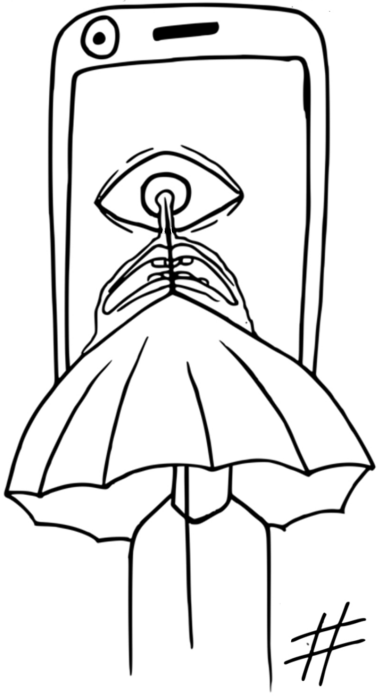
GUIDA ALL'AUTODIFESA DIGITALE



#0

SOMMARIO

PREFAZIONE ALL'EDIZIONE ITALIANA

Scrivere una guida d'autodifesa digitale è un progetto ambizioso. Ci sono un mare di cose da dire, dettagli a cui prestare attenzione, responsabilità a cui non devi sottrarti. A volte corri il rischio di generare troppe paranoie, a volte troppo poche. Hai bisogno di precisione, di un certo grado di intransigenza, eppure anche di molta duttilità e capacità di immedesimazione.

Scrivere una guida d'autodifesa è un progetto ambizioso, perché spesso chi ti legge alla fin fine vorrebbe solo faticare il meno possibile. E non esiste ricetta, non esiste guida, non esiste manuale, per chi ha troppa fretta e poca attenzione.

La Guide d'Autodefénse Numerique può darsi non sia perfetta, ma sicuramente ha un pregio che ce l'ha fatta stare a cuore: insegna un approccio lento e non pigro alla tecnologia. Il che, forse, è il primo vero buon consiglio. E il più importante.

Questa guida è quindi una lunga lettura, che nella sua traduzione italiana abbiamo deciso di pubblicare un po' alla volta, per avere noi il tempo di tradurla e per chi la legge quello di digerirla. E' in un piccolo formato, stampabile a costo zero o quasi, perché si possa moltiplicare e diffondere il più facilmente possibile.

E chi siamo noi? Siamo alcune traduttrici che respirano insieme alla comunità italiana di Hackmeeting, autogestiscono quanto più riescono del proprio giorno, amano le autoproduzioni e la condivisione dei saperi.

Questo primo numero avrà il sapore di un'introduzione, cercherà di spiegare gli intenti e lo spirito con cui è stata scritta questa guida e inizierà a dare una prima infarinata su alcune nozioni di base. Dal prossimo numero ci addentreremo meglio nella materia oscura.
Buono studio!

CHI PARLA?

Purtroppo non abbiamo una risposta semplice da dare a questa domanda, ma ci piacerebbe dire lo stesso qualcosa.

Innanzitutto ci teniamo alla possibilità di pubblicare un libro in modo anonimo, e questo per diverse ragioni.
Una di queste, che abbiamo sviluppato nella prefazione, è la domanda “niente da nascondere?”, a cui noi rispondiamo all’unisono: " sì! ".
L’anonimato insomma è una maniera di proteggersi.
Abbiamo poi scelto di non metterci in mostra individualmente, per spostare l’attenzione dal “chi” e lasciare invece sotto i riflettori il “cosa”.
Inoltre, dopo i primi rilasci di questa guida, il numero delle persone che hanno partecipato, da vicino o da lontano, alla sua redazione, correzione e pubblicazione, ha fatto diventare

ampio, in evoluzione e dai contorni indefiniti il collettivo che fa vivere questo progetto.
Infine, crediamo di aver lasciato abbastanza tracce in queste pagine per permettere a tutte le persone che ci leggono di collocarci, almeno parzialmente, all'interno dell'ambito dell'informatica, tecnica, politica o etica.

Ci sono però due caratteristiche di quest'opera che ci obbligano a far fronte, per certi aspetti, alle domande relative alla sua provenienza. Questo lavoro ha la pretesa di trasmettere dei saperi e delle pratiche tecniche, riservati normalmente a pochi specialisti. D'altra parte, la correttezza delle indicazioni fornite può avere delle conseguenze sulla serenità delle persone che le mettono in pratica. Piccoli errori in cui potremmo essere incappati potrebbero avere gravi ricadute.

E' importante quindi spendere qualche parola su chi ha prestato la propria voce per questa guida. Mettere in chiaro la portata dei nostri saperi e ciò

che sappiamo fare – compresi i nostri limiti – permette di trovare un rapporto di apprendimento più adeguato a questo scritto, ma anche di decidere il livello di fiducia tecnica che si merita.
Quindi, collettivamente possiamo dire che:
delle questioni sollevate da questa guida ci occupiamo, tecnicamente e politicamente, da una decina d'anni;
conosciamo piuttosto bene il funzionamento di alcuni sistemi operativi, in particolare di quelli Debian GNU/Linux;
abbiamo delle buone basi di crittografia, ma siamo molto lontani dal poter pretendere di padroneggiare l'argomento.
E per finire, affermiamo un'ultima volta che le parole dette in questa opera, come tutte le parole di una guida, devono essere prese con delle pinze proporzionali alla posta in gioco.

UNA GUIDA?

Questa Guida è un tentativo di mettere insieme e condividere quello che abbiamo potuto imparare nel corso di anni di pratica, errori, riflessioni e discussioni. Nel contesto in cui viviamo, la sola via praticabile sembra quella di sapere immaginare e mettere in atto delle policy di sicurezza adatte.

Non solo le tecnologie evolvono molto velocemente, ma in queste pagine potremmo aver commesso degli errori o aver scritto delle cose non vere.

Cercheremo quindi di aggiornare queste annotazioni all'indirizzo: https://guide.boum.org/.

L'intento che sta dietro alla Guida è quello di fornire mappe, sestante e bussola a chiunque voglia intraprendere questo cammino. Da leggere, rileggere, praticare in solitaria o in più persone, da far scoprire e condividere. Per affinare l'arte della navigazione nelle acque torbide del mondo digitale.

Per rendere il tutto più digeribile, e data la mole

di materiale prodotto, abbiamo diviso tutto quello che volevamo raccontare in due tomi (Offline / Online). A seconda che ci troviamo con un solo computer o se quest'ultimo è invece connesso a una rete, ci troviamo in contesti differenti, con minacce, bisogni e risposte diverse.

L`ALTRO LATO DELLA MEMORIA DIGITALE

Oggi i computer, Internet e i telefoni cellulari tendono a prendere sempre più spazio nelle nostre vite. Il digitale sembra spesso molto pratico: è rapido, si può parlare con un sacco di gente molto lontana, si può avere tutta la nostra storia espressa in foto, si possono scrivere facilmente dei testi ben formattati...ma tutto questo non comporta solo vantaggi; o perlomeno, questi vantaggi non sono solo a nostra disposizione, ma anche di altre persone che possono non essere necessariamente benevole.

In effetti è molto più facile ascoltare discretamente delle conversazioni attraverso i telefoni cellulari piuttosto che in mezzo a una strada rumorosa, o trovare delle informazioni all'interno di un hard-disk, piuttosto che in uno scaffale strabordante di carte.
Inoltre, un'enorme parte dei nostri dati personali finisce per essere pubblicata da qualche parte, da noi stessi o da altre persone, perché ci incitano a farlo – è un po' il tema di fondo del web 2.0 commerciale – perché sono le stesse tecnologie a lasciare tracce o semplicemente perché non facciamo attenzione.

NIENTE DA NASCONDERE?

"Basta essere paranoici: io non ho niente da nascondere!" si potrebbe rispondere alla considerazione precedente. Ma riguardo a questo ci sono due esempi, che in modo molto semplice, tendono tuttavia a dimostrare il contrario: nessuno vorrebbe vedere i propri codici della

carta di credito o dell'account eBay finire nelle mani di qualcun altro. E a nessuno piacerebbe farsi svaligiare la casa perché il proprio indirizzo è stato a sua insaputa pubblicato su Internet e il fatto che proprio in quel momento non era in casa era stato confermato sui social network.

Aldilà di queste futili questioni di difesa della proprietà privata, la riservatezza dei dati dovrebbe essere un fatto interessante di per sé stesso.

Innanzitutto perché non siamo noi a decidere chi è autorizzato o no a fare cosa con un computer. C'è chi viene arrestato sulla base di tracce lasciate attraverso l'utilizzo di strumenti digitali nel quadro di attività che non piacciono a un governo, non necessariamente il proprio, e non solamente in Cina o in Iran.

In molti, governanti, datori di lavoro, pubblicitari o sbirri (1), hanno interesse a ottenere l'accesso ai nostri dati. Il crescente posto che prende l'informazione all'interno dell'economia e della politica mondiale non può che incoraggiarli.

Sappiamo già da soli che non si fanno problemi a tracciare le intersezioni tra gli individui. Cosa sappiamo delle pratiche, legali e illegali, attuate su chi ci sta vicino?
Come sapere inoltre se chi è autorizzato oggi lo sarà anche domani? I governi cambiano, le leggi e le situazioni anche. E le cose possono andare estremamente veloci, come hanno potuto constatare in molti dal 2015 con l'applicazione dello Stato d'Emergenza in Francia. Se non abbiamo niente da nascondere oggi, per esempio la frequentazione abituale di un sito web militante, come sappiamo che quello stesso sito non si ritroverà legato a un processo repressivo in futuro? Verranno lasciate varie tracce sul computer e potranno essere impiegate come elementi di prova.
Mettere in atto delle pratiche di protezione dei dati anche quando si sente di non averne direttamente bisogno permette di renderle più "normali", più accettabili e meno sospette. Le persone che non hanno altra possibilità di

sopravvivenza se non quella di nascondere le proprie attività digitali ce ne saranno riconoscenti, senza alcun dubbio.

Generalmente, tendiamo a contenere le nostre azioni quando sappiamo che altri possono ascoltarci, guardarci o leggerci.
Canteremmo sotto la doccia se sapessimo che abbiamo delle microspie installate? Ci metteremmo a imparare a ballare se delle telecamere fossero puntate su di noi? Scriveremmo una lettera intima così liberamente se ci fosse una persona dietro le nostre spalle a leggere?
Avere delle cose da nascondere non è soltanto una questione di legalità, ma anche di intimità.
E così, nell'epoca delle società con un controllo sempre più paranoico, sempre più decise a scovare la sovversione e a vedere dietro a ciascun essere umano un potenziale terrorista che va sorvegliato da vicino, nascondersi diventa un interesse politico e di fatto collettivo. Non

fosse altro che per mettere i bastoni tra le ruote di coloro che ci vogliono trasparenti e reperibili in ogni momento.
Tutto ciò può portarci a dire che non abbiamo voglia di essere controllabili da nessun “Grande Fratello”.
Sia che esista già o che ne stiamo profetizzando la venuta, la cosa migliore è senza dubbio quella di impedire che tutti questi meravigliosi strumenti che le tecnologie moderne ci offrono (e offrono anche al Grande Fratello) ci si rivoltino contro.
Insomma, dobbiamo avere anche noi qualcosa da nascondere, se non altro per confondere le tracce!

COMPRENDERE PER POTER SCEGLIERE

Questa Guida vuole essere un tentativo di descrivere in termini comprensibili l’intimità- o piuttosto la sua assenza- nel mondo digitale. Si tratta di un chiarimento su alcuni concetti che ci

sono stati dati, per capire meglio ciò a cui ci esponiamo con l'utilizzo di strumenti che non sono neutri. Ma vuole anche offrire un ventaglio di possibili "soluzioni", mai inoffensive se non ci si rende conto di quello da cui non sono in grado di proteggerci.
Attraverso la lettura di queste pagine, si potrebbe arrivare a pensare che niente è veramente sicuro con un computer; ebbene sì, è vero. Ed è anche falso. Ci sono degli strumenti e degli utilizzi appropriati. E spesso la questione alla fine non è tanto se utilizzare o no queste tecnologie, ma piuttosto quando e come utilizzarle (o non utilizzarle).

PRENDERSI IL TEMPO PER CAPIRE

I software semplici da utilizzare muoiono dalla voglia di sostituirsi al nostro cervello. Se ci consentono un utilizzo facile dell'informatica, ci privano anche delle decisioni sui frammenti di vita che gli affidiamo.

Con l'accelerazione dei computer e delle nostre connessioni a Internet, è arrivato il regno dell'istantaneità. Grazie al cellulare e al Wi-Fi, il gesto di riattaccare il telefono o di collegare un cavo di rete al proprio computer per comunicare è già qualcosa di desueto.

Avere pazienza, prendersi il tempo per imparare o riflettere è diventato superfluo: vogliamo tutto, subito, vogliamo la soluzione. Ma questo implica il confidare nelle molte decisioni prese da esperti distanti ai quali crediamo sulla parola. Questa Guida ha come scopo quello di proporre altre soluzioni, che necessitano di prendersi il tempo per capirle e applicarle.

Adattare le proprie pratiche all'utilizzo che si ha del mondo digitale è quindi necessario nel momento in cui vogliamo, o dobbiamo, avere una certa attenzione al suo impatto. Ma l'impresa non ha molto senso se è solitaria. Vi sproniamo quindi a costruirvi una zattera digitale, saltarne gioiosamente a bordo, senza dimenticare di portarvi dietro questa Guida e qualche razzo di

soccorso per inviarci le vostre osservazioni a guide@boum.org

Note
1) Utilizziamo qui il termine “flics” (sbirri) con l’accezione con cui è definito nell’introduzione di "Face à la police / Face à la justice"
(http://guidejuridique.net/).

ULTIMI AGGIORNAMENTI E REVISIONI

Meno di un anno dopo la pubblicazione dell’ultima edizione online della Guida, ci siamo apprestati a prepararne un’altra, sia per offrire una nuova edizione cartacea sia per seguire l’evoluzione dei software che avevamo raccomandato nelle precedenti, ma anche a causa dei mutamenti nella situazione politica francese.
Qualche mese dopo la più grande fuga di

documenti confidenziali della CIA, la creazione di uno Stato d'Emergenza in Francia ha confermato la tendenza politica verso una vera e propria normalizzazione della sorveglianza. Una tendenza che il rilascio dei documenti segreti della Nsa da parte di Edward Snowden aveva già anticipato. In effetti, l'armamentario di software di sorveglianza o di infiltrazione elettronica extra legale venuto a galla man mano insieme agli scandali è stato fatto rientrare zitto zitto nell'arsenale legislativo. E, quando serve, il fine giustifica i mezzi e viene permesso agli agenti governativi di utilizzare questi strumenti senza scrupoli e senza rischio di scandalizzare l'opinione pubblica.

La magra consolazione che possiamo trarre da questo nuovo contesto è che sappiamo con più chiarezza da cosa dobbiamo proteggerci. Ma questo rilancia anche la palla alla sicurezza informatica, obbligando "gli attaccanti" a ricorrere a tecniche ancora più potenti, come l'utilizzo di falle informatiche ancora sconosciute al pubblico,

contro le quali è difficile trovare rimedio. Vulnerabilità che vengono chiamate Zero Day.
Una vulnerabilità di questo tipo è stata per esempio utilizzata dall'FBI nel 2015 durante l'operazione Pacifier, un'altra simile è quella del caso ransomware Wannacry che ha coinvolto più di trentamila computer di tutto il mondo nella primavera del 2017.

Sul piano legale, in Francia, ci sono state almeno quattro nuove leggi riguardanti la sorveglianza informatica e di Internet: la Legge di rinforzo ai dispositivi relativi alla lotta contro il terrorismo (1), la Legge relativa all'informazione (2), la Legge in materia di misure di sorveglianza delle comunicazioni elettroniche internazionali (3) e infine la Legge di rinforzo alla lotta contro il crimine organizzato, il terrorismo e il loro finanziamento (4). Quest'ultima legge autorizza per esempio gli sbirri a installare da remoto dei captatori, quando si trovano all'interno di un'inchiesta che riguarda una lista di reati

talmente lunga da poterci far rientrare quello che gli conviene. Inoltre lo Stato d'Emergenza (5) ha permesso di ampliare il loro raggio d'azione in modo da concedergli di agire senza l'avvallo di un giudice, in particolare permettendo il sequestro di materiale informatico durante una perquisizione amministrativa, ovvero senza l'autorizzazione di un giudice.
Insomma, la protezione dell'intimità e della libertà d'espressione su Internet sono più che mai d'attualità.

Per ciò che riguarda Internet, un esempio evidente è la criminalizzazione della consultazione "abituale" dei siti web "che fanno apologia di terrorismo" (6), cosa che ha già mandato in prigione due persone: il primo si definiva un "apprendista giornalista" (7) mentre il secondo ha detto di agire per curiosità (8). I due si sono beccati due anni di prigione. Questo reato è stato depenalizzato dal Consiglio costituzionale all'inizio di febbraio 2017, ma reintrodotto soltanto

18 giorni più tardi (9).
Diverse persone sono state condannate per la pubblicazione di articoli, accusati di fare “apologia di terrorismo”. Il rapporto Freedom of the net del 2015 riporta che “a Nantes un sedicenne è stato arrestato per aver condiviso su Facebook una vignetta legata all’attacco di Charlie Hebdo. La caricatura in questione prendeva in giro la copertina di luglio 2013 di Charlie Hebdo, pubblicata dopo il massacro di centinaia di egiziani che manifestavano contro il vecchio presidente islamista Mohamed Morsi, e rappresentava un uomo mussulmano che reggeva il Corano per proteggersi dai proiettili e sopra c’era scritto “questo non ferma i proiettili”. L’artista Dedko ha sostituito il corano con il giornale di Charlie Hebdo e l’uomo mussulmano con uno dei suoi disegnatori. Diverse voci hanno accusato le autorità francesi di usare due pesi e due misure per i casi di libertà di espressione. (10) Gli scenari più allarmisti finalmente sono divenuti pane quotidiano in materia di

sorveglianza elettronica. Malgrado la diffusione di un sentimento d'impotenza, queste differenti rivelazioni sullo stato generale della sorveglianza digitale, rendono ancora più necessario dotarsi di strumenti in grado di farne fronte.

Riguardo ai software, il mese di giugno 2017 ha visto l'uscita della nuova versione di Debian, battezzata "Stretch" e anche la versione 3.0 del sistema live Tails, d'ora in avanti basato su "Stretch". Questo aggiornamento ha portato numerosi cambiamenti tanto a livello grafico, quanto nei software proposti. Abbiamo dunque dovuto rivedere le cose per correggere gli howto su questi nuovi sistemi. Questo ha portato all'aggiunta del programma OnionShare e all'arricchimento del programma OpenPGP con la cifratura e decifratura dei documenti.
Grazie a questa revisione, speriamo che le pagine che seguono vi siano d'aiuto durante la vostra traversata della giungla digitale…almeno, fino al prossimo aggiornamento..

Note

1) République française, 2014, legge n. 2014-1353 del 13/11/2014
2) République française, 2015, legge n. 2015-912 del 24/07/2015
3) République française, 2015, legge n. 2015-1556 del 30/11/2015
4) République française, 2016, legge n. 2016-731 del 03/06/2016
5) République française, 2016, legge n. 2016-987 del 21/07/2016
6) République française, 2016, legge n. 2016-731 del 03/06/2016
7) http://nbl.gs/qgf
8) http://nbl.gs/qgg
9) http://nbl.gs/qgh
10) http://nbl.gs/qgi

ONLINE

Il primo tomo di questa guida si occupa di fornire le basi sul funzionamento dei computer offline, chiarire quanto sono in grado di rivelare su chi li utilizza, proporre qualche caso d'impiego concreto e consigliare software inerenti alle problematiche emerse. Il secondo tomo si focalizza invece sull'uso dei computer online. Un programma piuttosto vasto: se immergersi negli arcani anfratti di queste macchine così familiari s'è già rivelata una faccenda complessa, cosa dovremo affrontare connettendo due computer tra di loro? Ricordiamoci intanto che un computer connesso è prima di tutto un computer; leggere approfonditamente il primo tomo è dunque un prerequisito essenziale per comprendere tutte le sfaccettature della sicurezza online.

Almeno nei paesi ricchi, l'uso di Internet è divenuto abituale. Consultare le e-mail, scaricare allegati, ottenere delle informazioni in rete, sono ormai per molti di noi gesti quotidiani. Ogni

persona potrebbe sostenere in qualche modo di sapere cosa sia Internet. Ma forse è più corretto dire che siamo in grado di servircene per qualche attività.

In questo secondo tomo non definiamo nei minimi dettagli la natura e il funzionamento di Internet. Piuttosto forniamo qualche elemento di comprensione sufficiente per permettere di navigarci dentro – termine ambiguo che rinvia sia alla "navigazione sul web" che alla possibilità di orientarsi in uno spazio complesso, con l'ausilio di appositi programmi.

Cominciamo dal principio. Internet è una rete. O piuttosto un insieme di reti connesse tra di loro. Nata da un'oscura applicazione militare, si è estesa negli ultimi quarant'anni al mondo intero. Si tratta di una rete che ha visto il moltiplicarsi di applicazioni, utilizzi, utenti, tecnologie e tecniche di controllo.

In tanti hanno discusso della “nuova era” che andava ad aprirsi, delle infinite possibilità di orizzontalità e di trasparenza nella diffusione delle informazioni e delle risorse, i vantaggi per le organizzazioni collettive, almeno quelle che hanno potuto abbracciare queste nuove tecnologie, l’utilità nelle lotte politiche. Ma poiché il potere non ama ciò che può sfuggirgli anche solo in parte, parallelamente all’espansione di Internet, è avvenuto un perfezionamento delle tecniche di controllo, di sorveglianza e di repressione, sempre più opprimenti mano a mano che il tempo passa.

Durante il 2011, per la prima volta alcuni governi hanno disconnesso la popolazione da Internet. I governanti di Egitto e Iran, hanno ritenuto che per meglio contenere le rivolte in atto, avrebbero dovuto limitare al massimo le comunicazioni in rete e parallelamente organizzare la sorveglianza e il pedinamento su Internet. Il governo iraniano è riuscito anche a mettere insieme un sistema di

analisi del traffico, impiegando importanti risorse per sorvegliare i rivoltosi, noti o meno, stabilire una mappa delle loro relazioni e più tardi confondere e condannare chi utilizzava la rete per organizzare le proteste.
Un altro esempio è quello della creazione di una versione cinese di Google nel 2006, dove l'azienda ha accettato in maniera più o meno docile la politica del governo cinese di filtraggio dei risultati di ricerca.
Metodi simili vengono usati anche nei cosiddetti paesi democratici. Alla fine dell'estate del 2011, dopo varie giornate di scontri a Londra, due giovani inglesi sono stati condannati (1) a quattro anni di carcere per aver provato ad organizzare tramite Facebook un corteo nel loro quartiere. E questo nonostante la loro chiamata non avesse poi avuto seguito.
E ancora, le rivelazioni di Edward Snowden sullo stato di sorveglianza elettronico della NSA (2) su scala mondiale hanno reso credibili le ipotesi dei più pessimisti.

A partire da tutto questo, ci sembra indispensabile rendersi consapevoli che l'utilizzo di internet, e dell'informatica in generale, è tutto tranne che innocuo, perché ci espone alla sorveglianza e alla repressione che può derivarne. L'oggetto principale di questo secondo tomo è quello di permettere a ciascuno di comprendere quali siano i rischi e i limiti associati all'utilizzo di Internet. Quali sono alcune scelte che provino a complicare il lavoro di sorveglianza e ad aggirare i dispositivi di censura, quali ci permettano di mettere in piedi degli strumenti e delle infrastrutture in maniera autonoma. Un primo assist da cogliere per provare a riprendere il controllo di tecnologie che sembrano a volte destinate a scapparci di mano, ambizione che da sola supera però di gran lunga gli obiettivi di questa guida.

Eccoci qui, sulla strada per un viaggio nelle acque torbide del mondo digitale. La nostra traversata sarà divisa in tre parti, una prima che

spiega il contesto, le nozioni di base per una comprensione generale, una seconda parte che tratta tipici casi d'impiego e infine una terza parte che descrive nel dettaglio i programmi necessari alle policy di sicurezza trattate nella seconda parte e come utilizzarli.

Note:
1) France Soir, 2011, scontri a Londra: due giovani condannati a 4 anni di prigione http://nbl.gs/qgj
2) National Security Agency, agenzia che dipende dal dipartimento della difesa degli USA, incaricata di raccogliere e analizzare i dati provenienti dai paesi stranieri e della protezione dei dati statunitensi.

COMPRENDERE

Di fronte alla grande complessità degli strumenti informatici e numerici, la quantità di informazioni da ingurgitare per tentare di acquisire qualche pratica di autodifesa può apparire enorme. Lo è sicuramente per chi cerca di capire tutto quanto insieme.
Il primo tomo si concentra quindi sull'utilizzo di un computer "offline" – o, per meglio dire, prima di connetterlo a qualunque cosa. Ci sono delle conoscenze più generali che valgono nel caso in cui il computer sia connesso o no a una rete. Mettiamo quindi da parte, fino al secondo tomo, le minacce specificatamente legate all'uso di internet e delle risorse web.

Su questa parte offline, come sulle altre, ci prenderemo il tempo di attardarci su alcune questioni di base, le loro implicazioni in termini di sicurezza / fiducia / intimità (1). Dopo aver analizzato alcuni casi concreti di impiego, potremo esaminare alcune ricette pratiche.

Un'ultima precisazione prima di buttarci: l'illusione di sicurezza è molto peggio della consapevolezza netta di una vulnerabilità. Quindi, prendiamoci il tempo di leggere bene queste parti introduttive prima di gettarci sulle nostre tastiere.. o di gettare i nostri computer dalla finestra.

Note

1) Intendiamo qui riferirci a una nozione un po' imprecisa: qualcosa che riguarda la possibilità di decidere cosa rivelare a chi e cosa invece tenere segreto; qualcosa che include anche una certa attenzione nell'ostacolare i tentativi di violare questi segreti. Il termine impiegato in inglese per definire ciò di cui parliamo qui è privacy. Nessuna parola francese ci è sembrata adatta per includere tutti i sensi che vorremmo sottointendere con questo termine. Altrove incontreremo spesso il termine "sicurezza", ma l'utilizzo che ne viene fatto comunemente ci ha fatto venire voglia di evitarlo.

INFORMAZIONI DI BASE SU UN COMPUTER

COMINCIAMO DALL`INIZIO.

Un computer non è un cappello magico in cui si possano infilare e togliere conigli quando se ne ha bisogno, o che ci permette di avere una finestra aperta sull'altro capo del mondo premendo il tasto giusto. Un computer è composto da un insieme di macchine più o meno complesse, collegate tra loro da connessioni elettriche, cavi, e a volte onde radio. Tutto questo materiale accumula, trasforma e replica dei segnali per manipolare l'informazione che poi vediamo su un bello schermo pieno di bottoni da cliccare.

Comprendere come si articolano questi principali componenti, comprendere le basi di quello che fa funzionare tutto questo, è il primo passo per capire quali sono i punti forza e i punti deboli di queste macchine a cui affidiamo un buon numero dei nostri dati.

MACCHINE CHE TRATTANO DATI

I computer sono delle macchine inventate per occuparsi delle informazioni. Sanno quindi registrare, trattare, analizzare e classificare con precisione informazioni, anche in grande quantità.

Nel mondo digitale, copiare un'informazione costa solo qualche micro-watt, ovvero poca roba: è importante capire questa cosa se vogliamo limitare l'accesso a delle informazioni.

Bisogna molto semplicemente considerare che mettere un'informazione su un computer (ed è ancora più vero quando sta in rete), vuol dire accettare che questa informazione possa sfuggirci di mano.

Questa guida può aiutare a limitare il danno, ma bisogna malgrado tutto prendere atto di questa realtà.

IL MATERIALE

Somma di componenti collegati tra loro, il nostro computer è quindi innanzitutto un accumulo di oggetti che possiamo toccare, spostare, moddare, rompere.
L'insieme di schermo / tastiera / case, o il computer portatile, è pratico quando vogliamo semplicemente collegare i cavi al posto giusto. Ma per sapere cosa accade ai nostri dati è necessario un esame più raffinato.

Qui di seguito prendiamo in esame il contenuto di un computer "classico", talvolta chiamato PC. Ma troveremo la maggior parte di questi componenti, con delle leggere variazioni, su altre macchine: telefoni cellulari, modem, tablet, lettori MP3, registratori di cassa, contatori Linky (1), centraline digitali delle automobili, etc..

note
1) I contatori Linky sono i discendenti digitali dei vecchi contatori elettrici in Francia.

LA SCHEDA MADRE

Un computer è composto più che altro da componenti elettronici. La scheda madre è un grosso circuito stampato che permette di collegare la maggior parte di questi componenti attraverso l'equivalente di fili elettrici. Sulla scheda madre vengono attaccati almeno un processore, della ram, un dispositivo di stoccaggio (hard-disk o un altro tipo di memoria), ciò che fa avviare il computer (il firmware), altre schede e periferiche, a seconda dei bisogni.

Andiamo a fare rapidamente un piccolo tour attraverso tutto questo per avere una vaga idea di chi fa cosa: ci sarà utile per il futuro.

IL PROCESSORE

Il processore (chiamato anche CPU, Central Processing Unit o Unità di Elaborazione Centrale, in italiano) è il componente che si occupa del trattamento dei dati.

Per immaginarsi il lavoro di un processore, l'esempio più concreto sul quale basarsi è la calcolatrice. In una calcolatrice si inseriscono dati (i numeri) e delle operazioni da fare (somma, moltiplicazione o altre) poi si osserva il risultato, utile eventualmente in seguito come base per altri calcoli.

Un processore funziona esattamente alla stessa maniera. A partire da alcuni dati (che possono essere una lista di operazioni da effettuare), esso

esegue semplicemente la catena di procedure da fare. Fa solo questo, ma lo fa veramente molto veloce.

Ma se il processore non è altro che una semplice calcolatrice, com'è possibile che riesca a eseguire delle operazioni su delle informazioni che non sono numeri, per esempio su un testo, delle immagini, dei suoni o lo spostamento del mouse?
Semplicemente trasformando in numeri tutto ciò che non lo è, utilizzando un codice definito in precedenza. Per un testo, potrebbe essere ad esempio una cosa tipo A = 65, B = 66, etc. Una volta che si è definito questo codice, si possono far diventare numeri le nostre informazioni. Usando il codice di prima possiamo per esempio trasformare "GUIDE" in "71, 85, 73, 44, 69".

Questa serie di cifre permette di rappresentare le lettere che compongono le nostre parole. Ma il processo di digitalizzazione perderà sempre delle

informazioni. Nell'esempio di prima, nel passaggio si perde la specificità della scrittura manoscritta dove per esempio una cancellatura, delle lettere esitanti, fanno parte anch'esse dell'"informazione". Quando le cose passano al setaccio del mondo digitale, nel passaggio si perdono per forza ogni volta dei pezzi.

Al di là dei dati, le operazioni che il processore deve effettuare (le sue istruzioni) sono anch'esse codificate sotto forma di numeri binari. Un programma è insomma una serie di istruzioni, trattate come qualsiasi altro dato.
All'interno del computer, tutti questi numeri sono a loro volta rappresentati usando gli stati elettrici: assenza di corrente o presenza di corrente. Ci sono quindi due possibilità, i famosi 0 e 1 che troviamo ovunque. Questo è il motivo per cui si parla di codice binario, dove l'unità di misura è il bit. Ed è soltanto attraverso un gomitolo di cavi e diversi miliardi di transistor (interruttori, non molto diversi da quelli che accendono e spengono la

luce in cucina) che si compie il trattamento dei dati.

I processori non funzionano tutti allo stesso modo. Alcuni sono stati progettati per essere più efficaci con certi tipi di calcolo, altri per consumare meno energia, etc. Inoltre non tutti i processori dispongono esattamente delle stesse istruzioni. Ne esistono diverse grandi famiglie, che vengono chiamate architetture. Questo è abbastanza importante, perché un programma previsto per funzionare su una certa architettura generalmente non funzionerà su un'altra.

LA RAM

La memoria (o RAM, Random Access Memory) si presenta spesso sotto forma di barrette, e si infila direttamente sulla scheda madre.

La memoria serve ad archiviare tutti i programmi e i documenti aperti. E' qui che il processore va a cercare i dati da trattare e a immagazzinare i risultati delle operazioni. Per effettuare i calcoli, queste informazioni devono quindi per forza trovarsi in una forma utilizzabile direttamente.

L'accesso alla RAM è molto rapido: il tempo necessario a girare gli interruttori che collegano il processore alla zona di memoria da leggere (o da scrivere).

Quando la RAM non è più alimentata dall'elettricità, i dati che essa conteneva diventano illeggibili entro pochi minuti o ore, secondo i modelli.

L'HARD-DISK

Dato che la RAM si dissolve quando non ha più corrente, il computer ha bisogno di un altro posto dove archiviare dati e programmi tra un'accensione e l'altra. Si parla anche di memoria persistente o memoria secondaria: una memoria dove le informazioni scritte rimangono anche senza alimentazione elettrica.

Per fare ciò si utilizza in genere un hard-disk. Spesso questo è costituito da un involucro di metallo nel quale si trovano alcuni dischi che girano senza sosta. Sopra questi dischi si trovano dei piccolissimi pezzi di ferro. Al di sopra di ciascun disco si trovano delle testine di lettura. Con l'aiuto dei campi magnetici, quest'ultime individuano e modificano la posizione dei pezzetti

di ferro. La posizione del pezzetto di ferro permette di codificare le informazioni da archiviare. Queste informazioni sono immagazzinate sotto forma di bit, di cui esistono varie unità di misura, che permettono di quantificare più semplicemente la capacità di un hard-disk in termini di Megabyte (MB), Gigabyte (GB) etc.

A causa dei movimenti meccanici, gli hard-disk che girano sono lenti. Questo spiega come mai, nel 2016, più di un terzo dei computer portatili nuovi conteneva un disco SSD invece di un hard-disk (1). Un disco SSD è infatti una memoria flash, la stessa presente nelle penne USB e nelle schede SD. Questa memoria interamente elettronica è molto più rapida degli hard-disk magnetici (circa 25 volte più rapida).

Sia gli hard-disk che i dischi SSD permettono di conservare molte più informazioni rispetto alla RAM. Le informazioni che si mettono quindi in

genere su un disco (hard-disk o SSD) sono, ovviamente, i documenti, ma anche i programmi e tutti i dati che quest'ultimi utilizzano per funzionare, come i file temporanei, i log, i file di salvataggio, i file di configurazione, etc.
Il disco conserva insomma una memoria semi-permanente e semi-esaustiva di tutti i tipi di tracce che parlano di noi, di ciò che facciamo, con chi e come, da quando abbiamo iniziato a utilizzare il computer.

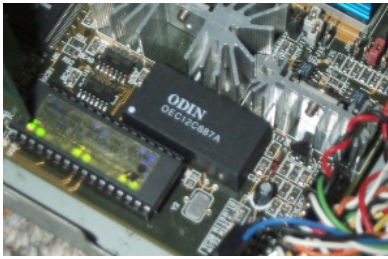
NOTE
1) http://nbl.gs/qgk

LE ALTRE PERIFERICHE

Già soltanto con un processore, della ram e un supporto di archiviazione, si è in grado di ottenere un computer. Non molto fruibile, però. Quindi gli si aggiungono generalmente altre periferiche come una tastiera, un mouse, uno schermo, una scheda di rete (con o senza fili), un lettore DVD, etc. Alcune periferiche necessitano di bus supplementari per fare in modo che il processore possa accedervi. Questi bus possono essere saldati direttamente sul circuito della scheda madre (tipicamente nel caso della tastiera) o talvolta possono aver bisogno di un circuito supplementare, sotto forma di scheda.

Per ridurre il numero di bus specifici (quindi costosi e complicati da mettere a punto), i sistemi di accesso alle periferiche tendono a uniformarsi. Per esempio, lo standard USB (Universal Serial Bus) è diventato velocemente lo standard per connettere stampanti, tastiere, mouse, hard-disk esterni, schede di rete o quelle che chiamiamo in genere “penne USB”.

IL FIRMWARE DELLA SCHEDA MADRE



Per far funzionare il computer, bisogna fornire al processore un primo programma in grado di caricare a sua volta i programmi da eseguire in seguito.

Questo piccolo software, chiamato firmware della scheda madre, è contenuto in un chip di memoria fissato sulla scheda madre stessa. Questa fa parte di una terza tipologia di memorie: le memorie flash. Lo stesso tipo che troviamo nelle penne USB o negli hard-disk chiamati SSD (Solid State Drive). È una memoria che conserva le nformazioni finché è attiva, ma se ne può sovrascrivere il contenuto attraverso un'operazione chiamata flash.

Il firmware storico per la maggior parte dei personal computer è stato chiamato BIOS (Basic Input/Output System). Dal 2012 in poi sempre più computer utilizzano un nuovo standard chiamato UEFI (Unified Extended Firmware Interface).

Questo primo programma che esegue il computer permette, tra l'altro, di scegliere dove si trova il sistema operativo da utilizzare che sarà caricato a partire da un hard-disk, da una penna USB, da un CD o un DVD, oppure dalla rete.

L'edizione originale integrale (in francese) è
leggibile online e scaricabile liberamente qui:
http://guide.boum.org