



Phil Zimmermann è stato il creatore nel 1991 di **Pgp** (acronimo di Pretty Good Privacy – Riservatezza niente male), un software libero per la protezione dei documenti personali e per più di dieci anni è stato combattuto dal governo americano perché ritenuto pericoloso per la sicurezza nazionale. Negli Stati Uniti i software crittografici infatti sono stati a lungo considerati vere e proprie armi e per tale motivo la loro esportazione è stata soggetta a rigorose restrizioni. Il progetto Pgp di Zimmermann intendeva incorporare le codifiche **RSA** e **IDEA** rendendo più semplice e veloce la generazione e la gestione delle chiavi pubblica e privata in modo da consentire a chiunque l'utilizzo di sofisticate tecniche crittografiche per la protezione dei messaggi di posta.

Nel 1996 si passò dalla versione free del programma a quella commerciale, con la fondazione, da parte dello stesso Zimmermann, della società **Pgp Incorporated**, acquisita l'anno successivo da Network Associates (Nai). Il 19 febbraio 2001 Zimmermann abbandonò il progetto Pgp, uscendo dalla Nai per dedicarsi esclusivamente alla creazione di un nuovo consorzio chiamato **OpenPgp**, destinato alla creazione di un nuovo standard crittografico pubblico. Uscendo di scena, Phil Zimmermann pubblicò una lettera aperta a tutti gli utenti Pgp, garantendo che fino alla versione 7.0.3 il software era stato privo di **back doors**, ossia di password nascoste per una decodifica non autorizzata dei documenti cifrati.

Abbiamo quindi cercato il paladino della Privacy Phil Zimmermann per chiedere il suo parere su alcuni temi particolarmente critici nel nostro paese e fondamentali per i lavori della nostra commissione di studio.

MN: Durante il discorso di apertura che hai tenuto durante la scorsa edizione di Infosecurity 2002 hai dichiarato che le istituzioni dovrebbero imparare ad analizzare ciò che accade nell'ambito di uno specifico settore (per esempio quello dell'Information Technology), identificare comportamenti, regole di comportamento e quindi tradurli in leggi. Ma in questo modo non si corre il rischio di delegittimare la funzione delle leggi il cui compito è quello di guidare i comportamenti piuttosto che adattarsi ad essi? Puoi descrivere un caso in cui l'approccio da te suggerito abbia avuto successo?

PZ: Quello che intendevo dire è che dovremmo stare attenti ai pericoli derivanti da una regolamentazione applicata prematuramente. E' meglio prendersi il tempo necessario per esaminare come una tecnologia si adatta a una società e una società riesce ad adattarsi a una tecnologia prima di racchiudere tutto entro i limiti inflessibili di una legislazione, senza permettere al naturale processo di adattamento di terminare correttamente. Un esempio di quello che intendo dire è rappresentato dal problema della standardizzazione prematura. Per esempio, se gli Stati Uniti avessero aspettato solo una paio d'anni in più prima di procedere alla standardizzazione del TV Broadcast System, oggi negli USA avremmo una migliore qualità dell'immagine TV.

MN: Non pensi che PGP potrebbe essere utilizzato da malintenzionati per rendere inutilizzabili dati fondamentali o 'tenere in ostaggio' documenti aziendali?

PZ: Qualsiasi dipendente scontento può distruggere i dati aziendali con oppure senza l'aiuto di PGP. Cosa può impedirgli di formattare il disco fisso e distruggere tutti i dati in esso contenuti? Questi dipendenti potrebbero inoltre effettuare una copia di backup dei dati per 'tenerli in ostaggio' prima di procedere alla formattazione. Non ho bisogno della crittografia per fare quello che ho appena descritto. La crittografia non cambierebbe la situazione.

MN: Pensi che PGP potrebbe essere utilizzato anche per proteggere le comunicazioni Wireless?

PZ: Sì, e in effetti è già possibile. Esiste una versione di PGP per PDA. Gli utenti devono capire che ogni dispositivo wireless è, a tutti gli effetti, una stazione radio trasmittente e che la necessità di codificare e proteggere i dati è ancora più forte nell'ambito delle comunicazioni 'senza fili'. Nelle comunicazioni wireless è inoltre necessario adottare anche altri tipi di codifica come per esempio **SSL** e **IPSEC**, infatti la necessità in

tale ambito non è solo quella di proteggere i messaggi di posta elettronica.

MN: In Italia alcune istituzioni hanno iniziato a controllare alcuni luoghi pubblici come piazze e strade con telecamere. In molti pensano che tali iniziative costituiscano una sorta di violazione della privacy personale. Quale è il tuo parere in proposito?

PZ: Penso che l'espansione di una tecnologia di sorveglianza come questa può condurci a un terrificante futuro Orwelliano, specialmente quando dietro a tutto questo viene messo un computer per analizzare i dati, con l'utilizzo di algoritmi per il riconoscimento facciale e OCR per leggere le targhe delle macchine attraverso le telecamere per il controllo del traffico. La popolazione umana non raddoppia ogni 18 mesi, ma la Legge di Moore dice che la capacità dei computer di monitorarci sta invece raddoppiando ogni 18 mesi.

MN: Sicurezza e privacy. Due concetti collegati che, secondo alcuni sono in contraddizione tra di loro. Pensi sia effettivamente impossibile che possano coesistere?

PZ: Dipende dalla tua definizione di sicurezza. Io penso che la perdita di riservatezza in fondo non è altro che una minaccia alla sicurezza di una democrazia.

MN: E-government, dati personali e documenti in formato digitale, l'utilizzo sempre più frequente di sistemi informatici per la gestione delle tasse e dei dati personali: le società e le organizzazioni moderne sono ormai tutte basate su questi elementi. Pensi sia possibile combinare questo enorme aumento di strumenti informatici per il trattamento di dati sensibili con il concetto stesso di privacy? In caso di risposta affermativa come pensi sia possibile realizzarlo?

PZ: Penso esistano modi per applicare la tecnologia informatica a problemi di gestione dati su larga scala senza per questo perderne il riserbo. Per descrivere nel dettaglio questi modi dovrei scrivere almeno due pagine di testo e non penso che oggi ve ne sia il tempo. Solo un esempio: la moneta digitale anonima può essere utilizzata per effettuare pagamenti online, oppure le smartcard possono essere parimenti utilizzate per effettuare acquisti presso i punti vendita. Quelli appena descritti sono sistemi per raccogliere dati e utilizzarli solo per studi statistici e di marketing, senza che sia possibile comunque risalire alle abitudini d'acquisto di un singolo utente.