(nuovo)Partito comunista italiano

Comitato Centrale
Sito: http://www.nuovopci.it
e.mail: lavocenpci40@yahoo.com

Delegazione:
BP3 4, rue Lénine 93451 L'Île St Denis (Francia)
e.mail: delegazionecpnpci@yahoo.it

Avviso ai naviganti 59
2 febbraio 2016

Intervista a Edward Snowden

Darsi i mezzi della propria politica!
Valorizzare gli appigli che il corso delle cose offre!
Sfruttare le contraddizioni del campo nemico!

Le tre parole d'ordine che introducono questo AaN indicano in sintesi i motivi per cui raccomandiamo lo studio dell'intervista a Edward Snowden ai compagni desiderosi di imparare per instaurare il socialismo o anche solo di progredire nel far fronte al catastrofico corso delle cose in cui la borghesia imperialista trascina l'umanità.

In primo luogo Snowden denuncia la dilagante e frenetica sorveglianza a cui la Comunità Internazionale dei gruppi imperialisti europei, americani e sionisti che ha il suo centro a Washington, cerca di sottoporre ogni individuo e ogni attività nel mondo intero e indica alcuni mezzi tecnici (procedure e programmi) per sfuggire ad essa e aggirarla e alcuni criteri (principi) con cui impostare la difesa della propria autonomia d'azione.

La sinistra borghese (pensiamo ai vari "garanti della privacy" alla Stefano Rodotà e soci) si esibisce senza fine e si esaurisce in piagnucolii e deplorazioni della prevaricazione delle autorità borghesi attuali (che effettivamente stanno alla democrazia borghese d'un tempo come una carogna di cavallo sta al cavallo) e dei loro Servizi di informazione e controllo. Snowden va un passo oltre: indica come sfuggire ad essa e aggirarla. Chi vuole lottare contro la borghesia imperialista può e deve approfittare, imparare e servirsi delle sue indicazioni. In particolare deve liberarsi dalla superstiziosa fede nell'onnipotenza del nostro nemico, fede che paralizza tanti che pur sono indignati del corso delle cose. "Non c'è niente da fare!" è il loro motto.

Noi comunisti diciamo che niente e nessuno è in grado di arrestare il corso della storia che gli uomini stanno facendo. Il nostro futuro dipende dalle masse popolari, dalle classi sfruttate e dai popoli oppressi, quindi dipende da noi comunisti che siamo la loro avanguardia. Non dipende dalla borghesia e dai suoi servi. Il sistema di sorveglianza universale che la classe dominante ha montato e ogni giorno cerca di perfezionare, testimonia della sua debolezza. Come lo testimonia l'intero regime di controrivoluzione preventiva a proposito del quale rimandiamo i nostri lettori al *Manifesto Programma* del (nuovo)PCI e all'articolo *Controrivoluzione preventiva e mondo virtuale* di *La Voce* 51 (novembre 2015).

La borghesia non ha più egemonia sulla massa della popolazione né ha fiducia di poterla riconquistare. Non può fare di meglio che difendere il suo potere, cercare di dividere i suoi avversari, cercare di confonderli, cercare di intossicare le loro menti e i loro cuori ed è sostanzialmente tentata dal destino di Sansone: "che muoia Sansone con tutti i Filistei".

Per condurre con successo la nostra lotta noi comunisti possiamo e dobbiamo adottare sistematicamente misure atte a sottrarci alla sua sorveglianza. Snowden ne indica alcune. Dobbiamo smetterla con misure infantili come ricorrere a sigle, pseudonimi e iniziali per nascondere alle polizie l'identità delle persone che un normale servizio di polizia ricostruisce facilmente: misure addirittura dannose perché ingenerano un falso senso di sicurezza. Dobbiamo adottare il meglio che la tecnica e la scienza hanno prodotto. È a questo livello che si pone l'intervista di Snowden.

La nostra forza strategica sono le masse popolari. Possiamo e dobbiamo metterci al livello delle più avanzate conquiste della tecnica, appropriarcene e usarle contro la classe dominante e le sue istituzioni. Per ogni attacco c'è una contromisura adeguata, dice giustamente Snowden. Possiamo e dobbiamo andare più in là: spiare gli spioni. Possiamo arrivare dappertutto, perché la borghesia e il clero non possono sottrarsi alle masse popolari: cercano di comperare e corrompere i singoli individui, ma non ne possono fare a meno. Quando il movimento comunista era forte e l'Unione Sovietica era la base rossa della rivoluzione proletaria mondiale, il movimento comunista aveva occhi e orecchie dappertutto: perfino ai vertici del Servizio Segreto di Sua Maestà Britannica vi erano persone che gratuitamente lo tenevano al corrente delle manovre dei reazionari. La nostra egemonia e la nostra influenza non hanno confini.

In secondo luogo infatti Snowden, Assange, Manning e gli altri della schiera sono la dimostrazione vivente della intrinseca debolezza della borghesia imperialista, anche del feroce e criminale sistema di sorveglianza, repressione e sterminio montato dai "democratici" eredi di Hitler che hanno il loro centro dirigente nel sistema militare-finanziario-industriale che governa e opprime la popolazione degli USA. Essi sono la conferma della nostra concezione: che il nostro futuro dipende dalle masse popolari e quindi da noi comunisti. La borghesia imperialista ha dovunque abbandonato il servizio militare universale, del tutto inaffidabile e anzi pericoloso per una classe dominante in declino. Essa ovunque si affida a mercenari professionisti della sorveglianza, della repressione e dello sterminio. Ma anche dalle file dei suoi mercenari sorgono ribelli, nauseati dai crimini che sono indotti a commettere, resi folli dalle azioni insensate per cui sono comandati e remunerati. L'indignazione prorompe e rende inaffidabili per la borghesia anche i suoi eserciti mercenari.

Questo vale anche nel nostro paese, per tutti i corpi che la Repubblica Pontificia erige a difesa di se stessa e per l'esercizio della sua criminale attività contro la massa della popolazione e gli immigrati: dai Carabinieri, alla Polizia, alle Forze Armate, ai Sevizi. Man mano che il regime marcisce, essi diventano sempre meno affidabili per la classe dominante, tanto meno affidabili quanto più cresce la forza delle masse popolari e del movimento comunista, la loro attrazione e la loro forza di convinzione. Noi possiamo sempre più contare anche sulla defezione di componenti di questi corpi.

Il corso delle cose offre mille appigli per l'attività di noi comunisti: sta a noi vederli e portare le masse popolari a usarli per far montare colpo su colpo l'onda della rivoluzione socialista che travolgerà la Repubblica Pontificia. Le file del nemico sono indebolite da mille contraddizioni: sta a noi comunisti scorgerle e portare le forze popolari che già dirigiamo a colpire nei punti e nei momenti a noi più favorevoli. Ma per vedere e scorgere, bisogna assimilare la scienza a ciò necessaria: un botanico vede in una foresta cose che un ignorante non vede. Il materialismo dialettico è la nostra scienza, il nostro metodo di conoscenza. Esso ci porta a cercare in ogni cosa quello che essa è e quello che per sua natura può diventare se trattata adeguatamente. Esso ci fornisce strumenti di analisi per arrivare a conoscere il movimento che ogni cosa sta compiendo e strumenti di sintesi per tracciare la linea da seguire per agire su di essa.

Infine Snowden mostra anche, in particolare nella parte finale della sua intervista, il lato debole della ribellione che nasce spontaneamente (cioè non direttamente promossa dall'attività del movimento comunista né ancora illuminata dalla sua scienza) nelle file dei servitori della borghesia: l'ingenua fiducia che il sistema imperialista sia capace di migliorare, la speranza che sia possibile indurlo ad attenuare il suo carattere criminale che invece si accentua col procedere della sua crisi, il misto di fiducia nella tecnologia che permetterebbe di costruire nicchie individuali per "tirare a campare" e "vivere felici e contenti" e di sfiducia nella capacità degli uomini di costruire quel mondo migliore che la scienza marxista ha chiamato comunismo, la soggezione al mito della fine della storia ("non c'è altro sistema oltre quello capitalista") che intralcia oggi gli uomini come un tempo li intralciava la fede nell'onnipotenza di dio e dei suoi rappresentanti in terra.

Questo indica e conferma quanto è importante che il movimento comunista cosciente e organizzato si armi della

concezione comunista del mondo, la propagandi con ricchezza di metodi e di iniziative e la usi. Essa illumina il percorso che l'umanità ha compiuto dalle lontane epoche di uno stadio sostanzialmente non dissimile da quello di altre specie animali, fino ad oggi e mostra il futuro che sta a noi costruire perché nella società di cui siamo membri esistono le sue premesse che sta a noi scorgere e valorizzare.

"Per quanto mi riguarda, non a me compete il merito di aver scoperto l'esistenza delle classi nella società moderna e la loro reciproca lotta. Molto tempo prima di me, storiografi borghesi [Thierry, Guizot, Mignet, Thiers e altri - ndr] hanno descritto lo sviluppo storico di questa lotta delle classi ed economisti borghesi [Smith, Ricardo, Malthus e altri - ndr] la loro anatomia economica. Ciò che io ho fatto di nuovo è stato:

1. dimostrare che l'*esistenza delle classi* è legata puramente a *determinate fasi storiche di sviluppo della produzione*;
2. che la lotta delle classi conduce necessariamente alla *dittatura del proletariato*;
3. che questa dittatura medesima non costituisce se non il passaggio all'*abolizione di tutte le classi* e a una *società senza classi*.

Mascalzoni ignoranti come Heinzen [uno dei rivoluzionari movimentisti dell'epoca, ndr], i quali non solo negano la lotta tra le classi, ma persino l'esistenza delle classi, dimostrano soltanto, nonostante i loro latrati sanguinari e le loro pose umanistiche, di ritenere le condizioni sociali nelle quali la borghesia domina, come il prodotto ultimo, come il non plus ultra della storia, di non essere che servi della borghesia, una servitù che è tanto più ripugnante, quanto meno questi straccioni riescono a capire anche solo la grandezza e la necessità transitoria del regime borghese stesso." (dalla lettera di Karl Marx a Joseph Weydemeyer, 5 marzo 1852).

***

https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy/
Edward Snowden Explains How To Reclaim Your Privacy

Edward Snowden spiega come difendere la vostra privacy

Micah Lee
12 novembre 2015

Avvertenza: nel seguito, quanto è in corsivo tra parentesi quadre, è di Micah Lee; quanto è in tondo corpo 8 tra parentesi quadre precedute da asterisco, è del traduttore.

Il mese scorso ho incontrato Edward Snowden in un hotel nel centro di Mosca, a pochi isolati dalla Piazza Rossa. Era la prima volta che ci incontravamo di persona. Mi aveva scritto un paio di anni fa, poi avevamo creato un canale di comunicazione criptato per i giornalisti Laura Poitras e Glenn Greenwald, ai quali Snowden voleva rivelare la dilagante e frenetica sorveglianza di massa messa in atto dalla National Security Agency (NSA) e dal suo equivalente britannico GCHQ (Government Communications Headquarters).

Oramai Snowden non era più nascosto nell'anonimato. Tutti sapevano chi era, molte delle informazioni che aveva rivelato erano di dominio pubblico ed era noto che viveva in esilio a Mosca, dove era rimasto bloccato quando il Dipartimento di Stato USA gli aveva annullato il passaporto mentre stava recandosi in America Latina. La sua situazione adesso era più stabile e le minacce contro di lui un po' più facili da prevedere. Quindi ho incontrato Snowden con meno paranoia di quella che era invece giustificata nel 2013, ma con più precauzioni per la nostra sicurezza personale, visto che questa volta le nostre comunicazioni non sarebbero state telematiche ma di persona.

Il primo incontro è avvenuto nella hall dell'hotel. Mi ero portato dietro tutto il mio armamentario elettronico. Avevo spento il mio smartphone e l'avevo messo in una gabbia di Faraday, uno strumento progettato per bloccare tutte le emissioni radio. La gabbia era nello zaino assieme al mio computer portatile (che avevo configurato e reso più sicuro appositamente per questo viaggio in Russia). Sia il computer che lo smartphone erano spenti. Entrambi erano configurati in modo da stoccare le informazioni in forma criptata, ma il sistema di criptazione non è inattaccabile e lasciarli in camera sarebbe stato un invito alla manomissione.

La maggior parte dei divani della hall erano occupati da russi ben vestiti che sorseggiavano cocktail. Mi sono installato su un divano vuoto, appartato e fuori dal campo di sorveglianza dell'unica telecamera di sicurezza che sono riuscito a individuare. Snowden mi aveva detto che avrei dovuto aspettare un po' prima di incontrarlo e per un attimo mi sono chiesto se fossi sorvegliato. Un uomo con la barba, occhiali e impermeabile, stava in piedi a pochi passi da me, senza far altro che fissare una vetrata colorata. Dopo un po' ha fatto un giro attorno al divano dove ero seduto e, quando i nostri sguardi si sono incrociati, se n'è andato.

Finalmente è comparso Snowden. Ci siamo sorrisi e ci siamo detti quanto ci facesse piacere incontrarci. Prima di incominciare a parlare sul serio, siamo saliti per una scala a chiocciola accanto a un ascensore fino alla camera dove avrei fatto l'intervista.

Poi è risultato che avrei potuto prendere meno precauzioni a proposito della sicurezza. Snowden mi ha detto che potevo servirmi del mio telefono, così ho potuto combinare un appuntamento con alcuni amici comuni che erano in città. La sicurezza operativa *[operational security, opsec] è stato uno dei temi ricorrenti delle diverse conversazioni che abbiamo avuto a Mosca.

Nella maggior parte delle sue precedenti dichiarazioni, Snowden ha parlato dell'importanza della privacy, del bisogno che ci sia una riforma dei sistemi di sorveglianza e della criptazione. Ma raramente ha avuto l'occasione di entrare nei dettagli e aiutare anche persone prive di una grande formazione tecnica a capire i metodi della sicurezza operativa e quindi a rafforzare la propria sicurezza e la propria privacy.

Ci siamo trovati d'accordo sul fatto che la nostra intervista si dovesse incentrare più sulle questioni da nerd *[fanatici dell'informatica] che su quelle politiche, perché siamo entrambi dei nerd e non c'erano altre interviste su questo tono. Credo che Snowden abbia voluto usare il nostro incontro per promuovere progetti all'avanguardia nella sicurezza e per spingere la gente a usarli.

Ad esempio, Snowden mi ha detto che prima del nostro incontro aveva scritto su Twitter a proposito di TOR, il sistema per usare Internet mantenendo l'anonimato e che era rimasto sorpreso di quante persone pensano che TOR è un complotto del governo. Voleva dissipare questo genere di fraintendimenti.

La nostra intervista, realizzata mentre mangiavamo hamburger serviti in camera, è iniziata discutendo di alcune nozioni di base.

Micah Lee: Quali sono le pratiche di sicurezza operativa che tutti dovrebbero adottare? Diciamo quelle utili per un utente medio.

Edward Snowden: La sicurezza operativa è una cosa importante, anche se non ci si sente preoccupati per lo spionaggio della NSA. Perché quando si parla di vittime di sorveglianza abusiva, si deve pensare a persone che hanno relazioni extra-coniugali, a vittime di stalking, a giovani preoccupati dell'invadente controllo dei genitori. Si tratta innanzitutto di pretendere un certo grado di privacy.

- Un primo passo che chiunque può fare è quello di criptare le telefonate e i messaggi di testo (sms). Si può farlo usando l'app *[l'application, il programma specifico] per smartphone Signal, messa a punto dalla Open Whisper Systems. È gratuita, basta scaricarla. Anche se le vostre conversazioni sono intercettate, non possono essere comprese da un eventuale spione. *[Signal è disponibile per iOS e Android e, a differenza di molti altri strumenti per la sicurezza, è molto facile da usare]*

- Si dovrebbe anche criptare il disco rigido in modo che, se il computer viene rubato, le informazioni registrate su di esso non sono leggibili - foto, indirizzo di casa, indirizzo del posto di lavoro, i luoghi che frequentano i vostri figli, dove si trova la vostra università, ecc. *[Ho scritto una guida per la criptazione del disco per Windows, Mac e Linux reperibile in https://theintercept.com/2015/04/27/encrypting-laptop-like-mean/]*

- Utilizzare un gestore di password. Una delle cose che rende le informazioni personali più esposte, anche agli spioni meno dotati, sono i data dump *[ad esempio i flussi di dati trasferiti da un computer all'altro, i dati che i computer registrano quando vanno in tilt e creano copie della memoria sul disco]. Le vostre credenziali (come username e password) possono essere ottenute anche da qualcuno che hackera un sito che voi avete smesso di usare, poniamo, nel 2007, ma ad esempio la password a suo tempo utilizzata per quel sito Internet è la stessa che state ancora usando per la vostra casella Gmail. Un gestore di password consente di creare password sicure, ognuna dedicata a un solo sito Internet, ma senza il problema di doverle memorizzare. *[Il gestore di password KeePassX è gratuito, open source, funziona su Windows, Linux e Apple e non memorizza nulla su Internet]*

- Un'altra misura da adottare è l'identificazione a due fattori. Il punto di forza di questo metodo è che se qualcuno si appropria della vostra password, oppure se avete lasciato la password in bella mostra … l'identificazione a due fattori consente al provider *[al fornitore di servizi Internet] di fornirvi un mezzo alternativo di identificazione - per esempio un sms o qualcosa di simile. *[Se attivate l'identificazione a due fattori, un hacker avrà bisogno sia della password (primo fattore), sia di un dispositivo fisico, come il vostro telefono, come secondo fattore. Gmail, Facebook, Twitter, Dropbox, GitHub, Battle.net e una miriade di altri servizi permettono l'utilizzo dell'identificazione a due fattori (una lista di questi servizi la trovate sul sito: https://twofactorauth.org/)]*

Non dobbiamo vivere come se fossimo elettronicamente nudi. Dobbiamo corazzarci con sistemi su cui possiamo contare nella vita di tutti i giorni. Questo non deve comportare un enorme cambiamento nello stile di vita. Non deve essere qualcosa che sconvolge le nostre abitudini. Deve essere invisibile, far parte della quotidianità, deve essere qualcosa che si attua in maniera indolore, senza sforzo. Questo è il motivo per cui mi piacciono i programmi per smartphone come Signal, perché sono facili. Non vi chiedono di cambiare le vostre abitudini. Non richiedono un cambiamento nella vostra maniera di comunicare. Li potete usare già da subito per comunicare con gli amici.

Lee: Cosa pensi di TOR? Pensi che tutti dovrebbero avere familiarità con esso o che lo deve usare solo chi ne ha assoluto bisogno?

Snowden: Penso che TOR sia il progetto più importante che oggi abbiamo a disposizione per quanto concerne la tutela della privacy. Io uso sempre TOR. Sappiamo che funziona, lo abbiamo verificato almeno in un caso esemplare che ora molti ben conoscono *[Snowden si riferisce all'operazione con cui ha reso pubbliche le informazioni che ha sottratto ai servizi segreti USA]. Questo non vuol dire che TOR sia a prova di bomba. TOR è solo una misura di sicurezza che consente di dissociare la vostra posizione geografica dalla vostra attività su Internet.

Ma l'idea di base, il concetto che fa di TOR uno strumento così prezioso, è che la rete TOR è gestita da volontari. Chiunque può attivare un nuovo nodo della rete TOR, che si tratti di un nodo d'ingresso, intermedio o di uscita, basta che accetti di correre un certo rischio. La natura volontaria di questa rete significa che è capace di far fronte a ogni colpo, è resistente, è flessibile.

[TOR Browser è un ottima via per l'uso di TOR per accedere a un dato su Internet senza lasciare traccia. Può anche aiutare ad aggirare la censura quando siete in una rete in cui alcuni siti sono bloccati. Se desiderate coinvolgervi di più, si può volontariamente avviare il proprio nodo TOR, come faccio io: questo aumenta le capacità di comunicazione e la sicurezza della rete TOR]

Lee: Quello che dici sono cose che tutti dovrebbero fare. Ma che dire di persone che sono sottoposte a minacce eccezionali, come i futuri "lanciatori di allerta" *[i "lanciatori di allerta", nel mondo anglosassone whistleblowers: quelli che lavorano in una struttura e rendono pubbliche le informazioni a cui hanno accesso grazie al lavoro che fanno e che i loro padroni abusivamente vorrebbero restassero segrete, tipo Snowden stesso, Assange, Manning, ecc.] che svelano le manovre dei servizi segreti e altre persone che hanno tra i loro avversari lo Stato? Cioè i giornalisti, gli attivisti e le persone impegnate nella denuncia politica?

Snowden: La prima risposta è che non si può imparare da un solo articolo tutto quello che occorre sapere. Le esigenze d'individui che si trovano in una situazione ad alto rischio sono diverse da caso a caso. Le capacità degli spioni sono in costante miglioramento e cambiano di continuo anche gli strumenti di cui disponiamo per difenderci.

Quello che conta davvero è essere consapevoli della necessità di un compromesso. In generale, bisogna porsi alcune questioni: come può il nemico avere accesso ai vostri dati sensibili? Quali sono le informazioni da proteggere? Perché, naturalmente, non c'è bisogno di nascondere tutto all'avversario. Non è necessario vivere in stato di paranoia, isolarsi e nascondersi nei boschi del Montana.

Quello che cerchiamo di proteggere sono le informazioni sulle nostre attività, le nostre convinzioni e le nostre vite, che potrebbero essere utilizzate contro di noi, contro i nostri interessi. Pensiamo ad esempio ai whistleblowers: se avete assistito a un qualche tipo di azione illecita, avete deciso di rivelare queste informazioni e credete che ci siano persone che vogliono impedirvi di farlo, allora è necessario pensare a come frazionare tutto ciò in compartimenti separati.

Non parlate con nessuno che non ha bisogno di sapere. *[Lindsay Mills, per anni la ragazza di Snowden, non era a conoscenza del fatto che lui stava raccogliendo documenti da rivelare ai giornalisti, fino a che non venne a saperlo dai mass-media, come tutti gli altri]*

Quando si parla di whistleblowers e di come agire, si deve pensare a strumenti per proteggere la propria identità, per proteggere l'esistenza di una relazione tra voi e le vostre informazioni da e in qualsiasi tipo di sistema di comunicazione tradizionale. Si deve utilizzare per esempio un sistema come SecureDrop *[sistema che associazioni e quotidiani utilizzano per permettere ai cittadini di trasmettere loro informazioni in modo riservato] attraverso la rete TOR. In questo maniera non risulta alcun collegamento tra il computer che in quel momento state usando e le informazioni che inviate attraverso Internet. Possibilmente utilizzando un sistema operativo live come Tails *[Sistema Linux su chiavetta USB già predisposto per l'uso di TOR], così da non lasciare alcuna traccia utile alla polizia e alla magistratura sul computer che state usando. Che, per di più, potrebbe essere un computer o telefono di cui vi potete sbarazzare in seguito, che non può essere trovato durante una perquisizione, che non può essere analizzato. In tal modo, l'unica traccia delle vostre attività saranno gli articoli dei giornalisti a cui avrete inviato le vostre informazioni. *[SecureDrop è un sistema di contatto per* whistleblowers. *Ecco una guida all'utilizzo del server SecureDrop del sito Intercept nel modo più sicuro possibile]*

Tutto questo anche per essere sicuri che chi è coinvolto nell'affare illecito che rivelate, non è in grado di distrarre l'attenzione dalla questione in gioco per concentrarla sulla vostra identità fisica. In tal modo, l'avversario dovrà confrontarsi con i suoi misfatti, piuttosto che con le persone coinvolte.

Lee: Cosa suggerire, allora, alle persone che vivono sotto un regime repressivo e stanno cercando di ...

Snowden: Di usare TOR!

Lee: Usare TOR?

Snowden: Se non usate TOR, state sbagliando. Ovviamente qui c'è un problema: l'uso di tecnologie di protezione della privacy, in certi paesi, espone all'aumento delle misure di sorveglianza e di repressione. Questo è il motivo per cui è così importante che gli informatici che stanno lavorando per migliorare gli strumenti di sicurezza, facciano in modo che i loro protocolli *[il modo di comunicare di questi strumenti] siano indistinguibili dagli altri.

Lee: Hai detto che ciò che vuoi diffondere sono i principi della sicurezza operativa. Hai ricordato alcuni di questi, come la divisione in compartimenti stagni basata sul principio need-to-know *[dire solo a chi deve sapere]. Ci puoi parlare più in dettaglio di quali sono i principi dell'operare in modo sicuro?

Snowden: Alla base del concetto di sicurezza operativa c'è l'idea di pensare alla vulnerabilità. Pensate a quali sono i rischi del compromesso sulla base del quale lavorate e a come fare per diminuirli. Ad ogni passo, in ogni azione, in ogni questione, in ogni decisione, bisogna fermarsi a riflettere e domandarsi: "Quale sarebbe l'effetto se il mio avversario

venisse a conoscenza delle mie attività?". Se l'effetto è qualcosa d'insormontabile, che vi costringerebbe a cambiare attività o a cessarla, dovete diminuire le possibilità che il vostro avversario vi spii, adottando strumenti e sistemi adatti a proteggere le informazioni e a ridurre il rischio insito nel compromesso, oppure, in ultima analisi, dovete accettare il rischio di essere scoperti e avere già un piano per ridurre i danni. Perché a volte non si può tenere qualcosa segreto per sempre, però è possibile pianificare la mossa successiva.

Lee: Ci sono principi di sicurezza operativa che pensi si possano applicare alla vita quotidiana?

Snowden: Sì, la condivisione selettiva. Non è necessario che tutti sappiano tutto di noi. Il tuo amico non ha bisogno di sapere in quale farmacia vai. Facebook non ha bisogno di conoscere le domande di sicurezza che hai predisposto per il recupero della password. Non è necessario mettere il nome da nubile di tua madre sulla tua pagina di Facebook se lo utilizzi anche per recuperare la password di Gmail. L'idea è che la condivisione è una buona cosa, ma deve essere sempre fatta volontariamente e consapevolmente. Questa è un principio a cui fare molta attenzione. Le informazioni condivise devono essere reciprocamente vantaggiose e non semplicemente cose che ti vengono prese.

Quando usate Internet ... i modi di comunicazione oggi in uso tradiscono silenziosamente, in modo invisibile, a ogni click. Delle informazioni personali vengono sottratte a ogni pagina che visitate. Esse sono raccolte, intercettate, analizzate e registrate dai governi, da quello nazionale come da quelli stranieri, e da aziende private. È possibile ridurre questo rischio prendendo alcune semplici contromisure. La cosa fondamentale è assicurarsi che le informazioni che vengono raccolte su di voi, lo siano per vostra scelta.

Ad esempio, se utilizzate i plugin dei browser *[programmi accessori di Firefox e di altri navigatori Internet] come HTTPS Everywhere *[già installato se usate TOR Browser] messo a punto da EFF *[Electronic Frontier Foundation -https://www.eff.org/ - associazione per la divulgazione e l'uso di sistemi di comunicazione a tutela dei giornalisti], potete servirvi di comunicazioni cifrate e sicure in modo che i dati scambiati restino protetti.

Lee: Pensi che si dovrebbero usare software adblock *[advertising block - programmi accessori di Firefox e altri navigatori Internet che bloccano le finestre della pubblicità durante la navigazione Internet]?

Snowden: Sì. Tutti dovrebbero avere installato un software adblock, anche solo per una questione di sicurezza ...

Abbiamo visto che certi provider come Comcast, AT&T e altri, inseriscono propri annunci pubblicitari durante le connessioni in chiaro http *[piccola sigla nell'indirizzo Internet che appare nel navigatore quando siete collegati ad un sito che non cripta i dati]. Quando i provider si servono di annunci pubblicitari con contenuti attivi che, per essere visibili, richiedono l'uso di Javascript, o che incorporano un contenuto attivo come Flash, insomma qualunque cosa che può essere vettore di un attacco al vostro navigatore Web (browser) – dovete prendere l'iniziativa di bloccare questi annunci. Perché se il fornitore d'accesso a Internet, il provider, non vi protegge da questo tipo di pubblicità, viene a cadere il rapporto di fiducia tra fornitore e utente del servizio. Avete quindi non solo il diritto, ma il dovere di prendere delle misure per proteggervi.

Lee: Bene. Ci sono poi un sacco di attacchi un po' misteriosi di cui si sente parlare nei media. Attacchi alla criptazione del disco, "evil maid attacks" e "cold-boot attacks" *[l'avversario congela con ghiaccio secco o altro la memoria del computer per recuperare da essa anche quando si toglie la corrente le informazioni che senza congelamento sparirebbero dalla memoria quando si toglie la corrente al calcolatore]. Ci sono attacchi al firmware *[programmi che il costruttore del computer registra sui componenti elettronici che servono a impartire i primi ordini per l'avvio del computer]. Ci sono BadUSB e BadBIOS, ci sono i "baseband attacks" sui telefoni cellulari *[interposizione tra il cellulare e la stazione ricevente di una stazione attrezzata a spiare la comunicazione. Sfruttano il basso livello di criptazione dei cellulari basati sul GMS (un sistema vecchio, ma ancora largamente diffuso) per spiare le conversazioni]. Per la maggior parte delle persone è altamente improbabile subire questo tipo di attacchi. Quali persone dovrebbero preoccuparsi di questi

problemi? Come si fa a decidere se si è fra quelli che potrebbero essere minacciati e che dovrebbero cercare di difendersi da essi?

Snowden: Tutto si riduce alla valutazione del vostro profilo di rischio. Questa è la questione di fondo che dovete porvi per definire la vostra sicurezza operativa. È necessario fare un bilancio fra il rischio insito nel vostro compromesso e quanto deve essere investito per ridurre tale rischio.

Nel caso di "cold-boot attacks" e altri attacchi del genere, ci sono molte cose che si possono fare. Ad esempio, i "cold-boot attacks" possono essere sconfitti semplicemente non lasciando mai il computer incustodito. Si tratta di una questione che non riguarda la stragrande maggioranza degli utenti, perché la maggior parte delle persone non hanno bisogno di preoccuparsi che qualcuno rubi il loro computer.

Per quanto riguarda gli "evil maid attacks", vi potete proteggere da essi mantenendo il bootloader *[programma di gestione dell'avvio del sistema operativo] fisicamente su di voi: potete ad esempio tenerlo appeso al collo in una chiavetta USB come se fosse una collana.

Da BadBIOS potete proteggervi tenendo una copia del BIOS *[BIOS è un programma che gestisce le prime fasi di avvio del computer prima di cedere il controllo a Linux o Windows], facendo l'hashing della copia (comunque spero non con il metodo SHA1) *[l'hashing si fa passando la copia del BIOS ad un programma tipo Winrar o 7zip: sono entrambi programmi di compressione dei file che oltre che comprimere il file contemporaneamente fanno l'hashing del file. L'hashing è un procedimento che permette di associare un numero al file: se per un qualche motivo il file viene modificato, cambia il numero ottenuto con l'hashing] e poi semplicemente confrontandola con il risultato dell'hashing del vostro BIOS. *[Il traduttore non garantisce di aver ben inteso il passaggio dell'intervista che segue. Nel testo originale il passaggio è il seguente: "In theory, if it's owned badly enough you need to do this externally. You need to dump it using a JTAG or some kind of reader to make sure that it actually matches, if you don't trust your operating system". Se qualche lettore ci invierà una traduzione affidabile, ne faremo uso.] In teoria se il vostro computer è stato gestito piuttosto male, dovete fare questa operazione su un altro computer. Se non avete fiducia nel vostro sistema operativo, dovete fare una copia del BIOS con JTAG o con un qualche altro tipo di lettore di file binari *[un elenco di questo tipo di programmi lo trovate al seguente link: https://en.wikipedia.org/wiki/Comparison_of_hex_editors].

Per ogni attacco c'è una contromisura adeguata. Si può immaginare di giocare al gatto e al topo all'infinito.

Potete andare a fondo fino a diventare matti pensando alle cimici nascoste nelle pareti e alle telecamere nel soffitto. Oppure potete pensare serenamente a quali sono le minacce più realistiche nella vostra situazione concreta. Su questa base, potete prendere misure adeguate per ridurre le minacce più realistiche. Posto in questi termini, il problema, per molte persone, si riduce a cose molto semplici. Usare un navigatore (browser) sicuro. Disabilitare gli script *[piccoli programmi che si avviano quando visitate una pagina Internet. Per disabilitarli su Firefox è disponibile ad esempio il plugin "noscritp" (https://noscript.net/)] e i contenuti attivi *[esempio Adobe Flash per quanto riguarda i contenuti attivi], preferibilmente utilizzando una macchina virtuale *[un programma che crea un sistema operativo separato da quello installato sul vostro computer. Utilizzando questo programma si simula un secondo computer. Se questo se viene infettato, lo si distrugge semplicemente cancellando il file che lo contiene e se ne ricrea uno nuovo. Tutto questo senza che il vostro sistema operativo originale subisca danni e che i virus eventualmente contratti si propaghino sul vostro computer] o qualche altra forma di navigatore (browser) in modalità sandbox *[un sistema che isola un certo programma dal vostro sistema operativo e, come per la macchina virtuale, lo si può distruggere se infettato dai virus]. Se c'è un'intrusione o un virus, semplicemente si butta nel cestino la sandbox o la macchina virtuale. *[Ho scritto di recente su come impostare le macchine virtuali]*. Un'altra cosa alla portata di tutti è fare in modo che le comunicazioni quotidiane vengano condivise selettivamente *[in modo compartimentato] e attraverso canali criptati.

Lee: Quale strumento di sicurezza attira oggi la tua attenzione e per quale caratteristica lo trovi interessante?

Snowden: Mi limiterò a citare Qubes. Sono davvero entusiasta di Qubes. L'idea di utilizzare macchine virtuali separate dal vostro sistema operativo – che richiederebbero dunque dei sistemi complessi per essere resi stabili su un computer –

è un grande passo avanti, perché obbliga gli spioni a ricorrere a operazioni onerose e complicate per continuare a spiarvi. Mi piacerebbe vedere questo progetto continuare a svilupparsi. Mi piacerebbe che lo rendessero più facile da usare e ancora più sicuro. *[Si può leggere di più su come utilizzare Qubes qui e qui*]

Una questione che non abbiamo affrontato e che invece dobbiamo affrontare è quella di una maggiore difesa dei kernel di ogni sistema operativo *[il kernel, nel gergo informatico, è il nocciolo più interno del sistema operativo: quello esterno è il sistema delle icone e delle cartelle che usate per interagire col computer, quello interno gestisce il disco, il trasferimento dei dati dalla memoria all'unità centrale di calcolo (la famosa CPU) del computer e reagisce a tutti i dati in ingresso tramite i vari connettori] tramite strumenti come i grsecurity *[un insieme di programmi per migliorare la sicurezza di Linux],* ma purtroppo c'è un grande divario tra i benefici che apportano e lo sforzo che deve fare un utente medio per farli funzionare.

Lee: Molte persone usano continuamente lo smartphone. È possibile utilizzare lo smartphone per comunicare in sicurezza?

Snowden: Qualcosa che la gente si dimentica a proposito dei telefoni cellulari di qualsiasi tipo, è che in generale il loro uso lascia una registrazione permanente di tutti i vostri spostamenti ... Il problema con i cellulari è che forniscono informazioni su di voi anche quando non li state usando. Questo non vuol dire che si dovrebbero bruciare i cellulari ... Ma si deve pensare al contesto più adatto al loro uso. Vi state portando dietro un dispositivo che, per il solo fatto di averlo con voi, registra che avete frequentato un certo luogo al quale non volete essere associati, anche se è qualcosa di banale come il vostro luogo di culto.

Lee: Ci sono moltissimi sviluppatori di software che vorrebbero capire come porre fine alla sorveglianza di massa. Come dovrebbero impegnare le loro risorse per raggiungere questo scopo?

Snowden: Il "Mixed routing" *[cioè l'invio delle proprie comunicazioni attraverso più macchine reali o virtuali] è una delle cose più importanti di cui abbiamo bisogno nel campo delle infrastrutture Internet. Non abbiamo ancora risolto il problema di come separare il contenuto della comunicazione dalla traccia che la comunicazione lascia. Per avere una privacy reale bisogna ottenere la separazione tra il contenuto e la traccia della comunicazione. Non solo quello di cui avete parlato con vostra madre, ma anche il fatto che avete parlato con vostra madre deve far parte della vostra privacy …

Il problema con le comunicazioni di oggi è che il fornitore di servizi Internet (il provider) sa esattamente chi siete. Sa esattamente dove vivete. Conosce il numero della vostra carta di credito, l'ultima volta che l'avete utilizzata e il montante della transazione.

Ognuno dovrebbe essere in grado di comprare un bel po' di quello che Internet offre allo stesso modo di come si acquista una bottiglia di acqua in un negozio.

Abbiamo bisogno di strumenti che possano connettersi anonimamente a Internet. Meccanismi che consentano che ci si associ privatamente. Soprattutto, abbiamo bisogno di sistemi che permettano la difesa della privacy nei pagamenti e nella consegna delle merci, che sono le basi del commercio.

Questi sono i problemi che devono essere risolti. Dobbiamo trovare un modo per trasmettere i diritti che noi abbiamo ereditato anche alla prossima generazione. Dobbiamo fare subito qualcosa, perché oggi ci troviamo di fronte al bivio tra una società libera e un regime di controllo. Se non facciamo nulla, quelli che verranno dopo di noi si domanderanno perché abbiamo lasciato che ciò accadesse. Vuoi vivere in un mondo completamente "quantificato"? Un mondo nel quale il contenuto di ogni conversazione è conosciuto, così come i movimenti di tutte le persone e, persino, la posizione di tutti gli oggetti. Dove il libro che hai prestato a un amico lascia una traccia su chi lo ha letto? Queste cose potrebbero essere delle potenzialità se arricchissero la società, ma lo saranno solo se potremo ridurre la raccolta di informazioni che riguarda le nostre attività, le nostre condivisioni e le nostre frequentazioni.

Lee: In teoria, nessun governo al mondo dovrebbe spiare tutti. Ma così è. Qual è allora la tua opinione, quale pensi sia la via per risolvere questo problema? Pensi che la soluzione sia criptare ogni comunicazione o piuttosto cercare di ottenere dal Congresso *[il parlamento USA] l'approvazione di nuove leggi - cioè che la politica sia importante come la tecnologia? Dove ritieni si trovi l'equilibrio tra la tecnica e la politica, al fine combattere la sorveglianza di massa? E cosa pensi che il Congresso dovrebbe fare, o che la gente dovrebbe costringere il Congresso a fare?

Snowden: Penso che le riforme abbiano molteplici aspetti. C'è una riforma legislativa; c'è, più in generale, una riforma di norme e statuti; ci sono i risultati delle decisioni prese nei tribunali ... Negli Stati Uniti si è ritenuto che questi programmi di sorveglianza di massa, che sono stati attuati in segreto, senza informare né chiedere il consenso dei cittadini, violano i nostri diritti e che quindi dovrebbero cessare. Di conseguenza, essi sono stati modificati. Ma ci sono molti altri programmi e molti altri paesi in cui queste riforme non hanno ancora avuto quel seguito indispensabile a ogni società libera. Riforme che sono vitali per una società libera. In tali contesti, in queste situazioni, io credo che noi dobbiamo - come comunità, come società aperta, sia se parliamo di semplici cittadini, che di quanti si occupano di tecnologia - cercare delle maniere per incrementare a ogni costo i diritti umani.

Può esser fatto tramite la tecnologia, tramite la politica, con il voto o cambiando il comportamento individuale. Ma la tecnologia è probabilmente, fra tutte queste possibilità, quella più promettente e più rapida per far fronte alle violazioni dei diritti umani. La tecnologia è un metodo di risposta che non dipende dal fatto che ognuno dei corpi legislativi del pianeta si riformi contemporaneamente agli altri: cosa che è forse troppo ottimistico sperare. Con la tecnologia siamo invece in grado di creare sistemi … che fanno rispettare e garantiscono i diritti che sono necessari per mantenere una società libera e aperta.

Lee: Cambiamo completamente argomento. In molti mi hanno detto che avrei dovuto domandarti di Twitter. Da quanto tempo hai un account Twitter?

Snowden: Da due settimane.

Lee: Quanti seguono il tuo Twitter?

Snowden: Un milione e mezzo di persone, credo.

Lee: Sono moltissimi. Come fai a far fronte a un numero così elevato di utenti?

Snowden: Sto cercando di non farmi sommergere, ma è molto difficile.

Lee: Di recente hai utilizzato molto Twitter anche quando a Mosca era notte fonda.

Snowden: Non nascondo il fatto che io vivo con l'orario "occidentale". La maggior parte del mio lavoro, delle associazioni con cui ho contatti e del mio attivismo politico si svolge ancora a casa mia, negli Stati Uniti. Quindi è ovvio che io lavori quando è giorno negli USA e notte qui.

Lee: Non senti come se il tuo tempo fosse risucchiato da Twitter? Io mi tengo collegato tutto il giorno a Twitter e a volte resto invischiato nelle discussioni. A te cosa accade?

Snowden: Ci sono stati giorni in cui la gente continuava a twittare foto di gatti per l'intera giornata. So che non avrei dovuto, avevo un sacco di lavoro da fare, ma non riuscivo a smettere di guardarle.

Lee: La mia vera curiosità è se hai avuto un account Twitter prima di quello attuale. Perché eri ovviamente su Twitter anche prima. Eri sempre aggiornato.

Snowden: Io non posso né confermare né smentire l'esistenza di altri miei account Twitter.

Snowden e io siamo entrambi esponenti della Freedom Press Founfation [http://freedom.press/].