ICT E DIRITTO

Rubrica a cura di

Antonio Piva e David D'Agostini

Scopo di questa rubrica è di illustrare al lettore, in brevi articoli, le tematiche giuridiche più significative del settore ICT: dalla tutela del *domain name* al *copyright* nella rete, dalle licenze software alla *privacy* nell'era digitale. Ogni numero tratterà un argomento, inquadrandolo nel contesto normativo e focalizzandone gli aspetti di informatica giuridica.

L'accesso abusivo ai sistemi informatici e telematici:
Aspetti giuridici e informatici di un attacco hacker

1. Criminalità informatica

Il progresso dell'ICT, oltre a portare indiscutibili benefici in ogni settore della società, ha sollevato alcune problematiche legate alla sicurezza dei sistemi di comunicazione e alla loro integrazione; in un contesto caratterizzato da un intrinseco elevato tasso di vulnerabilità, ha avuto terreno fertile lo sviluppo dei così detti *computer crimes*. Con questa espressione si vuole indicare una categoria di illeciti penali, in cui l'elaboratore può essere, da un lato, lo strumento per la consumazione del reato (si pensi alle frodi informatiche), dall'altro l'oggetto sul quale il reato stesso viene commesso (per esempio, nel danneggiamento informatico).
L'esigenza di disciplinare in maniera sistematica il settore della criminalità informatica, ha portato all'approvazione della legge 23 dicembre 1993 n. 547, con la quale è stato modificato il Codice penale italiano mediante l'aggiornamento di alcuni reati già esistenti e l'inserimento di altri completamente nuovi. Tra questi ultimi, l'art. 615 *ter* c.p. rubricato "*Accesso abusivo a un sistema informatico o telematico*", prevede che chiunque si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà, espressa o tacita, di chi ha il diritto di escluderlo, sia punito con la reclusione fino a tre anni.

2. L'accesso abusivo

I fenomeni di accesso abusivo costituiscono sul piano criminologico una categoria piuttosto eterogenea che, secondo la finalità perseguita dall'intruso, possono essere classificate in ipotesi meramente ludiche (hackeraggio) o in ipotesi che precedono la consumazione di altri reati dove all'accesso segua la distruzione di dati o il compimento di frodi, spionaggio industriale ecc..
L'intrusione informatica può concretizzarsi tramite l'accesso fisico al locale in cui è ubicato l'elaboratore, ovvero può essere compiuta in modo autonomo, mediante accesso da remoto, costituendo, in ogni caso, un fatto separato e distinto rispetto all'accesso fisico.
Le statistiche evidenziano come l'accesso abusivo sia compiuto in misura maggiore da personale interno all'organizzazione piuttosto che da estranei, dato estremamente significativo di cui tener conto sia nella progettazione e realizzazione di una rete aziendale che nella stesura di un'adeguata *policy* di sicurezza e di riservatezza dei dati.
Dal punto di vista giuridico, l'art. 615 *ter* (si veda il Riquadro 1), punisce alternativamente due condotte diverse:
a. l'introduzione abusiva in un sistema informatico o telematico protetto da misure di si-

Riquadro 1
Accesso abusivo a un sistema informatico o telematico: *reclusione fino a 3 anni*.
Se il fatto è commesso con abuso della qualità di operatore di sistema: *reclusione da 1 a 5 anni*.
Se il colpevole usa violenza su cose o persone: *reclusione da 1 a 5 anni*.
Se ne deriva il danneggiamento del sistema, dei dati o dei programmi: *reclusione da 1 a 5 anni*.

curezza, vale a dire l'operazione con la quale un soggetto, connettendosi a un sistema di elaborazione, acquisisce la possibilità di prendere cognizione di dati, informazioni e programmi, alterarli in tutto o in parte, cancellarli, aggiungerne dei nuovi; l'accesso abusivo, ossia fraudolento, si prefigura anche nel caso di formale proibizione o di semplice mancanza di autorizzazione;

b. il mantenimento nel medesimo contro la volontà, espressa o tacita, di chi ha il diritto di escluderlo. Infatti, un soggetto pur essendo autorizzato a entrare in un sistema, potrebbe mantenervisi indebitamente compiendo operazioni non autorizzate; ciò può accadere nei luoghi di lavoro nel caso di utilizzo temporaneo della postazione di un collega.

3. Le misure di sicurezza

In via del tutto generale, per poter punire il colpevole ai sensi dell'art. 615 *ter*, appare necessario che il sistema informatico o telematico attaccato sia protetto da misure di sicurezza, ove, in tale termine, sono ricomprese le misure tecniche, informatiche, organizzative, logistiche e procedurali che si frappongono al libero utilizzo di un sistema da parte delle persone non autorizzate come, per esempio, meccanismi di *autentificazione* degli utenti tramite opportune *password* o dispositivi biometrici, profili di autorizzazione, programmi *software* dedicati, *firewall* o altri apparati *hardware*, *server* chiusi a chiave ecc. (misure previste anche nell'allegato B, contente il disciplinare tecnico in materia di misure minime di sicurezza, del "Codice in materia di protezione dei dati personali", decreto legislativo 30 giugno 2003 n.196).

Se in una LAN è attiva la condivisione di tutti i dischi rigidi, non può essere condannato per accesso abusivo il dipendente infedele che vada a esplorare le risorse dei colleghi; il discorso si fa ancora più significativo nel caso di connessione da remoto allorché nell'elaboratore (in genere, un *server*) siano attivi processi e servizi, liberamente accessibili dall'esterno, tramite connessione a determinate porte, o siano configurati in maniera da consentire determinate operazioni senza richiedere particolari *permission* (basti pensare al Netbios sulla 138 e 139 ovvero all'FTP sulla 21, si veda il Riquadro 2).

Riquadro 2

Misure di sicurezza: un hacker si è introdotto nel sito telematico del GR1, sostituendo il *file* contenente l'edizione del giornale radio con un proprio file. Le indagini chiarirono che l'imputato aveva sfruttato una caratteristica tipica del sistema operativo Windows 95 sul quale risulta di *default* attiva la condivisione file e stampanti sul protocollo Netbios, senza richiesta di alcuna password; il giudice, pertanto, lo ha assolto.

Le misure di sicurezza predisposte devono, inoltre, essere effettive: non sarebbe sufficiente, per esempio, la semplice richiesta di *user name* e *password* fatta all'avvio dal sistema operativo se tali campi sono vuoti e, quindi, per accedere si rivela sufficiente la pressione del tasto "invio" (o, peggio, un click su "annulla", si pensi al Windows 95/98).

Risulta, quindi, fondamentale che i responsabili della sicurezza dei sistemi prendano cognizione delle tecniche utilizzate dagli hacker (sintetizzate nei successivi paragrafi) per porre in essere un attacco telematico e/o per effettuare un accesso abusivo, in modo da rendere effettive le contromisure di ordine tecnico e organizzativo, minimizzando i rischi di introduzione non autorizzata ai sistemi.

È d'obbligo, comunque, segnalare che la Corte di Cassazione ha ritenuto che la condizione determinante per la configurazione del reato, sia non tanto la presenza di misure di protezione interne o esterne al sistema, quanto l'aver agito contro la volontà di chi dispone legittimamente del sistema. Infatti, un sistema dovrebbe essere giuridicamente tutelato sempre e non solamente quando il titolare lo abbia dotato di *firewall* o di IDS (*Intrusion Detection System*).

4. Il footprinting

Il primo passo di un attacco telematico, posto in essere in maniera metodica, consiste nella ricerca del maggior numero possibile di informazioni sul potenziale obiettivo, al fine di determinarne il *footprinting*, ossia l'impronta, e quindi di ricostruire il suo profilo informatico e, in ultima analisi, il suo livello di protezione.

Tale fase ricognitiva viene condotta sistematicamente per assicurare la raccolta di tutti gli elementi utili, vale a dire: nome di dominio, blocchi della rete, indirizzi IP, tipo di connessio-

ne, servizi TCP e UDP in esecuzione su ciascuno dei sistemi identificati, architettura di sistema, meccanismi di controllo degli accessi, sistemi di intercettazione delle intrusioni, meccanismi di autenticazione.
Come punto di partenza usualmente viene sfruttato il sito Internet della vittima sul quale possono essere rinvenibili informazioni (identità del soggetto, sede fisica, numeri telefonici, indirizzi e-mail, e in alcuni casi si deduce la *privacy policy* ecc.); mediante un'interrogazione (cosiddetti, *whoi*) alla banca dati della *Registration Autority* si ottiene il nominativo della persona fisica o giuridica a cui il nome di dominio è registrato, nonché del *provider/manteiner* e ulteriori dati tecnici quali i *server* DNS primari e secondari, indirizzi IP della rete ed eventuali sottoreti.
Nel codice sorgente HTML delle pagine web possono essere contenuti informazioni utili ed eventuali commenti non visibili in quanto nascosti nei cosidetti *metatag*, pertanto non è infrequente la pratica di scaricare un intero sito per analizzarlo accuratamente *offline*, anche allo scopo di comprendere la struttura del sito. È possibile, inoltre, utilizzare i motori di ricerca, consultare *newsgroup* e database di file da cui ricavare notizie e indizi circa lo stato della struttura e il suo livello di protezione.
Una volta identificate le potenziali reti, viene cercato di stabilirne la topologia e individuare possibili percorsi di accesso; validissimo strumento è il programma *Neotrace* che, sfruttando la proprietà TTL (*time-to-live*) del pacchetto IP, permette di risalire al suo percorso nel passaggio da un *host* al successivo, riuscendo inoltre a identificare eventuali dispositivi di controllo degli accessi (*firewall, router* con filtri sui pacchetti, *switch*), il tutto in modalità grafica che integra tali informazioni con le interrogazioni *whoi*.
Per quanto la maggior parte delle informazioni ricavabili con questi metodi debba in forza di legge o per effettive esigenze pratiche essere resa pubblica, tuttavia è importante che il titolare effettui un'attenta e consapevole valutazione e classificazione del tipo di informazioni distribuite.

5. La scansione

Se il *footprinting* è una ricognizione per la raccolta di informazioni, con il passo successivo, la scansione, vengono stabiliti quali sistemi siano attivi e raggiungibili via Internet e, in base a tali informazioni, viene identificato quale tipo di attacco è attuabile, utilizzando una serie di strumenti e tecniche come il *ping sweep*, la scansione delle porte e il tool di ricerca automatica.
Il ping sweep consiste nell'esecuzione automatizzata di una serie di comandi ping su un intervallo di indirizzi IP e blocchi della rete che, oltre a restituire l'elenco dei sistemi in funzione, ove opportunamente impostato, può risolvere il nome degli host.
Si rivela, pertanto, di fondamentale importanza per la vittima riconoscere questo genere di attività valutando attentamente il tipo di traffico consentito sulla rete o in sistemi specifici.
I metodi principali per l'intercettazione di questo genere di attacchi consistono nell'adozione di programmi di IDS (*Intrusion Detection System*) funzionanti sulla rete; inoltre, sia router che i firewall, possono essere configurati in modo tale da non rispondere a eventuali ping inviati, dando in tal modo l'illusione all'esterno che la rete o le macchine in oggetto non siano collegate in rete.
Mediante interrogazioni ICMP (*Internet Control Messaging Protocol*) è possibile ottenere la *netmask* di una scheda di rete, informazione preziosa perché permette di identificare tutte le sottoreti utilizzate e, di conseguenza, di concentrare gli attacchi su una specifica porzione della rete, evitando per esempio gli indirizzi *broadcast*.
Uno dei rimedi più consigliati consiste nel bloccare sui *router* esterni i messaggi ICMP che forniscono informazioni (quanto meno la richiesta di *address mask*).
Ulteriore passo in avanti viene compiuto con la scansione delle porte, vale a dire la connessione alle porte TCP e UDP presenti nel sistema scelto come obiettivo per stabilire quali servizi siano in esecuzione e quali in stato di *listening*, cioè in ascolto. L'identificazione delle porte è fondamentale per risalire al tipo di sistema operativo alle applicazioni in uso; inoltre, eventuali servizi attivi potrebbero consentire a utenti non autorizzati di accedere a sistemi configurati in maniera non corretta o sui quali sia installato un *software* con vulnerabilità note.
In realtà, esistono diverse modalità di scansione a seconda del tipo di pacchetto inviato e del-

la risposta provocata; alcuni sono facilmente intercettati (TCP *connect scan*), altri garantiscono un funzionamento su tutti gli host (scansioni SYN e *connect*).
Si osserva che si possono facilmente reperire su Internet numerosi programmi che facilitano il compito dell'aspirante intrusore: *Strobe, Netcat, Nmap* per piattaforme Unix; *NetScan, WinScan, SuperScan* per quelle Windows sono i più noti in ragione della loro efficacia.
I principali metodi utilizzati per l'intercettazione di tentativi di scansione delle porte sono l'utilizzo di programmi di *Intrusion Detection System* (*Snort*) e l'attivazione di meccanismi di *reporting* delle anomalie che indichino i tentativi di scansione, configurando il sistema in modo che vengano inviati gli *alert* in tempo reale via e-mail e sms. È, inoltre, possibile ridurre al minimo i rischi disattivando tutti i servizi non strettamente necessari o quantomeno frapponendo un firewall software o hardware tra la macchina e la rete.
Il passo successivo consiste nel rilevamento del sistema operativo mediante il cosiddetto *fingerprinting* dello *stack* (attivo o passivo a seconda che vi sia l'invio di pacchetti al sistema *target* ovvero il mero esame del traffico di rete); tale tecnica, basandosi sulle differenze tra le diverse implementazioni dello *stack* IP, permette appunto di riconoscere con una certa sicurezza il sistema operativo in uso.

6. L'enumerazione

In seguito, mediante l'enumerazione si procede all'identificazione di *account* validi o di condivisioni di risorse poco protette; la differenza principale tra la raccolta di informazioni esaminate finora e l'enumerazione è il livello di invadenza: l'enumerazione richiede connessioni dirette ai sistemi e interrogazioni esplicite e dovrebbe di conseguenza essere "loggata", cioè registrata dalla vittima.
I dati che trapelano da questa attività potrebbero rilevarsi decisivi ai fini dell'intrusione, dal momento che, una volta enumerato un nome utente valido o una condivisione, risalire alla password corrispondente o a un punto debole del protocollo di condivisione è solo questione di tempo.
Le informazioni enumerate sono relative a risorse e condivisioni di rete, utenti e gruppi, applicazioni e *banner*; le tecniche di enumerazione si differenziano a seconda del sistema operativo (per questa ragione è fondamentale conoscere tale dato).
Le tecniche maggiormente diffuse sfruttano l'interfaccia NetBios, i sistemi SNMP (*Simple Network Managment Protocol*), i trasferimenti di zona DNS e altre funzioni integrate nel sistema operativo.
La cattura dei banner, invece, è l'operazione di connessione ad applicazioni remote e l'attenta osservazione dell'*output* da queste prodotto e può rivelarsi particolarmente istruttiva permettendo di identificare il software e la versione in esecuzione sul server, sufficienti a individuare le relative vulnerabilità.
La cattura di *login* e password spesso viene effettuata tramite lo *sniffing* dei pacchetti di trasmissione, tramite appositi software detti *sniffer* e facilmente reperibili su Internet, che si mettono in ascolto sulla rete, catturando tutti i pacchetti dati da e per una particolare macchina o rete, consentendo in pratica di vedere tutti i dati trasmessi e ricevuti, tra cui anche eventuali password di accesso ai sistemi.
Un altro modo per condurre l'enumerazione su applicazioni NT/2000 consiste nel visionare il contenuto del Registro di configurazione di Windows, dopo averlo copiato dal sistema *target*, nel quale vi si trovano dati relativi all'utente e alla configurazione.
In ambiente Unix, a tale scopo viene impiegato il ben noto comando *finger*.

7. L'attacco

Nel corso di un attacco informatico sono spesso utilizzate le tecniche di sniffing e anche di *spoofing*:
In particolare, lo *spoofing*, utilizzando una debolezza intrinseca del protocollo TCP/IP, permette il mascheramento della propria identità, facendo, in tal modo, credere alla vittima di essere un altro computer.
Se non è possibile individuare le password di accesso al sistema, l'alternativa più valida consiste nel cercare i difetti dell'architettura del sistema operativo e delle sue applicazioni.
Il più temuto è il *buffer overflow*: quando le applicazioni non verificano la lunghezza dell'*input*, tendono a verificarsi errori nelle applicazioni dovuti a sovraccarichi di dati che pos-

sono essere spinti nello *stack* di esecuzione della CPU, con la conseguenza che, se i dati immessi vengono scelti opportunamente, l'errore può comportare l'esecuzione di righe di codice. Poiché la programmazione genera inevitabilmente errori, l'unico rimedio efficace consiste nell'aggiornamento continuo dei programmi (come del resto previsto dalla già citata legge sulla *privacy*, il "Codice in materia di protezione dei dati personali"), mediante l'applicazione di *patch* che vanno letteralmente a tappare le falle.
Ulteriore tipologia di attacco è il DoS, ossia *Denial of Service*; in realtà, il rifiuto di servizio non è tecnicamente un accesso, ma sembra opportuno farne menzione, seppur brevemente, in ragione della sua diffusione, della semplicità con cui può essere condotto, nonché del danno che arreca alle imprese, dovuto al mancato guadagno, al tempo e al lavoro necessario per identificare e annullare questo disservizio, nonché per ripristinare il corretto funzionamento del sistema.
Gli attacchi DoS, in pratica, vengono attuati "bombardando" di richieste un particolare servizio attivo nella macchia (per esempio, il servizio Web); il risultato di tale attività di richieste dirette o più spesso amplificate, può portare all'esaurimento della larghezza di banda di una determinata rete e/o, in breve tempo, a un sovraccarico di lavoro e il conseguente esaurimento delle risorse di sistema, che si traduce in un blocco della macchina attaccata.
A tal fine, possono, ancora una volta, essere sfruttati difetti di programmazione che, impedendo a un'applicazione o al sistema operativo di gestire condizioni eccezionali, permettono l'invio di dati non previsti dall'elemento vulnerabile.

8. Il social engeenering

Un argomento sicuramente ben noto non solo a chi si occupa di sicurezza informatica, suscitandone timore, ma anche ai non addetti ai lavori è l'ingegneria sociale.
Tale espressione, affermatasi nel gergo hacker è ormai di uso comune; descrive l'insieme delle tecniche di persuasione e/o di inganno messe in campo per accedere a un sistema informatico; generalmente, si presenta con modalità simili alla conversazione umana, meglio se telefonica o tramite e-mail e consiste nell'ottenere direttamente dall'interlocutore le informazioni desiderate. La casistica è pressoché infinita e può consistere nello spacciarsi per un collega, un tecnico, un cliente ecc., e nel fingere di avere dimenticato la password, di necessitare urgentemente di un certo codice e così via.
Non è necessario che l'informazione sia sempre direttamente impiegabile, ben potendo essere utilizzata in un secondo momento; per esempio, può rivelarsi importante conoscere la data di nascita o il nome della moglie di un utente, posto che tale potrebbe essere la password ingenuamente assegnata dal medesimo.
Proprio dall'intima convinzione che l'anello debole della sicurezza informatica sia rappresentato dal fattore umano, si ritiene indispensabile adottare severe contromisure per prevenire gli attacchi basati sull'ingegneria sociale e in particolare: limitare rigorosamente la fuoriuscita di dati; stabilire una seria politica per le procedure di supporto tecnico; usare estrema cautela nella configurazione dei firewall, anche in uscita; utilizzare la posta elettronica in modo consapevole, e, soprattutto, istruire i dipendenti fornendo loro le nozioni base sulla sicurezza dei sistemi informatici.

9. Conclusioni

L'intrusione abusiva spesso si rivela propedeutica o successiva rispetto alla commissione di altri reati, pertanto può concorrere con la violazione di domicilio di cui agli artt. 614 e 615 c.p. (per esempio, accesso fisico nel centro di calcolo e successiva penetrazione nella banca dati), con la detenzione e la diffusione abusiva di codici di accesso a sistemi informatici e telematici, nonché con la diffusione o comunicazione di programmi informatici diretti a danneggiare o interrompere un sistema informatico ovvero dati o programmi in esso contenuti, delitti previsti e puniti rispettivamente dagli artt. 615 *quater* e *quinquies* c.p. (per esempio, ricerca e detenzione sul pc di password, programmi di *crack, exploit*, nonché di software finalizzati a rilevare e sfruttare le vulnerabilità del sistema *target* e il successivo utilizzo degli stessi nel corso dell'accesso).
L'art. 615 *ter* può, altresì, essere contestata in concorso con la frode informatica (art. 640 ter

c.p.), che comporta necessariamente l'alterazione di un sistema mediante manipolazione di dati, informazioni o programmi contenuti.
Si deve, invece, escludere il concorso con il reato di danneggiamento di sistemi informatici e telematici di cui all'art. 635 *bis* c.p., in quanto tale evento ne costituirebbe solo una circostanza aggravante.
In conclusione, non si può omettere di considerare che, per i motivi sopra illustrati, il fenomeno dell'accesso abusivo a un sistema informatico o telematico debba essere combattuto in primo luogo creando negli operatori un'adeguata e diffusa cultura della sicurezza.
Si ritiene, pertanto, auspicabile un'iniziativa di formazione permanente finalizzata alla sensibilizzazione degli utenti sul presupposto che solamente attraverso un utilizzo consapevole delle nuove tecnologie da parte di tutti si possa consentirne uno sviluppo armonico e un'ampia diffusione nel pieno rispetto della legalità.

Antonio Piva laureato in Scienze dell'Informazione, Presidente, per il Friuli - Venezia Giulia, dell'ALSI (*Associazione Nazionale Laureati in Scienze dell'Informazione ed Informatica*) e direttore responsabile della Rivista di Informatica Giuridica.
Docente a contratto di Informatica giuridica all'Università di Udine.
Consulente sistemi informatici, valutatore di sistemi di qualità ISO9000 e ispettore AICA per ECDL base e advanced.
antonio_piva@libero.it

David D'Agostini avvocato, ha conseguito il master in informatica giuridica e diritto delle nuove tecnologie, fornisce consulenza e assistenza giudiziale e stragiudiziale in materia di *software, privacy* e sicurezza, contratti informatici, *e-commerce*, nomi a dominio, computer crime, firma digitale. Ha rapporti di partnership con società del settore ITC nel Triveneto.
Collabora all'attività di ricerca scientifica dell'Università di Udine e di associazioni culturali.
david.dagostini@adriacom.it