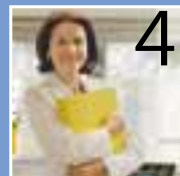


# Metti al **SICURO** la tua **IMPRESA**

*Linee guida per la **SICUREZZA**  
informatica e la tutela della **PRIVACY***



Sicurezza e privacy  
secondo la nuova  
normativa



Protezione  
e affidabilità  
per PC e reti



Le 10 regole  
della sicurezza  
informatica



Manutenzione  
e costi  
sotto controllo

## SOMMARIO

*Metti al sicuro  
la tua impresa*

pag. **1**



*Prevenire  
le insidie  
informatiche*

pag. **2**

*Il rispetto  
della  
privacy*

pag. **4**



*Protezione e  
affidabilità  
per Pc e reti*

pag. **6**



*Top 10  
sicurezza*

pag. **8**



*La manutenzione  
ha un costo*

pag. **16**

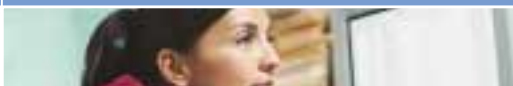
*La sicurezza  
nel tempo*

pag. **18**



*Glossario*

pag. **20**



# Metti al SICURO la tua IMPRESA

In questo periodo si parla tanto di sicurezza, ma vi siete mai chiesti che cosa significhi l'aggettivo "sicuro"? Nell'uso corrente della lingua italiana ha una doppia valenza: da una parte indica il fatto di essere "protetti", non soggetti a lesioni provocate dall'esterno, dall'altra indica l'impossibilità di arrecare danni, ovvero la certezza di non danneggiare altre persone. Si parla, infatti, di impianti elettrici sicuri o dell'airbag di un'automobile come sicura. Ma anche dei freni di un'auto o di giochi per bambini.

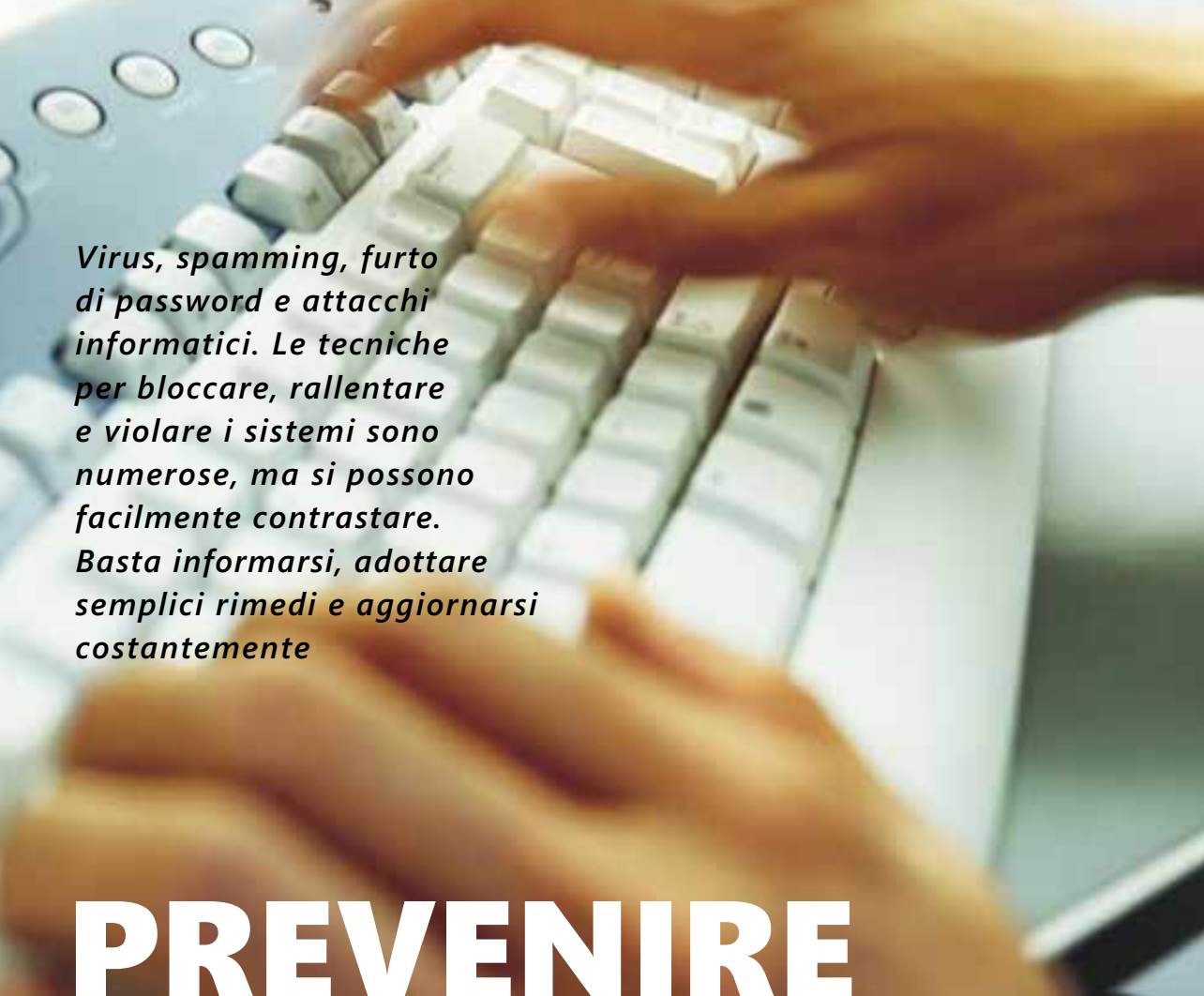
E i computer? Quando si può considerare un software "sicuro"? La prima risposta è certamente quando protegge i dati personali, le informazioni. Più in generale le attività svolte. Quando, cioè, garantisce che tutto quanto elaborato attraverso i sistemi informatici sia mantenuto in funzione, senza manomissioni, ritardi, cancellazioni. Un software è sicuro quando resiste agli attacchi esterni, prevede e annulla l'impatto negativo di eventi straordinari o attività illegali. Crea, cioè, un effetto "cassa-forte" intorno ai miei dati, li mantiene e garantisce continuità al mio lavoro o a quello dei dipendenti, impedendo pericolosi blocchi di produzione che avrebbero un impatto negativo sia economicamente sia dal punto di vista dell'immagine. Perdere dati, tempo e informazioni privilegiate (per esempio, facendole cadere nelle mani dei concorrenti) è, infatti, per un'impresa paragonabile a un incidente fisico o alla rottura di un impianto. Potrebbe fermare la produzione o far perdere competitività sul mercato, oltre a far spendere ingenti somme di manutenzione per il ripristino dei sistemi o il recupero dei dati. Ma non solo. Come per i freni di un'automobile, il software sicuro è anche quello che impedisce a chi lo possiede di arrecare danni, seppur involontariamente, ad altre persone o di riceverne. Si pensi all'uso illecito dei PC quando un hacker prende possesso dei computer di un'impresa. Oppure all'errato trattamento dei dati personali come previsto dalla nuova Legge sulla Privacy. In questo caso si va dalla multa fino alla reclusione. Non si tratta di semplici malfunzionamenti, ma di reati. Oltre ovviamente alla perdita di credibilità e dunque di clienti.

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 delle imprese e dei professionisti 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 rivenditori qualificati (Punto Microsoft) e di partner e consulenti certificati (Microsoft Certified Partners) - che sappiano tradurre le nostre attenzioni verso clienti e utenti finali. La nostra convinzione è semplice: informare e informarsi è meglio che curare. Non perdetevi tempo, dunque. Mettete al sicuro la vostra impresa.



Francesco Orrù,  
Responsabile del Programma Sicurezza  
di Microsoft Italia

A handwritten signature in black ink that reads "Francesco Orrù". The signature is fluid and cursive, written over the printed name.



*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 per accedere a siti finanziari o compiere operazioni bancarie. 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 gli impiegati a causa di un malfunzionamento della rete aziendale. C'è poi una questione di immagine. Subire una violazione dei propri sistemi di sicurezza, un sabo-

taggio o un'intrusione significa perdere credibilità e fiducia: un danno difficilmente quantificabile che crea forte imbarazzo con clienti e fornitori. Infine, i dati. I danni possono riguardare la modifica, il furto o addirittura la perdita totale di informazioni importanti, vero punto di forza delle società moderne, soprattutto di 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: ASSIFORM)**

## 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 di una società. Un altro pericoloso e silenzioso sistema di sfruttamento è l'uso non autorizzato di identità digitali, ovvero di login e password altrui. Attraverso di esso si possono controllare le reti private, accedere a informazioni, rubare dati, modificare siti Internet per arrivare talvolta a sfregiare l'immagine aziendale stessa. 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 impiegati, 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

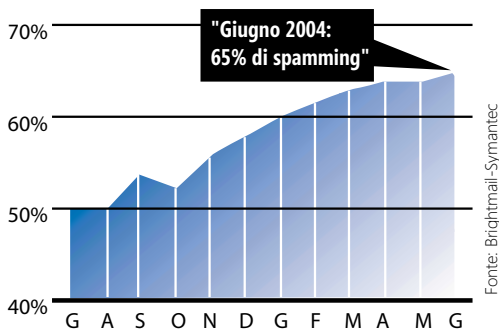
Per tornare alla vicenda scoperta da Bambenek si comprende ora come si tratti certamente di un caso estremo che mostra, però, due importanti verità. Primo: i pericoli informatici sono molti, difficilmente identificabili senza una costante attenzione o informazione, si moltiplicano in numero e virulenza, possono arrecare danni sia a livello economico, anche soltanto facendo perdere tempo, sia a livello di privacy, sottraendo e dis-

tribuendo 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 piccola impresa? Ebbene, taluni virus o lo spamming, per esempio, non fanno distinzione. Colpiscono in maniera indifferenziata, grandi e piccole imprese, liberi professionisti e multinazionali. Il rimedio da adottare è, però, lo stesso: aggiornamento, prevenzione, conoscenza. Questa guida vi porterà

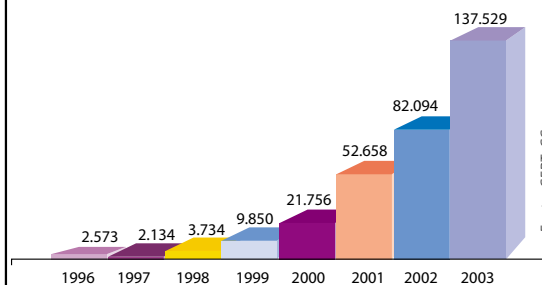
passo passo a comprendere quali accorgimenti e comportamenti adottare per rendere sicuro il vostro PC o la vostra Rete. Nessun panico, dunque. La sicurezza si può migliorare, basta sapere come e soprattutto che cosa fare. ■


### 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 impresa 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

**C**ambia 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. Tutte le imprese, le ditte, gli studi professionali e 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 statuto. 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 responsabile legale dell'impresa rischia, infatti, di incorrere in sanzioni penali. Ma che cosa si

**IL REQUISITO  
MINIMO:  
LA SICUREZZA**

deve fare in concreto? Entro il 30 giugno 2005 le imprese 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, ecc. - e gli interventi che l'impresa intende realizzare per adeguarsi alla nuova normativa. Questo documento dovrà essere allegato al bilancio della società e aggiornato ogni anno. Le aziende possono decidere di affidare all'esterno la realizzazione degli interventi richiesti, ma ogni operazione dovrà essere riportata nel DPS e certificata dalla società incaricata come conforme alle disposizioni previste dal codice.

## **Le misure minime**

Ci sono poi alcuni provvedimenti considerati "minimi" da adottare. 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 imprese devono applicare

opportuni interventi che tengano conto anche del progresso tecnologico e dell'utilizzo sempre più frequente 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'azienda. 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 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 alcu-

ne 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.

### **Disposizioni da attuare**


Per adeguarsi alle disposizioni richieste dal nuovo codice, le imprese 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 imprese i massimi livelli di sicurezza e la possibilità di essere in regola con le misure richieste dalla nuova normativa sulla privacy. ■

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

## **LE NUOVE MISURE RICHIESTE DAL CODICE DI PROTEZIONE DEI DATI PERSONALI (D.LGS 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 rimovibili;**
- 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 garanzie durante il lavoro quotidiano con i programmi di produttività individuale*

# PROTEZIONE e AFFIDABILITÀ per PC e reti

**P**rovate a pensare alle innumerevoli attività che oggi si possono fare attraverso un personal computer: dallo scambio di messaggi alle fatture, dall'agenda alla scrittura di una lettera. Quale altro strumento rappresenta meglio l'unità minima e più importante della nostra giornata lavorativa? Lo strumento più funzionale per la nostra produttività? Attorno a questo nucleo ruota gran parte del lavoro quotidiano e del business delle imprese.

È ovvio, però, che quanto più ci affidiamo 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 aziendale 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 LA PRODUTTIVITÀ  
E L'EFFICIENZA*

## 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 aziendale. Composta dalla coppia Microsoft Windows XP Professional e Microsoft Office 2003, questa combinazione di sistema operativo e di software per la produttività individuale permette alle imprese 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,

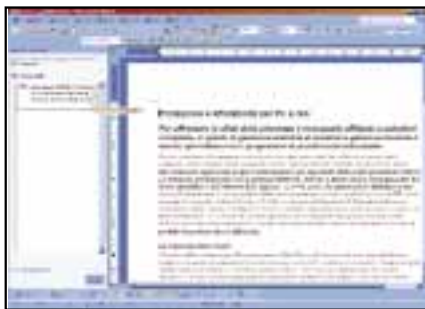
alla prevenzione della perdita di dati e informazioni, alla protezione di virus e worm inviati via posta elettronica o inseriti all'interno di macro, fino a nuovi filtri in grado di contrastare il fastidioso fenomeno dello spamming.

## 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 aziendali 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, 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 proposta commerciale per un nuovo cliente un malfunzionamento arrestasse il sistema.

Con Office 2003 il vostro 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.

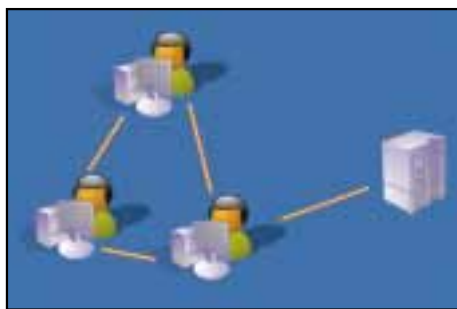
Innanzitutto, attiva in modalità predefinita (ovvero, non è necessario da parte dell'utente intervenire sulla configurazione del PC) un potente firewall che protegge il sistema già durante le prime fasi di avvio, impedendo intrusioni indesiderate o la diffusione di particolari tipi di worm attraverso una connessione Internet. 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. 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.

## 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 aziendali 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. La presenza di un server semplifica molte operazioni in un'impresa. 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

VUOI OTTENERE  
WINDOWS XP SP2?  
VISITA IL SITO

[HTTP://PML.MICROSOFT.COM/SICUREZZA](http://pml.microsoft.com/sicurezza)



Windows Small Business Server 2003 è particolarmente adatto alle esigenze della piccola e media impresa (fino a 75 PC)

Server 2003 è particolarmente adatto alle esigenze della piccola e media impresa. Collega in rete fino a 75 PC e offre, in un'unica piattaforma, tutte le funzionalità per la gestione delle attività e dei processi di business di cui la vostra azienda ha bisogno: connessione a Internet sicura, gestione della posta elettronica, supporto per i dispositivi mobili, accesso remoto, condivisione di file e stampanti, invio fax dalla postazione di ogni utente, strumenti per il backup e ripristino di dati, applicativi per la creazione di una Intranet aziendale per condividere dati e informazioni in maniera semplice ed efficace. ■

# TOP 10 SICUREZZA

*I dieci passi  
per rendere  
sicuro il PC  
e la rete  
aziendale*



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 quotidianamente 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 proprio computer, proteggendo lavoro e privacy. 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. Questa lista di 10 promemoria può aiutare ad assicurare meglio i propri computer:

- 1.1 posizionate i vostri 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;



## LE 10 REGOLE DELLA SICUREZZA

- 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 chiudete a chiave i locali quando non c'è nessuno;
- 1.6 controllate gli allarmi regolarmente;
- 1.7 marchiate i vostri computer con informazioni per identificare il proprietario, la società, 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 generatori di corrente continua, utili nel caso di black out, in particolare per portare corrente ai server o ai computer che non devono subire interruzioni o fermi macchina.

- 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. Navigare 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.**

La sicurezza fisica inizia dalla identificazione univoca del proprio PC



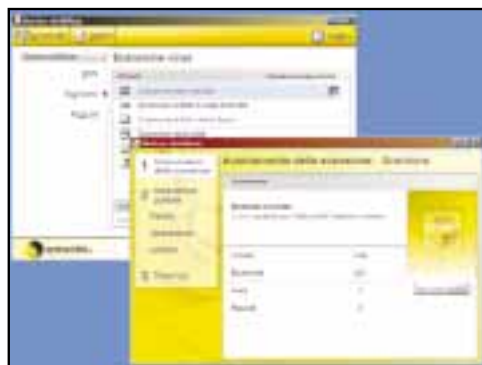
- E. non disattivare mai le protezioni antivirus sulla posta in entrata, in uscita, sugli script e sulle macro, se disponibili;
- F. lanciare periodicamente un controllo completo del proprio PC, come se fosse un malato su cui fare un check up per valutare lo stato di salute. Per questa analisi è possibile 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.

## 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;

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. 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 applicazione non richiesta è di conseguenza



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](http://www.symantec.com)]

**McAfee** [[www.mcafee.com](http://www.mcafee.com)]

**Sophos** [[www.sophos.com](http://www.sophos.com)]

**Trendmicro** [[www.trendmicro.com](http://www.trendmicro.com)]

**Computer Associates** [[www.ca.com](http://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](http://www.microsoft.com/italy/security/articles/software_antivirus.mspx)

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 download 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 e un capitale di uomini e conoscenze che rendono i software da loro creati estremamente affidabili.

### 3. Archiviare le informazioni utili

Si chiama "backup", 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 lavorativa o la conservazione di informazioni privilegiate.

La stessa nuova legge sulla privacy, di cui abbiamo parlato nelle pagine precedenti, impone alle imprese che conservano dati di terzi, 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 backup della vostra macchina.**

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 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 - 2,5 GB	Dvd
2 GB - 12 GB	DAT (Digital Audio Tape)
Più di 12 GB	Sequenze di DAT collegati

### 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 luogo di nascita o di residenza, oppure informazioni e dati facilmente riconducibili agli utenti.

**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:

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



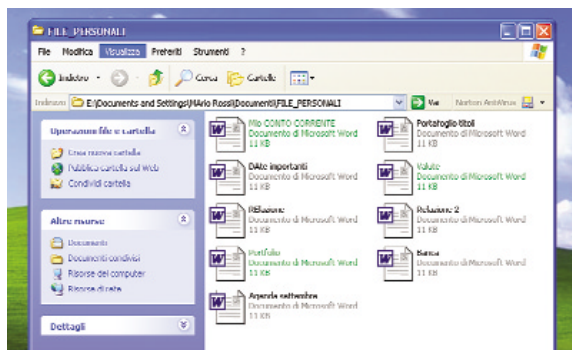
del tipo "1234", tipica per esempio delle segreterie telefoniche. Al contrario, invece, si possono definire queste regole per aumentare la forza di una password:

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: "Ek7!<g09". 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 vinco la lotteria!" oppure si possono creare frasi simili a rebus, come "AA=Agosto+America!". In ultimo, si possono usare acronimi, come per esempio "ILmNè01" che sta per "il mio nome è zero uno". 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 solo questione di tempo. Per cui ogni password va custodita come la chiave di casa. Non va mai ceduta a nessuno. Se qualcuno conosce la vostra password, il vostro PC è potenzialmente vulnerabile! Scontato poi di non scriverla vicino al vostro 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 vi 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.

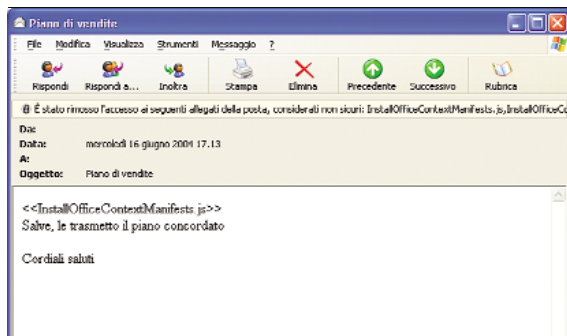
## 6. Sul Web senza paura

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.

**Come sesta regola si può dunque dire: navigare 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 lavorativo, per cercare opportunità, contatti e risorse legate al proprio business.

Ecco alcuni principi chiave, ovviamente da interpretare secondo le esigenze individuali:

1. non accedete a siti che non considerate affidabili;
2. non eseguite transazioni utilizzando circuiti bancari sconosciuti;
3. non navigate sul Web direttamente dal server di una rete.



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

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 aziendale per la navigazione e rendetela nota ai dipendenti. In particolare, stabilite quali comportamenti sono considerati illeciti (per esempio, la navigazione su siti pornografici, violenti, illegali, ecc.).

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.

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 connessioni 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 è già pronto a combattere i tentativi di intrusione. Il software, inol-

### ALTRI FIREWALL CONSIGLIATI

**Symantec** [[www.symantec.com](http://www.symantec.com)]

**McAfee** [[www.mcafee.com](http://www.mcafee.com)]

**ZoneLabs** [[www.zonelabs.com](http://www.zonelabs.com)]

## 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

tre, consente il flusso normale del traffico in uscita e filtra sessione per sessione tutte le attività 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 è possibile anche configurare una sola volta le caratteristiche di sicurezza desiderate e poi adattare i PC collegati senza perdite di tempo.

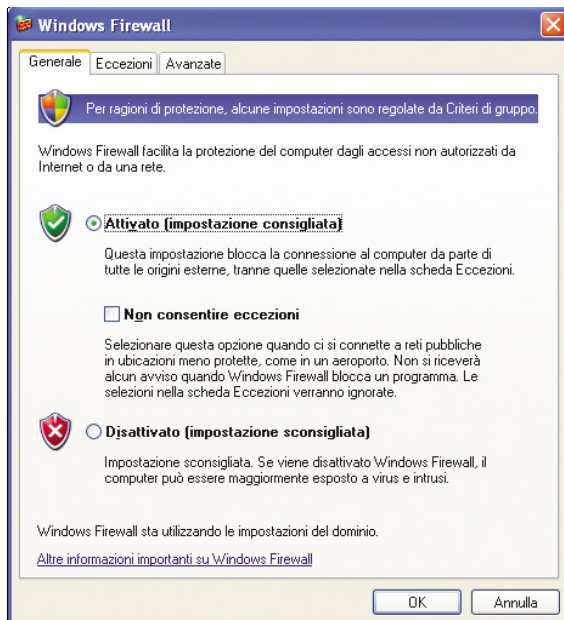
Due ultimi dettagli prima di passare alla posta elettronica. Tra i vantaggi di un firewall è giusto annoverare anche la capacità di nascondere i singoli PC di una rete all'esterno. In altre parole un firewall rende la vita difficile agli hacker che desiderano raggiungere una determinata macchina, poiché 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 lavorano nella stessa impresa.

## 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 competitivo. Considerato il crescente bisogno di utilizzare la rete per comunicare e condurre attività commerciali, tenere sotto controllo i sistemi di e-mail è infatti fondamentale per dare continuità, sicurezza e protezione al proprio lavoro. 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 mali-

### PER LE IMPRESE PIÙ ESIGENTI

*Tra le offerte Microsoft a maggiore valore aggiunto per il mercato delle piccole e medie imprese c'è una soluzione studiata per la protezione totale delle reti di medie dimensioni e complesse. Il nuovo firewall Microsoft ISA SERVER (Internet Security Acceleration Server), incluso anche nella versione Premium di Small Business Server 2003, facile da gestire e da configurare, consente di gestire in modo sicuro la rete aziendale. 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.*



**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.**

gni, 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 stesso modo è aumentato il livello di protezione della Rubrica, per



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

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 le piccole e medie imprese 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

**Nonna 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 siste-

ma 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 le imprese, invece, Microsoft ha predisposto una soluzione a più ampio raggio. Le aziende 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 aziendale. 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 aziendale. 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 intuitivi: 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 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 in questo modo presentano lo stesso grado di



**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**




aggiornamento e di sicurezza, diminuendo l'esposizione della rete aziendale ai pericoli informatici. In sostanza, SUS permette di tenere il passo delle più recenti protezioni e, al tempo stesso, abbatte i costi aziendali relativi alle operazioni d'aggiornamento.

## 10. Connessioni protette

**Decima regola: proteggete le vostre connessioni.** Lavorare da casa, collegarsi alla rete aziendale in viaggio, connettersi dalla sede di un cliente sono situazioni sempre più frequenti nelle imprese o per un singolo professionista. Consentire i collegamenti da remoto e mettere a disposizione l'e-mail aziendale anche a distanza permettono una flessibilità mai conosciuta in precedenza. Sono soluzioni che rappresentano una risorsa importante per l'impresa, per flessibilizzare il lavoro e la produzione. Al tempo stesso, però, sono elementi di grande esposizione al rischio. Lascereste, infatti, una vettura aziendale in mano a uno sconosciuto? Lo stesso deve valere per la banda di connessione 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-impos-

sessarsi 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, 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 l'azienda. ■



*La tecnologia Microsoft garantisce costanti aggiornamenti per la sicurezza informatica a costi limitati, aiutando le imprese 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'impresa. Ogni professionista, piccola o media impresa ha esigenze proprie, concrete, che cambiano anche con il tempo. Ma quale "meccanico" autorizzato saprà mettere mano ai sistemi informativi già collaudati?

### **POSSESSO DI HARDWARE E SOFTWARE**

**COSTO TOTALE = COSTO INIZIALE DI ACQUISTO + INSTALLAZIONE + MANUTENZIONE**

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 fermo macchina. Non si può improvvisare. È giusto optare per le soluzioni più sicure, i rivenditori più affidabili e veloci. La tecnologia Microsoft, a differenza di altre, per esempio di quelle open source, garantisce un costante livello di aggiornamento e da tempo gode di numerosi strumenti e canali di supporto. Non è affidata alla buona volontà di capaci programmatori che lavorano in maniera autonoma, ma regolarmente perfezionata dal lavoro di migliaia di ricercatori Microsoft attenti a mettere a disposizione delle imprese tutte le novità utili per rendere più sicuri i sistemi informativi e rispondere rapidamente alle esigenze di aggiornamento. Microsoft, inoltre, ha fissato un calendario preciso con cui rilascia novità e rimedi in ambito di sicurezza. Le soluzioni ai "guasti" non sono affidate alla semplice disponibilità di consulenti, ma suggerite di

### LA TECNOLOGIA MICROSOFT OFFRE:

- AGGIORNAMENTI COSTANTI
- UN SISTEMA AUTOMATICO DI INSTALLAZIONE
- L'ABBATTIMENTO DEI COSTI DI MANUTENZIONE

volta in volta attraverso bollettini e servizi Internet, con la finalità di evitare costosi blocchi di produzione o anticipare pericoli e nuove minacce. Inoltre, grazie alla tecnologia Software Update Services, il livello di servizio è completo: ogni utente è sempre informato sulle cose importanti da installare. Volendo, come illustrato nel decalogo della sicurezza di questa guida, l'installazione delle novità è, addirittura, 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? ■

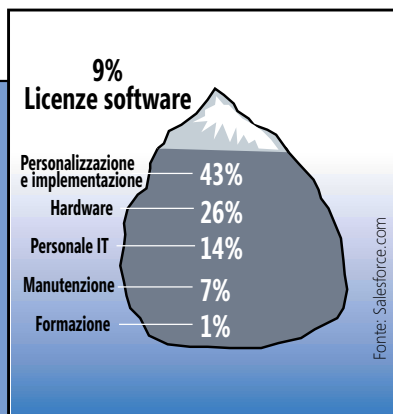
## IL COSTO DELLA SICUREZZA

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? 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. Le percentuali di incidenza sul costo legato al possesso di soluzioni informatiche nel corso del tempo sono:

- licenze software (9%): rappre-

sentano 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 IT (14%): tra gli asset in ambito informatico ci sono anche le risorse umane. 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.



# La SICUREZZA nel TEMPO

*Tutte le risorse Microsoft per tenersi aggiornati in materia di sicurezza: dal Cd-Rom "Bussola d'Impresa" al sito dedicato alle Pmi, dai bollettini e dai Webcast alla community, dal sito TechNet al supporto per combattere i virus*

**N**on 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 i propri clienti, le imprese e i consumatori, mettendo a disposizione aggiornamenti, suggerimenti e competenze in ambito di sicurezza.

## **La guida alla Sicurezza Informatica: "Bussola d'Impresa"**

Sul tema della sicurezza informatica è disponibile una semplice guida informativa creata appositamente per i professionisti e gli imprenditori impegnati a scegliere le soluzioni e i programmi più adatti al proprio business. La guida, di rapida consultazione e realizzata in tecnologia flash, illustra inizialmente la nuova legge sulla Privacy (Dlgs. 196/03) e le azioni indispensabili da intraprendere per essere in regola con la nuova normativa e rendere sicuri i dati personali. Successivamente sono illustrate da un lato le principali minacce - quali virus, perdita dei dati, intrusioni... - che incombono nella vita di tutti i giorni, e dall'altro le soluzioni messe a disposizione da Microsoft in termini di sicurezza informatica,

sia per prevenire i problemi sia per essere in regola con il Dlgs 196. Il CD può essere richiesto gratuitamente compilando il form al seguente link <http://pmi.microsoft.com/bussolaimpresa>.

## **Un sito a 360 gradi**

Uno spazio utile per tenersi sempre aggiornati in tema di sicurezza è l'area sicurezza sul sito PMI, all'indirizzo <http://pmi.microsoft.com/sicurezza>, correlata a TechNet ma dedicata ai professionisti e alle piccole e medie imprese. 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.

## **I bollettini sulla sicurezza**

Dai siti TechNet e Microsoft Security è possibile iscriversi ai bollettini Microsoft per la sicurezza. Si tratta di newsletter che le imprese e i professionisti 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 anche direttamente via Web. E non è tutto. Grazie al servizio di Microsoft Security

**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



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](http://www.microsoft.com/italy/security/security_bulletins/decision.asp)

## A lezione con i WebCast

Per chi ama la didattica 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 indirizzi Internet utili, sui bollettini Microsoft che contengono soluzioni già sperimentate, sugli articoli pubblicati online con le migliori risposte alle vostre domande,

Grazie ai Cd "Bussola d'Impresa" è possibile avere una panoramica sui temi più importanti per affrontare le sfide legate alla sicurezza, alle reti informatiche e al rispetto della nuova normativa in materia di privacy



## 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.aspx>  
**Microsoft Security Community**  
<http://www.microsoft.com/italy/technet/community/chat/default.aspx>  
**Microsoft Webcast**  
[http://www.microsoft.com/italy/technet/community/webcast/webcast\\_eventi.mspx](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](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 Software Update Services**  
<http://www.microsoft.com/italy/windowsserversystem/sus>

de, 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](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.

TechNet è raggiungibile all'indirizzo:

<http://www.microsoft.com/italy/technet/default.mspx>. ■

# 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 determina-

to 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 un 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. ■

# Scopri la soluzione Microsoft più adatta alla tua azienda...

CATEGORIA PRODOTTO	STUDI PROFESSIONALI E PICCOLE IMPRESE	MEDIE IMPRESE
Sistema operativo client	Windows XP Professional Service Pack 2	Windows XP Professional Service Pack 2
Applicativi	Microsoft Office Small Business Edition 2003. Per esigenze di databa- se e eseguire soluzioni integrate con Microsoft Office 2003 (Office Smart Client): Microsoft Office Professional Edition 2003	Microsoft Office Professional Edition 2003
Sistema operativo server	Windows Small Business Server 2003 Standard o Premium Edition	Windows Server 2003
Posta elettronica	Exchange Server 2003 (già incluso in Small Business Server 2003 Standard e Premium Edition)	Exchange Server 2003
Firewall, proxy e VPN	ISA Server (già incluso in Small Business Server 2003 Premium)	ISA Server

## ... e il Punto Microsoft più vicino a te.

I Punti Microsoft sono rivenditori specializzati su tecnologia Microsoft, in grado di supportare le piccole e medie imprese nella valutazione e nell'implementazione dei prodotti e delle soluzioni Microsoft più adatte alle proprie esigenze tecnologiche.



Puoi individuare il Punto Microsoft più vicino alla tua azienda collegandoti al sito: [http://www.microsoft.com/italy/punto\\_microsoft/pmi/default.mspx](http://www.microsoft.com/italy/punto_microsoft/pmi/default.mspx)

**Microsoft®**

© 2004 Microsoft. Tutti i diritti riservati.

Questa pubblicazione è puramente informativa.

MICROSOFT NON OFFRE ALCUNA GARANZIA, ESPLICITA O IMPLICITA SUL CONTENUTO.

Tutti i marchi e marchi registrati citati sono di proprietà delle rispettive società.

Microsoft - Centro Direzionale S. Felice - Pal. A - Via Rivoltana, 13 - 20090 Segrate (MI)

Web: [www.microsoft.com/italy/](http://www.microsoft.com/italy/)

Servizio clienti 02.70.398.398 - e-mail: [infoita@microsoft.com](mailto:infoita@microsoft.com)