Sos Internet

Autore: Giulio Meazzini
Fonte: Città Nuova

Gli attacchi hacker sono sempre più globali e frequenti, a causa della vulnerabilità del software. Tra guerre commerciali e strategiche, è la fine della Rete come strumento di libertà e condivisione?

La tendenza a rendere “intelligenti” gli oggetti del mondo è irresistibile. C’è un termine preciso a riguardo, “**Internet delle cose**”: basta inserire un programma software “dentro” un oggetto, per renderlo capace sia di comunicare su Internet la propria posizione e i propri dati, sia di leggere quelli degli altri oggetti. In questo modo le “cose” non sono più inerti, diventano invece capace di interagire, di operare autonomamente, ma anche di essere controllate a distanza. L’esempio più eclatante è il cellulare che, da oggetto utilizzato solo per telefonare, ora fa di tutto: gestisce posta elettronica, giochi in rete, foto, filmati, documenti, messaggistica, realtà virtuale e così via. Sono già disponibili la sveglia intelligente, che suona in anticipo se c’è molto traffico, o la confezione di medicine che lancia un allarme se dimentico di prendere la pillola mattutina. **Qualsiasi cosa può diventare “intelligente”**, quindi attiva e collegata in Rete. Ma c’è un lato negativo in tutto ciò: **inserire del software significa rendere l’oggetto vulnerabile (a distanza)**, perché le linee di codice possono contenere errori di programmazione, sfruttando i quali un malintenzionato può prenderne il controllo. Che sia una centrale nucleare o una scarpa da ginnastica intelligente, **qualsiasi oggetto collegato in Rete può essere “hackerato”**: tramite il collegamento internet uno sconosciuto può prenderne il controllo per fargli eseguire azioni impreviste. Come difendersi? Non è facile. Oggi qualsiasi strumento tecnologico è composto da una miriade di componenti prodotti da aziende diverse: il processore, il sistema operativo, la scheda video, i programmi software. Far colloquiare questi pezzi è molto complicato e gli errori sono frequenti. E poi bisogna considerare gli **inevitabili errori di programmazione** interni ad ogni componente. Basta pensare che Android, il sistema operativo contenuto nella maggior parte dei cellulari, ha 12 milioni di righe di codice, Windows 50 milioni, Google 2 miliardi! Controllare i programmi software per evitare errori costa, per cui molte aziende tirano via. Il risultato è che si va da un minino di 0,5 ad una media di **50 errori ogni mille righe di codice**. Quindi gli hacker devono solo trovare la falla per intrufolarsi, prendere il controllo dello strumento, e chiedere un riscatto per liberarlo. Pensiamo solo agli errori che ci sono sicuramente nel codice software che mantiene la riservatezza della nostra carta di credito in Rete. Vengono i brividi. A questo aggiungiamo che le grandi aziende che forniscono servizi in Internet costringono l’utente ad “accettare” (quasi sempre senza leggere) contratti capestro nei quali **declinano ogni responsabilità se qualcosa va storto** (anche in tema di sicurezza). Il fatto che gli attacchi informatici aumentano e sembra impossibile difendersi, sta convincendo tante aziende ad **assicurarsi** contro questi rischi. Con conseguente aumento dei costi. Ma l’utente finale chi lo tutela? Povera Internet! **Nata libera**, sulla base di un *gentleman agreement*, una specie di codice etico per cui ognuno condivideva la propria conoscenza liberamente e senza interessi privati, sta diventando sempre più teatro di guerre commerciali e strategiche tra Stati, aziende, hacker e polizie. E anche a livello privato la situazione non è molto migliore, con l’aumento degli scontri tra gruppi che si odiano (le famose **bolle**: vedi *Città Nuova* rivista n.7/2017). Cosa succederà: alla fine Internet verrà spezzettata, limitata, censurata, piegata agli interessi politici ed economici prevalenti? Perderemo questo **formidabile strumento di conoscenza e condivisione a livello planetario**?