il FRIULI
Dir. Resp.: Bertoli GIovanni
Tiratura: n.d. Diffusione: n.d. Lettori: n.d.
Edizione del: 02/08/14
Estratto da pag.: 7
Foglio: 1/2

Attenti al Grande fratello globale!

Siamo tutti spiati - Marino Miculan, docente di Reti di computer all'ateneo friulano, racconta i rischi che corriamo in Rete

» DI **HUBERT LONDERO**

Quanto sono sicuri i nostri dati sensibili nella Rete? Considerando le notizie sui sistemi informatici, verrebbe da dire "ben poco". Basti pensare allo scandalo Datagate del 2013, all'allarme lanciato dall'Autorità garante per la protezione dei dati personali, che riferisce come ci sia un enorme 'buco' nella sicurezza delle telecomunicazioni italiane. Senza contare le 'falle' dei database della Sanità regionale emerse nei mesi scorsi. Abbiamo domandato al professore **Marino Miculan**, docente di Reti di calcolatori all'Università di Udine, quali siano i rischi che corriamo.

Che controllo possiamo avere sui nostri dati sensibili?

"Per lo più, sono fuori dal controllo del singolo. Ci sono ovunque enormi quantità di dati sanitari, amministrativi, fiscali e informatici, conservati da enti pubblici e privati, dei quali siamo proprietari, ma non titolari del loro trattamento. E, spesso, non sono al sicuro. In alcuni casi, ciò è dovuto alla sottovalutazione del problema sicurezza da parte di chi ha il compito di gestirli. In altri, i database vengono violati non perché la 'porta' è stata lasciata negligentemente aperta, ma a causa di 'bachi' nel software o della bravura di chi viola le misure di sicurezza".

Come si crea questa massa d'informazioni che ci riguarda?

"Una parte viene normalmente raccolta e conservata dalle strutture sanitarie, amministrative e fiscali. Un'altra parte la lasciamo noi".

In che modo?

"Banalmente, utilizzando i motori di ricerca. Quando immettiamo le parole chiave, tali termini sono tenuti in memoria e ci vengono attribuiti e lo stesso accade ai contenuti che inseriamo sui social network. Persino le smart tv mandano informazioni su ciò che guardiamo".

Cosa possiamo fare?

"Possiamo adottare piccole contromisure, che però lasciano il tempo che trovano. Per esempio, possiamo usare motori di ricerca alternativi a Google. Per quanto riguarda ciò che viene immagazzinato dagli enti pubblici, non resta che fidarci. Loro hanno la responsabilità, anche penale, della custodia di tali informazioni. Resta da capire quanto siano bravi a difendere le banche dati. Nel caso della posta elettronica (si legga l'articolo sotto, *ndr*) possiamo utilizzare sistemi di cifratura. Ce ne sono di abbastanza collaudati e robusti. Tuttavia, questi accorgimenti hanno un costo".

Dobbiamo sborsare soldi?

"La sicurezza ha sempre un costo, che può non essere economico. Può essere pagato in termini di facilità d'uso e comodità. Restando in tema di posta elettronica, chi riceve la nostra mail cifrata, dovrà avere le chiavi per aprirla. L'unico computer sicuro è quello scollegato dalla rete, ma paghiamo la tranquillità in termini di servizi non usufruiti".

A chi interessano le informazioni sul singolo cittadino?

"Alle agenzie di sicurezza di tutto il mondo. Per esempio, se sui social network parlo di cifratura o di altri argomenti sensibili, sono segnalato alla Nsa (potrei essere un terrorista). Se, poi, faccio ricerche più approfondite su tali temi, su di me viene aperto un dossier virtuale. Questo non è per forza un male. Tanti attacchi terroristici sono stati sventati in questo modo. Tuttavia, se le agenzie di sicurezza appartengono a Paesi non democratici, le tecniche serviranno a controllare i cittadini. Sappiamo che in Cina, per ogni 8 persone che navigano in Internet, ce n'è una che monitora la loro attività e impedisce l'accesso a informazioni 'meritevoli di censura'. Insomma, il prezzo che paghiamo è altissimo".

La cosa peggiore che ci può capitare?

"Le rispondo raccontandole cos'è successo a un collega, che aveva tenuto contatti on-line, peraltro del tutto leciti, con individui 'sgraditi' alle autorità statunitensi. Quando questo mio conoscente si è recato negli Usa, è stato fermato all'aeroporto e gli è stato chiesto di tornare indietro. Poi è riuscito a chiarire la sua posizione, ma a fatica. Insomma, se parli con qualcuno non gradito alle agenzie di sicurezza americane, puoi diventare sgradito a tua volta ed essere schedato. E senza aver fatto nulla di male".

E oltre agli 007 di tutto il mondo, a chi interessiamo?

"A tante aziende. I nostri dati (chi li raccoglie, li può vendere ad altre società) possono essere impiegati in maniera aggregata per previsioni statistiche, per cucirci su misura la reclame o per organizzare campagne pubblicitarie mirate. Se so che a in una località si consuma prevalentemente il prodotto di una determinata azienda, le imprese concorrenti avranno tutto l'interesse a 'colpire' di messaggi quella popolazione e non altre, risparmiando sui costi. Ciò accade anche con le tessere fedeltà dei supermercati: in cambio di un piccolo sconto, 'vendiamo' i dati che ci riguardano".

Ognuno di noi, insomma, ha un prezzo e un valore?

"Sì. E la cifra dipende dalla quantità di relazioni che abbiamo, dalla nostra attività in Rete o dal tipo di informazioni. I nostri dati sanitari, per esempio, sarebbero una manna

Peso: 87%

per le assicurazioni. Se queste vengono a sapere che nella tua famiglia c'è una certa tara ereditaria o che hai avuto alcuni problemi di salute, ti proporranno una polizza più o meno costosa, ottimizzando costi e rischi. Anche in questo caso, ci possono essere lati positivi. Se installiamo un sistema gps sull'automobile, avremo uno sconto sul premio assicurativo. E, se teniamo un comportamento lodevole alla guida, potremmo avere ulteriori benefici economici. Resta tuttavia in piedi la questione etica".