

DIRITTI DOPO LO SCANDALO DEGLI ABUSI NEI CONTROLLI SULLE TELEFONATE

# Non c'è sicurezza senza privacy

DI GIGI TAGLIAPIETRA

*Come fare per promuovere anche nella rete un bene ormai considerato primario e fondamentale per la fiducia degli utenti*

Abraham Maslow, lo psicologo famoso per la sua teoria dei bisogni, sostiene che la sicurezza è un bene primario per ciascuno di noi, viene subito dopo il soddisfacimento dei bisogni fisiologici vitali. Sentirsi sicuri nell'ambiente che ci sta attorno è la condizione essenziale per poter sviluppare relazioni sociali, la condizione per apprendere, la condizione per la crescita delle aziende e della società. Il mondo digitale non fa eccezione alla teoria di Maslow e l'impressionante aumento degli attacchi informatici, delle truffe online, dei furti di identità rappresenta una minaccia estremamente seria per tutti perché la posta in gioco non è solo economica ed è molto più alta di quanto si pensi.

un perimetro che non esiste più (semai è esistito) e se ne sono accorte le banche con il fenomeno del phishing. Se a essere attaccati sono i loro clienti si scopre che diviene imperativo anche farsi carico della sicurezza di un "altro" che non appartiene strettamente all'azienda: se sono sicuro ma tutti i miei clienti non lo sono, il mio business svanisce.

Non è nemmeno possibile, con lo scenario che abbiamo di fronte, delegare la protezione ai "tecnici" o ai "cyberpoliziotti" perché, come in un ecosistema, qualunque approccio che non abbia un coinvolgimento diretto dei partecipanti in un identico approccio sistemico è destinato al fallimento.

Come indurre comportamenti virtuosi? Come fare perché la protezione della Rete sia qualcosa che condividiamo?

Si deve innanzitutto ripartire da un mondo di valori: se non si crede nel valore etico della privacy, della confidenzialità, del rispetto, non c'è tecnologia che possa proteggerci: un'informazione che parli di me è "un pezzo di me" e devo esigere che sia trattata con il massimo rispetto così come esigo rispetto assoluto per la mia persona fisica e per la mia intimità.

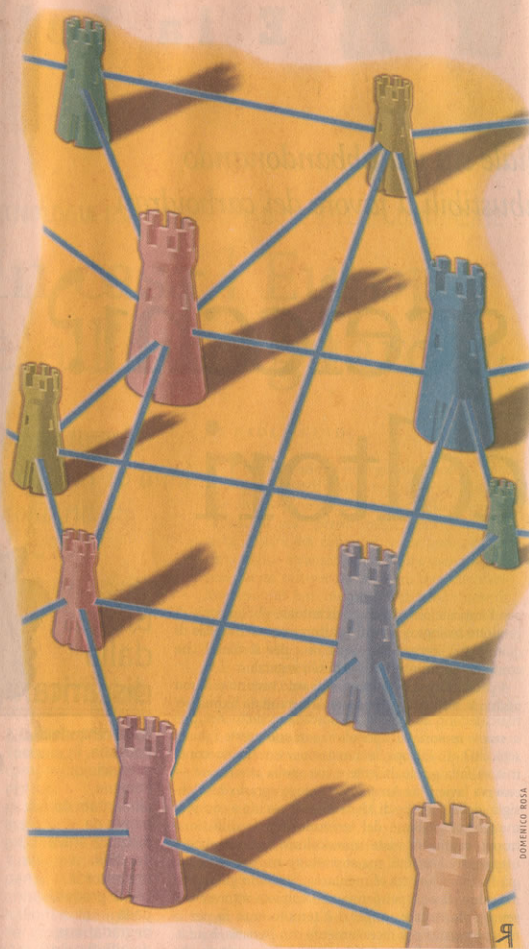
Non è vero che privacy e sicurezza siano concetti antitetici, che per avere più sicurezza si deve rinunciare all'intimità, è questione di rilevanza e di investimenti: se riteniamo che la privacy sia un valore supremo, investiremo risorse adeguate per trovare soluzioni che rendano sicuro un sistema salvaguardando la privacy degli interessati. Saranno soluzioni più costose ma quanto costerebbe altrimenti la perdita di fiducia da parte di tutti?

I vari scandali basati su intercettazioni telefoniche, le accuse di divulgazione di dati commerciali confidenziali, si inseriscono in questo contesto e aumentano la gravità della situazione per-

ché, a fronte di possibili reati che la magistratura dovrà provare e punire, si è scatenata una lotta di tutti contro tutti, con pesanti violazioni della privacy a dritta e a manca, del diritto alla dignità, della garanzia come condizione di coesistenza. Si sta cercando poi da un lato di scaricare sui singoli la responsabilità di attività che le organizzazioni hanno coltivato e incoraggiato con leggerezza e spregiudicatezza e dall'altro si vuole presentare l'idea che il custode della sicurezza sia uno spregiudicato mercante di segreti.

Chi si occupa di sicurezza ha una grande responsabilità non c'è dubbio, come ne ha il poliziotto o il magistrato e chiunque abbia il compito di mettere in atto regole e norme e di farle rispettare: la divisa o la toga non legittimano l'illegalità ma non sono nemmeno gli untori a cui dare la colpa dell'illegalità diffusa. Chi si occupa di sicurezza non deve avere solo competenze tecniche sia pure certificate, deve essere il portatore di un codice deontologico, farsi paladino del rispetto di principi etici che vengono prima dei bit e dei byte e che nei momenti di grande tensione, durante un attacco informatico, in presenza di un potenziale reato, alla richiesta di violare segreti, possano motivare scelte, comportamenti, decisioni, nell'impossibile discernimento oggettivo tra bene e male.

E chi controlla i controllori? Non un super controllore, non un'altra authority, ma la democrazia dei valori condivisi che ha retto in modo anarchico la rete fino a ora, la cosiddetta Netiquette, un codice autoimposto e condiviso, fortissimo perché imperativo ideale, fortissimo perché difeso da tutti, solido come la libertà.



## L'AUTORE



**Gigi Tagliapietra**, 52 anni, dal 1978 si occupa di reti di computer; nel 1983 è stato uno dei soci fondatori di Siosistemi (poi assorbita nel gruppo I.net). È presidente del Clusit e fa parte del comitato di certificazione del Lloyd Register e di Tuv Italia. Collabora con numerose Università e con le principali riviste di informatica italiane.

Come diceva John Thompson, Ceo di Symantec, nel suo discorso alla Rsa Conference lo scorso febbraio, la posta in gioco è «la fiducia», la fiducia delle organizzazioni nella Rete come infrastruttura solida e affidabile, la fiducia degli utenti nella Rete come ambiente sicuro e positivo. La fiducia non è un prodotto, non è un oggetto, non è un software o un servizio da dare in outsourcing: è un'emozione e proprio perché tale difficile da ottenere e facile da perdere. Preziosissima, perché se viene meno la fiducia non esiste relazione, non esiste commercio, non esiste crescita è la conclusione di Thompson.

La tecnologia della sicurezza cede il passo all'umanesimo della sicurezza. Con la crescita degli «Zero Day Attack», attacchi che sfruttano immediatamente vulnerabilità di cui non si ha conoscenza e di cui quindi non esistono antidoti informatici, non è possibile un approccio esclusivamente tecnologico sul modello "malattia-vaccino", servono sempre di più regole, attenzioni e consapevolezze che rientrano nelle categorie dei comportamenti umani virtuosi.

La protezione della Rete non è nemmeno un affare personale, la difesa di

Lo dicevamo dieci anni fa quando parlavamo di tutela dei minori, lo ripetiamo ancora più convinti oggi: la sicurezza nasce da regole che ci diamo liberamente per difendere valori etici a cui non possiamo rinunciare e non esiste valore economico con cui barattarle. In un mondo di valori condivisi e salvaguardati da ciascuno possiamo e dobbiamo poi agire concretamente mettendoci in moto il "think" e "act" che sono stati gli slogan iniziali della Rete. Le cose da fare non mancano anzi abbiamo ritardi gravi da recuperare per proteggere l'infrastruttura di rete del nostro Paese che in questi anni ha visto

aumentare in modo preoccupante il divario tra serietà delle minacce e livello dei sistemi di difesa.

Nell'ultima assemblea del Clusit sono state indicate le sei aree d'azione prioritaria in cui è necessario agire con tempestività vedendo nella sicurezza una funzione strategica che tutela una infrastruttura critica per l'intero Paese. Le sei aree sono: il quadro normativo, per dare leggi coerenti sulla security pubblica locale che gestisce dati vitali e i cui sistemi sono ad alta vulnerabilità; la rete a larga banda in cui non si promuove sicurezza ma solo velocità; il mondo delle imprese che devono essere aiutate a proteggere i propri sistemi; la tutela degli utenti più vulnerabili che vedono in primo luogo gli anziani; lo sviluppo di un'industria italiana della sicurezza per ridurre la nostra dipendenza e per avere soluzioni a misura di un sistema che ha caratteristiche specifiche.

Quello che è certo è che abbiamo una sfida molto importante di fronte e che non possiamo permetterci di perdere perché in caso di sconfitta non ci saranno vincitori, avremo perso tutti un bene prezioso.

## IN TRE PAROLE

- 1 La **fiducia** non è un prodotto o un software: se viene meno nella rete non esiste commercio e crescita
- 2 È **necessario** ripartire da un mondo di valori: senza un'etica della privacy non c'è tecnologia che tenga
- 3 Non **servono** neppure nuovi supercontrollori, bastano regole autoimposte e condivise, difese da tutti