

## Professioni

Qualsiasi computer collegato a internet è un **ricettacolo** di pericoli e **minacce**, sia per voi sia per la vostra azienda. Per fortuna, esistono **trucchi** e **professionisti** pronti a difendervi | **Riccardo Meggiato**

# A chi serve il **security** manager

**U**SATE IL COMPUTER, FISSO O PORTATILE CHE SIA, solo per gestire la posta elettronica e navigare sul web? Non per questo siete immuni dalle tipiche minacce informatiche, dette malware. Tutt'altro: GData, una delle aziende leader nel settore della sicurezza, stima che nella prima metà del 2010 siano stati scoperti ben 1.017.208 nuovi virus, pari al 50% in più rispetto allo scorso anno, e buona parte di questi sia in grado di arrecare danni mentre si scarica la posta o si naviga in internet. Se poi si fa anche altro (chat, qualche partita a poker on-line...), i rischi aumentano. I principali sono due e prendono il nome di trojan e phishing. Il primo è un programma in grado d'installarsi di nascosto nel computer per metterlo in contatto con un criminale informatico, il quale potrà disporre a suo piacimento. Il phishing, invece, è una tecnica con la quale un truffatore vi convince a visitare un sito che è identico



a uno che utilizzate spesso (per esempio, quello della banca) per sottrarre informazioni personali.

### **Kenzero, il trojan che ricatta**


A queste due minacce se ne aggiungono molte altre, ma il concetto è sempre lo stesso: i malviventi informatici puntano ai vostri dati. Codici bancari e carte di credito sono gli obiettivi principali, ma anche le password di accesso alla posta elettronica o al sistema informatico aziendale sono un bersaglio importante. Per non parlare delle informazioni strettamente riservate: immaginate che cosa accadrebbe se un piano con le strategie finanziarie da presentare in consiglio d'amministrazione cadesse nelle mani sbagliate. Esiste addirittura un trojan, chiamato Kenzero, che s'insinua tra video e immagini a luci rosse. Una volta che si attiva, registra tutti i movimenti sul web, in particolare nei siti erotici, e ricatta minacciando di sbandierare le abitudini più riservate... Insomma, che si tratti di rischi personali, professionali o economici, la criminalità informatica è più pericolosa e diffusa di quanto si possa immaginare: Symantec, altro colosso della sicurezza e produttore di programmi antivirus, stima che quest'anno circa il 65% degli utenti sia stato colpito da reati informatici. E che nel 2009 il 75% delle aziende esaminate sia stato bersaglio di qualche tipo di attacco, con un trend in crescita per il 2010. Per fortuna le difese esistono e, anche se la protezione totale non la può garantire nessuno (chi lo fa non è serio), ci sono parecchi modi per limitare rischi e danni.

Innanzitutto, occorre scegliere con attenzione i programmi di sicurezza. Evitare quelli gratuiti, che non beneficiano di un aggiornamento e un'assistenza paragonabile a quelli commerciali. Tra questi ultimi, i migliori sono quelli di Symantec ([www.symantec.it](http://www.symantec.it)), GData ([www.gdata.it](http://www.gdata.it)), Kaspersky ([www.kaspersky.it](http://www.kaspersky.it)) e McAfee ([www.mcafee.com](http://www.mcafee.com)): dispongono di prodotti dedicati sia ai privati sia alle aziende, e sono molto disponibili nel consigliare i più adatti secondo le diverse esigenze. Se l'azienda è dotata di una rete informatica complessa, è il caso di utilizzare un firewall hardware: si tratta di un apparecchio che funge da barriera contro gli attacchi informatici provenienti dal web. È una soluzione molto efficace ma complessa da installare e gestire, quindi, prima di adottarla, è bene rivolgersi a un professionista. Tra i marchi migliori ci sono Cisco ([www.cisco.com](http://www.cisco.com)) e Cyberoam ([www.cyberoam.com](http://www.cyberoam.com)).

### **A caccia dell'uomo giusto**

Se reputate che i vostri dati corrano grossi rischi, siete già stati vittime di crimini informatici e non volete ripetere questa brutta esperienza, è il momento di rivolgersi agli specialisti di sicurezza. Si tratta di professionisti pronti a studiare la situazione, valutarla e trovare soluzioni per prevenire o contrastare i malviventi. Un operatore serio si riconosce subito: non fa promesse, non propone soluzioni sommarie e, come prima cosa, compila una sorta

di anamnesi delle abitudini informatiche vostre e dell'azienda. Solo allora, stila un rapporto sui punti deboli e una serie di possibili rimedi.

La figura da cercare è quella del security manager in campo informatico (o security manager, o IT security manager) e, vista la delicatezza dei contenuti coi quali avrà a che fare, per la sua scelta è meglio rivolgersi a un'azienda di recruiting specializzata. Detto altrimenti: evitare di ingaggiare un professionista di questo tipo sulla base di annunci trovati su Google. Un ottimo punto di partenza è il sito [www.securitymanagement.com](http://www.securitymanagement.com), che nella sezione Marketplace elenca le principali aziende di consulenza informatica del mondo. La prospettiva di rivolgersi all'estero, eventualmente, per garantire la protezione del sistema informatico, piccolo o grande che sia, non deve spaventare. Il costo medio per l'azienda di un attacco informatico è di 2 milioni di dollari: dedicare un certo budget alla prevenzione della criminalità digitale porta in realtà a un notevole risparmio. E alla sicurezza che, al prossimo consiglio d'amministrazione, i vostri documenti saranno esaminati davvero per la prima volta. 

### **Manuale di auto-difesa**

Per prima cosa stabilite una policy informatica per voi, la vostra azienda ed eventuali collaboratori. Si tratta di una serie di regole di buona condotta di fronte ai dispositivi informatici. In genere, è meglio affidarsi ad apposite società di consulenze informatiche, ma le norme di base in realtà sono poche e semplici:

- Accettate e rispondete solo a e-mail di persone conosciute.
- Visitate solo i siti strettamente correlati al vostro lavoro.
- Installate e aggiornate sempre i programmi di sicurezza (antivirus e firewall), e non disattivateli mai, nemmeno quando vi viene chiesto di farlo dal computer stesso.
- Non scaricate software oltre a quelli in dotazione se prima non ne avete verificato la provenienza.
- Evitate di utilizzare il computer aziendale per attività personali (Facebook incluso).

