filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

I reati informatici (cyber crimes) e frodi informatiche

Parte IV
08 Agosto 2019
Angelo Fiori

Indice

1. Introduzione

I reati informatici, o “computer crimes”, possono essere definiti come il risvolto negativo dello sviluppo tecnologico dell’informatica e della telematica.

Lo sviluppo delle tecnologie informatiche ha infatti permesso di disegnare nuovi scenari da qualche decennio a questa parte.

Negli ultimi decenni la maggior parte delle attività umane svolte manualmente o attraverso apparecchiature meccaniche, hanno lasciato il passo a più efficienti implementazioni digitali.

Dal connubio informatica?reti telematiche originano inoltre ampie possibilità per la crescita delle aziende e delle comunità in genere.

Da ciò si sviluppano attività quali ad esempio l’e?commerce, l’e?government, l’home?banking, il trading online e tante altre attività che consentono di rendere più efficiente la società nel suo complesso, ma al contempo la rendono estremamente net?centrica.

Con ciò si vuole sottolineare il fatto che la maggior parte delle attività sociali, lavorative e di svago passano oggi attraverso reti telematiche

> **L’evoluzione e la diffusione delle tecnologie informatiche e telematiche degli ultimi anni hanno reso il computer, con frequenza sempre maggiore, strumento o oggetto di attività illecita. Di conseguenza, il legislatore è dovuto intervenire, anche sul piano penale, attraverso l’introduzione di nuove fattispecie criminose definite computer crimes o reati informatici.**

Per rendere più agevole la comprensione dei provvedimenti normativi previsti dalla legislazione italiana, appare conveniente suddividere in macrocategorie le diverse aree: a) Frodi informatiche; b) Falsificazioni; c) Integrità dei dati e dei sistemi informatici; d) Riservatezza dei dati e delle comunicazioni informatiche.

2. Frodi Informatiche

Il delitto di Frode informatica, disciplinato dal libro II, titolo XIII, articolo 640 ter codice penale, è stato introdotto dalla legge n. 547 del 1993.

Si parla qui di un reato consistente nel trarre in inganno un elaboratore elettronico, al fine di ricavarne un guadagno economico (per sé o per altri complici), a danno di un soggetto terzo (solitamente il detentore dell'elaboratore elettronico).

Si tratta perciò di un'estensione del reato di truffa descritto all'articolo 640 codice penale

articolo 640?ter ("Frode informatica"):

"*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 euro 51 a euro 1.032.*

La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante."

> **Tra i reati che più frequentemente vengono compiuti, e che ricadono, tra gli altri, all'interno della "frode informatica", vi sono le cd. pratiche di phishing e quelle di diffusione di appositi programmi truffaldini, definiti Dialer.**

Il phishing altro non è che un'attività finalizzata ad estorcere dati personali (in prevalenza legati alle carte di credito od ai conti bancari) attraverso una richiesta esplicita al suo legittimo possessore.

Il principale metodo per porre in essere il phishing è quello di inviare una mail simile a quella che verrebbe inviata da un regolare istituto (banca, sito d'aste, provider, ecc. e con relativo logo identificativo), nella quale si riportano vari tipi di problemi tecnici (aggiornamento software, scadenza account, ecc.) che motivano l'utente a cliccare sul link riportato nella mail per andare ad aggiornare i propri dati personali.

Chiaramente il link non porta al "vero" sito dell'istituzione, ma ad un sito fasullo ed opportunamente creato dall'autore del reato di phishing, che si impossesserà così dei dati inseriti dall'utente.

A tal scopo l'ABI (Associazione Bancaria Italiana) ha stilato una lista di 10 punti chiave nella prevenzione del phishing:

1. diffidate di qualunque e-mail che vi richieda l'inserimento di dati riservati riguardanti codici di carte di pagamento, chiavi di accesso al servizio di home banking o altre informazioni personali;

2. è possibile riconoscere le truffe via e-mail con qualche piccola attenzione: generalmente queste email non sono personalizzate e contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati; fanno uso di toni intimidatori; non riportano una data di scadenza per l'invio delle informazioni;
3. nel caso in cui riceviate un'e-mail contenente richieste di questo tipo, non rispondete all'e-mail stessa, ma informate subito la vostra banca;
4. non cliccate su link presenti in e-mail sospette, in quanto questi collegamenti potrebbero condurvi a un sito contraffatto, difficilmente distinguibile dall'originale;
5. diffidate inoltre di e-mail con indirizzi web molto lunghi, contenenti caratteri inusuali, quali in particolare @;
6. quando inserite dati riservati in una pagina web, assicuratevi che si tratti di una pagina protetta: queste pagine sono riconoscibili in quanto l'indirizzo che compare nella barra degli indirizzi del browser comincia con “https://” e non con “http://” e nella parte in basso a destra della pagina è presente un lucchetto;
7. diffidate se improvvisamente cambia la modalità con la quale vi viene chiesto di inserire i vostri codici di accesso all'home banking;
8. controllate regolarmente gli estratti conto del vostro conto corrente e delle carte di credito per assicurarvi che le transazioni riportate siano quelle realmente effettuate. In caso contrario, contattate la banca e/o l'emittente della carta di credito;
9. le aziende produttrici dei browser rendono periodicamente disponibili on-line e scaricabili gratuitamente degli aggiornamenti (le cosiddette patch) che incrementano la sicurezza di questi programmi;
10. Internet è un po' come il mondo reale: come non dareste a uno sconosciuto il codice PIN del vostro bancomat, allo stesso modo occorre essere estremamente diffidenti nel consegnare i vostri dati riservati senza essere sicuri dell'identità di chi li sta chiedendo. In caso di dubbio, rivolgetevi alla vostra banca.
Il dialer è un piccolo programma (pochi kilobyte) appositamente scritto per dirottare la connessione Internet dell’ignaro utente verso un altro numero telefonico, spesso di tariffazione internazionale e comunque sempre molto più caro rispetto alla comune chiamata telefonica al numero POP del proprio provider.
Attraverso l’utilizzo del dialer il guadagno è multiplo; operatori di telefonia, società produttrici dei dialer, webmaster.
È però da precisare che l’utente finale (singolo o azienda che sia) viene colpito dal dialer solo nel momento in cui effettivamente lo scarica e lo installa sul proprio computer.
Il dialer infatti è un normalissimo programma e come tale deve preventivamente essere installato per poter essere eseguito. Una volta installato sarà il dialer che automaticamente sostituirà il numero ordinario di connessione con un numero a tariffazione maggiorata.

3. Falsificazioni

La seconda macrocategoria, quella delle falsificazioni, è regolamentata dal Codice Penale attraverso l’articolo 491?bis contenuto nel Titolo VII “dei delitti contro la fede pubblica”, Capo III “della falsità in atti”:
articolo 491?bis (“Documenti informatici”):

> ***“Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.”***

l documento informatico acquista effettiva valenza legale con la legge 59/1997 (articolo 15 comma 2).
Per poter però essere valido un documento deve poter essere autenticato e se ne deve poter attribuire la paternità.
A tale scopo interviene la firma digitale, e nel D.P.R. 513/97 articolo 1 lettera “b” se ne dà una definizione: s’intende “per firma digitale, il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici”.
Con la firma digitale dunque si attesta anche l’integrità ed il non ripudio del documento (quindi si scongiura la falsità materiale), in quanto nella procedura di firma digitale viene generato un particolare codice crittografico derivante dalla “mescolanza” dei dati identificativi del mittente con il contenuto vero e proprio del documento (hash); qualora al momento della ricezione vi sia corrispondenza tra i codici crittografici ottenuti, si avrebbe conferma dell’integrità del documento e dell’autenticità del mittente.

4. Integrità dei dati e dei sistemi informatici

Il Codice Penale regolamenta poi una terza macrocategoria, che riguarda l’integrità dei dati e dei sistemi informatici, attraverso vari articoli, tra cui il 635?bis del codice penale sul “danneggiamento di sistemi informatici e telematici”, contenuto nel Titolo XIII “dei delitti contro il patrimonio”, Capo I “dei delitti contro il patrimonio mediante violenza alle cose o alle persone”; articolo 635?bis (“Danneggiamento di sistemi informatici e telematici”):
“*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. Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni*.”
Aggravante del reato “danneggiamento di sistemi informatici e telematici” è l’articolo 420 codice penale “attentato a impianti di pubblica utilità” contenuto nel Titolo V “dei delitti contro l’ordine pubblico”. Il Codice Penale interviene anche estendendo l’articolo 392 (“Esercizio arbitrario delle proprie ragioni con violenza sulle cose”), ai sistemi informatici (comma 3).
Bisogna infine sottolineare l’art articolo 615?quinquies (“Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico”):

> ***"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 euro 10.329."***

Con l'articolo 615?quinquies si mira a reprimere la "*diffusione di programmi diretti a danneggiare o interrompere un sistema informatico*", tutti i programmi cioè rientranti sotto la categoria di **malicious software (o malware)**.

5. Riservatezza dei dati e delle comunicazioni informatiche

Ultima macrocategoria dei reati informatici è quella inerente alla riservatezza dei dati e delle comunicazioni informatiche. In tale ambito il Codice Penale interviene con l'intento di reprimere forme di intrusione nella sfera privata altrui. Il primo provvedimento previsto dalla legge 547/93 in materia di riservatezza dei dati e delle comunicazioni informatiche è quello adottato con l'articolo 615?ter del Codice Penale "accesso abusivo ad un sistema informatico o telematico", Titolo XII "dei delitti contro la persona", Capo III "dei delitti contro la libertà individuale", Sezione IV "dei delitti contro la inviolabilità del domicilio".

articolo 615?ter ("Accesso abusivo ad un sistema informatico o telematico"):

"*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. La pena è della reclusione da uno a cinque anni:*

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio."

Con questo articolo si vuole tutelare il sistema informatico, inteso qui come vera e propria estensione del domicilio dell'individuo, al fine di proteggerlo da accessi non autorizzati e da permanenza non gradita
Altre disposizioni del Codice Penale in materia di riservatezza dei dati e delle comunicazioni informatiche, le si possono riscontrare nell'articolo 615?quater.
articolo 615?quater ("Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici"):

> ***"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 euro 5.164.***

La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater".
Sempre in riferimento alla macrocategoria sulla riservatezza dei dati e delle comunicazioni informatiche, il Codice Penale individua nell'articolo 621 (Titolo XII "dei delitti contro la persona, Sezione V "dei delitti contro la inviolabilità dei segreti") un ulteriore forma di protezione della riservatezza dei propri documenti.
articolo 621 ("Rivelazione del contenuto di documenti segreti"):
"*Chiunque, essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, di altrui atti o documenti, pubblici o privati, non costituenti corrispondenza, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto deriva nocumento, con la reclusione fino a tre anni o con la multa da euro 103 a euro 1.032.*
Agli effetti della disposizione di cui al primo comma è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi. Il delitto è punibile a querela della persona offesa
."
Più nello specifico dell'ambito informatico entrano gli articoli 617?quater, 617?quinquies e 617?sexies (Titolo XII "dei delitti contro la persona", Sezione V "dei delitti contro la inviolabilità dei segreti"), i quali tutelano la riservatezza delle comunicazioni informatiche proprio come nello stesso Codice Penale sono tutelate le comunicazioni per mezzo di apparecchiature telefoniche, telegrafiche ed epistolari attraverso gli articoli 617 e seguenti.
Il fine ultimo di tali articoli è comunque quello espresso attraverso l'articolo 616 codice penale sulla "**Violazione, sottrazione e soppressione della corrispondenza**", sostenuto, tra l'altro, anche dall'articolo 15 della Costituzione Italiana sulla libertà e segretezza della corrispondenza e della comunicazione.

Parte I, Parte II, Parte III, Parte V e Parte VI

Bibliografia

Frodi aziendali – Giuseppe Pogliani, Nicola Pecchiari, Marco Mariani – EGEA 2012.

Global economic crime survey 2016” di Price Waterhouse & Coopers.
Ernst & Young_14th_Global_Fraud_Survey – 2016.
ACFE-(association of certified fraud examiners) 2016 - “Report-to-the-nations 2016”.
Fondazione Luca Pacioli “Oltre il velo societario. L’utilizzo di strutture societarie per finalità illecite. Il rapporto dell’OCSE”.

TAG: *Reati informatici, Frode informatica, dati riservati*
