Linux e la sicurezza
Computer crimes e tutela della privacy

Avv. Giovanni Battista Gallus

LL.M. Master of Laws

Dottore di ricerca

g.gallus@tiscali.it

Linux e la sicurezza
Computer crimes e tutela della privacy

- Principali computer crimes secondo il codice penale
  (introdotti dalla L. 547/1993)
  - Accesso abusivo a un sistema informatico o telematico
  - Detenzione e diffusione di usernames e passwords
  - Diffusione di programmi atti a danneggiare o interrompere un sistema informatico
  - Intercettazioni telematiche
  - Falsificazione o soppressione di comunicazioni
  - Danneggiamento informatico
  - Frode informatica
- Sostituzione di persona
- Le sanzioni contenute nella legge sulla privacy (L. 675/1996)
  - Omessa adozione di misure necessarie alla sicurezza dei dati

L'accesso abusivo ad un sistema informatico o telematico
art. 615 *ter* c.p.

"Violazione di domicilio informatico"

Chiunque abusivamente si introduce 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, è punito con la reclusione fino a tre anni.

- L'accesso deve riguardare un "sistema informatico o telematico"
  - Secondo la Corte di Cassazione, "sistema informatico" è "una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche" (Corte di Cassazione, Sez. VI, sent. N 3067/1999)
- L'accesso deve essere "abusivo"
- Il sistema deve essere protetto da misure di sicurezza

L'accesso abusivo ad un sistema informatico o telematico

art. 615 *ter* c.p.

Principali ipotesi di accesso abusivo

- Attività di footprinting
  - Non consistono ancora in un accesso, e conseguentemente non dovrebbero avere alcuna rilevanza penale (salva la configurabilità del tentativo di reato)
- Attività di attacco
  - Spoofing
  - Attacco al DNS
  - Buffer overflow

Tutte queste attività configurano un "accesso abusivo al sistema"

- L'ipotesi più semplice: l'accesso locale non autorizzato

Requisiti generali

Il sistema deve essere protetto da misure di sicurezza (fisiche e logiche)

Il reato sussiste anche se non si arrecano danni

La detenzione e diffusione di codici di accesso a sistemi informatici

art. 615 *quater* c.p.

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a lire dieci milioni (€ 5164,57).

- Condotte punite
  - Il procurare o diffondere codici di accesso
  - Occorre il fine di profitto o di altrui danno
  - E' sufficiente fornire indicazioni per il reperimento delle passwords

Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico

art. 615 *quinquies* c.p.

Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a lire venti milioni (€ 10329,14).

- Condotte punite
  - Virus
  - Worms
  - Programmi utilizzati per attacchi DoS e DdoS
  - Non basta la mera detenzione, occorre la comunicazione o la consegna

E' un reato doloso, e dunque la diffusione colposa non è, sotto questo aspetto, penalmente rilevante

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

art. 617 quater c.p.

Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

- Condotte punite
  - Intercettazioni e interruzioni di comunicazioni
  - Rivelazioni del contenuto, mediante mezzo di informazione al pubblico
  - Occorre che l'intercettazione sia “fraudolenta”
- Anche la mera installazione di apparecchiature atte ad intercettare, impedire interrompere le comunicazioni relative a un sistema informatico costituisce reato (art. 617 quinquies c.p.)

Falsificazione o soppressione del contenuto di comunicazioni telematiche

art. 617 *sexies* c.p.

Chiunque al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni...

- Condotte punite
  - Anche per questa ipotesi occorre il fine di vantaggio o di altrui danno
  - E' irrilevante che la comunicazione sia stata intercettata occasionalmente
  - Non basta la falsa formazione o l'alterazione, occorre che il falso contenuto venga usato

Danneggiamento informatico

art. 635 *bis* c.p.

Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

- Condotte punite
  - Distruzione – deterioramento – inservibilità
  - Può riguardare:
    - Sistemi - programmi - informazioni e dati
  - In sintesi, hardware, software e dati
- Occorre il dolo, per cui il danneggiamento colposo non è reato
- Attacchi DoS e DDoS come danneggiamento informatico, qualora rendano inservibile in tutto o in parte un sistema informatico

Frode informatica

art. 640 *ter* c.p.

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila (€ 51,65) a due milioni (€ 1032,91).

- La condotta
  - Ci dev'essere un'alterazione o un intervento senza diritto
  - Deve riguardare:
    - Dati – informazioni - programmi
  - Occorre un ingiusto profitto con altrui danno

Il Wardriving o LAN jacking

- Accesso alle reti wireless (in particolare 802.11b)
- *"Driving around looking for unsecured wireless networks"*
  - Si tratta di "installazione di apparecchiature atte all'intercettazione", e come tale reato, ex art. 617 *quinquies* c.p.?
  - Può consistere in una intercettazione informatica, punita dall'art. 617 *quater* c.p.?
  - Può trattarsi di una violazione di domicilio informatico (art. 615 *ter* c.p.)?
- Maggiori informazioni su:
  - http://punto-informatico.it/p.asp?i=40825&p=2 (articolo dell'Avv. Daniele Minotti)
  - http://www.wardriving.com/

Sostituzione di persona

art. 494 c.p.

Chiunque al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome,... è punito se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino a un anno

- La condotta
  - L'attribuzione di un falso nome
  - Fine di vantaggio o di altrui danno
- Utilizzo di nome altrui per servizi in rete

Linux e la sicurezza
Computer crimes e tutela della privacy

Le sanzioni contenute nella legge sulla privacy (L. 675/1996)

Art. 3 L. 675/96

1. Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali non è soggetto all'applicazione della presente legge, sempreché i dati non siano destinati ad una comunicazione sistematica o alla diffusione.

2. Al trattamento di cui al comma 1 si applicano in ogni caso le disposizioni in tema di sicurezza dei dati di cui all'articolo 15, nonché l'articolo 18 .

- Risultato:
  - La legge non si applica ai trattamenti di dati per fini personali
  - Uniche due eccezioni:
    - Le misure minime di sicurezza (art. 15)
    - La responsabilità (art. 18)

Le misure minime di sicurezza

Art. 15 L 675/96 e D.P.R. n. 318/99

Ai sensi dell'art. 15, devono essere rispettate quantomeno le misure minime di sicurezza (definite dal D.P.R. n. 318/99*)*

- Per i trattamenti di dati esclusivamente personali, non destinati alla comunicazione sistematica o alla diffusione:
  - Nessuna misura
- Per i trattamenti di dati esclusivamente personali, riguardanti dati sensibili:
  - Qualora si tratti di computer in rete, è necessaria la password

Linux e la sicurezza
Computer crimes e tutela della privacy

Le misure minime di sicurezza

- Art. 15 L 675/96 e D.P.R. n. 318/99

I trattamenti a fini non esclusivamente personali,

- Postazioni di PC singole
  - Adozione di password
- Postazioni di PC collegate in rete
  - Password univoca, da disattivarsi in caso di mancato utilizzo per sei mesi
  - "gli elaboratori devono essere protetti contro il rischio di intrusione ad opera di programmi di cui all'art. 615-quinquies del codice penale, mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale" (art. 4, lett. C D.P.R. 318/99).
  - Traduzione: occorre un antivirus e un firewall (la norma sembra scritta per il mondo Wintel)

Linux e la sicurezza
Computer crimes e tutela della privacy

Sanzioni penali e responsabilità civile

Art. 36 L. 675/96

Omessa adozione di misure necessarie alla sicurezza dei dati

Chiunque, essendovi tenuto, omette di adottare le misure necessarie a garantire la sicurezza dei dati personali, in violazione delle disposizioni dei regolamenti di cui ai commi 2 e 3 dell'articolo 15, è punito con l'arresto sino a due anni o con l'ammenda da lire dieci milioni (euro 5.164,6) a lire ottanta milioni (euro 41.316,6).

- Si può estinguere il reato:
  - adottando le misure di sicurezza
  - pagando una sanzione amministrativa
- Art. 18 – Danni cagionati per effetto del trattamento di dati personali

Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

- Per evitare responsabilità civili, bisogna dunque provare di aver adottato tutte le misure di sicurezza necessarie e possibili