Warm war: la guerra tiepida ai tempi di internet

di Raffaele Danna

03-11-2016

La temperatura di esercizio di una normale CPU oscilla fra i 45 e i 75°C. Né caldo né freddo: tiepido. Una temperatura modesta, meno evocativa del "freddo" della seconda metà del secolo scorso, ma non per questo meno rilevante dal punto di vista delle possibili conseguenze.

A partire dagli anni Novanta la popolazione degli utenti di internet[1] è aumentata vertiginosamente. Stando ai dati Onu, nel 1995 le persone che avevano accesso alla rete erano meno dell'1% della popolazione mondiale. Oggi più del 40% degli abitanti del pianeta, vale a dire più di tre miliardi di persone, gode di un accesso stabile a internet. Si tratta di un incremento vertiginoso avvenuto nel giro di un ventennio, e il dato è in continua crescita.[2]

Internet garantisce una disponibilità immediata di informazioni e servizi a una popolazione di utenti in continua espansione. La crescita degli utenti alimenta l'aumento dei servizi, i quali a loro volta attirano un maggior numero di utenti in una sorta di circolo. Svariati settori sono stati radicalmente ristrutturati in seguito all'avvento della rete (edizioni online dei quotidiani, film e serie tv disponibili in streaming, siti di prenotazioni, social network, servizi di navigazione, di ricerca, telecomunicazioni, internet banking, pagamenti, transazioni...). Una cifra caratteristica dell'informatizzazione è la disintermediazione, vale a dire l'annullamento delle distanze spaziali e temporali. Si tratta di un cambiamento profondo, che sta iniziando a mostrare le sue conseguenze anche su alcuni elementi portanti della nostra società, dal mondo del lavoro (la cosiddetta 'on-demand/gig economy'), alla politica (in cui la disintermediazione sta trasformando le dinamiche dell'opinione pubblica, la struttura dei partiti, le forme della comunicazione politica), alla produzione (la cosiddetta 'quarta rivoluzione industriale').

Internet sta infatti entrando sempre più profondamente nella nostra quotidianità. Soprattutto a partire dall'avvento degli smartphone, la quantità di informazione prodotta e registrata sul web è aumentata esponenzialmente, tanto che si stima che negli ultimi due anni siano stati prodotti più dati che in tutta la precedente storia dell'umanità: [3] l'avvento dei big data è senza dubbio uno dei grandi cambiamenti degli ultimi anni. Il secondo fattore all'origine della forte crescita di dati prodotti e salvati su internet è il cosiddetto Internet of Things (IoT). Un numero crescente di oggetti (dagli elettrodomestici, alle abitazioni, ai macchinari, agli impianti, ai veicoli) viene dotato di dispositivi in grado di rilevare informazioni e di condividerle attraverso la rete. L'Internet of Things è a sua volta alla radice di un cambiamento profondo nei modelli di organizzazione della produzione, vale a dire il cosiddetto 'smart manufacturing' o 'industria 4.0'. Grazie all'utilizzo di macchinari, impianti e piattaforme di gestione collegate fra loro in cloud, è oggi possibile conoscere in tempo reale, anche da uno smartphone, lo stato della produzione, la performance, la produttività, le scorte e gli ordini di ogni impianto di un intero gruppo industriale, indipendentemente dalla posizione geografica dell'impianto e dell'utente, con la possibilità sia di 'zoommare' sui singoli macchinari sia di avere dati aggregati aggiornati.

L'era di internet, che sta iniziando a mostrare le sue cifre caratteristiche, è caratterizzata dalla preminenza dell'informazione come asset. Tale informazione viene organizzata in reti, spesso

monopolistiche (Google, Facebook, Amazon), talmente pervasive da obbligare chi non ne fa parte a entrarvi controvoglia, dato che la maggior parte dei suoi contatti si aspettano di poterlo contattare attraverso di esse. L'informazione viaggia su queste reti in tempo reale, eliminando virtualmente la distanza spaziale, diventando dunque globalmente disponibile e abbattendo drasticamente i costi di transazione. Diverse informazioni, anche preziose o riservate, non vengono più conservate in ambienti isolati, ma sono collocate all'interno di ambiente integrato che le rende continuamente accessibili e, soprattutto, intimamente connesse fra loro. Nel caso di informazioni riservate esistono naturalmente delle misure di sicurezza (password, PIN, one time password, etc.), ma è lecito domandarsi quanto tutto questo sia sicuro. Il controllo e il dominio dell'informazione - strumento di potere antico - assume forme nuove, e risponde a nuove logiche, come le logiche delle reti.

Continua a leggere - Pagina seguente

Pagina 2 - Torna all'inizio

Internet e la guerra tiepida

Da un punto di vista individuale, avere accesso all'identità e alle password di una persona significa poter entrare in controllo dei suoi social network, conoscere la rete dei suoi contatti, leggere le sue e-mail e i suoi messaggi, avere accesso al suo conto bancario, fare trasferimenti a suo nome etc. Avere accesso anche a una piccola parte di queste informazioni può costituire un asset molto prezioso, ma ciò che può risultare più preoccupante è che spesso, una volta ottenuto l'accesso a una parte di queste informazioni, può risultare abbastanza semplice riuscire a infiltrare numerosi altri dati, sia perché la maggior parte delle persone utilizza le stesse password e nomi utente per accedere a diversi servizi, sia perché alcuni dispositivi personali hanno in memoria i dati di accesso ai servizi stessi. Non sorprende dunque scoprire che esiste un trend consolidato e crescente di attacchi informatici. La Financial Fraud Action UK ha stimato un aumento del 25% di simili frodi informatiche nei primi 6 mesi del 2016 rispetto all'anno precedente, per una media di una frode ogni 15 secondi.

Dal punto di vista aziendale, la questione della sicurezza informatica è diventata di fondamentale importanza al crescere del livello di informatizzazione delle organizzazioni. Molto spesso i dipendenti utilizzano terminali che non sono collegati esclusivamente alla rete aziendale e che ricevono file da fonti esterne (memorie USB, allegati email, link, etc). La maggior parte dei gestionali

oggi lavora in cloud. L'industria 4.0 si fonda sull'utilizzo di tecnologie interconnesse. Tutto questo espone i database aziendali a possibili attacchi, dal momento che sempre più spesso anche alcune informazioni riservate vengono messe in rete, per quanto protette da sistemi di sicurezza sempre più sofisticati. La conseguenza naturalmente è l'evoluzione dello spionaggio industriale, il quale si è ormai essenzialmente trasformato in cyber-spionaggio. Naturalmente questo genere di spionaggio richiede un livello di sofisticatezza, di competenza e di strumenti incomparabile rispetto al furto dei dati di una carta di credito. È come passare da uno scippo al furto organizzato. Trovare informazioni riguardo a questi fenomeni è particolarmente difficile, dal momento che le aziende non hanno nessun interesse a rilasciare (e tutto l'interesse a nascondere) notizie intorno a simili casi. Da quello che trapela, tuttavia, si può affermare che il cyber spionaggio è un settore estremamente vivace e che esistono gruppi organizzati e specializzati nel furto e nella vendita di informazioni riservate. Uno dei grandi vantaggi del cyber spionaggio è la grande difficoltà a tracciare e rintracciare le spie, e anche per questo motivo si sospetta che diversi governi facciano ricorso a simili expertise, dato che è estremamente semplice negare ogni coinvolgimento in simili attività. Un caso spettacolare in questo senso è stato formulato l'anno scorso negli USA. Si tratta di un'accusa federale, contro cinque cittadini cinesi e il governo cinese sospettato di aver agito come loro sponsor, accusati di aver perpetrato una sistematica operazione di spionaggio industriale informatico ai danni di diverse aziende americane e tedesche.

Ma lo spionaggio informatico avviene con sempre maggiore frequenza anche su scala statale, tanto da essere diventato una componente fondamentale delle politiche di intelligence. Ovviamente, a questi livelli anche il grado di sofisticatezza delle misure di sicurezza è massimo. A parte i noti leaks di personaggi come Edward Snowden, i casi di attacchi informatici ai danni dei governi e di istituzioni stanno diventando sempre più interessanti e sofisticati dal momento che mirano a raggiungere informazioni estremamente preziose, come segreti di stato o database d'intelligence riservati (provate solo a immaginare che genere di informazioni devono essere in possesso di agenzie come la NSA). Un caso esemplare è quello di Stuxnet, un malware che sembra sia stato sviluppato dai servizi di intelligence americani e israeliani per sabotare il programma nucleare iraniano. Stuxnet riuscì a sabotare (fisicamente) un quinto delle centrali nucleari iraniane e comportò un radicale ripensamento dei sistemi di sicurezza informatica, dal momento che sfruttò dei bugs inediti e utilizzò delle debolezze strutturali dei sistemi di sicurezza di allora. Risale a pochi giorni fa un impressionante attacco ai danni dei server gestiti da Dyn, il quale ha reso difficile l'accesso a diversi siti, fra i quali Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud e il The New York Times. È particolarmente interessante notare che anche in questo caso l'attacco ha sfruttato un nuovo punto debole della rete internet americana, vale a dire gli oggetti IoT, dimostrando quanto potenzialmente vulnerabile sia il nostro sistema profondamente interconnesso. Per quanto questo attacco vi sia riuscito solo in minima parte, è chiaro che riuscire a impedire l'accesso al traffico internet a un paese profondamente informatizzato come gli USA significa gettare il paese nel caos per qualche ora. Mentre non è chiaro a chi si debba imputare questo attacco, sembra che l'attacco subito dalla rete tv francese TV5 sia dovuto a un gruppo di hacker russi. Sembra, infine, che i forti interessi russi nell'intromettersi nel complesso sistema delle elezioni presidenziali americane si stiano sfogando soprattutto sul terreno informatico. Il Democratic National Committe ha dichiarato di aver subito un attacco informatico ad opera di hacker russi i quali hanno sottratto informazioni in possesso del Democratic Party intorno a Donald Trump. In agosto, l'FBI ha dichiarato che due database del sistema di voto americano sono stati sottoposti a un attacco informatico proveniente dall'estero e ha emanato delle specifiche linee giuda di difesa e prevenzione.

Sembra insomma che, proporzionalmente all'espansione di internet, e di conseguenza

all'aumentare dell'informazione preziosa e/o strategica disponibile online, lo spionaggio e le guerre informatiche stiano diventando un terreno sempre più battuto. Le crescenti tensioni negli ultimi giorni fra blocco NATO e Federazione Russa hanno portato diversi commentatori a resuscitare il concetto di guerra fredda, ma forse in questo momento, più che in una nuova guerra fredda, stiamo entrando in un'era di guerra informatica, un'era di guerra tiepida. Un'era di logica delle reti, di sistemi globalmente connessi, di nuovi monopoli, di bassi costi di transazione, di lotta per il dominio e il controllo dell'informazione.

[1] Secondo l'agenzia delle Nazioni Unite ITU (International Telecommunication Unit), un "utente internet" è definito come un individuo in grado di accedere alla rete internet all'interno della propria abitazione attraverso un dispositivo fisso o mobile.

[2] Naturalmente, questi dati aggregati nascondono forti disparità regionali. Su scala continentale, il tasso di penetrazione va dall'89% della popolazione del Nord America al 28.7% della popolazione africana. L'Europa ha un tasso medio di penetrazione del 73.9%, andando dal 43.4% dell'Ucraina al 96.3% della Norvegia. L'Italia si colloca in una posizione intermedia, con un 62.0% della popolazione con un accesso stabile alla rete.

[3] Per avere un'idea della quantità di informazione che produciamo ogni giorno con uno smartphone, potete provare il seguente esperimento. Se avete un account Google, e non avete disattivato la cronologia della vostra posizione, provate a controllare su Maps-opzioni-cronologia.