smau
MILANO
22-24 OTTOBRE 2014

aipsi

La prevenzione dei reati informatici ex D. Lgs. 231/01

Paolo Dal Checco

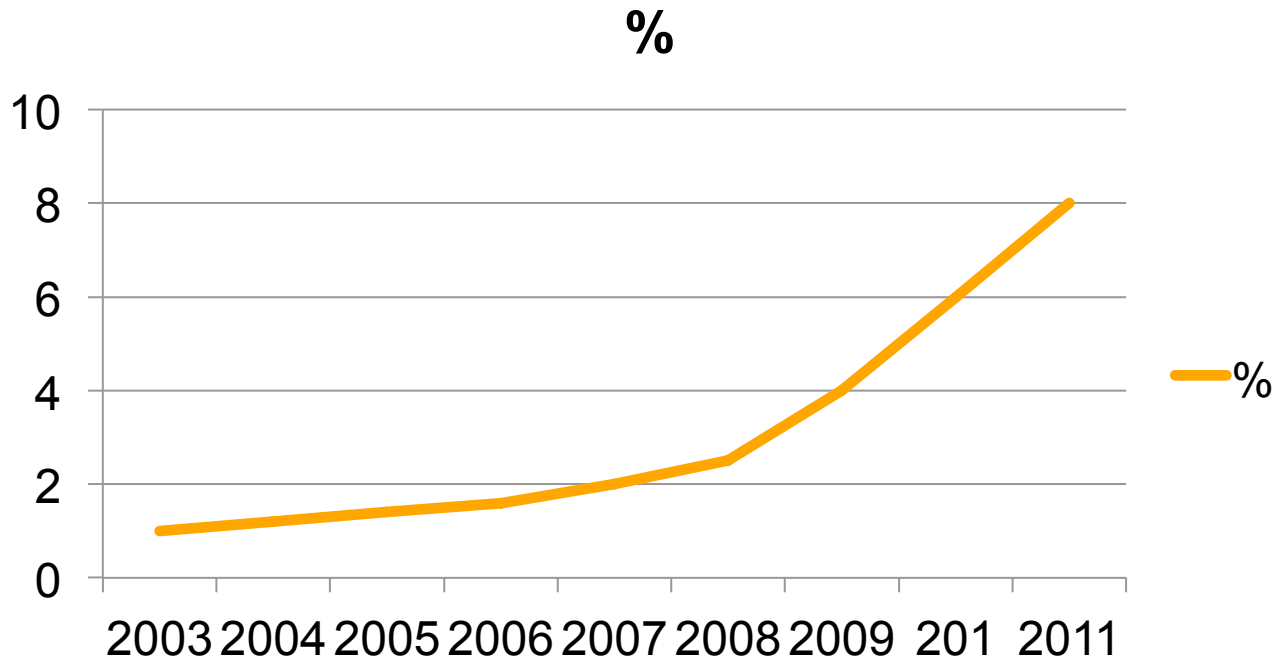
Presentazione relatore

Paolo Dal Checco

- PhD in Informatica @unito, gruppo Computer & Network Security
- Consulente Informatico Forense per Procure, Tribunali, Avvocati, Aziende e privati
- Frequenti attività di Polizia Giudiziaria a supporto delle F.F.O.O. durante perquisizioni e sequestri presso aziende e domicili
- Consulenza su sicurezza e prevenzione dei reati informatici Ex. Art. 231/2001
- Co-titolare, insieme a Giuseppe Dezzani, dello Studio “Digital Forensics Bureau”
- Socio IISFA, CLUSIT, AIP
- DEFT Developer tra i fondatori della DEFT Association

I reati informatici

- In base ad un'analisi dei dati relativi alle denunce presentate in Europa e negli Stati Uniti emerge che il reato informatico sta diventato rapidamente una nuova frontiera del crimine ove vi è una grande percentuale di impatto e di impunità rispetto ai reati tradizionali.



I reati informatici

- Un **crimine informatico** è un fenomeno criminale che si caratterizza nell'abuso della tecnologia informatica.

- I **reati informatici** si distinguono tra :
  - Reati compiuti verso sistemi informatici o telematici;
  - L'utilizzo dell'elaboratore nella realizzazione del fatto.

- La tipologia di reato più frequente è l'accesso a informazioni dei concorrenti, in diverse modalità:
  - Accesso abusivo alla rete informatica
  - Uso di credenziali non disabilitate
  - Acquisizione di informazioni da parte di personale interno

I reati informatici

- Cosa significa prevenire un reato informatico?

- In Informatica prevenire significa :

  – Sensibilizzazione (incluso il rendere consapevoli dei rischi)
  – Formazione
  – Monitoraggio
  – Audit

La Convenzione di Budapest

- La Convenzione, che risale al **23 novembre 2001**, suggerisce agli stati membri del Council of Europe alcuni prinicipi cui ispirarsi nella disciplina sanzionatoria del fenomeno dei reati informatici
- L'idea è di uniformarsi introducendo un minimum target di tutela dei beni giuridici offesi dai cybercrimes e un **livello minimo essenziale comune di strategie di contrasto a tali illeciti**, adottando legislazioni appropriate e promuovendo la cooperazione internazionale.
- Gli stati membri hanno firmato e ratificato in momenti diversi, il fine **è armonizzare e uniformare le normative**

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

La Convenzione di Budapest

- Definizione di alcuni termini:

  - «**sistema informatico**»: qualsiasi apparecchiatura o un gruppo di apparecchi interconnessi o collegati, uno o più dei quali svolge un trattamento automatico dei dati sulla base delle indicazioni fornite dal programma (software);
  - «**dati informatici**»: qualsiasi rappresentazione di fatti, informazioni o concetti idonei ad essere oggetto di trattamento ed elaborazione da parte di un programma o di un sistema informatico;
  - «**prestatore di servizi**»: qualsiasi soggetto pubblico o privato che fornisce agli utenti del suo servizio la capacità di comunicare per mezzo di un sistema informatico, nonché qualunque altro soggetto che, per conto di un primo prestatore di servizi, provvede alla memorizzazione dei dati inerenti le suddette comunicazioni; con l'espressione
  - **«dati relativi al traffico»**: idati – inerenti l'origine, la destinazione, il percorso, l'ora, la data, la dimensione, la durata ed il tipo di servizio – relativi ad una comunicazione realizzata per mezzo di un sistema informatico e generata dallo stesso sistema informatico2.

La Convenzione di Budapest

Situazione in data del : 23/10/2014

Stati membri del Consiglio d'Europa

	Firma	Ratifica	Entrata in vigore	Rinv.	R.	D.	A.	T.	C.	O.
Albania	23/11/2001	20/6/2002	1/7/2004				X			
Andorra	23/4/2013									
Armenia	23/11/2001	12/10/2006	1/2/2007				X			
Austria	23/11/2001	13/6/2012	1/10/2012		X	X	X			
Azerbaijan	30/6/2008	15/3/2010	1/7/2010		X	X	X	X		
Belgio	23/11/2001	20/8/2012	1/12/2012		X	X	X			
Bosnia e Erzegovina	9/2/2005	19/5/2006	1/9/2006				X			
Bulgaria	23/11/2001	7/4/2005	1/8/2005		X	X	X			
Cipro	23/11/2001	19/1/2005	1/5/2005				X			
Croazia	23/11/2001	17/10/2002	1/7/2004				X			
Danimarca	22/4/2003	21/6/2005	1/10/2005		X		X	X		
Estonia	23/11/2001	12/5/2003	1/7/2004				X			
Ex-Repubblica Jugoslava di Macedonia	23/11/2001	15/9/2004	1/1/2005				X			
Finlandia	23/11/2001	24/5/2007	1/9/2007		X	X	X			
Francia	23/11/2001	10/1/2006	1/5/2006		X	X	X			
Georgia	1/4/2008	6/6/2012	1/10/2012			X				
Germania	23/11/2001	9/3/2009	1/7/2009		X	X	X			
Gran Bretagna	23/11/2001	25/5/2011	1/9/2011		X		X			
Grecia	23/11/2001									
Irlanda	28/2/2002									
Islanda	30/11/2001	29/1/2007	1/5/2007		X		X			
Italia	23/11/2001	5/6/2008	1/10/2008				X			
Lettonia	5/5/2004	14/2/2007	1/6/2007		X		X			
Liechtenstein	17/11/2008									
Lituania	23/6/2003	18/3/2004	1/7/2004		X	X	X			
Lussemburgo	28/1/2003	16/10/2014	1/2/2015				X			
Malta	17/1/2002	12/4/2012	1/8/2012			X				
Moldavia	23/11/2001	12/5/2009	1/9/2009			X	X	X		

http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ITA&NT=185

La Convenzione di Budapest

Moldavia	23/11/2001	12/5/2009	1/9/2009			X	X	X		
Monaco	2/5/2013									
Montenegro	7/4/2005	3/3/2010	1/7/2010	55	X		X			
Norvegia	23/11/2001	30/6/2006	1/10/2006		X	X	X			
Paesi Bassi	23/11/2001	16/11/2006	1/3/2007				X	X		
Polonia	23/11/2001									
Portogallo	23/11/2001	24/3/2010	1/7/2010			X	X			
Repubblica Ceca	9/2/2005	22/8/2013	1/12/2013		X	X	X			
Repubblica Slovacca	4/2/2005	8/1/2008	1/5/2008		X	X	X			
Romania	23/11/2001	12/5/2004	1/9/2004				X			
Russia										
San Marino										
Serbia	7/4/2005	14/4/2009	1/8/2009	55			X			
Slovenia	24/7/2002	8/9/2004	1/1/2005				X			
Spagna	23/11/2001	3/6/2010	1/10/2010			X	X			
Svezia	23/11/2001									
Svizzera	23/11/2001	21/9/2011	1/1/2012		X	X	X			
Turchia	10/11/2010	29/9/2014	1/1/2015							
Ucraina	23/11/2001	10/3/2006	1/7/2006		X		X			
Ungheria	23/11/2001	4/12/2003	1/7/2004		X	X	X			

http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ITA&NT=185

La Convenzione di Budapest

Non membri del Consiglio d'Europa

	Firma	Ratifica	Entrata in vigore	Rinv.	R.	D.	A.	T.	C.	O.
Argentina										
Australia		30/11/2012 a	1/3/2013		X		X			
Canada	23/11/2001									
Cile										
Colombia										
Costa Rica										
Filippine										
Giappone	23/11/2001	3/7/2012	1/11/2012		X	X	X			
Israele										
Marocco										
Mauritius		15/11/2013 a	1/3/2014				X			
Messico										
Panama		5/3/2014 a	1/7/2014				X			
Repubblica Dominicana		7/2/2013 a	1/6/2013			X	X			
Senegal										
Stati-Uniti d'America	23/11/2001	29/9/2006	1/1/2007		X	X	X			
Sud Africa	23/11/2001									
Tonga										

Numero totale di firme non seguite da ratifiche :	9
Numero totale di ratifiche/adesioni :	44

Rinvii :
(55) Date of signature by the state union of Serbia and Montenegro.
a.: Adesione - s.: Firma senza riserva di ratifica - su.: Successione - r.: Firma "ad referendum".
R.: Riserve - D.: Dichiarazioni - A.: Autorità - T.: Applicazione Territoriale - C.: Comunicazione - O.: Obiezione.

Fonte: Ufficio dei Trattati, http://conventions.coe.int – * Disclaimer

http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ITA&NT=185

Legge 48/2008

- **18 marzo 2008, quasi 7 anni dopo la convenzione di Budapest**
- "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"
- Aggiornamento del nostro ordinamento in materia di cybercrime pubblicato nella Gazzetta Ufficiale n. 80 del 4 aprile 2008 Supp. Ord. n. 79
- Importante per le modifiche introdotte nel Codice di Procedura Penale
- **Causa l'introduzione dell'Art. 24 bis nel D.lgs 231/2001**
- Causa a sua volta aggiornamento del MOG introducendo una nuova Parte Speciale in cui, per la prima volta, le aziende devono iniziare a **prevenire la commissioni di reati informatici commessi a proprio vantaggio** e, di conseguenza, potenzialmente commessi all'interno del perimetro aziendale

Legge 48/2008

- La legge pone forte accezione sull'adottare "misure tecniche dirette ad assicurare la **conservazione dei dati originali e ad impedirne l'alterazione**", eseguire acquisizioni che avvengano "mediante copia di essi su adeguato supporto, con una procedura che assicuri la **conformità dei dati acquisiti a quelli originali** e la loro immodificabilità" e "custodire i reperti con l'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria" precisando che "**la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria**»"
  - Art. 244 CPP "Casi e forme delle ispezioni"
  - Art. 247 CPP "Casi e forme delle perquisizioni"
  - Art. 254-bis: Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni
  - Art. 259 CPP "Custodia delle cose sequestrate" Art. 260 "Apposizione dei sigilli alle cose sequestrate. Cose deperibili"
  - Art. 352 Perquisizioni
  - Art. 354 - Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro

Legge 48/2008

- A questo punto gli per gli amministratori di rete la problematica si inverte: devono non solo più pensare alla difesa del proprio perimetro esterno, ma anche iniziare a confrontarsi con una visione del tutto nuova della sicurezza, valutando gestione e tracciatura delle informazioni all'interno della rete aziendale.
- I cosiddetti *penetration test* – in genere eseguiti dall'esterno verso l'interno non bastano più

D.Lgs 231/2001

- **Responsabilità amministrativa** delle società e degli enti,
- Prevede il Modello di Organizzazione e Gestione", **MOG** o **"Modello ex D.Lgs. n. 231/2001"** che è un atto privato adottato da una persona giuridica, o associazione priva di personalità giuridica, volto a **prevenire la responsabilità penale derivante dal D.lgs 8 giugno 2001 n. 231**.
- Estende alle persone giuridiche la responsabilità per reati commessi in Italia ed all'estero da persone fisiche che operano per la società per alcuni **reati commessi nell'interesse o a vantaggio degli stessi**
- Non è obbligatorio dotarsi di un Modello Organizzativo (MOG), ma **l'organizzazione non risponde del reato** se dimostra di avere adottato ed efficacemente attuato un modello organizzativo idoneo a prevenire la commissione di tali illeciti

D.Lgs 231/2001

- Secondo il D.Lgs. n. 231/2001, la società è responsabile per i reati commessi nel suo interesse o a suo vantaggio:
  - da "**persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione** dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dell'ente stesso" (cosiddetti soggetti **apicali**);
  - da **persone sottoposte alla direzione o alla vigilanza di uno dei soggetti in posizione apicale** (cosiddetti soggetti **sottoposti** all'altrui direzione);
- La società non risponde, per espressa previsione legislativa (art. 5, comma 2, D.Lgs. n. 231/2001), se le persone indicate hanno agito nell'**interesse esclusivo proprio o di terzi**.

D.Lgs 231/2001

- L'art. 6 del D. Lgs. n. 231/2001 prevede che la società possa essere esonerata dalla responsabilità conseguente alla commissione dei reati indicati se prova che:

  - a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, **modelli di organizzazione e di gestione idonei a prevenire reati della specie di quelli verificatisi**;
  - b) il compito di vigilare sul funzionamento, l'efficacia e l'osservanza dei modelli nonché di curare il loro **aggiornamento** è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo, il cosiddetto **organismo di vigilanza**;
  - c) le persone fisiche **hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione**;
  - d) **non vi sia stata omessa o insufficiente vigilanza** da parte dell'organismo di cui alla precedente lettera b).

D.Lgs 231/2001

- Le sanzioni previste dalla legge a carico della società consistono in:
  - sanzione **pecuniaria**, applicata secondo quote;
  - **interdizione** dall'esercizio dell'attività (anche in via definitiva, art. 16 D.lgs 231/2001)
  - **sospensione** o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito,
  - **divieto** di contrattare con la Pubblica Amministrazione;
  - **esclusione** da agevolazioni, finanziamenti, contributi o sussidi ed eventuale **revoca** di quelli concessi;
  - divieto di **pubblicizzare** beni o servizi;
  - **confisca** del prezzo o del profitto che la società ha tratto dal reato (e sequestro conservativo, in sede cautelare);
  - **pubblicazione** della sentenza di condanna, che può essere disposta in caso di applicazione di una sanzione interdittiva.
  - **commissariamento** dell'ente

D.Lgs 231/2001

- Trai i reati identificati dal legislatore possiamo elencarne alcuni:

  - Indebita percezione di erogazioni pubbliche;
  - Truffa ai danni dello Stato o di altro Ente Pubblico;
  - Illegale ripartizione degli utili;
  - Falsità nelle comunicazioni sociali;
  - Operazioni in pregiudizio dei creditori;
  - Formazione fittizia del capitale;
  - Indebita influenza nell'assemblea;
  - Ostacolo all'esercizio della funzione di pubblica vigilanza;
  - Aggiotaggio;
  - Frode informatica a danno dello Stato o di altro Ente Pubblico;
  - Corruzione e Concussione;
  - Reati in tema di erogazioni pubbliche;
  - Reati contro la personalità individuale

D.Lgs 231/2001

- In particolare, per i **reati informatici** (introdotti dall'Art .48/2008) abbiamo un elenco di **reati presupposti**:

  - Attentato a impianti di pubblica utilità compreso il danneggiamento (Art. 420 c.p.)
  - Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.);
  - Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.);
  - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.);
  - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.);
  - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.);

D.Lgs 231/2001

- In particolare, per i **reati informatici** (continua da slide precedente):
  - Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 615-quinquies c.p.);
  - Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.);
  - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.);
  - Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.);
  - Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.);
  - Frode informatica del certificatore di **firma elettronica** (art. 640-quinquies c.p.)
  - Falsità di documenti informatici (art. 491 bis c.p.)

D.Lgs 231/2001

- Ma non dimentichiamo i reati sulla **violazione del diritto d'autore**:
  - Messa a disposizione del pubblico in un sistema di reti telematiche che, mediante connessioni di qualsiasi genere, e senza averne diritto di un'opera o di parte di un'opera dell'ingegno protetta (art. 171, co. 1, lett a-bis, L. 633/1941)
  - Abusiva duplicazione, per trarne profitto, di programmi per elaboratore;[…] (art. 171-bis, co. 1, L. 633/1941)
  - Riproduzione su supporti, non contrassegnati SIAE, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca da, al fine di trarne profitto; […] (art. 171-bis, co. 2, L. 633/1941)
  - […]

D.Lgs 231/2001 – Alcuni esempi

- **Esempi di reati commessi a vantaggio dell'Ente Collettivo**

- **Detenzione e diffusione abusiva di codici di accesso** a sistemi informatici o telematici (art. 615-quater c.p.): un soggetto A che passando da un'azienda X ad un'azienda Y continui ad accedere ai dati della società X attraverso gli strumenti della società Y impiegando codici di accesso ancora attivi e tragga vantaggio per se e per l'azienda Y dai dati acquisiti dal sistema informativo della società X (la condotta troverà anche contestazione nell'accesso abusivo ed in altri reati descritti nelle presenti slide)
- Un dipendente licenziato dovrebbe rimuovere ogni codice d'accesso o credenziale della società da cui proviene…

D.Lgs 231/2001 – Alcuni esempi

- **Esempi di reati commessi a vantaggio dell'Ente Collettivo**

- Installazione di **apparecchiature atte ad intercettare, impedire o interrompere comunicazioni** informatiche o telematiche (art. 615-quinquies c.p.): Il reato potrebbe configurarsi con il vantaggio concreto della società, nel caso in cui **un dipendente impedisca una determinata comunicazione** in via informatica al fine di evitare che un'impresa concorrente trasmetta i dati e/o l'offerta per la partecipazione ad una gara.
- Altra modalità attraverso cui è possibile compiere il reato è quello di **intercettare una comunicazione** informatica (tra cui sono comprese anche quelle tra apparati mobili con strumenti quali Pad, etc.) da cui acquisire dati utili ad attività vantaggiose per l'ente per da cui si dipende

D.Lgs 231/2001 – Alcuni esempi

- **Esempi di reati commessi a vantaggio dell'Ente Collettivo**

- **Danneggiamento di informazioni, dati e programmi informatici** (art. 635-bis c.p.): il danneggiamento potrebbe essere commesso a vantaggio della società laddove l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte di un fornitore della società o al fine di contestare il corretto adempimento delle obbligazioni da parte del medesimo o, ancora, nell'ipotesi in cui vengano danneggiati dei dati aziendali "compromettenti".

D.Lgs 231/2001 – Alcuni esempi

- **Esempi di reati commessi a vantaggio dell'Ente Collettivo**

- Un dipendente che fuoriesce da una società e trova impiego in una nuova società, in cui **trasferisce archivi informatici copiati dal precedente datore di lavoro**: L'utilizzo degli archivi costituisce un vantaggio per la società in cui si trova a prestare la propria attività lavorativa. Il datore di lavoro deve vigilare che condotte di questo tipo non accadano, mentre il dipendente ha commesso certamente un accesso abusivo al sistema informatico del precedente datore di lavoro in quanto ha effettuato un accesso per fini differenti da quello per cui le credenziali gli sono state assegnate.

- Non è facile per l'azienda monitorare questo illecito, ma non impossibile…

D.Lgs 231/2001 – Alcuni esempi

- **Esempi di reati commessi a vantaggio dell'Ente Collettivo**

- Un dipendente utilizza **software privi di licenza d'uso**: la condotta determina un ingente risparmio in termini economici sull'acquisto delle licenze che può costituire concorrenza sleale sul mercato, avendo un conseguente abbattimento dei costi di produzione.

- Un dipendente **falsifica scritture contabili** al fine di procurare provviste di denaro in nero da utilizzarsi nella libera disponibilità degli apicali: esempio, esegue delle scritture contabili da cui risulta l'acquisto di beni consumabili non facilmente controllabili, come servizi, il cui la somma pagata viene resa in nero, oppure non viene del tutto effettuato il pagamento, determinando il diretto occultamento della somma di denaro.

D.Lgs 231/2001

- Adempiere agli **obblighi legislativi** che ne derivano richiede, tra l'altro, di:
  - adottare, prima della commissione del fatto, **modelli organizzativi** e gestionali idonei a prevenire reati;
  - costituire un **organismo di vigilanza** dell'ente con compito di vigilare efficacemente sul funzionamento e sull'osservanza di modelli e curare il loro aggiornamento;
  - definire i modelli di **organizzazione** e **gestione**;
  - essere in grado di **evitare** la commissione del reato se non mediante l'elusione fraudolenta dei modelli stessi;
  - **individuare** le attività nel cui ambito possono essere commessi tali reati;
  - prevedere specifici protocolli diretti a programmare la **formazione** e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
  - individuare modalità di **gestione delle risorse finanziarie** idonee ad impedire la commissione di reati

D.Lgs 231/2001

- Alcune note sulla data retention e l'importanza dei log file.
- Il Garante per la Privacy indica la durata di retention:
    - 6 mesi per accessi amministrativi [doc. web n. 1577499 G. Privacy]
    - 12 mesi per accessi a posta elettronica
    - 24 mesi per telefonia
- Necessità di archiviazione sicura e policy di accesso
- Attenzione alla quantità di informazioni archiviate

D.Lgs 231/2001

- Come regola generale si può utilizzare il Doc. Eeb n. 1538224 del Garante della Privacy

CONSIDERATO che è ora previsto un periodo unico di conservazione pari a 24 mesi per i dati di traffico telefonico, a 12 mesi per i dati di traffico telematico e a 30 giorni per i dati relativi alle chiamate senza risposta, senza distinzioni in base al tipo di reato;

- Massimo rispetto comunque dei vincoli di riservatezza e accesso (soprattutto in tempo reale) dei dati, tenendo presente anche l'Art.4 dello Statuto dei Lavoratori

D.Lgs 231/2001

- Ci sono poi dei punti un po' oscuri, come il Doc. Eeb n. 1482111 del Garante della Privacy

Al contrario non rientrano, ad esempio, nell'ambito applicativo del presente provvedimento:

- i soggetti che offrono direttamente servizi di comunicazione elettronica a gruppi delimitati di persone (come, a titolo esemplificativo, i soggetti pubblici o privati che consentono soltanto a propri dipendenti e collaboratori di effettuare comunicazioni telefoniche o telematiche). Tali servizi, pur rientrando nella definizione generale di "servizi di comunicazione elettronica", non possono essere infatti considerati come "accessibili al pubblico". Qualora la comunicazione sia instradata verso un utente che si trovi al di fuori della c.d. "rete privata", i dati di traffico generati da tale comunicazione sono invece oggetto di conservazione *(ad es., da parte del fornitore di cui si avvale il destinatario della comunicazione, qualora si tratti di un messaggio di posta elettronica; cfr. documento di lavoro "Tutela della vita privata su Internet–Un approccio integrato dell'EU alla protezione dei dati on-line", adottato dal Gruppo di lavoro per la tutela dei dati personali il 21 novembre 2000)*;

- Che tramite un'interrogazione diretta al Garante siamo riusciti parzialmente a smarcare

D.Lgs 231/2001

- L'utente deve essere informato per poter tutelare i suoi diritti e i suoi dati

Garante Privacy: controlli sui PC aziendali

Date: 14/02/2013 Author: Paolo Reale

Like 0 Condividi +1 Share

L'Ufficio Stampa del Garante della Privacy pubblica nell'ultima *newsletter* (n. 369 del 14.02.2013) un'importante indicazione in merito ai controlli effettuati sui PC dei dipendenti: "*Una società non può controllare il contenuto del pc di un dipendente senza averlo prima informato di questa possibilità e senza il pieno rispetto della libertà e della dignità del lavoratore.*"

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

L'indicazione scaturisce da una contestazione fatta al Garante da un lavoratore, il quale **si è visto licenziare in base agli elementi trovati in una cartella personale del pc portatile assegnato. Detta cartella era stata analizzata dall'azienda quando il dipendente aveva riportato il computer in sede per la periodica operazione di salvataggio dei dati (back up) aziendali.**

Il Garante ha constatato che l'uomo non era stato informato né sui limiti di utilizzo del PC, né sulla possibilità che potessero essere avviate "*cosi penetranti operazioni di analisi e verifica sulle informazioni contenute nel pc stesso.*"

Il datore di lavoro può "*effettuare controlli mirati al fine di verificare l'effettivo e corretto adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro.* ***Tale attività, però, può essere svolta solo nel rispetto della libertà e della dignità dei lavoratori e della normativa sulla protezione dei dati personali che prevede, tra l'altro che alla persona interessata debba essere sempre fornita un'idonea informativa sul possibile trattamento dei suoi dati connesso all'attività di verifica e controllo.***"

D.Lgs 231/2001

Controlli sui pc aziendali sì, ma nel rispetto di precise regole

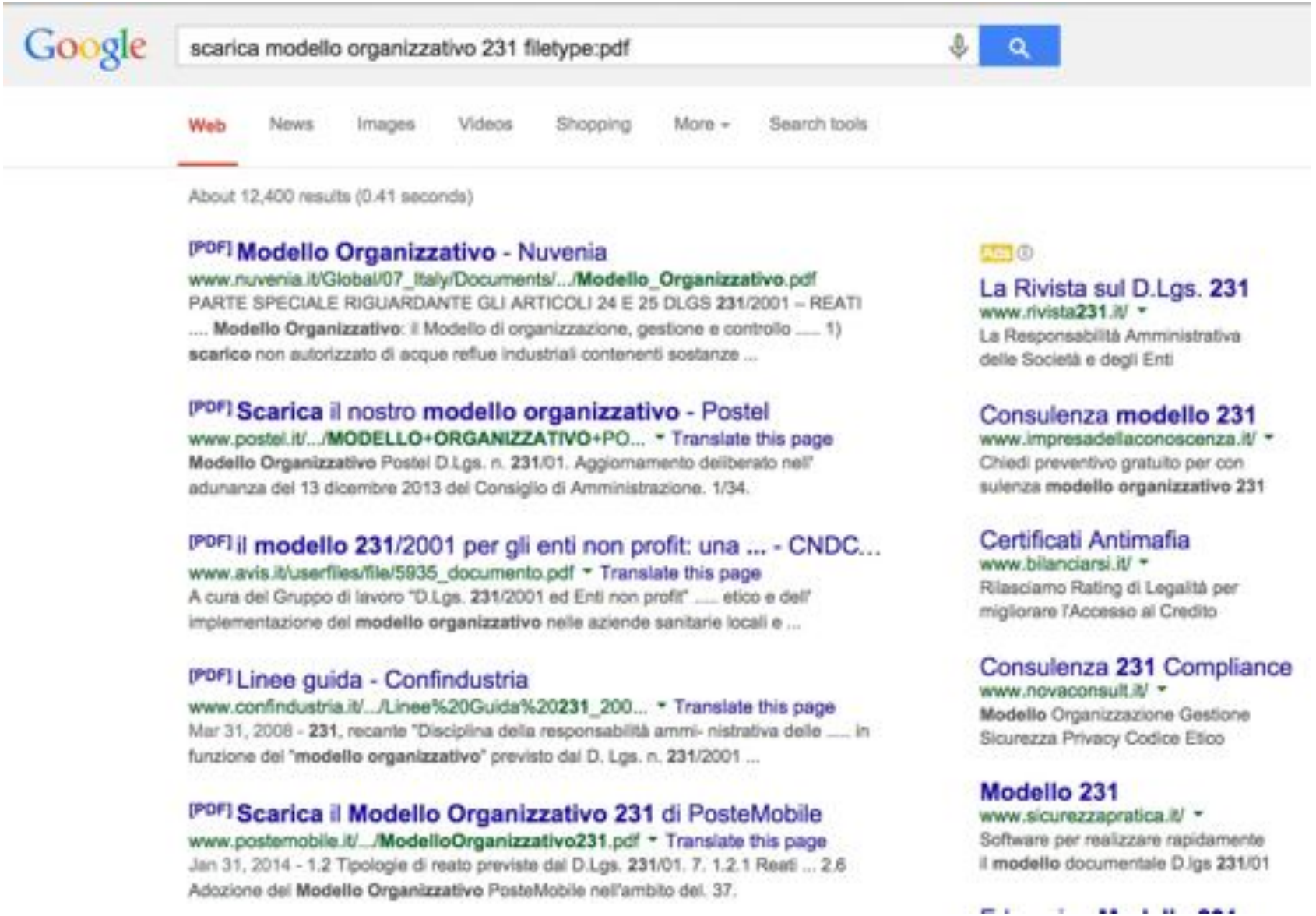
Una società non può controllare il contenuto del pc di un dipendente senza averlo prima informato di questa possibilità e senza il pieno rispetto della libertà e della dignità del lavoratore. Questa la decisione del Garante sul **ricorso [doc. web n. 2149222]** presentato da un dipendente che era stato licenziato senza preavviso dalla propria azienda. L'uomo si era rivolto sia alla magistratura ordinaria, per contestare la stessa fondatezza dell'accusa e il relativo licenziamento, sia al Garante per opporsi alle modalità con cui la società avrebbe acquisito e trattato i suoi dati.

Dai riscontri dell'Autorità è emerso che una serie di documenti, sulla base dei quali il datore di lavoro aveva fondato la sua decisione, erano contenuti in una cartella personale del pc portatile assegnato al lavoratore. La società vi aveva avuto accesso quando il dipendente aveva riportato il computer in sede per la periodica operazione di salvataggio dei dati (back up) aziendali. Contrariamente a quando affermato dall'impresa, non risulta però che l'uomo fosse stato informato sui limiti di utilizzo del bene aziendale, né sulla possibilità che potessero essere avviate così penetranti operazioni di analisi e verifica sulle informazioni contenute nel pc stesso.

Il Garante ha ribadito che il datore di lavoro può effettuare controlli mirati al fine di verificare l'effettivo e corretto adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro.

Tale attività, però, può essere svolta solo nel rispetto della libertà e della dignità dei lavoratori e della normativa sulla protezione dei dati personali che prevede, tra l'altro che alla persona interessata debba essere sempre fornita un'idonea informativa sul possibile trattamento dei suoi dati connesso all'attività di verifica e controllo. Il Garante ha quindi vietato alla società ogni ulteriore utilizzo dei dati personali così acquisiti. Sarà invece l'autorità giudiziaria a valutare l'utilizzabilità nel procedimento civile già in corso della documentazione acquisita agli atti.

D.Lgs 231/2001



D.Lgs 231/2001

10) REATI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

Art. 24 bis del D.Lgs. 231/01

Art. 615 ter c.p. – 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.

Sanzioni pecuniarie: da € 25.823 a € 774.865

Sanzioni interdittive: da 3 a 24 mesi

Test 231

- Un Modello Organizzativo non deve limitarsi alla sola valutazione cartacea dei reati, riducendo il documento ad un mero elenco dei reati (“reati presupposto), ripetendo di fatto quanto già documentato nel Codice Penale.

- La valutazione deve prevedere l’integrazione deii **Penetration Test** e dei **Vulnerability Assessment** con una verifica interna aggiuntiva, che chiamiamo “Test 231”

- Non può esistere un sistema in grado di prevenire i reati se non è – allo stesso tempo – sicuro.

- Pensiamo ad esempio a un’azienda con rete con classi non separate in base ai ruoli, autenticazioni deboli (es. IMAP, POP), vulnerabilità sui server, password semplici… ne abbiamo viste a decine e credo anche voi.

Test 231

- Cosa manca normalmente nei testi informatici : l'analisi dei LOG.

- I test hanno come obbiettivo la valutazione della sicurezza ad un certo momento storico della società, momento in cui viene commissionato. Non hanno come visione la futura valutazione di un evento.

- Un test svolto in campo 231 deve valutare anche la disponibilità di dati utili ad accertare un evento (incidente informatico) tipicamente avvenuto nel passato (più o meno recente) e documentabile solo attraverso i dati raccolti istantaneamente e conservati dai sistemi di analisi.

- Questa disponibilità, notificata ai dipendenti, crea consapevolezza del tracciamento e fa da deterrente circa i comportamenti previsti dai reati presupporto, permettendo di ottenere così **reale prevenzione dei reati**

Test 231

- Riteniamo utile valutare la possibilità di utilizzo di software o configurazioni di Windows finalizzati a eseguire, oltre che endpoint protection, anche logging o policy enforcing:

- **Windows: Policy di dominio opportunamente configurate**
- **Macafee http://www.mcafee.com/us/products/total-protection-for-data-loss-prevention.aspx**
- **Lumension: https://www.lumension.com/endpoint-management-security-suite.aspx**

Contatti

- www.dalchecco.it /www.difob.it
- paolo@dalchecco.it / pdc@difob.it
- @forensico, @studiodifob

Grazie...