Network 231

Reati informatici e 231

L'art. 24 bis stabilisce il dispositivo sanzionatorio in materia di reati informatici

Nell'ambito dei modelli di gestione della 231 I reati informatici stanno assumendo un rilievo importante, perche?

E' una questione che comprende privacy, segretezza, sensibilità del dato? Cosa in particolare rende l'aspetto dei dati informatizzati così importante?

Rispondiamo a due domande: siamo proprio sicuri che I dati personali valgano qualcosa? E che valore potremmo dare a delle informazioni elettroniche che riguardano l'azienda ed il suo lavoro?

Network 231

Reati informatici e 231

ECONOMIA
01/02/2012 - IL CASO

Facebook, la quotazione in Borsa potrebbe valere 5 miliardi di dollari

Oggi la compagnia presenta l'Ipo

Mark Zuckerberg

Che valore commerciale hanno i dati personali di milioni di persone? Facebook, il social network fondato da Mark Zuckerberg nel 2004, sta per scoprirlo, scrive il New York Times. Oggi Facebook presenterà infatti alla Sec, la Consob statunitense, la documentazione per debuttare in Borsa a maggio.

Lo sbarco in Borsa di Facebook potrebbe valere 5 miliardi di dollari. Lo indicava ieri sera il New York Times. La cifra appare ridimensionata rispetto a quelle circolate fino a ora. Venerdì scorso il Wall Street Journal aveva parlato di una Ipo da 10 miliardi di dollari, che valorizzerebbe la società creata da Mark Zuckerberg tra 75 e 100 miliardi di dollari.

FORSE TI INTERESSA ANCHE
+ Facebook: pronti per Wall Street
+ Facebook, ultima asta prima dell'Ipo "Il sito vale 103 miliardi di dollari"
+ Licenze, è scontro tra Yahoo e Facebook
+ Facebook, utili in calo del 12%
+ Avio presenta la domanda di quotazione in Borsa

Per oggi è atteso il deposito presso la sec del dossier preliminare per la quotazione che, comunque, non avrà ancora indicazioni precise sul numero di azioni in offerta e sul loro prezzo.

Per sette anni Facebook ha raccolto i dati personali di oltre 800 milioni di utenti che hanno liberamente scelto di iscriversi e di condividere le proprie informazioni. Il valore della società di Zuckerberg sarà determinato dalla possibilità di usare questi dati per attrarre pubblicità, nel rispetto però della privacy degli utenti e delle norme in materia fissate da ciascun paese.

Reati informatici e 231

Reati informatici e 231

Per **crimine informatico intendiamo ogni comportamento previsto e punito dal codice penale o da leggi speciali in cui qualsiasi strumento informatico o telematico rappresenti un elemento determinante ai fini della qualificazione del fatto di reato**

 Si utilizza il termine **‘reato informatico’ per indicare qualsiasi condotta realizzata per mezzo delle nuove tecnologie o comunque rivolta contro i beni informatici, sanzionata dall‟ordinamento penale. Può essere considerato reato informatico tanto la frode commessa attraverso il computer che il danneggiamento del sistema informatico**

Reati informatici e 231

Una definizione „dottrinaria" di crimine informatico è:
crimine nel quale un sistema di elaborazione o una sua parte ricopre uno dei seguenti ruoli:

- **oggetto (ciò include la distruzione o la manipolazione dell"elaboratore, dei dati e dei programmi in esso contenuti e delle relative apparecchiature di supporto)**
- **soggetto (quando l"elaboratore è il luogo, il motivo o la fonte del crimine)**
- **strumento (quando ciò che avviene in relazione all"elaborazione non è di per sé illegale, ma serve a commettere crimini di altro tipo, es. sabotaggio). In pratica un sistema di elaborazione, o ciò che viene prodotto dall"elaboratore, è usato come mezzo per compiere frodi, sabotaggi, falsificazioni.**

Reati informatici e 231

L’art.7, L. 18.03.2008, n.48 (*‘Ratifica ed esecuzione della Convenzione del Consiglio d’Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell’ordinamento interno’) pubblicata in G.U. n. 80 del 4 aprile 2008 ha introdotto l‟art. 24-bis all‟interno del Decreto il quale:*

- recepisce l‟art. 491-bis c.p. che, a sua volta, estende le ipotesi di **falsità in atti di cui al Libro II, Titolo VII, Capo III c.p. a tutte le fattispecie delittuose in cui una o più delle suddette falsità abbia ad oggetto un c.d. *‘documento informatico’***
- introduce all‟interno del Decreto alcune ipotesi di reato in materia di **criminalità informatica, già disciplinate all‟interno del Codice Penale.**

Reati informatici e 231

Art. 615-ter: Accesso abusivo ad un sistema informatico o telematico
Art. 615-quarter: Detenzione e diffusione abusiva di codici di accesso ai sistemi informatici o telematici
Art. 615-quinquies: Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informativo o telematico
Art. 617-quarter: Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
Art. 617-quinquies: Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche
Art. 635-bis: Danneggiamento di informazioni, dati e programmi informatici
Art. 635-ter: Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità
Art. 635-quarter: Danneggiamento di sistemi informatici o telematici
Art. 635-quinquies: Danneggiamento di sistemi informatici o telematici di pubblica utilità
Art. 640-quinquies: Frode informatica del soggetto che presta servizi di certificazione di firma elettronica
Art. 491-bis: Falsità di documenti informatici.

Reati informatici e 231

Reato	Condotta	Ipotesi di reato
ART. 615-*ter* 'Accesso abusivo ad un sistema informatico o Telematico'	Punisce la condotta di chi si introduce abusivamente, ossia eludendo una qualsiasi forma, anche minima, di barriere ostative all'accesso, in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà di chi a diritto di escluderlo.	Soggetti che si introducono nel sistema informatico della Società per effettuare operazioni che portino un interesse o vantaggio per la Società (diminuzione del credito dei clienti, maggiorazione dei costi dei servizi erogati, fatturazione di servizi non richiesti). Soggetti si introducono abusivamente in sistemi informatici esterni al fine di procurare un interesse o vantaggio alla Società. Ad esempio: • accesso abusivo nel sistema informatico di un concorrente al fine di conoscere l'offerta economica presentata per la partecipazione alla gara di appalto; • accesso abusivo nel sistema informatico di un concorrente al fine di conoscere il portafoglio clienti.
Es. Protocolli di controllo		
• Definizione di una Politica sulla sicurezza delle informazioni come la gestione e uso delle password, le modalità di effettuazione dei log-in e log-out, l'uso della posta elettronica, le modalità di utilizzo dei supporti rimovibili, l'uso dei sistemi di protezione (antivirus, spam, phishing, spy) • Inventario aggiornato dell'hardware e del software in uso agli utenti • Procedure formali per l'assegnazione di privilegi speciali (ad es. amministratori di sistema, super-user) • Tracciamento degli accessi degli utenti alla rete aziendale • Controlli sugli accessi agli applicativi effettuati dagli utenti • Tracciamento e monitoraggio degli eventi di sicurezza sulla rete.		

Reati informatici e 231

In seguito all'introduzione dei crimini informatici tra quelli previsti dal D.Lgs. 231/2001, gli enti dovranno adottare modelli e strumenti concreti di organizzazione, gestione, monitoraggio e controllo al fine di:

- garantire la protezione del patrimonio informativo
- assicurare il corretto utilizzo delle risorse tecnologiche
- disporre di evidenze che documentino l"efficacia dei controlli implementati.

Dovranno essere predisposte preventive ed idonee misure di sicurezza e di controllo per prevenire potenziali reati informatici mediante l'ausilio di strumenti tecnologici

Reati informatici e 231

L’ente non risponde dei reati informatici compiuti attraverso l’utilizzo dei propri sistemi informatici se e solo se prova:

 di avere adottato e attuato efficacemente **modelli di gestione idonei a prevenire il reato**

 di avere affidato ad un **organismo dotato di autonomi poteri d‟iniziativa e di controllo, la vigilanza e l‟aggiornamento di tali modelli**

 l‟elusione fraudolenta di tali modelli di organizzazione e gestione.

Attenzione: in ambito informatico la prova di alcune tipologie di attività è molto complessa da ottenere e può risultare addirittura impossibile, pertanto la prevenzione mediante i modelli 231 è la miglior tipologia possibile di iniziativa

Reati informatici e 231

Principi di controllo:

- Separazione dei ruoli
- Sistemi autorizzativi (processi, procedure e meccanismi tecnici)
- Sistemi di controllo degli accessi (processi, procedure e meccanismi tecnici)
- Tracciamento delle attività svolte sui sistemi/sulla rete
- Monitoraggio ed esecuzione di verifiche periodiche
- Documentazione dei controlli adottati e conservazione delle evidenze raccolte
- Gestione degli incidenti di sicurezza
- Formazione e sensibilizzazione del personale.

Reati informatici e 231

Analisi preliminare	Risk Self Assessment e Gap Analysis	Attuazione
• Richiesta, raccolta e analisi della documentazione • Analisi dell'ambiente aziendale, delle attività della società e ella relativa struttura organizzativa • Interviste preliminari con il management per l'individuazione delle attività sensibili e delle aree di rischio	• Interviste con il management responsabile delle aree sensibili individuate. • Control Risk Self Assessment ai fini della quantificazione dei rischi e dell'identificazione dei controlli per ciascuna attività sensibile. • Gap Analysis tra il sistema di controllo interno rilevato e il "desiderato" come confronto rispetto alle Best Practices.	• Aggiornamento o predisposizione di: – modello – procedure relative attività a rischio di reato – codice etico – criteri di formazione e modalità operative dell'OdV – attività di formazione e informazione
• Mappatura preliminare delle attività sensibili • Individuazione soggetti da intervistare e destinatari questionari	• Mappatura delle aree a rischio • Gap analysis • Piano di lavoro per le azioni migliorative o del sistema di controllo interno	• Parti speciali del Modello

Reati informatici e 231

Matrice attività di controllo/reati

	REATI										
ATTIVITA' DI CONTROLLO	Art.615-ter (accesso abusivo ad un sistema informatico o telematico)	Art.615-quater (detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici)	Art.615-quinquies (diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico)	Art.617-quater (intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche)	Art.617-quinquies (installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche)	Art.635-bis (danneggiamento di informazioni, dati e programmi informatici)	Art.635-ter (danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico, o comunque di pubblica utilità)	Art.635-quater (danneggiamento di sistemi informatici o telematici)	Art.635-quinquies (danneggiamento di sistemi informatici o telematici di pubblica utilità)	Art.491bis (documenti informatici)	Art.640-quinquies (frode informatica del soggetto che presta servizi di certificazione di firma elettronica)
Creazione, modifica, cancellazione di account e di profili	x	x	x	x		x	x	x	x		
Implementazione e manutenzione di nuove reti TLC	x		x	x	x						
Implementazione e manutenzione di sistemi hardware	x			x	x	x	x	x	x		
Implementazione, creazione e manutenzione di software	x		x	x	x	x	x	x	x		
Monitoraggio dei sistemi hardware e software (tentativi di accesso, accessi anomali per frequenza, modalità e temporalità, accesso a sotto-domini, lancio di script, utilizzo di alcuni siti come www.network-tools.com)	x		x			x	x	x			
Monitoraggio dei sistemi hardware e software(casi di disruption, interferenza, verifica fisica delle apparecchiature e scanning delle memorie di massa)			x			x	x	x			
Monitoraggio dei sistemi software (accessi ai database o agli applicativi)				x					x		
Gestione delle credenziali fisiche (badge, pin, codici di accesso, token authenticator, valori biometrici, ecc.)	x	x	x	x	x	x	x	x	x		
Gestione delle attività di security dei siti dei sistemi IT	x	x	x	x	x	x	x	x			
Scanning dei documenti										x	x
Verifica della firma digitale										x	x
Invio di documentazione in formato digitale										x	x
Storing ed accesso ai sistemi informatici										x	x

Esempio

Reati informatici e 231

Punti di attenzione

Identificazione e mappatura delle attività sensibili

Modello di valutazione dei rischi:

- Valutazione dei rischi di sicurezza
- Valutazione delle attività di controllo.

Modelli di controllo per i crimini informatici:

- Processi
- Policy e Procedure
- Controlli di sicurezza da implementare/monitorare.

Reati informatici e 231

Sicurezza delle informazioni – Standard di riferimento Lo standard ISO 27001 (Information security management systems – Requirements) è comunemente adottato a livello internazionale per l'"implementazione di *sistemi di gestione della sicurezza delle informazioni e la loro eventuale certificazione, nonché in ambito di sistemi di controllo interni come quello afferente alla 231, e fornisce indicazioni in merito alle seguenti aree di controllo*:

- - Security Policy
- - Organization of information security
- - Asset management
- - Human resources security
- - Physical and environmental security
- - Communications and operations management.
- - Access Control
- - Information systems acquisition, development and maintenance
- - Information security incident management
- - Business Continuity management
- - Compliance.

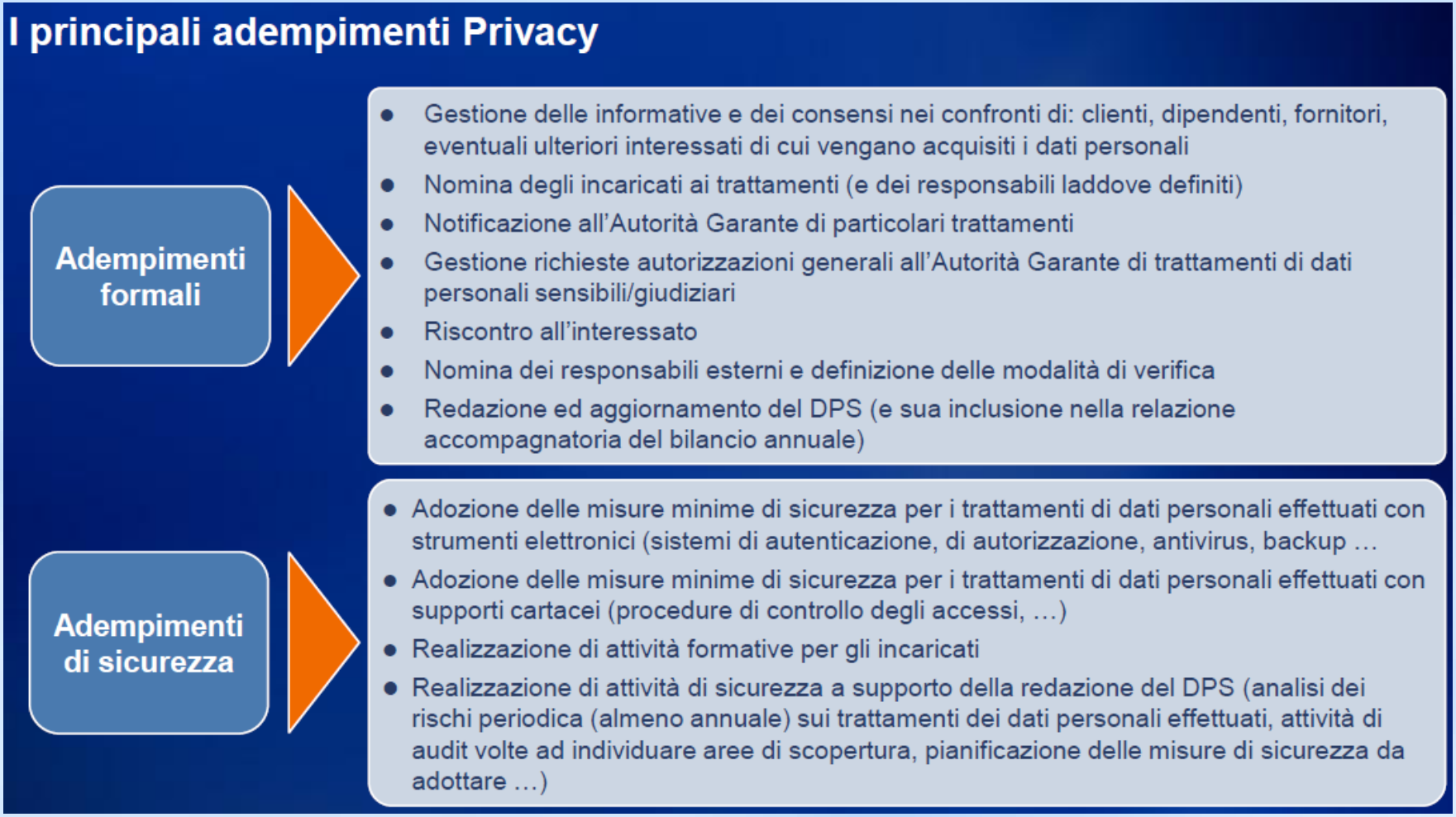
Reati informatici e 231

Reati informatici e 231

Anche la **normativa Privacy** **(D.Lgs. 196/2003)** **copre l‟intero ambito dei processi aziendali e, se implementata correttamente e mantenuta costantemente, offre strumenti utili per contribuire a prevenire e provare gli illeciti di cui alla disciplina del D.Lgs. 231/2001.**

L‟applicazione delle misure di sicurezza richieste dalla normativa Privacy è fondamentale per l‟adeguamento al sistema 231 per poter gestire una serie di rischi (accessi non autorizzati, trattamenti illeciti, ecc.).

Reati informatici e 231



Reati informatici e 231

Possibili punti di integrazione tra 27001 e Privacy con i modelli 231:

- Modelli organizzativi
- Processi e procedure
- Approcci e modelli di valutazione dei rischi – DPS
- Disciplinare utilizzo posta elettronica e internet (linee guida del Garante del marzo 2007)
- Formazione del personale
- Rapporti con l‟OdV (protezione della documentazione, protezione dei flussi informativi, rapporti con i responsabili Privacy, poteri di accesso alle banche dati, ecc.).

Reati informatici e 231

0) TUTTE LE AREE

Accesso ai sistemi ICT aziendali

Uso di posta elettronica

1) CORPORATE GOVERNANCE E DIREZIONE GENERALE

gestione documenti informatici

gestione dati riservati

gestione credenziali e certificati digitali

2) AMMINISTRAZIONE – LEGALE – AFFARI SOCIETARI

gestione documenti informatici

gestione dati riservati

gestione credenziali e certificati digitali per comunicazioni a uffici pubblici

3) FINANZA E CONTROLLO

processi di pagamento

accesso a sistemi di banche e istituzioni finanziarie

Reati informatici e 231

4) COMMERCIALE E VENDITE

accesso a sistemi di clienti e partner commerciali

gestione documenti informatici

5) R&S

accesso a sistemi esterni

gestione documenti informatici

gestione dati riservati

gestione credenziali e certificati digitali

6) RISORSE UMANE

gestione dati riservati, sensibili

7) APPROVVIGIONAMENTO E ACQUISTI

accesso a sistemi di fornitori e partner commerciali

gestione credenziali e certificati digitali per accesso a gare e processi di e-procurement

gestione documenti informatici

Reati informatici e 231

8) PRODUZIONE & LOGISTICA

accesso a sistemi di fornitori, clienti e partner commerciali

gestione credenziali e certificati digitali per comunicazioni a uffici pubblici (es. dichiarazione al registro INES – EPER [“emissioni inquinanti industriali”])

10) SICUREZZA FISICA

presidio e protezione fisica infrastrutture ICT

11) ICT

presidio e protezione logica sistemi ICT

gestione documenti informatici

gestione credenziali di accesso ai sistemi ICT interni, esterni

gestione procedure assegnazione credenziali e certificati digitali

Reati informatici e 231

Alcune Sentenze Cassazione 1993-2009 su reati informatici

41 di cui

18 con attribuzione responsabilità penale per un solo reato informatico

7 con attribuzione responsabilità penale per due reati informatici, tutte con 615-ter

Frequenza	articolo	Frequenza	articolo
5	491-bis	1	635-bis
11	615-ter	0	635-ter
5	615-quater	0	635-quater
0	615-quinquies	0	635-quinquies
4	617-quater	5	640-ter
1	617-quinquies,	0	640-quinquies

Fonte: interrogazione non esaustiva di banche dati giurisprudenza

Grazie. Ing Picchi Gabriele