ricambi. Infine, la sicurezza. Nel mondo dell'informatica il discorso è del tutto simile. Comperare software, hardware e servizi informatici dal punto di vista degli investimenti è paragonabile all'acquisto di un'auto o alla scelta di una Banca: è una spesa da valutare in relazione all'utilizzo e alla durata. In particolare, per non incorrere in cattivi affari, è necessario mettere a fuoco il cosiddetto total cost of ownership (TCO) dei beni materiali e immateriali, ovvero il costo generale di possesso di hardware e software, un parametro che somma il valore d'acquisto iniziale alle spese sostenute nel tempo per la manutenzione. Avere sotto controllo questo valore significa investire sui prodotti giusti, valutando ammortamenti, costi e benefici anche non immediati.

Investire sulla sicurezza

La sicurezza informatica e la personalizzazione entrano a pieno titolo tra i costi da pianificare nel tempo. Non esistono, infatti, soluzioni preconfezionate che siano compatibili con tutte le caratteristiche di un istituto scolastico.

Ogni scuola, centro professionale, laboratorio o Ateneo ha esigenze proprie, concrete, che cambiano anche con il tempo. Ma quale

POSSESSO DI HARDWARE E SOFTWARE

COSTO TOTALE = COSTO INIZIALE DI ACQUISTO + INSTALLAZIONE + MANUTENZIONE

"meccanico" autorizzato saprà mettere mano ai sistemi informativi già collaudati? Perché l'aggiornamento in ambito sicurezza sia un'operazione indolore, a basso costo e priva di rischi è necessario scegliere specialisti certificati e soluzioni affidabili, basate su una comprovata esperienza e su risposte immediate.

In tema di sicurezza informatica non si è mai sicuri di essere al passo con i tempi e un aggiornamento periodico è indispensabile. Il fattore tempo è fondamentale per evitare l'esposizione ai pericoli e costosi blocchi delle attività. Non si può improvvisare.

Occorre ponderare le scelte e optare per le soluzioni più sicure, oltre a individuare i fornitori più preparati. La tecnologia Microsoft, per esempio, garantisce un costante livello di aggiornamento.

Seguendo un preciso calendario, Microsoft rende noti i rimedi da adottare in ambito di sicurezza. Di volta in volta, attraverso bollettini e servizi Internet, mette a disposizione dei propri clienti informazioni, avvisi sulla sicurezza, patch e consigli con la finalità di evitare blocchi o anticipare pericoli e nuove minacce. Inoltre, grazie alla tecnologia Software Update Services (SUS), il livello di servizio è completo: ogni utente è sempre informato sulle cose importanti da installare per rendere più sicuri i sistemi Microsoft. Volendo - come illustrato nel decalogo della sicurezza di questa guida - grazie a SUS l'installazione delle novità può diventare anche automatica su tutti i PC della rete. Tutto questo significa risparmio, ovviamente. Ottimizzazione dell'investimento iniziale e minori spese nel tempo, proprio perché già previste fin dall'inizio. Quale meccanico riuscirebbe ad aggiustare la vostra auto in maniera così veloce? ■

LA TECNOLOGIA MICROSOFT OFFRE:

• AGGIORNAMENTI COSTANTI

• UN SISTEMA AUTOMATICO DI INSTALLAZIONE

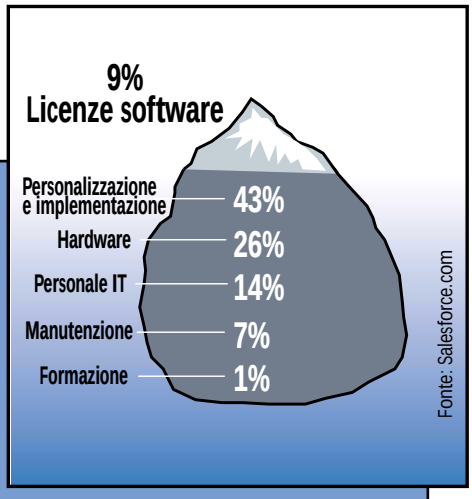
• L'ABBATTIMENTO DEI COSTI DI MANUTENZIONE

IL COSTO DELLA SICUREZZA

Mantenere un sistema informatico ha costi noti e spese nascoste. Basta l'eliminazione delle licenze software, per esempio adottando sistemi open source, per abbattere i costi?

Secondo SalesForce.com, se si considera la percentuale di incidenza delle personalizzazioni (che comprendono il "registro" dei sistemi su livelli di sicurezza ottimali), non sembra proprio così. In tema di sicurezza è giusto andare in profondità, sondando gli aspetti meno evidenti. Soltanto il supporto costante, la disponibilità di soluzioni immediate a pericolosi virus o falle dei sistemi facilita la gestione della propria rete e l'ottimizzazione dei costi di manutenzione. Secondo SalesForce.com le percentuali di incidenza sul costo legato al possesso di soluzioni informatiche nel corso del tempo sono:

- licenze software (9%): rappresentano un costo iniziale chiaro e ben identificabile;
- la personalizzazione e l'implementazione (43%): comprendono l'installazione iniziale e le modifiche da apportare nel tempo. Per la tecnologia Microsoft, per esempio in ambito di sicurezza, ogni aggiornamento è reso immediato e facilmente implementabile grazie ai Software Update Services;
- l'hardware (26%): conta in misura dell'uso e delle necessità relative alla potenza di calcolo e di archiviazione richieste;
- il personale informatico (14%): non si deve dimenticare il costo delle risorse umane specializzate in informatica. L'uso di tecnologie note, per le quali esiste un ampio supporto da parte del rivenditore e dei suoi partner, favorisce l'abbattimento di questo costo;
- la manutenzione (7%): si tratta di interventi di ripristino, update dei sistemi e di gestione straordinaria, per esempio durante attacchi informatici;
- formazione (1%): incide parzialmente, ma non va dimenticata. In relazione ai temi di sicurezza informatica anche questo aspetto è garantito regolarmente da Microsoft grazie a bollettini ad hoc.



Tutte le risorse Microsoft per tenersi aggiornati in materia di sicurezza: dalla Service Pack 2 per Windows XP al sito dedicato alla sicurezza, dai bollettini e dai Webcast alla community, dal sito TechNet al supporto per combattere i virus

La SICUREZZA nel TEMPO

Non esiste reale sicurezza senza un costante aggiornamento. Come abbiamo illustrato nelle pagine precedenti, prodotti e soluzioni sono fondamentali, ma è necessaria una cultura e una conoscenza specifica che non si esaurisce alla fine di un'installazione, ma prosegue nel tempo e continua prestando attenzione a novità, a pericoli informatici di nuova generazione, alla disponibilità di nuovi aggiornamenti software per contrastarli. Microsoft ha attivato numerosi servizi per rendere questo obiettivo più facile. Sfruttando canali e strumenti differenti, informa utenti e istituti scolastici, mettendo a disposizione aggiornamenti, suggerimenti e competenze in ambito di sicurezza.

Windows SP 2, come ottenerla?

Un primo importante aggiornamento, come abbiamo specificato nella top 10 della sicurezza, riguarda le patch. A partire dal 15 settembre Microsoft ha reso disponibile la Service Pack 2 di Windows XP in italiano che comprende le novità per una migliore protezione dei computer da pirati informatici, virus e altri rischi per la sicurezza. L'aggiornamento introduce nuove funzionalità in quattro aree principali: protezione della rete e della memoria, maggiore sicurezza nella gestione degli allegati di posta elettronica e durante la navigazione Internet. La Service Pack 2 è scaricabile gratuitamente dal sito Microsoft Italia all'indirizzo *http://www.microsoft.com/italy/windowsxp/sp2/default.mspx.*
In alternativa si può ordinare il Cd-Rom via Web. Il modo più semplice con cui assicurarsi di ricevere la Service Pack 2 è di attivare la funzionalità "Aggiornamenti automatici di Windows XP" o attraverso il servizio Windows Update. In ultimo, potete passare agli stand Microsoft durante le fiere per avere una copia del Cd-Rom.

Un sito a 360 gradi

Uno spazio utile per tenersi sempre aggiornati in tema di sicurezza è, invece, l'area sicurezza sul sito Microsoft, all'indirizzo *http://www.microsoft.com/italy/security*, dove si trova una panoramica su tutto quanto è necessario sapere per proteggere nel tempo sistemi, PC e strumenti informatici. Grazie a un aggiornamento costante, pubblica le notizie di maggiore spicco sulle nuove minacce della Rete, i virus più pericolosi, le patch Microsoft disponibili, le novità di prodotto.
Le notizie di maggiore importanza, comunque, sono presenti anche nell'area specifica per il mondo education, il sito Microsoft *http://www.microsoft.com/italy/education/default.mspx*

I bollettini sulla sicurezza

Senza passare ogni volta dal Web, si possono ricevere direttamente in posta le novità. Dai siti TechNet e Microsoft Security è possibile iscriversi, infatti, ai bollettini Microsoft

NON ESISTE REALE SICUREZZA SENZA UN AGGIORNAMENTO COSTANTE

Con il servizio Webcast Microsoft mette in rete, in esclusiva, le migliori lezioni tenute dagli esperti di sicurezza

per la sicurezza. Si tratta di newsletter che gli istituti scolastici, i direttori o i responsabili della sicurezza possono ricevere gratuitamente nella casella di posta elettronica. Contengono le ultime notizie in materia di sicurezza, i consigli degli esperti Microsoft e le novità di prodotto. Per chi avesse perso qualche numero o non volesse ricevere il bollettino, è possibile consultare i contenuti della newsletter direttamente via Web. E non è tutto. Grazie al servizio di Microsoft Security Update, il rilascio dei bollettini o allarmi virus sono annunciati via e-mail.
Anche in questo caso basta iscriversi sul sito, all'indirizzo *http://www.microsoft.com/italy/security/security_bulletins/decision.asp*

A lezione con i WebCast

Per chi ama la didattica via Internet ci sono anche sessioni formative di approfondimento, vere e proprie lezioni denominate WebCast. Sono repliche di eventi e seminari reali, tenuti da esperti Microsoft a Roma e Milano. Pensati per tutti coloro che non hanno potuto partecipare a questi workshop, i Webcast sono una replica degli eventi, tenuti dagli stessi speaker dei Security Workshop. Per parteciparvi basta registrarsi: dopo avere ricevuto una e-mail di conferma con una password e un link, si accede via Web a una pagina per seguire l'evento online.

Free virus support

Nei casi più seri, quando un virus ha infettato un PC o una rete, si possono ottenere indicazioni precise su come rimuovere il virus contattando direttamente Microsoft. Al numero 02.70.398.398 risponde un tecnico che può dirvi in tempo reale quali accorgimenti adottare per non aggravare la situazione e riportare alla normalità l'operatività delle vostre reti. Sempre a questo numero è possibile avere informazioni su

La SP2 di Windows XP in italiano si può scaricare gratuitamente dal sito Microsoft, altrimenti si può ordinare il Cd-Rom via Web

AGGIORNARSI SULLA SICUREZZA: TUTTI I LINK UTILI

Area sicurezza su PMI
http://pmi.microsoft.com/sicurezza
Microsoft Security
http://www.microsoft.com/italy/security
Cd-Rom Security Guidance Kit
http://www.microsoft.com/italy/security/guidance/order/default.mspx
Microsoft Security Community
http://www.microsoft.com/italy/technet/community/chat/default.mspx
Microsoft Webcast
http://www.microsoft.com/italy/technet/community/webcast/webcast_eventi.mspx
Microsoft TechNet
http://www.microsoft.com/italy/technet
Microsoft Security Update
http://www.microsoft.com/italy/security/security_bulletins/decision.asp
Bollettini sulla sicurezza
http://www.microsoft.com/italy/technet/security/bulletin
Eventi
http://www.microsoft.com/italy/technet/eventi
Microsoft Windows Update
http://windowsupdate.microsoft.com
Microsoft Office Update
http://office.microsoft.com/italy/ProductUpdates/
Microsoft Sofware Update Services
http://www.microsoft.com/italy/windowsserversystem/sus

indirizzi Internet utili, sui bollettini Microsoft che contengono soluzioni già sperimentate, sugli articoli pubblicati online con le migliori risposte alle vostre domande, sulle soluzioni antivirus di terze parti.
Informazioni sul Free virus support sono disponibili all'indirizzo: *http://www.microsoft.com/italy/security/supporto/free_support.mspx*

Formarsi e informarsi in community

Che cosa occorre fare quando si prende involontariamente un virus? O per installare un firewall? A chi serve un consiglio o una risposta specifica può rivolgersi alla community Microsoft dedicata alla sicurezza. Grazie al newsgroup si trova risposta a ogni domanda, occasioni di confronto con professionisti IT, nuove soluzioni. In questo punto di incontro virtuale si possono scambiare opinioni, cercare suggerimenti, fornire pareri a chi richiede soluzioni immediate. È una zona di scambio, utile nei momenti di verifica sulle proprie conoscenze in materia di sicurezza. Il sito di riferimento è *http://www.microsoft.com/italy/technet/community/chat/default.mspx*

Una rete per i professionisti: TechNet

Un importante servizio con cui affrontare il tema sicurezza è TechNet, spazio all'interno del sito Microsoft pensato come area di servizio in cui trovare strumenti e contributi di tipo tecnico e didattico per migliorare le proprie competenze e conoscenze. TechNet affronta la strategia generale per la sicurezza dei sistemi grazie ad attività di formazione online, documentazione tecnica, strumenti gratuiti. È rivolto principalmente a chi desidera approfondire l'aspetto tecnico, in particolare agli esperti di Information & Communication Technology o ai responsabili di laboratori e aule di informatica. TechNet è raggiungibile all'indirizzo: *http://www.microsoft.com/italy/technet/default.mspx.*

L'installazione della Service Pack 2 per Windows XP è semplice. Lasciatevi guidare da queste istruzioni

Passo dopo passo la NUOVA SP2

REQUISITI DI SISTEMA

La nuova SP2 può essere installata su PC che utilizzino Windows XP e che abbiano un processore a 300 MHz o superiore (Intel Pentium o Celeron, AMD K6 o Athlon o Duron, oppure processore compatibile). Sono necessari, inoltre, 128 MB di Ram e 800 MB di spazio disponibile su disco rigido. Se sono già installate versioni Beta della SP2 è necessario rimuoverle utilizzando il Pannello di Controllo.

1

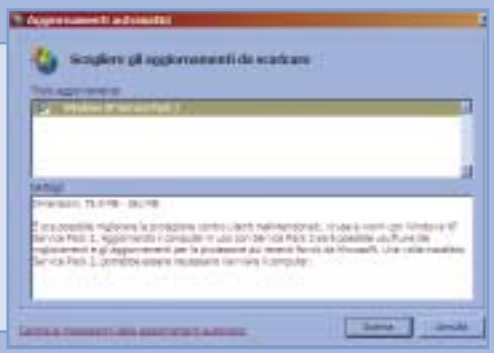
Microsoft mette a disposizione due modalità d'installazione della Service Pack 2 per gli utenti finali. Il software di aggiornamento si può scaricare da Web oppure si può eseguire un'installazione tramite Cd-Rom. Prima di iniziare, però, è opportuno accertarsi che si stia effettuando il download da siti appartenenti al network Microsoft o che il Cd-Rom sia originale, prodotto da Microsoft. Non dimenticate che per gli studenti del nostro Paese esiste una versione della Service Pack 2 di Windows XP in lingua italiana.

2

Se si decide di procedere via Web è possibile partire dal sito Windows Update http://windowsupdate.microsoft.com. Dopo un'iniziale ricerca automatica della versione del sistema operativo installato e degli aggiornamenti necessari, il servizio propone due tipologie di installazione: una "rapida", che consente di analizzare, scaricare e installare solo gli aggiornamenti critici necessari per il computer in uso, un'altra "personalizzata", per scegliere quali patch adottare in maniera mirata. L'installazione rapida è raccomandata per l'aggiornamento di un solo PC e per gli utenti meno esperti. Per portare a buon fine il download è necessario un buon collegamento a Internet: la procedura può durare, infatti, diverso tempo (l'applicazione per installare la Service Pack varia da 75 a 261 MB a seconda degli aggiornamenti necessari). Se la velocità di download è molto bassa, si consiglia di eseguire l'aggiornamento via Cd-Rom.

3 Una volta cliccato sul pulsante "Installa.." verrà chiesto all'utente si accettare il contratto di licenza d'uso. Una volta accettato, inizia il download. Prima di scaricare il file di aggiornamento valutate bene il tempo necessario, che viene indicato chiaramente da Windows Update. Al termine del download un avviso chiederà quindi all'utente se procedere o meno nell'installazione. Una volta scelto di andare avanti, nella finestra di dialogo che appare, è necessario scegliere la voce "Esegui l'applicazione dalla posizione corrente", quindi "OK".

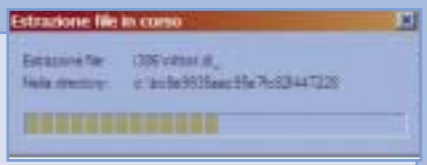
4 Un secondo metodo per eseguire il download da Internet è quello di procedere attraverso gli "Aggiornamenti automatici", una funzione di amministrazione del sistema operativo che solitamente prevede una icona sulla barra di stato, in basso a destra. Un doppio clic sull'icona lancerà la finestra qui rappresentata. Scelta poi la voce "Scarica", tutto procederà come descritto finora, passo passo, per il sito di Windows Update. La Service Pack 2 per Windows Xp viene trattata come gli altri aggiornamenti del sistema operativo. Al collegamento, Windows Update analizza il sistema e se non vi trova installata la SP2 procede a scaricarla.



5 Anche il procedimento basato sul Cd-Rom è semplice. Se si ha a disposizione il disco della Service Pack 2 per Windows XP, originale e prodotto da Microsoft, inseritelo nel drive del vostro PC. Una prima schermata vi chiederà di proseguire. Scelta la voce "Continua" avanzate con l'installazione selezionando la voce "Installa". Attenzione: prima delle operazioni d'installazione bisogna accertarsi che il software antivirus del PC non sia attivo.

6 Se inserendo il Cd-Rom nel drive del PC non è comparsa automaticamente la finestra iniziale di installazione, si possono richiamare le Risorse del Computer, poi aprire il drive in cui è inserito il Cd-Rom (per esempio <D:>), infine fare un doppio clic sul file eseguibile "XPsp2.exe".

7 Quanto tempo serve per installare la Service Pack 2 usando il Cd-Rom? Al massimo due ore. La durata dell'installazione dipende dalla configurazione del computer. Quando viene visualizzato l'indicatore di stato, non è necessario effettuare ulteriori operazioni. Il processo verrà eseguito automaticamente fino al completamento dell'installazione.



8 Il Setup Wizard della Service Pack 2 è quasi completamente automatico: l'utente deve solo avere l'accortezza di leggere gli eventuali avvisi che compaiono per scegliere le opzioni che desidera. Per esempio, se non vuole fare una copia di back up dei file, scelga "Non fare una copia dei file". Una volta avviata l'installazione di Windows XP Service Pack 2 è sufficiente seguire passo dopo passo tutte le informazioni che appaiono nel setup. Al termine dell'installazione sarà necessario riavviare il PC e quindi riattivare il software antivirus. Una volta completata l'installazione, per ulteriori informazioni sulla Service Pack 2 è possibile aprire "Guida in linea e supporto tecnico", selezionando "Novità di Windows XP", e poi "Novità".

Anche gli utenti che non hanno Windows XP possono mantenere elevati livelli di sicurezza per PC e reti: basta qualche accorgimento in più e una manutenzione costante

VECCHIE VERSIONI SOTTO CONTROLLO

Windows XP con Service Pack 2 offre funzionalità di sicurezza avanzate, in gran parte automatiche, centralizzate e dettagliate. Come abbiamo illustrato nell'articolo dedicato alla sicurezza di PC e reti, questo importante aggiornamento del sistema operativo riguarda Windows XP nelle versioni Professional e Home. In simbiosi con Office 2003 offre un livello di protezione difficilmente superabile.

Che cosa fare, però, se si possiede in sistema operativo precedente? Molto spesso gli istituti scolastici possiedono vecchi computer con installati sistemi operativi come Microsoft Windows 98 o Microsoft Windows 2000.

MICROSOFT NON ABBANDONA I SUOI VECCHI CLIENTI

Anche per loro valgono tutte le regole indicate in questa Guida, con la differenza, però, che non potendo installare la Service Pack 2, devono prestare maggiore attenzione a quegli accorgimenti che la SP2 risolve in maniera automatica. L'obiettivo principale di rendere PC e reti sicure è il medesimo.

Si devono tenere presenti tuttavia questi elementi di differenza. ■

	Windows XP SP2	Precedenti versioni
Firewall	Incorporato e attivo di default	Compatibilità garantita con firewall di altri produttori. Procedere con l'installazione manuale
Aggiornamenti Sistema	Windows Update, Aggiornamenti automatici	Windows Update nella sezione Archivio. Funzione da richiamare periodicamente
Antivirus	Compatibilità garantita con antivirus di altri produttori	Compatibilità garantita con antivirus di altri produttori
Livelli di protezione in Internet Explorer	Interni e automatici (blocco Pop-Up e blocco download automatico configurati sulla Protezione delle Opzioni Internet)	Manuali ed esterni (compatibilità a software di blocco Pop-Up di altri produttori, configurazione manuale dei livelli di Protezione delle Opzioni Internet)
Privacy e posta elettronica	Filtri automatici personalizzabili, blocco dei mittenti	Filtri parzialmente automatici, configurazione manuale regole di filtri, blocco dei mittenti
Protezione dati in Office	Ripristino automatico documenti	Salvataggio automatico documenti
Segnalazioni del sistema e controllo utente	Centralizzato, automatico, intuitivo (per esempio Security center o barra delle informazioni in IE)	Decentrato (avvisi in ogni componente), su impostazione manuale (per esempio, gli avvisi in IE dopo l'impostazione dei livelli di protezione)
Informazioni e risorse	Bollettini, siti Web, newsgroup, supporto telefonico	Bollettini, siti Web, newsgroup, supporto telefonico

SICURO?

Esegui questo veloce test di autovalutazione per capire il tuo livello di preparazione in materia di sicurezza. Un solo suggerimento: sii onesto, ne va della sicurezza del PC o della rete del tuo istituto...

1) **Di quanti di questi termini relativi alla sicurezza informatica conosci con certezza il significato?**
Virus, worm, hacker, cracker, trojan horse, firewall, spider, spy-ware, dialer, backdoor.
(Assegnati un punto per ogni parola conosciuta).

2) **Ogni quanto aggiorni il software antivirus?**
A - Mai, non ho un software antivirus (0 p.)
B - Da due volte l'anno a una volta ogni due mesi (2 p.)
C - Da una volta al mese a una volta la settimana (4 p.)
D - Ho configurato gli aggiornamenti automatici (10 p.)

3) **Ti arriva un messaggio di posta elettronica con un allegato sospetto. Che cosa fai?**
A - Elimino l'allegato senza aprirlo (3 p.)
B - Lo apro, lo salvo in una cartella e avvio l'antivirus (0 p.)
C - Lo salvo in una cartella senza aprirlo e avvio l'antivirus (10 p.)
D - Non faccio niente: non lo apro ma nemmeno lo elimino (3 p.)

4) **Dopo quanto tempo dal rilascio di patch critiche aggiorni il sistema?**
A - Non appena sono disponibili (10 p.)
B - Quando me ne accorgo (3 p.)
C - Che cosa sono le patch critiche? (0 p.)
D - Quando me ne accorgo, ma visito regolarmente i siti dedicati alla sicurezza (5 p.)

5) **Hai installato un firewall sul tuo PC?**
A - Sì, mantenendo le impostazioni predefinite (4 p.)
B - Sì e l'ho configurato secondo i miei parametri (10 p.)
C - No, non so che cos'è un firewall (0 p.)
D - Sì, e impedisco l'accesso a Internet a tutti i software escluso Internet Explorer e Outlook (2 p.)

6) **Quali rimedi hai adottato contro le e-mail spazzatura?**
A - Ho impostato filtri e inserisco i mittenti nell'elenco della posta indesiderata (10 p.)
B - Rispondo a ogni e-mail chiedendo di non riceverle più (0 p.)
C - Le cancello a una a una, dopo averle aperte e lette (1 p.)
D - Le cancello a una a una senza nemmeno aprirle (3 p.)

7) **Se navigando in Internet ti viene chiesto di aprire un file che cosa fai?**
A - Non apro nessun file su Internet (4 p.)
B - Cerco di capire se si tratta di un'applicazione, quindi salvo il file sul PC e avvio l'antivirus (10 p.)
C - Apro tutti i file: l'antivirus è già attivo sul sito (0 p.)
D - Apro il file, ma solo se antivirus e firewall sono attivi (6 p.)

8) **Ogni quanto tempo visiti i siti dei produttori di software legati alla sicurezza?**
A - Non seguo le questioni di sicurezza (0 p.)
B - Almeno una volta al mese (5 p.)
C - Non vado sui siti dei produttori, ma una volta alla settimana vedo altri siti informativi (5 p.)
D - Almeno una volta alla settimana, e comunque mi informo tutti i giorni tramite altri siti (10 p.)

9) **Hai impostato la Protezione tra le opzioni di Internet Explorer?**
A - Sì, ma ho impostato soltanto il livello generale di navigazione (5 p.)
B - Sì, e ho impostato il livello di tutte le aree (10 p.)
C - Non sapevo si potessero impostare livelli di sicurezza in Internet Explorer (0 p.)
D - Sì, ma ho impostato i livelli di tutte le aree a livello basso perché non voglio limitazioni (1 p.)

10) **La sicurezza informatica è:**
A - Una cosa da tecnici, da lasciare ai tecnici (2 p.)
B - Una mentalità nuova per migliorare l'attività digitale (10 p.)
C - Una frottola dei produttori per vendere nuovi software (0 p.)
D - Qualcosa di importante, anche se complica la vita dell'utente (5 p.)

RISULTATI

Punteggio da 0 a 29: sicurezza insufficiente. Faresti bene a correre ai ripari, prima di subire qualche danno grave.
Punteggio da 30 a 59: sicurezza bassa. Adottare contromisure sporadiche non ti mette al sicuro. È necessario pensare a tutte le soluzioni!
Punteggio da 60 a 79: sicurezza media. Sei stato abbastanza previdente, ma le insidie sono dietro l'angolo. Completa l'opera, ti manca poco.
Punteggio da 80 a 100: sicurezza elevata. Hai piena coscienza del problema e dei possibili rimedi. Non abbassare la guardia.

GLOSSARIO

Virus

Un virus è un codice informatico scritto con l'esplicita intenzione di replicare se stesso in modo autonomo attraverso programmi, messaggi di posta elettronica, ecc. Può danneggiare l'hardware, il software e le informazioni contenute su PC e periferiche. Esistono migliaia di virus diversi.
In comune hanno la capacità di duplicarsi, la possibilità di eseguire operazioni potenzialmente dannose sui sistemi infetti, attivarsi in contesti o momenti determinati. I virus vengono debellati tramite software denominati antivirus, in grado di intercettare un virus prima che entri sulla macchina locale (via posta elettronica, tramite un floppy disk infetto, tramite una condivisione di rete, ecc.) e di controllare ed eventualmente riparare i file infetti presenti sul computer.

Worm

Un worm ha caratteristiche simili a un virus: si duplica automaticamente e può farlo in modo estremamente rapido.
A differenza di un virus non si attacca ad altri programmi, ma tende a mantenersi autonomo e non necessariamente provoca danni diretti (per esempio cancellare dei file) ma con la sua esistenza può seriamente limitare banda e risorse a disposizione oppure essere causa di attacchi informatici a terze parti.
Tipicamente un worm si diffonde fra server in rete, sfruttando vulnerabilità note per penetrare in sistemi non protetti. I worm più noti sono quelli che replicano i messaggi di posta.

Hacker

Con il termine hacker si indica una persona esperta e abile nell'utilizzo di computer o programmi informatici, nella elaborazione di codici e di applicazioni.
Nell'uso corrente questo significato assume spesso una connotazione negativa, identificando l'hacker con qualcuno che "cerca di violare i sistemi informatici". Tipicamente questo tipo di hacker, più correttamente identificabile con il termine "cracker", è un programmatore esperto con sufficienti conoscenze tecniche per capire e sfruttare i punti deboli di un sistema di sicurezza.

Spamming

Lo spamming consiste nell'invio massiccio di messaggi di posta elettronica a carattere pubblicitario e commerciale, senza alcuna preventiva richiesta da parte del destinatario. Lo spamming è un vero bombardamento indiscriminato di messaggi, vietato secondo la normativa italiana sul trattamento dei dati personali (Decreto legislativo n. 196 del 30/6/2003) e secondo le regole europee e americane in materia.
Il danno più evidente creato dallo spamming è associato ai costi legati alla manutenzione per rimuoverlo.

Dialer

Dispositivo hardware o software capace di comporre un numero telefonico, come se fosse digitato manualmente. I dialer possono stabilire una connessione remota per l'accesso a un servizio (tipicamente per scaricare loghi e suonerie, file mp3, sfondi per computer, immagini pornografiche, ecc.) che viene pagato attraverso la bolletta telefonica.
Generalmente nascosto all'interno di un'applicazione autoinstallante, il dialer disconnette il modem dell'utente dal suo abituale provider e lo indirizza su un numero caratterizzato da una tariffa supplementare. La maggior parte dei dialer si installano sul PC degli utenti dopo un download automatico da Internet.

Patch

Una patch (denominata anche "fix") è la riparazione di una parte dei programmi informatici che mostrano instabilità o problemi connessi con la sicurezza. Spesso temporanea, in vista dell'integrazione nella versione successiva dei programmi, una patch sistema i problemi (chiamati anche "bug") riscontrati in un determinato programma durante la sua esecuzione. Una patch è la soluzione immediata fornita agli utenti da parte dei produttori di software. Quasi sempre può essere scaricata dai siti Internet dei produttori stessi.

Macro

Una macro è una sequenza di comandi e azioni eseguiti da tastiera o con il mouse e salvati, in ordine cronologico, per poter essere ripetuti in maniera automatica una seconda volta. Tipicamente si impiegano macro in programmi di office automation o desktop publishing per ottimizzare funzioni ripetitive o salvare azioni di particolare importanza.
In ambito di sicurezza informatica una macro è un virus, realizzato come una macro standard, ma con il potere di infettare i programmi e causare una sequenza di azioni dannose per il PC. I macro virus, innescati dalle applicazioni che le eseguono, possono creare sorpresa, ma spesso sono innocui. Si diffondono quasi sempre via e-mail.

Firewall

Con il termine firewall si indica sia un dispositivo hardware sia un'applicazione software che hanno lo scopo di proteggere la rete locale da accessi non autorizzati, bloccando le porte con cui un sistema comunica all'esterno. Posto normalmente fra la rete locale e Internet, nel perimetro della rete comprendente il router di accesso alla rete, il firewall viene configurato in modo da proteggere la rete o le singole applicazioni di un PC.

Trojan Horse

Il cavallo di Troia è un programma modificato che esegue funzioni particolari e potenzialmente nocive all'insaputa del possessore, a cui il programma appare funzionare normalmente. Lo scopo di un Trojan Horse, fedele al mito ellenico, è spesso quello di permettere dall'esterno un accesso, ovviamente non autorizzato, al sistema su cui viene eseguito. ■

CHE COSA OFFRE MICROSOFT PER IL MONDO DELLE ISTITUZIONI SCOLASTICHE SCOPRILO SUL WEB!

PROGETTI E INIZIATIVE DEDICATE

Per le istituzioni scolastiche e le università

Microsoft Education

Un'area dedicata a scuole e università dove puoi trovare news, progetti ed esperienze condivise.
http://www.microsoft.com/italy/education

Focus continuo sulla sicurezza informatica

Tutte le informazioni per migliorare la sicurezza informatica e garantire la tutela della privacy negli istituti scolastici.
http://www.microsoft.com/italy/education/scuola/sicurezza
http://www.microsoft.com/italy/education/uni/sicurezza

Fresh Start per Pc donati

Programma creato per gli istituti primari per garantire che i sistemi operativi dei PC donati siano coperti da una licenza valida.
http://www.microsoft.com/italy/education/pil/freshstart

Offerte su misura per il mondo education

Prodotti e soluzioni pensate per soddisfare le necessità di studenti, professori e istituzioni accademiche di ogni dimensione.
http://www.microsoft.com/italy/education/licenze

Per i docenti

Apprendere in rete

Uno spazio Web aperto e gratuito, pensato per gli insegnanti. Un punto di incontro virtuale, nato per diffondere nelle scuole la conoscenza e l'utilizzo delle tecnologie.
http://www.apprendereinrete.it

Microsoft Progetto Docente 2004-2005

Un programma sviluppato per accrescere le competenze IT nella scuola e tra gli insegnanti, promuovere le comunità scolastiche virtuali e sostenere i docenti nell'uso degli strumenti tecnologici nella didattica.
(Per maggiori informazioni visitate il sito di Apprendere in rete)

Per gli studenti

Microsoft IT Academy

Programma internazionale che mette a disposizione di scuole e università strumenti e servizi per erogare corsi di formazione IT di alto profilo, propedeutici alle certificazioni più richieste dal mondo del lavoro.
http://www.microsoft.com/italy/education/pil/itacademy

The Spoke

Spazio virtuale dove gli studenti possono conoscersi, scambiarsi conoscenze ed esperienze, trovare informazioni utili per un uso consapevole della tecnologia, confrontarsi su tematiche tecniche legate anche alla vita quotidiana.
http://www.thespoke.it

Microsoft®

Microsoft - Centro Direzionale S. Felice - Pal. A - Via Rivoltana, 13 - 20090 Segrate (MI)
Web: www.microsoft.com/italy/
Servizio clienti 02.70.398.398 - e-mail: infoita@microsoft.com