diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

La criminalità informatica

Autore: Giuseppe Dezzani - Studio Di.Fo.B.
In: Diritto penale

La sensibilità legislativa in campo di Criminalità Informatica inizia con la pubblicazione sulla Gazzetta Ufficiale n. 80 del 4 aprile 2008 – supplemento ordinario n. 79 - della legge 18 marzo 2008, n. 48. La nuova normativa introduce una serie di modifiche concernenti i reati in materia informatica. Il testo della legge, oltre alle modifiche al codice penale ed al codice di procedura penale, introduce nel d.lgs. 8 giugno 2001, n. 231, l'art. 24-bis recante la previsione di nuove fattispecie di reato in dipendenza di delitti informatici e trattamento illecito di dati.

Come è noto, la legge n. 48, come riporta il Capo I, ratifica le norme previste dal Consiglio d'Europa sulla criminalità informatica, previste nella Convenzione realizzata a Budapest il 23 novembre 2001. Il codice penale italiano, prima di queste modifiche, prevedeva alcuni articoli introdotti dalla legge 547/1993. L'ordinamento puniva - art. 635-bis – il "Danneggiamento di sistemi informatici e telematici". La legge 48/2008, oltre a sostituire integralmente nel codice penale l'art. 635-bis, introduce ulteriori tre fattispecie indicate agli artt. 635-ter, 635-quater, 635-quinquies. La modifica ottempera ad una puntuale applicazione di quanto disposto dalla Convenzione che ha distinto nettamente tra danneggiamento dell'integrità dei dati e danneggiamento dell'integrità del sistema (artt. 4 e 5). La disciplina è stata differenziata anche in relazione alla rilevanza pubblica dell'oggetto della tutela, prevedendo per questi casi pene più elevate.

L'introduzione degli artt. 635-ter e 635-quinquies c.p. determinava possibili conflitti con le norme indicate dall'art. 420 c.p., commi 2 e 3 - che hanno come oggetto la tutela agli impianti di pubblica utilità - le cui fattispecie sono molto simili a quelle introdotte dai nuovi articoli. Il problema è stato risolto con

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

l'abrogazione dei commi 2 e 3 dell'art. 420 (art. 6).
Oltre al citato art. 635, che è stato completamente riscritto, la legge 48/2008 introduce nel d.lgs. 231/2001 - in alcuni casi modificandone il contenuto - i seguenti delitti informatici:

1) art. 615-ter c.p., relativo all'accesso abusivo ad un sistema informatico o telematico;

2) art. 615-quater c.p. - che non ha subito modifiche da parte della legge 48 – in merito alla detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;

3) art. 615-quinquies che punisce la diffusione di apparecchiature, dispositivi o programmi diretti a danneggiare o interrompere il funzionamento di un sistema informatico. Modificato dalla legge 48/2008 in quanto precedentemente puniva la sola diffusione di programmi e non contemplava i dispositivi;

4) artt. 617-quater e 617-quinquies c.p., relativi alle intercettazioni - anche attraverso l'installazione di apparati - ed all'impedimento o interruzione di comunicazioni informatiche o telematiche;

5) art. 491-bis c.p., riguardante la falsità di un documento informatico;

6) art. 640-quinquies c.p., introdotto ex novo dalla legge 48/2008, che ha come oggetto la frode informatica del soggetto che presta servizi di certificazione di firma elettronica.

Prima di passare all'analisi tecnica degli articoli elencati, è necessario soffermarsi sull'art. 1 della Convenzione, che definisce il concetto di sistema e di dato informatico. La Convenzione di Budapest del

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

2001 risolve il problema di tale definizione, esistente da anni, esprimendo il concetto: “computer system means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data”. La cui traduzione porta alla seguente definizione di “sistema informatico”: “qualsiasi apparecchiatura, dispositivo, gruppo di apparecchiature o dispositivi, interconnesse o collegate, una o più delle quali, in base ad un programma, eseguono l’elaborazione automatica di dati”.
Si tratta di una definizione molto generale che permette di includere qualsiasi strumento elettronico, informatico o telematico, in rete (gruppo di dispositivi) o anche in grado di lavorare in completa autonomia. In questa definizione rientrano anche i dispositivi elettronici che, al giorno d’oggi, sono tutti dotati di un software (o anche solo un firmware) che permette il loro funzionamento elaborando delle informazioni (o comandi). Ad esempio, con questa definizione è possibile inserire come dispositivo

tutelato dalla legge un telefono cellulare, uno strumento PDA o un dispositivo elettronico inserito in un impianto per la produzione industriale.

Nel medesimo articolo è contenuta anche la definizione di “dato informatico”, che descrive il concetto derivandolo dall’uso: “computer data means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function”; tradotto letteralmente con la definizione: “qualunque rappresentazione di fatti, informazioni o concetti in forma idonea per l’elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informatico di svolgere una funzione”.

In questo caso la definizione ha dovuto comprendere due argomenti, il dato in senso stretto ed i programmi. Entrambi sono memorizzati in forma digitale di byte all’interno di files ma con due funzioni ben differenti. I primi sono i dati dell’utente che sono generati e salvati attraverso l’uso di un applicativo.

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

Per programma (o applicativo) s'intende il software. In questa definizione rientrano anche i sistemi operativi, driver, firmware ovvero tutti quei programmi anche di base che sono presenti su un elaboratore o apparato elettronico e necessari al loro funzionamento. La differenza tra i files di dati (o informazioni) e di programmi è che sono la rappresentazione digitale di un documento (testo, immagine, archivio, ecc.) realizzato attraverso l'uso di un software. Normalmente ogni documento è contenuto in un singolo file. Il programma invece è un insieme di files, che sono richiamati gli uni dagli altri a seconda di comandi impartiti dall'utente, contenenti algoritmi in grado di eseguire funzioni.

L'art. 1 della Convenzione riveste un'importanza rilevante in quanto per la prima volta viene chiarita, in modo univoco ed accettato da tutti i Paesi europei che hanno ratificato il trattato, la definizione di un sistema informatico o telematico, di dato e di programma. Per schematizzare la struttura, il sistema informatico è un dispositivo hardware che "contiene" uno o più programmi - tra cui obbligatoriamente un sistema operativo - con cui si possono gestire i dati. Da questa espressione generale si comprende la ragione del diverso trattamento sanzionatorio: colpire un dato informatico non significa impedire il funzionamento del sistema, colpire quest'ultimo significa impedire l'uso dell'intera struttura e di quanto in essa memorizzato. Di conseguenza deriva la necessità di differenziare, negli articoli del codice penale, gli illeciti che hanno come oggetto la struttura hardware rispetto a quelli relativi ai files (che siano questi contenitori di dati o di programmi).

Il d.lgs. 231/2001, com'è noto, introduce per la prima volta nel nostro ordinamento la punibilità di enti collettivi in quanto tali, sia dotati che non di personalità giuridica, per reati commessi nel loro interesse o a loro vantaggio da apicali e sottoposti che operano nella loro struttura. La legge 48/2008 inserisce tra questi i reati derivanti da delitti informatici. In particolare i crimini informatici sono suddivisi in tre gruppi, elencati all'art. 24-bis, commi 1, 2 e 3, attribuendo diversi livelli sanzionatori a livello pecuniario e - comma 4 - diverse applicazioni dell'art. 9 per le sanzioni interdittive, arrivando anche all'interdizione dell'attività aziendale.

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

In termini prettamente informatici, gli articoli del codice penale previsti nel comma 1 dell'art. 24-bis d.lgs. 231/2001 hanno come fattore comune il "danneggiamento informatico". Sono sanzionati con una pena pecuniaria da cento a cinquecento quote e con le sanzioni interdittive previste dall'art. 9, comma 2, lett. a), b) ed e), d.lgs. 231/2001 i reati che portano all'interruzione del funzionamento di un sistema informatico o al danneggiamento del software (sia sotto forma di programma che di dato).

Si parla di danneggiamento informatico quando, considerando sia la componente hardware che quella software, anche separatamente, interviene una modifica tale da impedirne il funzionamento, anche solo parziale. Come anticipato, la nuova legislazione ha suddiviso i reati in funzione che si abbiano come oggetto della tutela la parte fisica del computer, l'hardware appunto, oppure la parte logica, ovvero il software e i dati. Da un punto di vista tecnico possiamo invece tralasciare la differenza introdotta al fine di punire con pene più elevate i reati aventi come obiettivo i dati o i sistemi di pubblico interesse, considerato che le modalità attraverso cui vengono commessi sono identiche.

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

La normativa introdotta nel 2008 con grande lungimiranza, se considerato che in quegli anni non si parlava ancora di ramsonware o di truffe informatiche basate sulle infezioni tramite software,
ha introdotto la sanzionabilità delle condotte di detenzione e diffusione di programmi e/o strumenti atti al danneggiamento ed all'intercettazione. Gli spyware un tempo erano catalogati assieme ai virus informatici; mentre ora, dopo aver raggiunto una rilevanza sociale estremamente importante, gli è stata riservata una precisa collocazione nel panorama informatico, diventando una battaglia quotidiana per gli amministratori di sistema.

In particolare, negli ultimi anni si è assistito all'ascesa di tre tipologie di software utilizzati in ambito di criminalità informatica: ransomware, trojan bancari e keylogger. I primi sono diventati una delle minacce più diffuse su computer di privati, enti pubblici, studi professionali, ospedali e aziende dal 2014, in contemporanea con l'ascesa della moneta matematica nota come Bitcoin che ne ha tristemente aumentato il potenziale. I ransomware sono infatti software diffusi in diverse maniere, nascosti in: allegati di posta elettronica mascherati da finte fatture, note di credito, bollette di operatori telefonici o elettrici o all'interno di siti web compromessi in modo da attivare in automatico il download e l'avvio del malware da parte degli ignari visitatori.

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

L'effetto di un'infezione di un ransomware è devastante: i dati presenti sul proprio PC sono cifrati cancellando perennemente gli originali e proteggendoli con una chiave di cifratura (in pratica una sorta di "password") che l'utente non conosce e che quindi non potrà utilizzare per ripristinare i propri documenti. I delinquenti che hanno creato o diffuso il ransomware richiedono il pagamento di un riscatto da versarsi in Bitcoin entro alcuni giorni, pena il raddoppio del riscatto o persino la cancellazione per manente della chiave, il che implica l'impossibilità di riottenere i propri documenti.

Dal punto di vista giuridico, l'utilizzo di questo tipo di malware implica la commissione di almeno tre reati: accesso abusivo a sistema informatico, danneggiamento ed estorsione, oltre alle condotte sopra menzionate di detenzione e diffusione di software e/o strumenti atti al danneggiamento ed all'intercettazione. Di recente è emersa anche la necessità di approfondire le eventuali responsabilità – in termini di favoreggiamento – di exchange che procedono consapevolmente e come attività prevalente al cambio di moneta fiat in bitcoin finalizzata al pagamento del riscatto e nei confronti di eventuali società che supportano le vittime nel pagamento del riscatto. La giurisprudenza in tal senso non si è ancora pronunciata ma esistono indagini in corso per attività di tal genere e il tempo mostrerà quale direzione intenderanno seguire i Giudici.

L'unico aspetto fino a questo punto certo è che in presenza di una condotta estorsiva il soggetto passivo si configura quale vittima. Per questa ragione, anche in caso di pagamento del riscatto, non si configura un comportamento illecito, né un reato anzi se ci poniamo nell'ottica di un amministratore di sistema di ente collettivo, Ministero, Ente Pubblico, Società a partecipazione pubblica, autorità pubblica, il pagamento potrebbe persino rappresentare la scelta più logica per preservare i dati degli utenti e l'operatività. Il pagamento del riscatto però – nel caso ad esempio di un ente pubblico che utilizza la sua disponibilità finanziaria – sarà soggetta al successivo controllo amministrativo e contabile da parte della Corte dei

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

Conti e potrà esporre il funzionario a responsabilità personale per danno all'erario, a meno che egli non riesca a dimostrare che la sua condotta è stata volta ad evitare all'Amministrazione danni maggiori (inoperatività, perdita di dati, etc…).

In ultimo, come osserva ancora l'Avv. Sandro Bartolomucci, anche il D.Lgs 231 può implicare alcune responsabilità per l'azienda in caso di pagamento del riscatto, in particolare relativamente a probabili violazioni del codice etico di cui ne viola i principi, alimentando infatti la criminalità. Senza contare che il pagamento del riscatto potrebbe anche configurarsi come illecito da reato presupposto, essendo effettuata nell'interesse e a vantaggio dell'azienda stessa, soprattutto se per somme non indifferenti.

Il secondo tipo di software spesso coinvolto nei reati informatici è identificato dai cosiddetti "trojan bancari", programmi il cui unico scopo è quello di monitorare l'utilizzo del computer al fine di intromettersi nelle operazioni dispositive su portali di web banking per deviare i bonifici verso altre destinazioni rispetto a quelle intese dalle vittime. Ignari imprenditori si ritrovano così con estratti conto che riportano bonifici verso località estere inoltrati in momenti nei quali essi avevano effettivamente inviato disposizioni ma non ovviamente verso i beneficiari che hanno ricevuto il denaro. Dal punto di vista

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

pratico, questo tipo di malware vede la lotta tra la vittima che tenta la richiesta di risarcimento e la banca che si rifiuta dicendo che il bonifico proveniva dal PC della vittima e – dal punto di vista tecnico – era del tutto intenzionale.

Terzo tipo di programmi che rientrano nella categoria degli "spyware" sono i keylogger, software di monitoraggio che ormai oltre ad acquisire la pressione dei tasti (e quindi "leggere" ciò che la vittima digita, password incluse) intercetta qualunque tipo d'informazione anche visiva o uditiva del PC o dall'ambiente della vittima. Il tutto per gli utilizzi più disparati, tra i quali la truffa del cosiddetto "man in the mail", che prevede l'intromissione dei criminali nella mail aziendale al fine di ingannare clienti o fornitori deviando così pagamenti anche d'ingenti somme verso conti dai quali i fondi spariranno poi nel nulla in breve tempo. O ancora, può ritornare il fine estorsivo, che si realizza quando i delinquenti acquisiscono informazioni riservate e chiedono un riscatto per impedirne la diffusione. Non si parla soltanto in questo caso d'informazioni strategiche per l'azienda ma molto spesso di "leggerezze" come fotografie private che i delinquenti trovano su PC o cellulari e che minacciano la vittima di diffondere se non sarà corrisposta un'adeguata somma di denaro che in genere si aggira sui 5.000 euro ma, per aziende o grossi imprenditori, può salire anche in modo vertiginoso.

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887

Diritto & Diritti ISSN 1127-8579

In Italia sono ancora poche le indagini conclusesi in modo positivo relativamente alla diffusione, detenzione e creazione di software atto a intercettare o compiere azioni estorsive, anche a causa del sempre più massiccio utilizzo di mezzi di pagamento pseudo-anonimi come il Bitcoin o carte di pagamento anonime come Paysafecard. La via legale o tecnica ex-post, quindi, non sembra essere la soluzione migliore, quanto invece il rispetto di buone pratiche di sicurezza nella protezione dei dati e nella gestione di metodologie di disaster recovery, incident response e business continuity. Banalmente, per buona parte delle infezioni il cui fine è quello di sottrarre/criptare dati alle vittime, un semplice ma robusto backup è ciò che in genere mette al riparo da sgradite sorprese.

https://www.diritto.it/la-criminalita-informatica/

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887

Diritto & Diritti ISSN 1127-8579