CORSO DI ALTA FORMAZIONE IN
INFORMATION SECURITY MANAGEMENT

8ª EDIZIONE, ROMA
FEBBRAIO 2011- SETTEMBRE 2011

ICT Risk Management
Aspetti legali

L'impatto del Decreto Legislativo 231/01 sui sistemi informativi

Profili giuridici e applicativi

III parte

Michele Crudele
www.crudele.it
2011-04-14

CONSEL
CONSORZIO ELIS
per la formazione professionale superiore

CEFRIEL
FORGING INNOVATION
POLITECNICO DI MILANO

MIP
POLITECNICO DI MILANO
SCHOOL OF MANAGEMENT

RATIFICA 2008 DELLA CONVENZIONE DI BUDAPEST 2001

- Origine delle modifiche al DLgs 231/01
  - Legge 48/2008: *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*
    - *Service provider: any public or private entity that provides to users of its service the ability to communicate by means of a computer system*
    - *Obtain the expeditious preservation of specified computer data, including traffic data … oblige that person to preserve … to a maximum of ninety days*
- Nel 2001 si citava solamente la frode informatica a danno di ente pubblico

LE CATEGORIE DI REATI INFORMATICI

- Inviolabilità del domicilio informatico
  - Accessi abusivi
  - Diffusione di codici e apparecchiature dannose
- Inviolabilità dei segreti
  - Intercettazione
- Danneggiamento
  - Alterazione o distruzione di dati, programmi e informazioni
- Documento informatico e firma digitale
  - Frodi dei certificatori
  - Falso documento informatico
    - *Rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (Codice dell'amministrazione digitale 2005)*

I REATI INFORMATICI PIÙ COMUNI

- 640-ter: frode informatica
  - Nel Dlgs 231/01 si applica solo se contro lo Stato o ente pubblico
  - Il phishing tra truffa (raggiro) e frode (automatismi)
- 617-quinquies: installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche
  - Cavalli di Troia
- 617-quater: intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
  - “Sniffare” il traffico
    - La vulnerabilità delle connessioni senza fili

I REATI INFORMATICI TIPICI DI AZIENDE INFORMATICHE

- 491-bis: falsità in un documento informatico pubblico o privato
  - Dichiarazione mendace via posta elettronica
  - Manipolazione di documenti elettronici
- 615-ter: accesso abusivo ad un sistema informatico o telematico
  - Il più frequente tra le sentenze della Cassazione
  - Per spionaggio industriale
  - Il caso Wikileaks
- 615-quater: detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
  - Molto frequente, ma spesso a vantaggio del singolo
  - Leggerezza nell'autorizzare persone esterne
- 640-quinquies: truffa del certificatore di firma elettronica
  - C'è anche la posta elettronica certificata

GLI ALTRI REATI INFORMATICI

- 615-quinquies: diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
- 635-bis: danneggiamento di informazioni, dati e programmi informatici
- 635-ter: danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità
- 635-quater: danneggiamento di sistemi informatici o telematici
- 635-quinquies: danneggiamento di sistemi informatici o telematici di pubblica utilità

Gradazione di sanzioni penali: aggravante dell'essere operatore di sistema

Delibera del Garante della privacy 27/11/2008 sugli amministratori di sistema

Forte correlazione e concorso tra tutti i reati informatici

SICUREZZA INFORMATICA

- È un processo, non un prodotto
  - È una mentalità, analoga a quella del sapersi muovere per le strade di una città affollata e trafficata
  - La sicurezza non si raggiunge mai
    - Le tipologie di violazione si evolvono
- Non è solo questione di tecnica
  - Comportamenti prudenti
- Vivere in un ecosistema protetto, ma non isolato
  - Condividere vuol dire rischiare
  - La legislazione imperfetta: il decaduto decreto Pisanu
- Comportamenti con rischio per la sicurezza informatica
  - Il valore del bene digitale
- La sottrazione di identità
  - Più frequente di quanto si pensi
- Il diritto all'oblio su Internet
  - La persistenza dei dati, anche contro la volontà del proprietario

DELIBERA 13/2007 DEL GARANTE DELLA PRIVACY

Linee guida del Garante per posta elettronica e Internet

1. Utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro
2. Codice in materia di protezione dei dati e discipline di settore
3. Controlli e correttezza nel trattamento
4. Apparecchiature preordinate al controllo a distanza
5. Programmi che consentono controlli “indiretti”
6. Pertinenza e non eccedenza
7. Presupposti di liceità del trattamento: bilanciamento di interessi
8. Individuazione dei soggetti preposti

PROVVEDIMENTO 27 NOVEMBRE 2008 DEL GARANTE DELLA PRIVACY

- Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema
  - 2f. *Le registrazioni (access log) devono avere caratteristiche di completezza... Devono comprendere i riferimenti temporali e la **descrizione dell'evento** che le ha generate e ... conservate per un congruo periodo, **non inferiore a sei mesi***
  - FAQ 15: ***non** chiede in alcun modo che vengano registrati **dati sull'attività interattiva** (comandi impartiti, transazioni effettuate) degli amministratori di sistema*
  - Precisazioni: L'Autorità ha constatato che informazioni imprecise o anche talune azioni promozionali da parte di consulenti rischiano di disorientare alcune aziende, soprattutto quelle di piccole dimensioni, esponendole a immotivati aggravi economici.
    - *Le prescrizioni riguardano solo quei soggetti che, nel trattare i dati personali con strumenti informatici, devono ricorrere o abbiano fatto ricorso alla figura professionale dell'amministratore di sistema o a una figura equivalente*
    - *Le prescrizioni non si applicano, invece, a quei soggetti anche di natura associativa che, generalmente dotati di sistemi informatici di modesta e limitata entità e comunque non particolarmente complessi, possano fare a meno di una figura professionale specificamente dedicata alla amministrazione dei sistemi o comunque abbiano ritenuto di non farvi ricorso*
    - *Per quanto concerne gli aspetti tecnici del provvedimento (in particolare, la conservazione dei log degli accessi effettuati dagli amministratori di sistema), l'adeguamento può avvenire anche con **soluzioni a basso costo**, validamente proposte e disponibili in rete (per esempio basate su software gratuito, anche con licenze di tipo open source), che possono costituire valide alternative all'impiego di prodotti commerciali o di apparati più sofisticati*

UN DISCIPLINARE D'USO DELLE RISORSE INFORMATICHE

1. Utilizzo della Posta Elettronica
   - Uso strettamente aziendale
2. Accesso ed utilizzo di Internet
   - Filtering
3. Prescrizioni interne sulla sicurezza dei dati e dei sistemi
   - Tutele automatiche e buone pratiche
   - Lecito scaricare *freeware*
4. Controlli sull'utilizzo degli strumenti elettronici
   - Analisi aggregate anonime
   - Analisi nominali previa comunicazione alla RSU e agli interessati
5. Conseguenze in caso di mancato rispetto delle prescrizioni
   - Provvedimenti disciplinari

LE RISORSE DEI SISTEMI INFORMATIVI

- In relazione al sistema di controlli delle attività sensibili
  - Abilitare funzioni esistenti
  - Completarle e renderle congruenti con le normative
  - Garantire continuità di servizio
    - Prevedere procedure alternative
  - Gestire correttamente il *backup*
  - Simulare *audit* esterno
- Considerare i sistemi informativi come attività sensibile
  - Controllo incrociato delle operazioni degli amministratori
    - Utile anche per evitare errori
  - Ogni amministratore di sistema accede con le sue credenziali

DOCUMENT MANAGEMENT

- Gestisce il flusso in entrata e in uscita
  - Protocollo informatico
- Gestisce la creazione di un progetto
- Gestisce acquisti e vendite
- Facilita il rispetto delle procedure di approvazione
- Autenticazione personale
  - Firma digitale in alcuni casi
- Il potere dell'amministratore di sistema
  - Richieste di eccezione al flusso standard
    - Documentarle fuori dal sistema

LOG MANAGEMENT

- Attivazione della registrazione degli eventi
  - Livello di dettaglio da definire
  - Differenza tra sistema operativo, applicazioni e traffico Internet
- Abilita la tracciabilità
  - Tutto o solo attività sensibili?
    - Decisione
    - Autorizzazione
    - Svolgimento
    - Controllo
- Consente di analizzare lo storico degli eventi
  - Problemi di privacy
- I tempi di conservazione
  - Non inferiore a sei mesi, ma non superiore a...
  - Attenzione a provvedimenti specifici per tipo di registrazione
- La situazione con il *cloud computing*

INTRANET

- Punto di comunicazione centrale
  - Accesso obbligatorio all'inizio di una sessione
- Pubblicazione di procedure e prassi consolidate
  - *Melius abundare quam deficere*
  - Sistema di verifica della lettura da parte degli interessati
- Equilibrio tra formalismo e comunicazione facilitata
  - Lavorare con l'ufficio comunicazione interna
- Opportunità della pubblicazione su web esterno
  - Non tutto
  - Codice etico

FONTI LEGALI AUTOREVOLI

- Il problema dei continui aggiornamenti delle leggi italiane
- La ricerca su Google può dare risultati non affidabili

www.normattiva.it

http://def.finanze.it

http://dbase.ipzs.it

www.garanteprivacy.it

www.confindustria.it

Servizi associativi / Responsabilità degli enti e modelli organizzativi