L’evoluzione della sicurezza informatica: la prospettiva del CERT-IT

Danilo Bruschi, Mattia Monga, Emilia Rosti
Università degli Studi di Milano
Dipartimento di Informatica e Comunicazione
Computer Emergency Response Team ITaliano

1 Introduzione

Il Computer Emergency Response Team ITaliano (CERT-IT, http://security.dico.unimi.it) è un gruppo di ricerca e attività sul campo del Dipartimento di Informatica e Comunicazione dell’Università degli Studi di Milano che, dal 1994, opera nel settore della sicurezza dei sistemi informatici. I Computer Emergency Response Team, talvolta anche detti Computer Security Incident Response Team (CSIRT) sono presenti in tutte le nazioni tecnologizzate. Essi nascono nell’intento di fornire un punto di riferimento qualificato per aiutare gli utenti di Internet appartenenti ad una data organizzazione o, come nel caso del CERT-IT, all’insieme nazionale degli utenti, a gestire i problemi legati alla sicurezza informatica. L’attività di consulenza permette loro di raccogliere molte informazioni privilegiate sulla natura degli attacchi (quale vulnerabilità è stata sfruttata, che attacco è stato portato a termine e con quali effetti), che risultano di grande interesse nella parallela attività di ricerca, tesa invece ad identificare modi e strumenti per rendere più sicuro l’uso dell’informatica nella vita quotidiana.

Nel 1995 il CERT-IT ha ottenuto l’affiliazione al Forum of Incident Response Team (FIRST, http://www.first.org) una comunità internazionale, formatasi in seguito al primo caso eclatante di incidente informatico, l’Internet Worm del novembre 1988, che ha lo scopo di coordinare gli sforzi dei gruppi che ne fanno parte, favorendo lo scambio di informazioni fidate e intraprendendo ricerche congiunte e attuando difese comuni nel caso di attacchi distribuiti. Attualmente il FIRST conta 136 membri, di cui una trentina di nazionalità differenti, e il CERT-IT è a tutt’oggi l’unico membro italiano.

In queste brevi note cercheremo di descrivere l’evoluzione storica delle problematiche legate alla sicurezza informatica durante il decennio in cui abbiamo operato nel settore.

2 La sicurezza informatica negli anni ‘90

2.1 Gli inizi

Lo scenario informatico degli anni ’90 era costituito soprattutto da mini-computer e workstation, il più delle volte collegate a Internet per mezzo di un indirizzo IP staticamente determinato. Gli intrusori agivano in un ambiente sostanzialmente omogeneo in cui i sistemi operativi Unix-like erano la grande maggioranza. Agli inizi del decennio in Italia i principali utilizzatori della rete erano le università e i centri di ricerca, le reti locali erano ancora alquanto eterogenee e l’uso domestico di Internet e del computer non era ancora stato immaginato. Oltreoceano la scena è più varia, ai centri di ricerca, accademici e no, si affiancano le grandi aziende. I servizi disponibili sulla Rete erano limitati essenzialmente alla possibilità di collegamento remoto ad un altro sistema, al trasferimento di file e alla posta elettronica. Nonostante l’esperienza traumatica dell’attacco del novembre 1988,

l'attenzione verso la sicurezza informatica intesa come problematica a sé stante degna di appropriati investimenti, anche nel settore della ricerca, era abbastanza limitata: l'approccio più diffuso era quello di ignorare il problema finché le circostanze non costringevano a prenderlo in considerazione.
L'insieme di questi due fattori (omogeneità dell'ambiente e scarsa attenzione delle vittime) contribuiva a formare una classe di attaccanti estremamente preparata contrapposta ad una classe di vittime molto spesso completamente indifese. L'attacco del resto finiva per essere in molti casi un *virtuosismo tecnologico*, volto più che altro a soddisfare il narcisismo degli attaccanti, che agivano peraltro nel contesto di un sostanziale vuoto legislativo (La prima legge italiana che configura specificatamente il reato di frode informatica è del 1993). L'attacco più diffuso era l'accesso non autorizzato con la conseguente compromissione del file delle password e dell'account di amministrazione. In questa situazione il ruolo dei CERT era soprattutto di sensibilizzazione e trasferimento tecnologico: gruppi di esperti di sicurezza *white hat*[1] che fornivano le proprie competenze a chi incappava nelle maglie degli intrusori. Conseguentemente, le segnalazioni ricevute dai CERT riguardavano soggetti del tutto impreparati in materia che chiedevano consulenze per allestire rimedi o anche solo per capire l'entità dell'incidente verificatosi. Comprensibilmente una delle principali richieste di tali soggetti era la riservatezza delle informazioni: nessuno di essi aveva piacere che fosse resa pubblica la propria inadeguatezza strutturale a rispondere agli attacchi verso i proprii sistemi informatici.

2.2 Il boom di Internet

A metà degli anni '90 lo scenario cambiò radicalmente grazie principalmente a due fattori:

1. l'introduzione del *word wide web*;
2. la disponibilità di sistemi operativi Unix-like open source come Linux e FreeBSD.

Il "web" venne immediatamente apprezzato come una modalità semplice ed efficace di condivisione delle informazioni e fornì a molti una ragione forte per connettersi a Internet. La disponibilità a costi irrisori di sistemi operativi di buona qualità[2] e in grado di gestire servizi di rete favorì la crescita della richiesta delle connessioni Internet, costringendo i produttori di sistemi operativi proprietari a fornire i medesimi servizi. Nel contempo si diffondono gli Internet Service Provider, i fornitori di connettività alla Rete, di cui fanno parte le grandi Telecom nazionali e piccole società nate sull'onda del boom, le une e le altre spesso ugualmente impreparate ad affrontare i problemi di sicurezza cui la connessione a Internet espone.
Il risultato netto di tale trasformazione dal punto di vista della sicurezza informatica fu uno scenario completamente nuovo:

- Grande varietà di ambienti e protocolli;
- Diffusione della figura del *provider*, che, pur fornendo la connettività ai propri clienti, non ha con essi alcun vincolo organizzativo;
- La gestione dei "server" smette di essere patrimonio dei soli operatori e sistemisti cresciuti nei centri di calcolo.

Nella giungla della tecnologia diventa più facile trovare uno spiraglio per scatenare un attacco e per portarlo a termine servono, mediamente, meno competenze. Alla figura dell'attaccante degli inizi, un po' sfuggente ma affascinante per la competenza tecnica che vi si cela, si aggiunge quella dei

[1] Si suole spesso distinguere in esperti di sicurezza black hat e white hat. I primi sfruttano le loro conoscenze per colpire gli utenti della rete, mentre i secondi mettono le loro competenze al servizio della comunità. Storicamente, come sempre accade fra buoni e cattivi, l'intersezione dei due gruppi non è mai stata nulla.
[2] E' bene ricordare a questo proposito il ruolo fondamentale del progetto GNU, portato avanti dalla Free Software Foundation, teso a fornire un'intera piattaforma informatica open source, dall'elaborazione di testi di tipo Unix, alle applicazioni di rete, sia lato client che lato server.

cosiddetti script kiddies, i ragazzini che scaricano dalla Rete programmi preconfezionati per portare a termine attacchi anche alquanto sofisticati. Qualcuno si limita a giocarci, quallcuno impara. La sicurezza informatica fa notizia e diventa un tema di ricerca di punta. Nel campo degli attacchi la novità che chiude il decennio ruggente di Internet e apre il nuovo millennio sono i cosiddetti attacchi Distributed Denial of Service (DDos) che compromettono la disponibilità di un servizio, sfruttando la complicità, spesso inconsapevole, di decine di macchine della rete. Nel febbraio 2000 uno di questi attacchi mette in ginocchio per varie ore grandi portali commerciali quali yahoo.com, amazon.com, e-bay.com. La sicurezza diviene uno dei fattori abilitanti per quella nuova attività che prende il nome di commercio elettronico, assai diffuso negli Stati Uniti e ai suoi albori nel nostro Paese.
Sono questi gli anni del boom della sicurezza informatica: non a caso il CERT-IT nasce e conosce i suoi momenti di massima prosperità, fornendo un centinaio di consulenze ogni anno. Gli incidenti di cui si occupa sono di vario tipo, dalla semplice segnalazione di attività di scansione delle porte ai casi di compromissione di server di grosse dimensioni, ad attacchi internazionali gestiti in collaborazione con altri CERT del FIRST in cui macchine del dominio .it vengono usate per "connection laundering" (l'eliminazione delle tracce che permettono di risalire all'origine di un attacco mediante l'uso di macchine intermedie) o come trampolino finale da cui lanciare l'attacco. I CERT sono chiamati a svolgere non solo il ruolo di sensibilizzatori ed educatori alla sicurezza, ma sopperiscono spesso alla mancanza di un supporto istituzionale alle vittime degli attacchi.

3 La sicurezza informatica negli anni 2000

Il contesto odierno è di nuovo differente. Da un lato l'opera di sensibilizzazione ha avuto effetto e gli utilizzatori di sistemi informatici sono oggi molto più attenti alla loro sicurezza e tutela della privacy di qualche anno fa. Gli strumenti, tecnologici e giuridici, sono aumentati significativamente. Si pensi, ad esempio, alla completa scomparsa delle connessioni *telnet*, ormai del tutto sostituite dalle più sicure *ssh*, e alla comparsa nelle legislature di vari paesi di leggi per la protezione dei dati personali gestiti con sistemi informatici, quali la Legge 675 in Italia.
D'altra parte, l'eterogeneità e la complessità degli ambienti è ulteriormente aumentata, aprendo nuove sottili possibilità di intrusione. La diffusione di connessioni radio (*wireless*) ha aperto nuovi fronti d'attacco di difficile difesa, in quanto intrinsecamente accessibili a tutti (*broadcast communication)*.
I pericoli per gli utenti di Internet, dunque, non sono affatto diminuiti. Ma la società odierna è assai meglio strutturata per difendersi. In Italia, per esempio, dal 1999 esiste una Polizia Postale e delle Comunicazioni, specializzata negli interventi legati a reati informatici. Le aziende sempre più spesso si dotano di esperti di sicurezza e di strutture organizzative atte a gestire le situazioni di attacco. I provider, anche grazie alla presenza di norme specifiche, sono sempre più abituati e disposti alla collaborazione con le forze dell'ordine nell'indagine dei reati informatici. La stessa Internet ha assunto una struttura molto più gerarchica, trasformandosi in una rete di isole ben protette e il più possibile inaccessibili dall'esterno (*intranet* e VPN). La diffusione ormai capillare dei prodotti open source e di prodotti commerciali immessi sul mercato ancora immaturi per battere la concorrenza su un tempo che la connessione globale fa scorrere più rapidamente ha abituato gli utenti all'idea di prodotti software sempre imperfetti, da mantenere continuamente con l'applicazione di *patch*[3]. Ciò nonostante, la maggioranza degli attacchi sfrutta comunque

[3] L'intrinseca imperfezione del software non è naturalmente legata alle modalità della distribuzione, ma alla sua complessità. La diffusione dei prodotti open source, però, ha abituato all'idea che *è normale* applicare una patch al proprio sistema, senza aspettare la prossima release, come invece accadeva nel modo dominato dal software

vulnerabilità ben note, ma a cui non si è posto (ancora) rimedio, nella continua ricorsa tra attaccanti e difensori.
In questo contesto il ruolo di consulenti svolto dai CERT autonomi (ossia non legati ad una specifica organizzazione) come il CERT-IT, si è notevolmente ridotto. Infatti, gli attacchi di un certo livello vengono generalmente segnalati direttamente agli organi istituzionali o, semmai, gestiti dalle strutture interne. La segnalazione degli allarmi è diventata attività troppo onerosa perché gruppi come i CERT no-profit riescano a dare un contributo sufficientemente tempestivo e accurato. Anche il contributo di CERT commerciali fortemente strutturati quali il CERT-CC della Carnegie Mellon University risente della estrema crescita delle segnalazioni e dell'accorciamento dei tempi di reazione, che fanno della tempestività la qualità primaria di un CERT.

4 Conclusioni

Conseguentemente, negli ultimi anni l'attività del CERT-IT si è per lo più rivolta verso la ricerca. Come già rilevato, l'ambiente Internet è oggi assai più complesso di quello con cui si aveva a che fare anche solo cinque anni fa. Risulta pertanto sempre più necessario sviluppare strumenti concettuali e metodologici per gestire tale complessità. E' necessario concordare standard metodologici a livello europeo ed internazionale. Occorre riflettere sui temi della sicurezza informatica fin dal progetto delle applicazioni ed abbandonare le soluzioni ad-hoc formulate a posteriori e studiare meccanismi di responsabilità nei confronti dei progettisti.
Inoltre l'impatto che la Rete tende ad avere sulla nostra vita quotidiana è sempre più ampio e risulta quindi urgente la maturazione di fondamentali principi tecnici che possano essere metabolizzati dall'intera società. Per esempio, si pensi alla giurisprudenza, per sua natura sempre "arretrata" rispetto al costume; gli esperti di diritto hanno grande difficoltà ad incasellare le problematiche di tipo informatico nelle categorie concettuali loro familiari. Devono cioè basare le loro considerazioni *giuridiche* su dati di fatto *tecnologici*, in perpetuo mutamento ed evoluzione e talvolta non del tutto noti nemmeno agli esperti del settore. Si pensi al caso emblematico delle cosiddette "prove informatiche" (*digital evidence)*, quando cioè un qualche dato informatico viene utilizzato come fonte di informazione in un processo ove vengano contestati reati informatici o reati "tradizionali" in cui gli accusati abbiano fatto uso di sistemi informatici a vario titolo. Attualmente è estremamente difficile stimarne obiettivamente l'affidabilità, mancando gli opportuni strumenti concettuali e spesso agendo in condizioni di informazione assai incompleta (Con quali modalità il dato è stato rilevato? Quali sono le specifiche hardware e software dei dispositivi di rilevazione?)
Un altro esempio interessante è la legislazione italiana in tema di *firma digitale.* Nel nostro ordinamento le firme digitali, al contrario di quanto avviene per le firme tradizionali, non sono ripudiabili: ciò significa che l'onere della prova è capovolto nei due casi e dovrà essere il firmatario a dimostrare la falsità della firma, ritenuto evento improbabile dal legislatore. In realtà è noto da tempo che i sistemi di firma digitale possono essere soggetti a compromissione se nelle operazioni necessarie non ci si è attenuti ad una ferrea disciplina. Inoltre, essendo tali sistemi realizzati con componenti software, non si possono ritenere immuni da errori di programmazione che potrebbero essere sfruttati per abusare del sistema da un malintenzionato.
Problemi analoghi sorgono ogni volta che le tecnologie informatiche coinvolgono la vita politica dei cittadini: sempre più numerose sono le iniziative di e-government e di voto elettronico. Ancora una volta, però, la valutazione dei rischi cui ci si espone introducendo la tecnologia in questi settori così delicati è assai difficile e diventa pertanto difficile compararne pregi e difetti con le procedure consolidate da secoli di pratica.

---

proprietario, dove una nuova release significava un nuovo investimento del cliente.

Voci per l’indice analitico
Sicurezza informatica
Computer emergency response team
Attacco informatico
Internet
Open source
Digital evidence
Reato informatico