Philippe Bolgiani
consulente informatico

febbraio 2011

Proteggere il proprio computer domestico non è un compito difficile. Bastano poche semplici regole per evitare quasi tutti i problemi.

Proteggere il proprio computer domestico in poche mosse

Proteggere il proprio computer è indispensabile, in particolare quando ci si collega ad Internet. Per una protezione di base, quella necessaria per un normale uso domestico, non è necessario essere degli informatici esperti. Alcune regole di base, divise in due grandi categorie, forniscono una sicurezza ragionevole, fermo restando che la sicurezza assoluta non esiste. Centrali sono la configurazione del sistema e il comportamento dell'utente.

Dopo aver superato il primo grosso scoglio (la scelta del computer da comprare) vi è la necessità di proteggerlo adeguatamente. Questa è la fase decisiva per evitare quasi tutti i problemi e soprattutto per riuscire a superarli se qualcosa dovesse andare storto (purtroppo capita, di regola nel momento peggiore).

Premessa: non esistono computer assolutamente sicuri e inattaccabili. Tutti i tipi di computer sono attaccabili (e non si pensi unicamente ai computer classici: anche, ad esempio, gli smartphone sono ormai in tutto e per tutto dei comupter). Il rischio dipende in gran parte dalla diffusione del tipo di computer in questione, in quanto gli autori dei virus hanno interesse a colpire il maggior numero possibile di computer. Non proteggere il proprio computer solo perché è di un tipo poco diffuso e quindi poco soggetto ad attacchi, è una pessima idea.

Nei seguenti paragrafi presenteremo poche semplici regole con le quali si può raggiungere un grado di sicurezza ragionevole, fermo restando che la sicurezza assoluta non esiste. Queste regole, valide per dei computer domestici, possono venir divise in due grandi gruppi: la configurazione del sistema e il comportamento degli utenti. Per gli utenti ai primissimi passi, è consigliabile chiedere l'aiuto di un amico più esperto che possa aiutare. L'approccio migliore, per poter imparare e diventare indipendenti, è non limitarsi a far semplicemente eseguire il lavoro dall'amico più esperto, ma piuttosto eseguirlo di persona con la persona esperta pronta a correggere in caso di necessità.

Le ditte hanno normalmente dei sistemi informatici più complessi rispetto ai normali cittadini e dispongono di Proxy, webserver, mailserver, diversi router, backup giornalieri, settimanali e mensili, diversi Firewall, zona demilitarizzata, molti utenti con profili diversi, diverse stampanti di rete, ecc. Un piccolo errore di configurazione può compromettere tutta la sicurezza. Per questa ragione è indispensabile avvalersi dell'aiuto di un professionista del settore.

Configurazione del sistema:

- **Installazione e ripristino**: all'acquisto di un computer è importante chiedere di avere anche i dischi originali per l'installazione del computer o almeno avere un disco di ripristino (o crearselo: cercare le istruzioni su internet o nel help integrato nel computer). Nel caso di un problema maggiore potrebbe essere necessario o più semplice dover partire da zero, reinstallando tutto. Custodite gelosamente questi dischi. La speranza è di non doverli mai usare, ma non averli in caso di necessità crea grossi problemi.
- **Aggiornamenti**: i programmi informatici contengono errori e punti deboli. Essi vengono regolarmente scoperti e corretti con degli aggiornamenti. Il consiglio è di impostare gli aggiornamenti automatici, in modo che il computer, quando è collegato ad Internet, si accorga da solo se è necessario scaricare una correzione. Il principio secondo cui "*Adesso funziona, quindi non cambio più nulla*" è un approccio pericoloso.
- **Antivirus**: si tratta di una protezione indispensabile, per tutti i tipi di computer. Per un uso domestico i programmi antivirus disponibili gratuitamente (*Avast, AVG, AntiVir, Panda, ecc*) forniscono una protezione sufficiente. Importante è installare un solo programma antivirus (due antivirus assieme si disturbano l'un l'altro). I programmi antivirus contengono una lista di virus conosciuti e contro i quali sono efficaci; aggiornare questa lista regolarmente (possibilmente quotidianamente e in automatico) è indispensabile, in quanto vengono continuamente scoperti nuovi virus.
- **Antispyware**: Gli spyware sono programmi malevoli, il cui scopo è raccogliere informazioni riguardanti l'attività online di un utente (siti visitati, password, codici bancari, numeri di carte di credito, ecc). Contro questo tipo di attacco esistono delle soluzioni mirate: gli antispyware. Come per gli antivirus esistono diverse soluzioni gratuite (*Spybot, Ad-Aware, Windows Defender, SpywareBlaster, ecc*) che forniscono una protezione sufficiente. Essi sono da aggiornare regolarmente.
- **Programmi di pulizia**: l'uso dei computer lascia tantissime tracce elettroniche nel computer stesso. Esse, oltre ad occupare inutilmente memoria, rallentano il sistema. Esistono dei programmi, gratuiti (*CCleaner, Disk Cleaner, Easy Cleaner, ecc.*), per eliminare in pochi secondi tutte queste tracce.
- **Reti wireless**: la comodità delle reti wireless è indubbia, in quanto permettono una maggiore mobilità evitando di tirare cavi. I dati circolano via etere e sono quindi teoricamente accessibili da tutti gli apparecchi nel raggio di alcune decine di metri. Per impedire a terzi di prendere conoscenza dei propri dati è dunque necessario proteggere le propria rete wireless, prevedendo una cifratura robusta dei dati protetta da una password d'accesso. Inoltre la "centraline wireless" (in gergo *router*) prevedono delle configurazioni. Per poter modificare quest'ultime è necessario conoscere la password del router. I router hanno una password standard (normalmente banale, tipo "1234"), la quale va cambiata.

Comportamento degli utenti:

- **Gestione e complessità delle password**: gli utenti devono ricordare molte password. È una pessima abitudine usare sempre le stesse per tutti i differenti servizi. D'altra parte è oggettivamente difficile ricordare tutte le password, specie se alcune di esse vengono usate molto raramente. Per ovviare a que-

sta problematica, esistono dei programmi gratuiti (*Password Corral, PasswordSafe, KeePass*), che permettono di custodire tutte le password in modo sicuro. Altri aspetti importanti riguardanti le password sono la loro complessità e la loro lunghezza. Consigliabili sono password di almeno 8 caratteri e che contengano lettere minuscole, lettere maiuscole e cifre, evitando dati collegabili alla persona (data di nascita, numero di targa, nome dei figli, squadra del cuore, ecc.).

- **Email**: le email, visto il loro carattere gratuito, vengono spesso utilizzate quale veicolo per attaccare dei computer. Esistono ditte (in gergo *spammer*) che non fanno altro che spedire email - tipicamente con in allegato dei virus o dei riferimenti a siti fasulli - a milioni di indirizzi, nella speranza che anche solo una piccola percentuale li apra cadendo nella trappola (questo genere di tecnica viene definita *phishing*). Il consiglio è cancellare queste email senza aprirle. In ogni caso non bisogna mai rispondere a queste email, in quanto rispondendo si conferma agli spammer che l'indirizzo email in questione viene effettivamente utilizzato.
- **Programmi di dubbia provenienza**: non aprire mai programmi di dubbia provenienza. Essi possono nascondere al proprio interno dei virus. Se scaricate un programma (ad esempio un antivirus), cercatelo sul sito ufficiale del produttore o da altre fonti sicure. Questo vale in particolare per programmi ricevuti tramite email, tipicamente (ma non solo: si pensi al computer di un amico a sua volta infettato da un virus che vi manda una email) da persone che non si conoscono.
- **Backup**: i documenti ritenuti importanti (foto, lettere, filmati, indirizzari, email, ecc) meritano una protezione supplementare. È buona abitudine farne una copia di sicurezza (in gergo *backup*) su un supporto esterno (una pennetta USB o un Harddisk esterno, ecc). Se il computer dovesse guastarsi, se venisse smarrito o se dovesse essere necessario reinstallarlo, senza un backup non potreste recuperare questi documenti. Un backup ha senso solo se esso viene aggiornato a scadenze regolari, normalmente ogni volta che si aggiungono o modificano documenti importanti e che non si vuole perdere.
- **Social network**: una delle mode più diffuse sono i social network (*Facebook, Badoo, Twitter, ecc*). L'approccio corretto è pensare che tutto quanto viene pubblicato in Internet, ad esempio sui social network, potrebbe diventare, per sempre, di pubblico dominio. Se non si vuole che delle informazioni, fotografie, opinioni, filmati, ecc diventino, oggi o in futuro (vicino o lontano), di pubblico dominio, l'unica soluzione è non pubblicarli su Internet.

E se nonostante tutto il proprio computer venisse infettato? La maggior parte dei programmi Antivirus, oltre ad individuare i virus conosciuti, è in grado anche di rimuoverli automaticamente, seguendo le istruzioni fornite dal programma stesso. Si tratta della soluzione più semplice in caso di infezione. Se la rimozione non riesce, l'ultima ratio, a condizione di avere i dischi di installazione, è partire da zero, installando nuovamente il computer e recuperando i propri documenti a partire dall'ultimo backup. Tra questi due estremi c'è la rimozione manuale del virus (per utenti esperti). Il consiglio è cercare su Internet, nei vari forum di discussione, istruzioni su come procedere in base al nome del virus rilevato. Per alcuni virus particolarmente dannosi, le case produttrici di antivirus hanno sviluppato dei programmi ad hoc per la rimozione. Essi sono facilmente reperibili su Internet.