LO SPIONAGGIO FA MALE AL COMMERCIO

Lo scandalo delle intercettazioni della NSA potrebbe balcanizzare Internet o renderla più sicura? Si può ancora avere fiducia in una Rete che è diventata un'arma in mano ai governi?

Antonio Regalado

A seguito di un summit di un giorno tenuto a Brasilia, a febbraio, i negoziatori di Brasile ed Europa hanno raggiunto un accordo per un investimento di 185 milioni di dollari destinato alla posa di cavi a fibra ottica lungo le 3.476 miglia che dividono Fortaleza da Lisbona. La cablatura verrà effettuata da un consorzio di aziende spagnole e brasiliane. Secondo la Presidente del Brasile, Dilma Rousseff, si tratta di un investimento "in difesa della libertà". Il traffico Internet nel Sud America non dovrà più passare per Miami, permettendo alle spie americane di intercettare le comunicazioni.

La Rousseff non è paranoica. I documenti diffusi lo scorso giugno da Edward Snowden, ex tecnico della CIA, rivelano l'esistenza di una politica di sorveglianza globale coordinata dalla NSA statunitense e dal suo corrispettivo brasiliano, il GCHQ. Tra le centinaia di obiettivi prescelti spiccano la Petrobras, la compagnia petrolifera di Stato del Brasile, e il telefono cellulare della Rousseff.

C'è da chiedersi in quale misura le rivelazioni di Snowden stiano condizionando il mercato tecnologico. Alcune delle conseguenze sono già sotto gli occhi di tutti. I consumatori stanno privilegiando le applicazioni che permettono di mantenere l'anonimato. Le grandi aziende su Internet, come Google, si sono affrettate a crittografare le loro comunicazioni. In Germania, i legislatori stanno discutendo per definire la realizzazione di una rete autonoma dei paesi europei.

Eugene Kaspersky, fondatore dell'azienda moscovita che produce l'omonimo antivirus, mette in guardia sulla frammentazione di Internet. Dal suo punto di vista la scelta brasiliana di posare un sistema di cavi ricorda quella cinese del Great Firewall (il sistema di sorveglianza di Internet), o le richieste dei nazionalisti russi di bloccare Skype, o il progetto tedesco di indirizzare il traffico Internet interno solo su router nazionali. Le nazioni stanno limitando l'accesso alle loro reti. L'azienda di Kaspersky prevede che si possa arrivare «al collasso dell'attuale Internet, che potrebbe suddividersi in decine di reti nazionali».

Gli esperti, tra cui l'americana Forrester Research, la società di ricerca indipendente, ipotizzano miliardi di dollari di perdite per aziende Internet come Dropbox e Amazon, a causa dei timori da parte degli utenti di queste tecnologie, particolarmente in Europa, sulla scia degli scandali legati alle intercettazioni. «Le rivelazioni di Snowden hanno disegnato l'immagine di una infrastruttura di Rete controllata dagli Americani e le persone si guardano intorno alla ricerca di alternative», spiega James Lewis, direttore del programma di strategie tecnologiche al Center for Strategic and International Studies, a Washington.

Molte nazioni fanno spionaggio, anche se per ragioni diverse. Alcune utilizzano i malware per entrare nei computer dei dissidenti. Altre, come la Cina, praticano lo spionaggio industriale al fine di carpire segreti sugli aerei militari e sulle turbine eoliche. Le nuove tecniche di intrusione informatica si sono sviluppate al punto che due anni fa il generale Keith Alexander, allora direttore della NSA, rilevò «come il ciber-spionaggio stesse determinando il più grande trasferimento di ricchezze della storia». Secondo le sue stime, le aziende americane perdono 250 miliardi di dollari l'anno per il furto di proprietà intellettuale.

Questa situazione alimenta la tendenza a rivolgersi a reti più sicure o persino a disconnettersi. In una delle note seguenti, si parla di una piccola azienda impegnata sul fronte dell'energia, per cui i cavi di rete sono come i capelli di Medusa. L'azienda è preoccupata al punto da conservare le sue idee migliori su computer non connessi a Internet. Le tecnologie passate stanno guadagnando soldi e nuovi campi di intervento. Dopo le rivelazioni di Snowden, il servizio segreto russo ha ordinato macchine da scrivere e nastri per un valore di 15mila dollari, sostenendo che la carta garantiva un livello superiore di sicurezza per i documenti presidenziali.

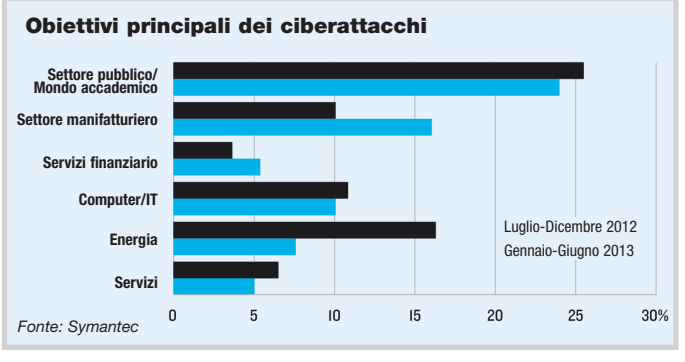
Gli esperti di sicurezza già da qualche tempo denunciano che le reti di computer non sono al riparo da intrusioni esterne. Ma nel 2013 si è capito che regna il caos. I governi scrivono i virus informatici e, se non possono farlo, li acquistano. Alcune softwarehouse, come la italiana Hacking Team, vendono sistemi di intercettazione ad agenzie statali in grado di penetrare silenziosamente un computer, per poi prenderne il controllo e monitorarne le attività.

I criminali sfruttano le debolezze dei computer per attaccare quante più macchine possibili. I governi, invece, mettono insieme gruppi di ricercatori e spendono cifre considerevoli per raggiungere

Immagine: Daniel Zender

passo dopo passo obiettivi definiti. Costin Raiu, un ricercatore di Kaspersky che indaga su queste "minacce tecnologiche persistenti", confida di collegarsi al suo computer sapendo perfettamente che non è solo. «Parto dal principio che il mio computer è sotto il controllo di almeno tre governi», dice Raiu.

Questa è la principale minaccia che le aziende tecnologiche stanno fronteggiando. Il governo americano ha aggirato le misure di sicurezza di Google e ha raccolto segretamente i dati degli utenti. Le spie inglesi hanno collezionato milioni di immagini di webcam da Yahoo. A dicembre, sul blog ufficiale di Microsoft, l'avvocato generale dell'azienda, Brad Smith, ha sostenuto di avere ottime ragioni per ritenere le intercettazioni segrete governative alla stregua dei malware criminali. Microsoft, insieme con Google e Yahoo, ha reagito rafforzando i suoi sistemi di crittografia. «Stiamo vivendo un passaggio storico molto particolare, in cui le aziende si ritrovano a essere pedine recalcitranti di una guerra cibernetica», afferma Menny Barzilay, un ex funzionario dell'intelligence israeliana che ora si occupa della sicurezza IT per il Bank Hapoalim Group, a Tel Aviv. In questo nuovo contesto, non si capisce più dove finiscano le responsabilità di un'azienda e comincino quelle di una nazione. Una banca commerciale dovrebbe investire risorse per difendersi se chi la sta attaccando è un paese? «Non si parla di una situazione "possibile". Sta accadendo veramente», dice Barzilay. «E non è che l'inizio».



Le rivelazioni di Snowden hanno offerto il quadro di una Internet USA-centrica. Ora la gente è alla ricerca di un'alternativa.

L'inaffidabilità di Internet che conseguenze può avere sul commercio? Si prenda il caso di Huawei, l'azienda cinese che lo scorso anno ha conseguito la leadership mondiale nella vendita di apparecchiature per le telecomunicazioni. La sua quota di mercato statunitense è esigua, perché il governo ha da tempo denunciato che le apparecchiature di Huawei sono il cavallo di Troia dell'intelligence cinese. Le aziende americane come Cisco Systems dicono che i loro clienti cinesi si stanno allontanando per la stessa ragione. D'altronde, i documenti resi pubblici da Snowden indicano quanto vigorosamente la NSA si sia impegnata a inserire backdoors per aggirare i sistemi di sicurezza in apparecchiature, computer e cavi sottomarini, in alcuni casi in collaborazione con quelli che l'agenzia definisce «significativi rapporti di collaborazione con partner industriali», identificati da nomi in codice.

La diffidenza sta anche creando opportunità commerciali. In un'altra delle note che seguono si parla di un vecchio bunker in Svizzera che gli imprenditori locali hanno trasformato in una "fattoria" di server, sperando di replicare per i dati ciò che gli Svizzeri hanno fatto una volta per l'oro dei nazisti e i conti in banca per i miliardari. Grazie alla legislazione sulla privacy e a una cultura radicata della riservatezza, il paese sta diventando il polo d'attrazione delle tecnologie avanzate per la sicurezza. Secondo Lewis, questo tipo di iniziative tecnologiche minacciano la leadership americana in servizi Internet come l'archiviazione remota dei dati: «Non è trascorso un tempo sufficiente per capire quanto siano serie le conseguenze economiche, ma la comparsa della concorrenza straniera è un segnale che lascia pensare a un fenomeno grave».

C'è anche da registrare un cambiamento in corso nelle abitudini dei consumatori, che si stanno rivolgendo con sempre maggiore frequenza ad applicazioni testuali, come il servizio di messaggistica istantanea Snapchat, che fa scomparire i messaggi dopo alcuni secondi. L'utenza opta per gruppi di discussione anonimi, come Whispr, e compra "criptotelefoni" che criptano le chiamate. Gli spy-shop godono di grande popolarità. Phil Zimmermann, uno strenuo difensore del diritto alla privacy, ha contribuito alla creazione di uno di questi criptotelefoni, il Blackphone (629 dollari) presentato a febbraio al Mobile World Congress, a Barcellona, in Spagna.

Queste sono le conseguenze delle rivelazioni di Snowden sul mondo commerciale. Le persone si fanno domande sui prodotti tecnologici e le aziende del settore, che prima non si erano mai fatte. La connessione è sicura? Di che paese è l'azienda? «Qualcosa è cambiato da quando sono filtrate le prime indiscrezioni sulle intercettazioni», dice Mikko Hypponen, responsabile della sicurezza dell'azienda finlandese F-Secure. «Prima, l'idea era che il Web non avesse confini. Si trattava di un'utopia. Ora ci siamo svegliati». ■

Antonio Regalado è responsabile dell'area affari di MIT Technology Review USA.

I segreti dell'energia

Gli hacker sono alla ricerca di dati sulle tecnologie d'avanguardia dei giacimenti di petrolio.

Kevin Bullis

Facendo una visita a 1366 Technologies, una startup vicino a Boston che sta sviluppando un sistema a basso costo per la produzione di celle solari, si possono ammirare larghi spazi aperti suddivisi in piccole postazioni, con ingegneri alle loro scrivanie, una officina meccanica e un'attrezzatura per il controllo dei wafer al silicio. Ma è quello che non si vede a essere veramente interessante. In un'altra parte dell'edificio – con un'entrata nascosta – siedono gli ingegneri che lavorano al cuore della tecnologia e si trovano macchine che potrebbero dimezzare il costo dei wafer di silicio per le celle solari. Inoltre, ancora più importante, i computer utilizzati in questa sala nascosta non sono collegati a Internet. «Siamo quasi paranoici», dice il CEO Frank van Mierlo. «Abbiamo messo off-line tutti i server legati alla progettazione, isolandoli dalle reti non protette, come il Dipartimento della Difesa».

Di recente, si è molto parlato a Washington della necessità di proteggere le infrastrutture critiche, come le centrali nucleari, da possibili ciberattacchi nemici. Ma le aziende del settore energetico dicono che le loro invenzioni chiave e i dati commerciali sono già nel mirino delle azioni di ciberspionaggio.

Gli attacchi possono passare inosservati per anni o non venire mai scoperti. Il risultato è che le stime sui furti di proprietà intellettuale variano «così tanto da non avere significato», secondo un rapporto del 2011 sul ciberspionaggio straniero del Director of National Intelligence, che cita cifre oscillanti tra i 2 e i 400 miliardi di dollari l'anno.

Alcuni hacker stanno cercando di accedere ai dati protetti sui giacimenti petroliferi, raccolti faticosamente utilizzando costose indagini sismiche, che sottendono un giro d'affari di circa 3 trilioni di dollari l'anno. Poche aziende ammetteranno di essere state vittime dello spionaggio. Una che lo ha fatto è stata American Superconductor. Nel 2011, l'azienda del Massachusetts ha intentato causa al suo migliore cliente, il cinese Sinovel, produttore di turbine eoliche, sostenendo che gli aveva trafugato la sua tecnologia chiave, un sistema per rendere più semplice l'integrazione delle turbine eoliche con la rete elettrica. In agosto, un grand jury federale ha incriminato Sinovel, asserendo che l'azienda cinese avrebbe offerto denaro a un dipendente di American Superconductor per indurlo a trasmettere per e-mail il codice sorgente della tecnologia alla Cina.

La vicenda mostra come spesso il furto della proprietà intellettuale non si affidi solo a sofisticati attacchi informatici, ma anche a personale interno. Tutto ciò giustifica le precauzioni prese da 1366. ■

Kevin Bullis è responsabile dell'area energia di MIT Technology Review USA.

Minaccia invisibile

I recenti ciberattacchi alle aziende del settore energetico sono rimasti senza colpevoli

	Anno della scoperta	Probabile fonte	Obiettivo
Stuxnet	2010	USA/Israele	Impianti nucleari iraniani
Night Dragon	2010	Cina	Dati sull'esplorazione petrolifera
Energetic Bear	2012	Federazione Russa	Aziende del settore energetico in 10 paesi
Shamoon	2012	Hacktivisti	Computer della Saudi Aramco

Fonte: McAfee, Crowdstrike, MIT Technology Review.

Huawei, prima e dopo

La storia travagliata dell'azienda di telecomunicazioni cinese è un esempio dei danni connessi allo spionaggio.

Antonio Regalado

Quanto è difficile per un'azienda cinese vendere in un altro paese? In America, i rappresentanti commerciali di Huawei offrono apparecchiature per le telecomunicazioni di ottima qualità con uno sconto del 35 per cento. Ma ogni volta che stanno per concludere una vendita, i loro clienti ricevono una visita da parte del FBI o del Dipartimento del Commercio statunitense. Il messaggio da parte dello Stato è inequivocabile: comprate qualcos'altro.

Huawei, con sede centrale a Shenzhen, in Cina, è il più grande venditore al mondo di apparecchiature per le telecomunicazioni, con una quota di mercato del 20 per cento. Tuttavia, occupa una posizione solo marginale in Nord America, dove la sua quota di mercato nelle apparecchiature ottiche raggiunge solo l'1,4 per cento e nei commutatori e router scende addirittura allo 0,1 per cento.

Così come Huawei è stata emarginata dal mercato americano, allo stesso modo le rivelazioni sulle intercettazioni su larga scala effettuate dalla NSA e da altre agenzie d'intelligence statunitensi potrebbero creare dei seri problemi al commercio americano all'estero.

Huawei è stata fondata nel 1987 da Ren Zhengfei, ex ufficiale militare che condivide il suo ruolo di CEO con altri dirigenti che ruotano ogni sei mesi. Appena si è spostata all'estero, Huawei è stata subito al centro delle polemiche, soprattutto negli Stati Uniti. Il suo tentativo di acquistare 3Com, leader nell'ambito del networking, è stato bloccato da una commissione per gli investimenti esteri sul territorio americano, che lo ha considerato pericoloso per la sicurezza nazionale.

Nel 2012, in parte dietro richiesta della stessa Huawei, l'House Intelligence Committee statunitense ha compiuto delle indagini e ha stilato un Rapporto in cui non c'era alcuna prova reale di spionaggio, anche se si concludeva affermando che gli Stati Uniti devono "guardare con sospetto" i progressi

delle aziende cinesi nel mercato delle telecomunicazioni del Nord America.

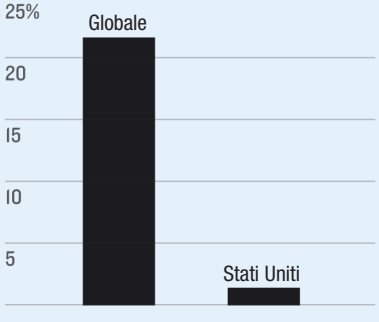
La preoccupazione era che in qualche modo, con la complicità di Huawei o senza, il governo cinese potesse utilizzare le apparecchiature vendute dall'azienda per spiare o per guadagnare dei vantaggi nella ciberguerra. Huawei ha sempre negato con forza le accuse, parlando di "discriminazione".

L'aspetto paradossale della situazione è che ora le rilevazioni sulle attività della NSA hanno ribaltato completamente i ruoli. I documenti indicano che gli Stati Uniti potrebbero avere manomesso i router di Cisco, Juniper e Huawei. Emerge, inoltre, la manipolazione dei codici crittografici del software commerciale. Tutte le aziende coinvolte in queste rivelazioni dichiarano di non averne mai saputo nulla e di stare investigando per capire cosa è successo. Ma la mancanza di fiducia sta investendo le aziende americane. A dicembre, Cisco ha detto che le accuse hanno determinato una significativa caduta delle vendite in Cina.

Huawei si può sentire vendicata, ma solo in parte. Le sue vendite non sono mai decollate negli Stati Uniti e anche qualche paese europeo potrebbe ridiscutere la sua posizione rispetto all'azienda cinese. In diversi documenti ufficiali, Huawei ha indicato che per migliorare la sicurezza è necessario adottare standard comuni e, forse, controlli di autorità indipendenti. Ma il pericolo maggiore potrebbe essere la diffusione del protezionismo. Oggi, con la crescita delle preoccupazioni per la sicurezza, i paesi potrebbero cogliere l'occasione per alzare barriere contro la concorrenza straniera o rafforzare le industrie nazionali. ■

Fuori gioco

La sfiducia nei confronti della Cina limita le quote di mercato di Huawei



Fonte: Ovum; in riferimento alle attrezzature ottiche per telecomunicazioni.

Sicurezza: l'oro svizzero

Il sistema adottato dalla Svizzera per garantire la sicurezza dei dati è tra i più sofisticati al mondo.

Russ Juskalian

La protezione dei dati è una cosa, la protezione dei dati in Svizzera è qualcosa di completamente diverso. La differenza mi è stata spiegata da Stéphan Grouitch in una sala conferenze nel cuore delle Alpi svizzere, con il sottofondo del ronzio di una illuminazione sotterranea fluorescente.

«Il paese ha sempre custodito valori per i cittadini di tutti gli stati europei, ancor prima del denaro», dice Grouitch, CEO di Deltalis, l'azienda proprietaria del bunker. La prima volta che ha dichiarato il suo interesse all'acquisto della struttura militare svizzera, Deltalis aveva in mente di custodirvi lingotti d'oro. Invece, ora vi ha collocato una batteria di server nei quali sono salvaguardati dati protetti da rigorose leggi sulla privacy e da una tradizionale cultura della discrezione.

Del ruolo svizzero nella protezione dei dati si parla già da circa un decennio, soprattutto in riferimento al settore bancario. Ma le controversie sulla sorveglianza globale suscitate dalle rivelazioni sulla NSA hanno rappresentato un "passaggio in avanti decisivo", afferma Franz Grüter, CEO di Green, un provider di servizi Internet il cui centro dati d'avanguardia nel comune di Lupfig è stato riempito "con un anno d'anticipo" rispetto ai tempi previsti.

Per capire la posta in ballo, è sufficiente pensare alle perdite previste che l'industria statunitense di servizi cloud (tra cui aziende del calibro di Google, Microsoft e IBM) si trova ad affrontare a causa della preoccupazione e dell'indignazione per le intercettazioni americane. Le stime delle quote di mercato perse fino al 2016 variano da 35 a 180 miliardi di dollari (secondo Forrester Research).

La Svizzera non è l'unico paese che spera di trarne vantaggio. La finlandese F-Secure ha di recente prodotto Younited, un diretto concorrente di Dropbox. Un consorzio di aziende di telecomunicazioni statunitensi, ISPs, e i provider di e-mail stanno sostenendo un programma per "e-mail made in Germany" che vuole mantenere, se possibile, l'archiviazione e l'instradamento dei dati all'interno del paese. A febbraio, il Cancelliere tedesco Angela Merkel ha partecipato ai colloqui di Parigi sulla costruzione di una rete di comunicazioni esclusivamente europea per evitare che "si inviino e-mail e altre informazioni oltre Atlantico".

Le aziende europee, secondo Grüter, prestano ora un'attenzione costante all'archiviazione fisica dei dati, e declinano le offerte americane. Un esempio di questa nuova tendenza è rappresentato dalla formazione, in Svizzera, di un gruppo di aziende private impegnate sul fronte della difesa della privacy. ID Quantique ha prodotto Centauris CN8000, uno dei primi sistemi commerciali di crittografia che utilizza la meccanica quantistica.

Richard Straub, responsabile per lo sviluppo del mercato a ID Quantique, sostiene che le innovazioni svizzere sono spalleggiate dalle ricerche condotte in università importanti come EPFL, a Losanna, ETH-Zürich e l'Università di Ginevra. Una spinta significativa viene anche dalla domanda locale. Quando ID Quantique ha commercializzato i suoi prodotti, ha subito trovato clienti nell'ambito governativo e del settore bancario.

Quindi a chi altri affidare i dati? Grouitch ritiene che la risposta non possa che essere una: «La Svizzera è il caveau al centro dell'Europa». ■

Russ Juskalian collabora con varie riviste di scienza e informatica.


La sede della Deltalis.