Giovanni Ziccardi

Il giornalista hacker

Piccola guida per un uso sicuro e consapevole della tecnologia



Marsilio

Giovanni Ziccardi (Castelfranco Emilia, 1969) è Professore di Informatica Giuridica presso la Facoltà di Giurisprudenza dell'Università degli Studi di Milano, dove ha fondato e dirige il Corso di Perfezionamento in computer forensics e investigazioni digitali. Giornalista pubblicista e avvocato, è Dottore di Ricerca in Informatica Giuridica e Diritto dell'Informatica presso l'Università degli Studi di Bologna. Tra il 1997 e il 2003 ha svolto la professione di avvocato, occupandosi di diritto dell'informatica e delle nuove tecnologie: ora è iscritto all'Albo Speciale dei professori universitari a tempo pieno presso il Consiglio dell'Ordine degli Avvocati di Modena.
Ha fondato e dirige, dal 2000, la Rivista Scientifica «Ciberspazio e Diritto», Mucchi Editore, Modena. Scrive soprattutto di diritti di libertà e nuove tecnologie, di attivismo, di crimini informatici, di hacking, di open source e di investigazioni digitali. Ha pubblicato con i più autorevoli editori mondiali oltre dieci monografie e sessanta articoli scientifici in lingua italiana, inglese e giapponese.
È autore, con Marsilio Editori, del saggio *Hacker. Il richiamo della libertà* (2011) e del thriller *L'ultimo hacker* (2012).

giovanni.ziccardi@unimi.it
http://www.ziccardi.org



Giovanni Ziccardi

Il giornalista hacker

Piccola guida per un uso sicuro e consapevole della tecnologia

Marsilio

Il giornalista hacker è distribuito gratuitamente in collaborazione con il Festival Internazionale del Giornalismo, Perugia 25-29 aprile 2012.

Hanno contribuito: **Claudio Agosti**, **Cristiano Cafferata**, **Arturo Filastò**, **Antonio Mauro, Pierluigi Perri** e tutti i ragazzi (e ragazze) dell'***Hacker's Corner***.

© 2012 by Marsilio editori® s.p.a. in Venezia

www.marsilioeditori.it
www.facebook.com/marsilioeditori
www.twitter.com/marsilioeditori

La strada verso la conoscenza...

Che interesse può avere un professionista – sia esso un giornalista, ma anche un avvocato, uno scrittore, un politico, un blogger o un attivista – nell'imparare a utilizzare, seppure nelle loro funzioni di base, programmi che sono solitamente adoperati da **hacker** o, comunque, da utenti più attenti del normale, a volte sino a sfiorare livelli di paranoia, alla **sicurezza** in possibili contesti critici o "ostili"?
Di certo, il senso delle regole elementari che seguono non è quello di voler far diventare chiunque"hacker in un'ora". Il percorso verso l'hacking è lungo, tormentato, fatto di tante prove e curiosità, di tentativi, di errori, di notti insonni passate a digitare codice e di un approccio per così dire naïf agli strumenti elettronici che ci circondano che, anche a causa di una tecnologia sempre più *touch* e semplice da utilizzare (e che spinge poco l'utente a ragionare), è ormai fuori moda.
Però è pur vero che **tutti**, anche coloro che pensano di essere negati per il computer o che sono convinti

di non aver tempo da dedicare a nuove esperienze, possono essere **un po' hacker nella vita quotidiana**, ossia possono cercare di superare quel velo di normalità cui le tecnologie di oggi ci abituano – inteso come utilizzo tipico – e spingersi, anche solo per **curiosità**, verso strumenti che possano portare **benefici immediati** anche nella vita informatica di tutti i giorni e, soprattutto, nelle professioni più delicate.

I **dieci** approcci che illustrerò in questo percorso, scelti appositamente sia per garantire **un'utilità immediata** sia per accrescere la **curiosità** e la conoscenza, non sono gli unici – e forse non sono neppure i migliori – per raggiungere un determinato fine. Ma sono **interessanti** e, soprattutto, sono già utilizzati da decine di migliaia di persone nel mondo per i fini più vari.

Ho strutturato questo "percorso verso la conoscenza" in **livelli**, come se fosse un videogioco, anche se ogni strumento vanta una sua indipendenza e può essere analizzato *ex se*.

Soprattutto, non ho scritto, né detto, **tutto** ciò che c'è da sapere su questi strumenti, ma mi sono limitato a "suggerire" delle strade per poi lasciare l'approfondimento dei temi a chi è realmente **interessato** e **curioso**. E un po' hacker dentro.

Milano, aprile 2012

Primo Livello
CRITTOGRAFIA
Imparare a **cifrare** i dati

La società odierna è una società che vive e si nutre di **dati in chiaro**. Che cosa significa? Che smarrire il telefono, essere derubati del computer o dimenticare una chiave USB in un luogo pubblico comporta quasi sempre la possibilità, in capo a chi entra in possesso del nostro strumento, di **conoscere tutto di noi**. Tutto. Ogni nostro dato. Di vedere ogni foto e video. Di leggere ogni mail. Di analizzare ogni documento.
Non vi è, allora, da stupirsi se la crittografia, l'arte di **nascondere** le informazioni in chiaro antica come l'uomo, si sia sviluppata in ambito militare, ambiente dove il **segreto** è tenuto in gran conto, e sia utilizzata, nell'era tecnologica, non solo da paranoici e terroristi ma anche da **dissidenti** o soggetti che semplicemente non vogliono che le loro informazioni siano **comprensibili** in caso di intercettazione e sorveglianza da parte di terzi. La crittografia, poi, è particolarmente temuta dagli **investigatori**, perché un disco o un supporto cifrato creano non pochi problemi in fase di analisi, e

perché di solito la crittografia è molto efficace, ossia **offusca veramente i dati**.
Il primo passo, allora, è quello di procurarsi un **software per cifrare i dati**. **TrueCrypt** può essere un buon inizio, così come strumenti derivati dallo storico **PGP**. Installato il software, si può iniziare a fare delle prove per cifrare dei dati. Consiglio di utilizzare, all'inizio, una **chiave USB** o un supporto esterno non contenente dati importanti. I passi dell'utente saranno i seguenti:
1. installare il **software** di crittografia sulla macchina ed eventualmente installare anche la **versione portable** su una chiavetta;
2. individuare il supporto da cifrare: una chiavetta USB, una cartella, un file, una partizione, un intero disco, TrueCrypt lascia solo l'imbarazzo della scelta;
3. provare a "montare" e "smontare" un supporto cifrato per permettere al nostro computer (e a noi) di vederlo e di spostare file all'interno di esso;
4. estrarre la chiavetta improvvisamente, come se fosse in corso un accadimento pericoloso, per osservare la **reazione della nostra macchina e del sistema di cifratura**, tenendo sempre però presente che una simile operazione potrebbe causare una perdita di dati;
5. verificare la reazione e i messaggi di errore di un computer quando si collega alla presa USB un sup-

porto (disco esterno o chiavetta) cifrato (ed evitare di dare il comando "inizializza");
6. Abituarsi a gestire in maniera corretta la **passphrase**, ossia la password che permette la cifratura e la decifratura dei dati.

Link

TrueCrypt (http://www.truecrypt.org/).
GnuPG (http://www.gnupg.org/).
The International PGP Home (http://www.pgpi.org/).

Da non fare

Non fare le prime prove cifrando il disco fisso o cartelle utili, ma **utilizzare supporti non importanti** (per evitare di non riuscire più a recuperare i dati). La crittografia è uno strumento **forte**, un utilizzo sbagliato può comportare danni.

Approfondimento

Per gli utenti Mac OS, analizzare il funzionamento di **FileVault** all'interno delle **opzioni di sicurezza**: è un sistema per cifrare la cartella home dell'utente o dell'intero disco, a seconda del sistema operativo, e consente di proteggere i dati. Per gli utenti Windows, analizzare **BitLocker**. Per gli utenti GNU/Linux, studiare il funzionamento di **encryptfs**.

E le connessioni cifrate?

Vero, può essere molto utile verificare sempre che la connessione Internet del nostro **browser** avvenga

in maniera cifrata (**https**) soprattutto verso siti critici o che trattano nostre informazioni. Le connessioni cifrate aumentano i margini di sicurezza.

Secondo Livello
ANONIMATO
Navigare anonimi con **Tor** e aggirare filtri e blocchi

Tor, nato come progetto della marina militare americana e ora diffuso in tutto il mondo, è un software sviluppato dai ragazzi del **Tor Project** che si propone di garantire un buon livello di **anonimato** durante la navigazione in rete. Senza entrare troppo nel tecnico, il funzionamento è tanto banale quanto sofisticato: i pacchetti di dati che partono dal computer dell'utente **non arrivano direttamente a destinazione** (ad esempio: verso un sito web che si vuole consultare) ma transitano **attraverso almeno tre computer** che li reindirizzano, **cifrati**, sino al collegamento finale. Detto così può sembrare complicato, ma anche l'utente meno esperto è in grado di usare questo sistema perché è totalmente **trasparente** per l'utente (tranne, a volte, nel causare un leggero **rallentamento** nella navigazione). Ci si collega al sito di Tor, si scarica il software o un **bundle** che comprende anche un browser già configurato, si accede alla rete Internet passando per la rete Tor e il gioco è fatto.

Ovviamente, accanto alla tecnica, occorre **accortezza umana**: i nodi di uscita di Tor (ossia il collegamento al sito finale) sono in chiaro, quindi occorre evitare di inserire informazioni personali che possano essere **intercettate** in quella fase. Meglio: Tor provvede all'**anonimato** ma **non alla riservatezza della trasmissione**, tanto che deve essere l'utente a provvedere, se interessato (ad esempio: usando https, o mail cifrate, o sistemi di chat cifrata). Inoltre Tor può permettere altri "giochini" divertenti come, ad esempio, cambiare l'IP della macchina scegliendo lo "Stato di uscita" (ad esempio: per aggirare filtri o blocchi, o per acquistare un bene che non si può acquistare dal Paese d'origine dal momento che viene riconosciuto l'IP) o cambiare costantemente l'IP. Tor è utilizzato spesso anche dai **dissidenti** per evitare di essere individuati o per **aggirare filtri e blocchi** alla navigazione del Paese in cui si trovano.

Come fare?

Semplice. Ci si collega al sito del Tor Project (https://www.torproject.org/) e si scarica e si installa Tor. Esiste per **qualsiasi** sistema operativo: Windows, Mac, Linux/Unix e Android.

Ora sono anonimo?

C'è la possibilità di fare un **check** per verificare se stiamo **realmente** navigando anonimi sulla rete Tor (https://check.torproject.org/).

Posso contribuire al progetto?
Certo, a diversi livelli, anche mettendo a disposizione un po' della **potenza del tuo computer** per rendere più potente la rete Tor. Sul sito sono indicate le modalità migliori per aiutare il progetto a vivere.
Cosa rischio?
Lentezza nella connessione, **convinzione** di essere anonimi indipendentemente dal nostro comportamento che, però, porta a commettere **errori umani** (rilascio di informazioni che ci rendono comunque **tracciabili**).

Terzo Livello
CANCELLARE
Cancellare file in maniera sicura con **Eraser** e **recuperare** file cancellati

Può sembrare un'affermazione banale, ma **cancellare** file, cartelle, documenti e informazioni da un computer è diventato sempre più **complesso**. Tutti sanno, o dovrebbero sapere, che gli "spostamenti dei file nei cestini" con successivo svuotamento, o le formattazioni rapide, **non servono a nulla**. Un soggetto mediamente abile, usando software *ad hoc*, può, senza difficoltà, **recuperare** i file e le informazioni che si reputano cancellate, anche da supporti esterni (memory flash di macchine digitali o telefoni, chiavette, etc). Non deve stupire, allora, che in contesti politici critici i dissidenti dedichino grande attenzione alla **distruzione**, anche fisica e non solo logica, dei **dati** e dei **supporti**.
Il primo concetto da tenere a mente è che una cancellazione **sicura** di un dato (meglio: una sovrascrittura) richiede una discreta quantità di **tempo**. Grandi moli di dati possono richiedere **ore** o **giorni** prima che sia

completato un processo di cancellazione corretto.
Fortunatamente esistono software **pensati proprio per questo**: aiutano l'utente nel cancellare **veramente** i file o nel **ripulire** il proprio computer da dati importanti, anche se il tempo necessario (tanto) rimane lo stesso.
Al contempo, esistono dei software, denominati di **recovery** o di **data carving**, che eseguono il processo contrario: ricercano file cancellati male o blocchi di dati apparentemente informi e cercano di recuperare informazioni in maniera la più integra possibile.

Perché cancellare seriamente i dati?

Per evitare che qualcuno li recuperi, soprattutto se, ad esempio, metto in vendita il mio cellulare o il mio computer su eBay, o se devo sostituire il disco in assistenza, o se ho timore che siano sequestrati i miei dispositivi.

È facile?

Sì. Ad esempio: il software **Eraser** (http://eraser.heidi.ie/) è di semplice utilizzo e, in ambiente Windows, permette di effettuare operazioni interessanti.

È pericoloso?

Sì, tanto. È meglio **fare prove**, prima, con file o supporti che non utilizziamo, perché si possono fare danni notevoli. Di solito, comunque, il software richiede **conferme esplicite** di cancellazione del file

o del supporto scelto, e ciò dovrebbe aumentare la consapevolezza di quello che si sta per fare.

Posso provare anche a recuperare dati?

Certo, può essere interessante provare a recuperare dati dai nostri supporti, chiavette, memorie flash o dischi, anche datati, utilizzando software di **recovery** e di **data carving**. Queste azioni riserveranno molte sorprese.

È diffusa l'abitudine della distruzione del dato digitale?

No, per nulla. Gran parte delle investigazioni trovano, sui computer oggetto d'attenzione, **dati in chiaro**. È sufficiente provare ad acquistare su eBay computer o dischi e verificare se chi ha messo in vendita il supporto ha provveduto, prima, a una reale cancellazione del dato. Anche in questo caso, le soprese sarebbero molte.

Quarto Livello
KIT
Usare **applicazioni portable** e crearsi il proprio kit

Esistono applicazioni, denominate **portable**, che sono molto interessanti nel loro utilizzo. Sono applicazioni (ad esempio: per **scrivere**, gestire la **posta elettronica**, **cifrare** i dati, **chattare**, **navigare**, **cancellare** informazioni) che sono, appunto, *portable*, ossia non hanno bisogno di essere installate in un sistema operativo ma possono "vivere" tranquillamente su una chiave USB abbastanza capiente o su un disco esterno.
I vantaggi sono numerosi: lasciano **tracce minime** sul sistema operativo che le ospita (in particolare non lasciano tracce di configurazioni o preferenze del proprietario), permettono di **creare un kit** che il soggetto si può portare sempre con sé indipendentemente dal computer che si troverà davanti (anche se dipenderà da quel sistema operativo) e potranno essere utilizzate quando non ci si fida del computer di fronte a noi (anche se, come è noto, se non ci si fida completamente del computer di fronte a noi è meglio **evitare** un suo utilizzo a meno che proprio non sia indispen-

sabile, oppure fare un **boot** con una **distribuzione live**, come si vedrà in seguito).
Una applicazione portable interessante è quella che ricrea, a fini di accessibilità, una **tastiera su schermo**, al fine di non utilizzare neppure la tastiera del computer ospite ma solo il mouse (in tal modo, se il computer ha installato **keyloggers** di vecchia generazione, il software "spione" non riesce a registrare e inviare all'esterno la lista dei tasti premuti e dei caratteri immessi).

È semplice?

Sì, basta collegarsi a un sito che contenga **una lista delle portable apps** (esistono anche dei kit o **bundle** completi) e installare le apps che interessano su una chiave USB o un disco esterno. Poi basta **cliccare** sulla app per farla partire dal supporto su cui sono state installate.

Davvero non lasciano tracce sul sistema operativo ospite?

No, non è del tutto vero. Il sistema operativo, nei suoi **file di registro**, può tenere traccia del fatto che sia stata **inserita** una chiavetta e lanciata una certa app, ma il grande vantaggio è comunque che, se ben configurate, queste app non lasciano tracce circa **l'attività svolta** (i siti visitati, le mail scaricate, i documenti scritti).

Posso combinare le portable apps con la cifratura

della chiavetta (per evitare che la perdita della chiavetta renda pubblici i miei dati)?
Certo, è una buona idea. Si possono creare **due partizioni**, una in chiaro con all'interno un programma di cifratura portable, e una seconda cifrata che viene "aperta" da una password e che contiene le applicazioni e i dati.

Quinto Livello
LIVE
Usare una distribuzione **live** (anche) per l'anonimato (ad esempio: TAILS)

Esistono alcune distribuzioni LIVE (insieme di ambiente operativo e applicazioni) che sono pensate anche per fornire **un ambiente il più sicuro e anonimo possibile** per l'utilizzatore: le potremmo definire come particolarmente orientate all'anonimato. L'uso è semplicissimo: la distribuzione può risiedere su una chiavetta, un CD o un DVD e il computer dell'utente (o di un terzo, anche non fidato) viene avviato (**boot**) da questo supporto senza far avviare il sistema operativo e i programmi del computer ospitante. Di solito queste distribuzioni, una volta avviate,"cercano" una connessione di rete e, nel momento in cui si connettono, lanciano programmi, ad esempio **Tor**, che già garantiscono sin dall'inizio se usati correttamente, un buon grado di anonimato.
L'uso di tali distribuzioni è molto semplice: è sufficiente scaricare da Internet l'immagine di un disco, spostarlo (masterizzarlo) su un CD o una chiavetta e

avviare il computer da quel supporto (eventualmente cambiando, nel BIOS, l'ordine di boot o tenendo premuti alcuni tasti in fase di accensione e avvio). Occorre sempre ricordare che tali sistemi danno un **primo livello di anonimato**, e che tutto ciò che poi l'utente compie una volta collegato deve essere anch'esso anonimo.

Dove trovo TAILS?

Sul sito degli sviluppatori (https://tails.boum.org/).

È semplice crearsi un disco LIVE?

Sì, basta collegarsi al sito di una distribuzione live, masterizzare la distribuzione su CD o DVD e avviare il computer da quel CD.

Posso fare di tutto con le distribuzioni LIVE?

Dipende. Alcune distribuzioni sono **molto specifiche** per utilizzi *ad hoc* (ad esempio: investigazioni) mentre altre sono più **generiche** (ad esempio: Ubuntu). Di solito riconoscono il collegamento a Internet (anche wireless) ma **non possono salvare dati e configurazioni** a meno che non sia espressamente detto loro di salvare sul disco fisso (ma, in tal caso, ovviamente, si lasciano tracce sul computer che ci ospita).

Perché imparare a usare TAILS?

Crea un ambiente anonimo, è una distribuzione leggera, non è complicata da utilizzare anche in un'ottica iniziale di comprensione del concetto di sicurezza.

Sesto livello
VIRTUALE
Usare una **macchina virtuale**

L'idea di **macchina virtuale** è tecnicamente complessa ma di una **semplicità** disarmante nel suo utilizzo. Si tratta, in un certo senso, di avere uno o più computer dentro al nostro computer, di poter usufruire di un ambiente "asettico" che può contenere **uno o più sistemi operativi** che possiamo tranquillamente utilizzare senza influenzare (e danneggiare) il sistema principale. A cosa può servire? A tante cose. A operare da un sistema operativo (ad esempio: Windows 7) per poi farlo **sparire** (basta cancellare la macchina virtuale facendo attenzione ai dati rimasti in RAM, riavviare la macchina e magari "ripulire" il disco), a fare **esperimenti** che non condizionino l'ambiente principale (testing di programmi, anche di virus!), ad avere su un computer **più sistemi operativi**, a creare **ambienti anonimi**.

Il suo fine?

Quello di creare un ambiente **dentro** il sistema operativo che non influenzi l'ambiente principale e non causi malfunzionamenti.

Perché può essere interessante far girare sistemi operativi diversi?
Per aumentare la propria conoscenza e curiosità, per usare i sistemi operativi su cui ci siamo formati o che non sono più commercializzati, per vedere **diversi ambienti** e non solo Windows.
Da dove cominciare?
Da *VirtualBox* (https://www.virtualbox.org/), un software molto interessante che funziona con tanti sistemi operativi diversi. Per gli utenti Mac è anche interessante *Parallels Desktop* (http://www.parallels.com/it/), e anche VMWare è un prodotto molto noto (http://www.vmware.com/it/).
Cosa provare?
Una distribuzione GNU/Linux sotto Windows, o Windows dentro Mac, o un vecchio applicativo o videogioco che non gira più nei sistemi moderni ma può girare dentro una macchina virtuale con un vecchio sistema operativo.
Che livello di sicurezza hanno in caso di trojan sul computer o sistemi di intercettazione?
Purtroppo **molto basso**. Se un trojan è presente, e intercetta ogni informazione, acquisisce anche quelle da macchine virtuali. Possono essere molto utili se oggetto di attacco fossero **le stesse macchine virtuali**, consentendo di non "contaminare" il sistema principale.

Settimo Livello
HUMANWARE
Una gestione "umana" intelligente dei propri dati e account

È troppo facile pensare che una sicurezza assoluta la possa dare solo la tecnologia. Tre sono i componenti fondamentali per garantire un ambiente sicuro: **hardware** senza difetti, **software** senza difetti e **essere umano** senza difetti. Tutti e tre hanno la stessa importanza, e molte volte tanti errori che portano a svelare dati, o a compromettere la nostra sicurezza, non sono altro che **colpa nostra**. Solo colpa nostra.
Ecco allora che meditare sui nostri **comportamenti** "tecnologici" è altrettanto importante che parlare di strumenti per l'anonimato o la cifratura dei dati.
Il sistema più forte al mondo di cifratura crolla se la passphrase viene **annotata**, viene inserita in un **contesto non sicuro**, è identica a **tutte** le nostre altre password o se viene fatto un backup dei dati **in chiaro**.
L'anonimato crolla se tanti singoli dati apparentemente anonimi che rilasciamo, se **correlati** permettono di individuarci e di arrivare a noi.
Il **non sapere** se le foto che rendiamo pubbliche, o

inviamo per mail contengono metadati che indicano la nostra posizione geografica, o il dispositivo (modello della macchina fotografica) che ha scattato quelle foto, o vengono processate e correlate a un nostro profilo (ad esempio: su Facebook), comporta vulnerabilità altrettanto importanti.

Come fare?

Conoscenza, conoscenza e conoscenza. Leggere i manuali dei dispositivi che utilizziamo, leggere i forum di discussione sulle caratteristiche nascoste di siti, database e dispositivi che possono profilare l'utente o tracciare una persona.

Mi devo fidare?

Mai. Un livello di paranoia e di diffidenza molto alto è sempre sano.

Ottavo Livello
DISTRUGGERE
Cancellare o **distruggere** un intero hard disk o un altro supporto

Può venire la necessità, spesso l'urgenza, di **cancellare** completamente i dati di un intero hard disk affinché non siano più recuperabili o affinché il recupero, se comunque potesse avvenire, richieda sforzi di calcolo e di tempo molto ampi.
La **distruzione** dei **dati**, la **distruzione fisica** del disco e la sua **smagnetizzazione** sono tre metodi molto usati ed efficaci per eliminare tracce su un supporto.
La prima va effettuata con software che sono pensati appositamente per riscrivere le tracce di un hard disk più volte al fine di cancellare i dati.
Il secondo metodo è più **fisico**, e consiste nella distruzione (martellate, incendio) del disco con la consapevolezza, però, che esistono ditte specializzate anche nel recupero di supporti danneggiati e che intervengono soprattutto in caso di incendio o allagamento all'interno di aziende.
Il terzo metodo consiste nell'utilizzare sofisticati apparecchi, denominati **degausser**, che emettono campi magnetici per cancellare i dati in quel modo.

Perché dovrei distruggere il mio hard disk o attivare una lunga operazione di cancellazione delle informazioni?
Per non lasciare tracce se il supporto conteneva dati importanti, per impedire che qualcuno recuperi i dati, semplicemente per installare nuovamente un sistema operativo e un ambiente di lavoro facendo sparire i dati che c'erano sotto.
Mi posso far male a distruggere fisicamente supporti?
Sì. Particolare attenzione va fatta alla rottura di un CD o DVD a mano (pericolo di tagli), al collocamento di un hard disk in un forno a microonde o all'utilizzo di cacciavite, martelli o liquidi infiammabili.
Posso "pulire" un supporto usando un software?
Certo. Sono numerosi i programmi che permettono di "bonfiicare" un intero supporto. Active KillDisk è uno di questi (http://www.killdisk.com/). Oppure si può usare DBAN (http://www.dban.org/) che permette di eliminare in modo definitivo (utlizzando anche tecniche militari) tutti i dati presenti nei supporti Hard Disk, Pendrive USB, etc. È sufficiente scaricare il programma e spostarlo (masterizzarlo) su un CD o una chiavetta e avviare il computer da quel supporto (eventualmente cambiando, nel BIOS, l'ordine di boot o tenendo premuti alcuni tasti in fase di accensione e avvio), riavviare il computer e il gioco è fatto!

Nono livello
IDENTITÀ
Creare un'identità in rete o un blog che abbia
un buon livello di anonimato

Giocare con le identità, in Internet, è una delle cose più **complesse**.
Facilissimo è creare un'identità di fantasia; molto difficile è far sì che tale identità **resista a controlli**, anche semplici, effettuati per svelare la reale natura del soggetto. Se si vuole creare una identità, una mail, un profilo su Facebook, un blog che voglia essere **realmente anonimo** e, quindi, capace di resistere a controlli anche accurati, occorre seguire un insieme di regole, spesso di **buon senso**, condite da alcuni espedienti tecnologici.
Innanzitutto, il primo passo, ossia da dove si crea l'identità, è il **passo più delicato**. Creare un account di mail o un blog anonimo **usando il proprio indirizzo IP** è il primo **errore** tipico. Un'analisi a ritroso, in cooperazione con il provider, può portare alla identificazione immediata. Ciò comporta che la prima azione in assoluto subito dopo aver pensato alla strategia, ossia il **collegarsi in rete** per creare qualcosa,

deve essere compiuta **da un contesto non riferibile** al soggetto o con un IP non riferibile.
Il **mantenimento dell'anonimato** è la seconda cosa difficile: mai indicare riferimenti personali, anche incrociabili, mai caricare foto che contengano informazioni sulla macchina fotografica o il telefono che le ha scattate o, peggio, le coordinate GPS, mai parlare di luoghi, eventi, orari che possano portare a una riconoscibilità.
Tor, già citato, permette alcune funzioni, denominate **hidden services**, che sono molto interessanti e che meritano un approfondimento: sono molto utilizzare per creare blog anonimi o sistemi di leaking e di gestione di fonti confidenziali.
Un progetto interessante?
Globaleaks (http://globaleaks.org/). Un ambiente per il **whistleblowing** molto interessante che cerca appunto di sfruttare la tecnologia per garantire l'anonimato di chi diffonde informazioni.

Decimo Livello
FIREWALL
Tenere sempre nello zainetto un (piccolo)
***firewall** hardware*

Il **firewall** è uno strumento molto utilizzato a livello **aziendale** ma, sovente, poco noto da un punto di vista *personal*, ossia da parte dell'**utente comune**.
Eppure, un uso accorto di questo dispositivo, che può diventare in pochi giorni **un'abitudine** semplice da comprendere, può aumentare notevolmente il **livello di sicurezza** del professionista, soprattutto quando è obbligato a utilizzare connessioni a Internet in **contesti non sicuri** quali, ad esempio, Internet Café, postazioni in hotel o villaggi turistici, linee UMTS e HSDPA, biblioteche o altri luoghi pubblici.
Il principio fondamentale alla base della necessità di un firewall, che molti professionisti della sicurezza già applicano, è quello di **non collegarsi mai direttamente** a un *access point*, a un cavo di rete e, in generale, a una connessione a Internet offerta da terze parti **e non fidata** senza prima porre **nel mezzo**, tra il computer e il collegamento, una **scatoletta** o un **software** (firewall) che, oltre a funzionare come un **filtro**, si com-

porti in base a regole ben precise che il possessore del computer ha elaborato e che operano sui **pacchetti di dati**, sulle modalità di connessione, sui siti ammessi in visione e contro il possibile **malware** intenzionato ad attaccarci. Ciò comporta un **controllo del traffico** e delle applicazioni in tempo reale, **l'analisi** di tutto il traffico in entrata e in uscita per evitare **virus**, **spam**, **spyware** ed **eventi dannosi**, la possibilità di **accesso sicuro** con SSL e VPN, una grande attenzione alle possibili **intrusioni** e, spesso, anche un **controller wireless sicuro** con una verifica del traffico.
I firewall esistono, si è detto, anche in versione software (di solito sono denominati **personal firewall**) e cominciano anche ad essere sintegrati nei sistemi operativi più moderni. Un **firewall hardware**, di piccole dimensioni (grande come un libro) e dal costo contenuto e da tenere sempre nella borsa, può essere molto utile, ma non ha di certo i vantaggi immediati di un **firewall software** (ad esempio: l'hardware richiede anche un cavo di alimentazione e uno di rete, e può essere più facilmente individuato da un amministratore di sistema o di rete).
La configurazione e la scelta delle regole sono spesso semplici, e la configurazione "di fabbrica" è sovente più che sufficiente per ottenere un buon risultato anche da parte dell'utente comune.

Costo necessario
Circa 300/400 Euro per un buon hardware e servizi annuali d'aiuto nella configurazione.
Tempo di apprendimento
Da poche ore a un mese, a seconda che si utilizzi la configurazione del produttore o si voglia intervenire sulle **regole**.
Vantaggi
Protezione del proprio computer e della propria connessione a Internet quando si è costretti a collegarsi a una **rete non fidata**. Protezione da virus, spam, spyware e malware. Comprensione delle regole per i pacchetti di dati. Possibilità di consentire o meno il funzionamento di certi servizi e applicazioni.
Come si usa (in sintesi)
Si porta il firewall nello zainetto. Si collega alla rete non fidata e si connette il proprio computer al firewall, il quale si preoccupa di fornire una connessione sicura e pulita.
Link di approfondimento (hardware)
Il produttore *SonicWall* (http://www.sonicwall.com/it/).
Il produttore *Cisco* (http://www.cisco.com/web/IT/index.html).
Il produttore *NetGear* (http://www.netgear.it/).
Il produttore *Linksys* (http://home.cisco.com/it-eu/

home?referrer=www.linksysbycisco.com).

Link di approfondimento (software)

ZoneAlarm (http://www.zonealarm.it/).
Comodo (http://personalfirewall.comodo.com/).
Bitdefender (http://www.bitdefender.it/).
Agnitum (http://www.agnitum.com/).
Kaspersky Lab (http://www.kaspersky.com/it/).



Festival Internazionale del Giornalismo
Perugia, 25-29 aprile 2012
www.festivaldelgiornalismo.com
info@festivaldelgiornalismo.com

Il Festival Internazionale del Giornalismo è stato fondato nel 2006 da Arianna Ciccone e Christopher Potter. L'obiettivo? Parlare di giornalismo, informazione, libertà di stampa e democrazia secondo il modello 2.0. Un evento nato dal basso, aperto alle "incursioni" degli utenti, un evento unico dove i protagonisti dell'informazione provenienti da tutto il mondo si incontrano con i cittadini, i lettori, gli studenti, i professionisti, in un flusso continuo di idee, scambi, confronti. I media giocano un ruolo fondamentale nelle nostre vite quotidiane ma spesso vivono di autoreferenzialità. Il festival rompe in qualche modo questo muro grazie al suo format e rende vivo e vitale l'incontro tra chi fa informazione e chi ne usufruisce.

«Un viaggio nell'ideologia e nelle pratiche di chi usa la tecnologia per squarciare veli di omertà e per urlare una verità scomoda» WIRED



Un appassionante e originale romanzo giallo
che esplora i lati oscuri del mondo delle nuove tecnologie

