ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

La legge di recepimento della direttiva 136/2009/Ce sulla Security Breach Notification (Violazione dei dati personali) e sulle comunicazioni elettroniche

FABIO DI RESTA

SPECIALISTA LEGALE PRIVACY E DIRITTO DELLE NUOVE TECNOLOGIE

ISO 27001 ICT SECURITY AUDITOR - LLM

STUDIO LEGALE DI RESTA – WWW.STUDIOLEGALEDIRESTA.IT

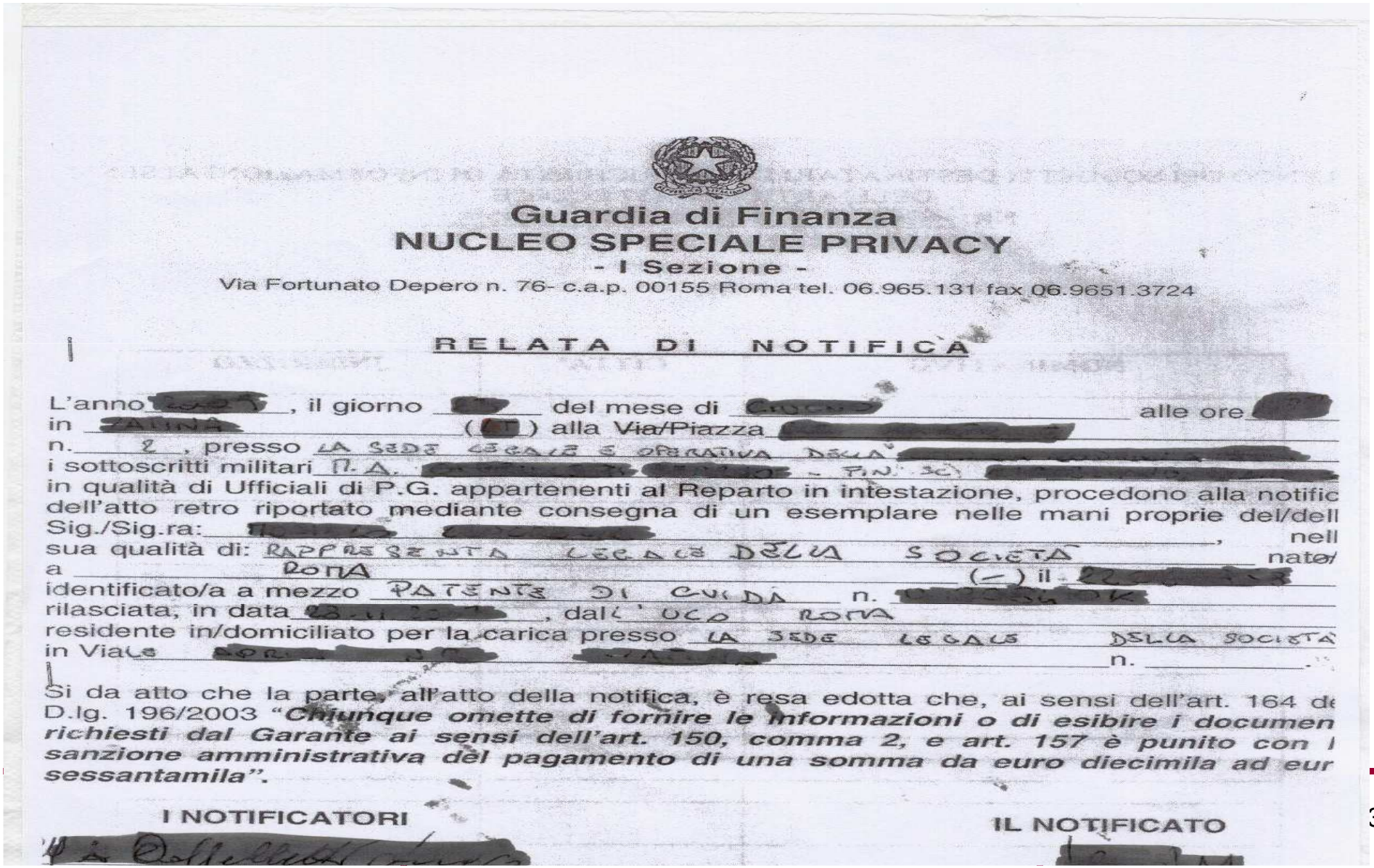
INFO@STUDIOLEGALEDIRESTA.IT

Esigenza di Integrare delle misure logiche ed organizzative

Esigenza di adottare Policy, linee guida e atti regolamentari, informative (procedure,linee guida, ecc.), le quali devono delimitare l'ambito generale in cui opera l'ente e che vincola l'ente stesso.

Le misure organizzative hanno un forte impatto sulle misure logiche in ambito IT: Provv. Garante privacy sulla navigazione e posta elettronica e il Provv. Garante privacy sulle attribuzioni degli amministratori di sistema.

Contestazione mancata adozione del regolamento sulla navigazione e l'accesso alla posta elettronica



Guardia di Finanza
NUCLEO SPECIALE PRIVACY
- I Sezione -
Via Fortunato Depero n. 76- c.a.p. 00155 Roma tel. 06.965.131 fax 06.9651.3724

RELATA DI NOTIFICA

L'anno [redacted], il giorno [redacted] del mese di [redacted] alle ore [redacted]
in [redacted] ([redacted]) alla Via/Piazza [redacted]
n. [redacted], presso LA SEDE LEGALE E OPERATIVA DELLA [redacted]
i sottoscritti militari M.A. [redacted] - F.N. [redacted]
in qualità di Ufficiali di P.G. appartenenti al Reparto in intestazione, procedono alla notific
dell'atto retro riportato mediante consegna di un esemplare nelle mani proprie del/dell
Sig./Sig.ra: [redacted], nell
sua qualità di: RAPPRESENTA LEGALE DELLA SOCIETA' nato/
a ROMA (-) il [redacted]
identificato/a a mezzo PATENTE DI GUIDA n. [redacted]
rilasciata, in data [redacted], dall'UCO ROMA
residente in/domiciliato per la carica presso LA SEDE LEGALE DELLA SOCIETA'
in Viale [redacted] n. [redacted].

Si da atto che la parte, all'atto della notifica, è resa edotta che, ai sensi dell'art. 164 d
D.lg. 196/2003 "***Chiunque omette di fornire le informazioni o di esibire i documen
richiesti dal Garante ai sensi dell'art. 150, comma 2, e art. 157 è punito con l
sanzione amministrativa del pagamento di una somma da euro diecimila ad eur
sessantamila***".

I NOTIFICATORI

IL NOTIFICATO

Illecito contestato

E' stata contestata l'omessa adozione del regolamento per l'utilizzazione della navigazione e della posta elettronica (Provv. Garante, 1 marzo 2007, Bollettino, n. 81)

Qual è il contesto dell'ispezione?

Violazione della libertà e dignità del dipendente – Segnalazione/ricorso oppure iniziativa d'ufficio

<u>Possibili reati</u> connessi:

Accesso alle email del dipendente senza una corretta procedura: art. 616 c.p.: violazione, sottrazione e soppressione della corrispondenza? Cass. 19 dicembre 2007 n. 47096 (policy aziendali)

Reato sul divieto di controllo a distanza reato ex art. 38 dello Statuto dei lavoratori e art. 114 del Codice della Privacy (prevista oblazione)

<u>Sanzione amministrative</u>

La inosservanza delle misure prescritte dal provvedimento del Garante privacy ex art. 162 comma 2 ter, C.d.P., da 30 mila a 180 mila euro (rif. Provv. pronunciati ai sensi dell'art. 154 lett. c e d)

Illecito contestato

E’ sufficiente un accordo sindacale per tutelare la azienda?

I profili di riservatezza dei dati personali vanno tenuti distinti dai profili di monitoraggio (controllo a distanza del lavoratore)

Ci sono due profili distinti: Divieto di controllo a distanza (giurisprudenza) e protezione dei dati personali (Provvedimenti Garante privacy)

Punti essenziali delle Linee Guida - Illecito

Controllo a distanza (Art. 114 C.d.P. e Art. 4 S.d.L./legge 300/70)

Il Garante riconosce la possibilità di effettuare controlli difensivi per tutelare il patrimonio aziendale e prevenire atti illeciti dei dipendenti infedeli, purchè vi siano le **policy aziendali specifiche ed i dipendenti siano adeguatamente informati** sulle modalità per effettuare i controlli graduali sulla:

Navigazione - **controlli limitati ai dati esteriori sul traffico telematico e controlli graduali** (in caso di traffici anomali, prima avvisi generalizzati o di gruppo, poi controlli su base individuale)

Posta elettronica - **controlli limitati ai dati esteriori (header del messaggio),** accesso al contenuto delle email tramite il fiduciario

Privacy – Sicurezza e Tutela del lavoratore – Tabella riepilogativa

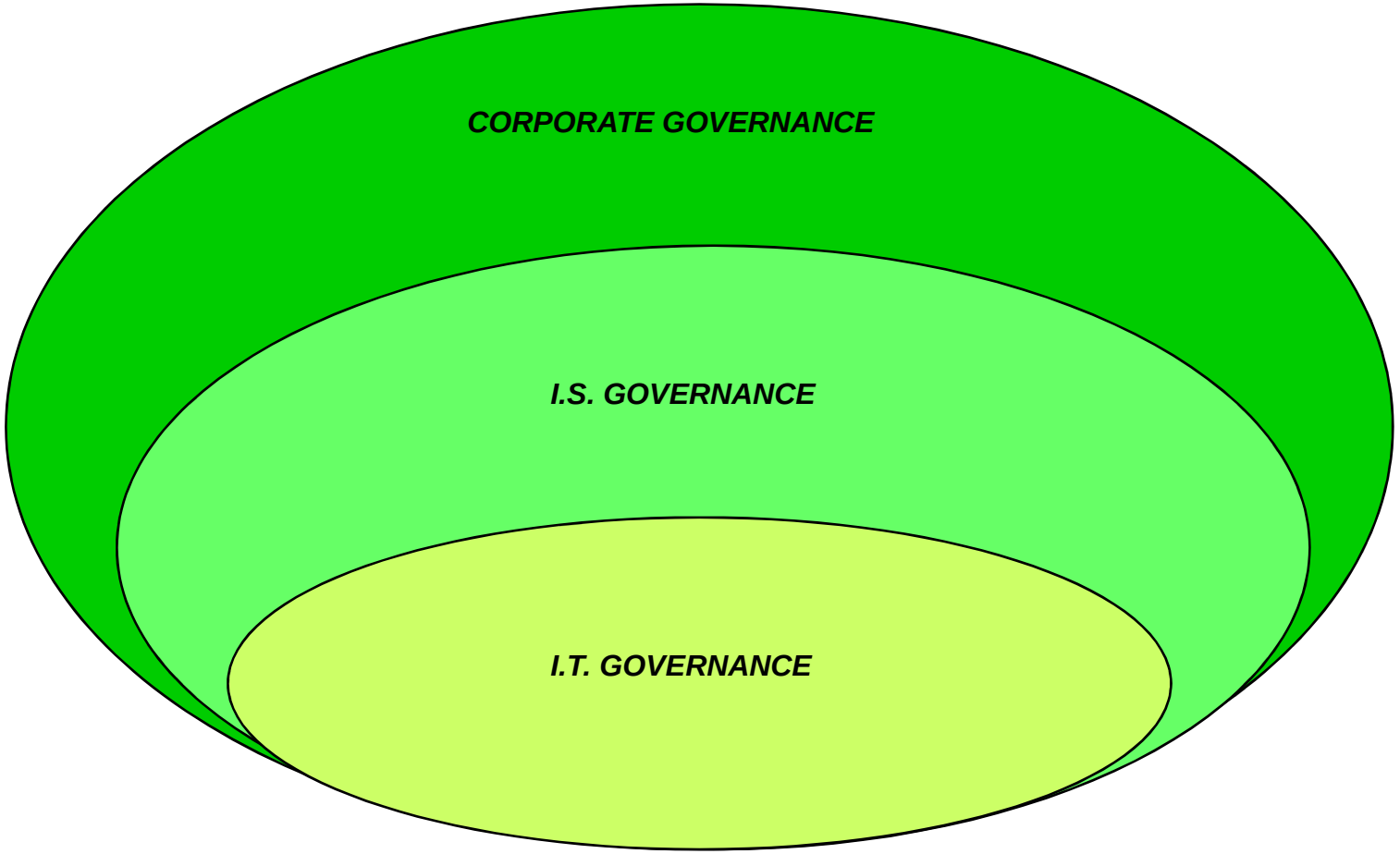
Controlli in ambito IT – Privacy, sicurezza e tutela dei lavoratori			
	Monitoraggio	Audit	Verifiche dettagliate su dati di traffico esteriori
Misura di sicurezza obbligatoria/consentita	Sì	Sì	Sì, ma solo adottando una procedura di controllo graduale e volta ad individuare anomalie dannose per l'azienda
Frequenza	Quotidiana	Annuale	Occasionale
Obiettivi	Rilevazione anomalie di traffico del sistema informatico	Verificare l'operato degli AdS	Individuare specifiche responsabilità di comportamenti anomali

La deficienza organizzativa riscontrata attiene alla sicurezza organizzativa e non alla sicurezza IT, ma ha un impatto sull'ambito IT

Esigenza di integrare la sicurezza informatica con la sicurezza delle informazioni

Tutte e due sono parte integrante della più generale corporate governance

Corporate Governance



C.d. Due deligence – d.lgs. 231/2001 esteso ai crimini informatici

Il Provvedimento è un primo approccio – realtà italiana non ancora matura

La scelta organizzativa deve soddisfare i requisiti soggettivi di competenza e professionalità, l'individuazione può essere effettuata nella forma di un responsabile privacy ex art. 29 o di un incaricato ex art. 30 del Codice (in realtà si tratta di sub-responsabile o di super-incaricato) – designazione del responsabile da parte di altro responsabile?

Requisiti di esperienza, capacità e affidabilità (Art. 29 C.d.P.)

- Cosa si intende per professionalità e competenza?
- La professionalità può essere intesa come la preparazione teorica in termini di titoli e corsi
- La competenza/adeguatezza deve essere invece riferita alla idoneità a svolgere i compiti affidati e quindi l'esperienza lavorativa relativa a quel ruolo (Cv allegato alla lettera di designazione)
- Per quanto attiene alla affidabilità, un'autocertificazione specifica allo stato può essere un'azione di controllo sufficiente.

Requisiti di esperienza, capacità e affidabilità (Art. 29 C.d.P.)

- La legge dovrebbe prevedere una formazione specifica per assumere il ruolo degli amministratori di sistema, quale dovrebbe essere il percorso professionale?

- Con riguardo al requisito di professionalità, la soluzione migliore per le imprese al fine di presidiare questo aspetto potrebbe essere costituita dalla programmazione di corsi periodici con annesso sistema di verifica di apprendimento.

- Si tratta di un modello già adottato dal legislatore in materia di sicurezza del lavoro (vedi D.Lgs. 81/08).

- I titolari dovrebbero erogare corsi di formazione graduali connessi ai rischi connaturati all'attività e che andrebbero inseriti nel piano di formazione previsto all'interno del documento programmatico sulla sicurezza

Registrazione degli accessi

Conservazione dei file di log relativi agli accessi degli amministratori (log in, log out e tentativi di accesso falliti) – garanzia di completezza, inalterabilità dei file di log degli amministratori

Quale soluzione adottare?

Le grandi aziende adottano per lo più soluzioni software ad hoc

In capo al Titolare permangono le responsabilità connesse alla culpa in vigilando e culpa in eligendo

Si dovrebbero adottare modelli di gestione e prevenzione dei reati presupposto (due diligence – D.Lgs 231/01)

Il responsabile ha visibilità di tutte le attività? È in grado di interpretare i segnali di allarme?

Gradualità delle qualifiche – principio di imparzialità tra chi compie le attività e chi effettua le verifiche

Quis custodiet ipsos custodes?

File di log degli accessi dovrebbero essere inalterabili come?

Nella Piccole realtà tramite esportazioni periodiche su supporti non riscrivibili (p.e. CD e DVD non riscrivibili)

Genericità del termine "esportazione periodica di log"?

In automatico, ogni giorno, ogni settimana, ogni mese?

Conservati per sei mesi a quale scopo? Le investigazioni e l'accertamento dei reati

Strutture più complesse log server centralizzati e certificati

Elenco degli AdS
Regime di conoscibilità degli AdS

Si deve tenere un elenco aggiornato del AdS in documento interno non più il DPS (Documento Programmatico per la Sicurezza).

Si deve rendere nota l'identità degli amministratori di sistema che trattano dati personali dei lavoratori nell'ambito dell'organizzazione aziendali; il provvedimento individua i seguenti modi di comunicazione:

- Informativa art. 13
- Disciplinare interno (Provv. 1 marzo 2007 Linee Guida)
- Tramite la intranet aziendale, strumenti di comunicazione interna
- Tramite un'istanza del lavoratore

Come bilanciare le esigenze di sicurezza e di privacy nel rapporto di lavoro?

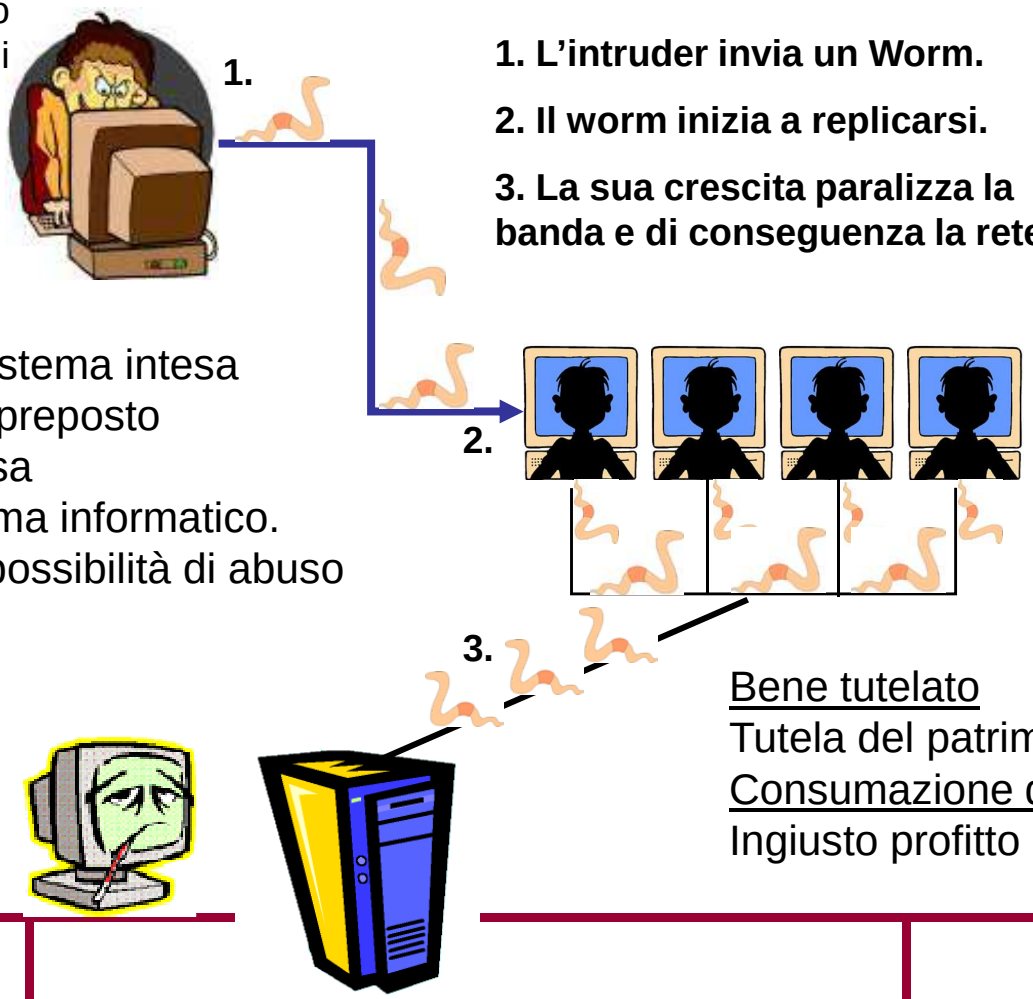
L'attività di audit deve essere bilanciata con la privacy nel rapporto di lavoro - un'attività con una granuralità spinta può scontrarsi con il divieto di controllo a distanza, necessario ottenere un accordo sindacale ex art. 4 comma 2 Statuto dei Lavoratori e tener in conto i profili di riservatezza

Tipologia di adempimento	Titolare	Responsabile privacy interno[1]	Responsabile privacy esterno	Amministratore di sistema
Misura organizzativa: designazione amministratore di sistema e rispondenza ai requisiti di professionalità ed esperienza	X			
Elenco aggiornato degli amministratori di sistema in documento interno	X			
Elenco aggiornato degli amministratori di sistema (attività comprende anche i dati personali relativi ai dipendenti): rendere conoscibili i nominativi e funzioni, per esempio tramite intranet, istanza dei lavoratori, ecc..	X			
Verifica annuale delle attività degli amministratori di sistema	X	X[2]		
Attribuzione del servizio di amministratore di sistema all'esterno (outsourcing)	X	X		
Tenuta di un elenco degli estremi identificativi degli amministratori di sistema in outsourcing	X	X	X	
Tenuta delle registrazione degli accessi[3] rispondenti ai requisiti di completezza ed inalterabilità (log in, log out, tentativi di accesso falliti)	X			X

Frode informatica e accesso abusivo al sistema informatico e telematico

Frode informatica – Worm (art. 640 ter)

Reclusione da 6 mesi e tre anni e multa fino a 1031 euro.
Perseguibile a querela di parte e d'ufficio nelle ipotesi aggravate oppure quando ricorre l'abuso della qualità di operatore di sistema



1. L'intruder invia un Worm.

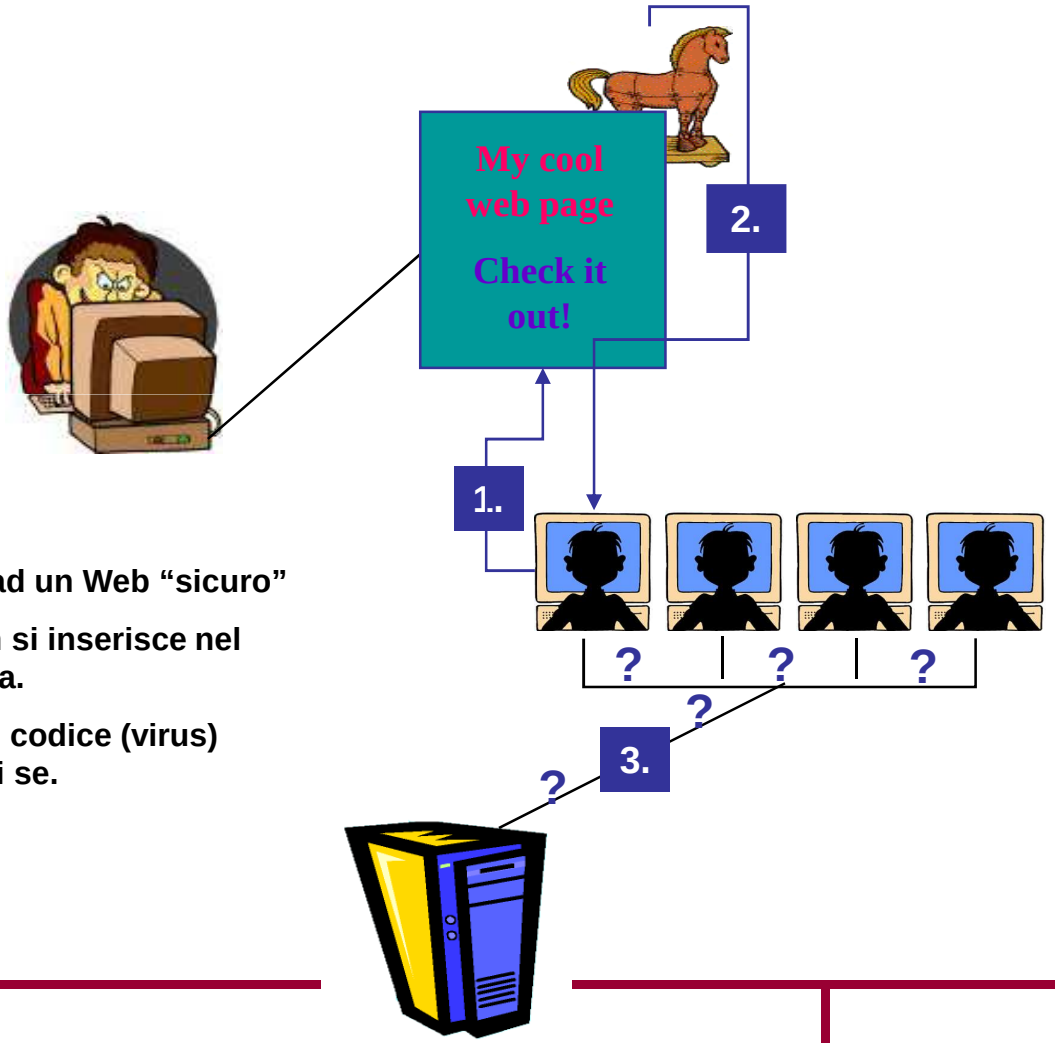
2. Il worm inizia a replicarsi.

3. La sua crescita paralizza la banda e di conseguenza la rete.

Qualità di operatore di sistema intesa
In senso atecnico come preposto
ad una funzione connessa
all'utilizzazione del sistema informatico.
Posizione privilegiata e possibilità di abuso

<u>Bene tutelato</u>
Tutela del patrimonio
<u>Consumazione del reato</u>
Ingiusto profitto con danno

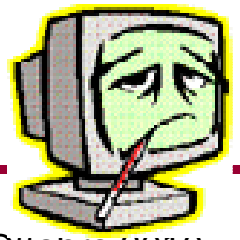
Frode informatica - Trojan Horse (art. 640 ter)



1. L'utente accede ad un Web "sicuro"

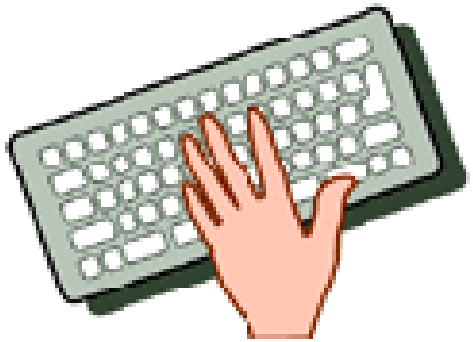
2. Il software Trojan si inserisce nel sistema della vittima.

3. Il trojan rilascia il codice (virus) contenuto dentro di se.



Password e accesso abusivo (art. 615 ter)

- Metodo piu' diffuso per l'autenticazione informatica
- Storicamente le passwords erano memorizzate su un file del S.O. rendendole particolarmente vulnerabili

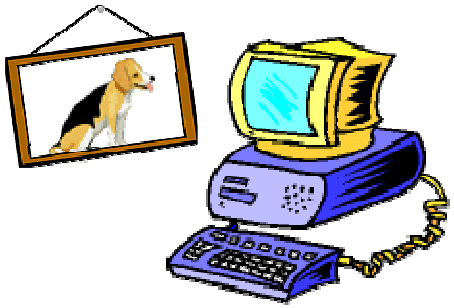


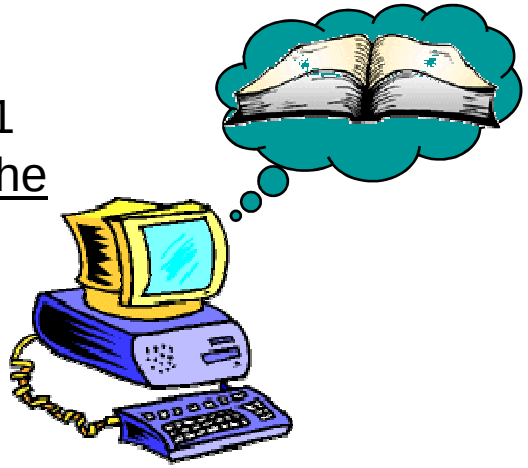
Fino a tre anni di reclusione
Reato perseguibile a querela
Salvo le ipotesi aggravate
Misure di protezione: indice di
Volontà contraria all'accesso

Password e accesso abusivo

Tutela del domicilio informatico:
Accesso abusivo al sistema protetto

In tema di password
Cass., sez. II, 25 sett. 2008, n.36721
In tema di misure organizzative fisiche
Cass., sez. V, 1 ott. 2008, n. 37322





La password è “bagel”?

No.

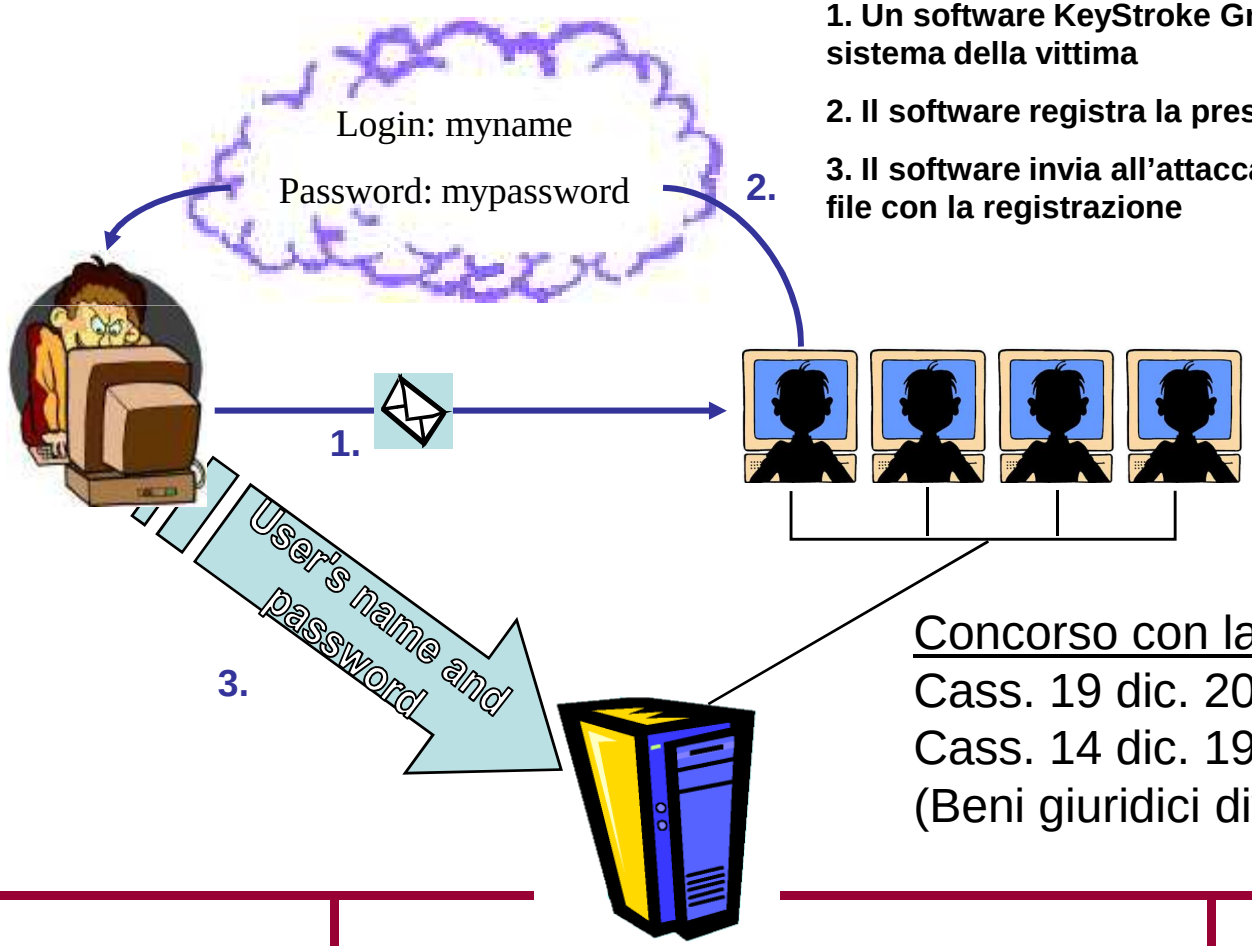
La password è “beaker”?

No.

La password è “beagle”?

Si! Accesso autorizzato

Keystroke Grabbers e accesso abusivo



1. Un software KeyStroke Grabber viene inviato al sistema della vittima

2. Il software registra la pressione di tutti i tasti

3. Il software invia all'attaccante una mail contenente il file con la registrazione

Concorso con la frode informatica
Cass. 19 dic. 2003, n.2672
Cass. 14 dic. 1999, 3067
(Beni giuridici diversi)

La legge di recepimento della direttiva 2009/136/Ce sulle comunicazioni elettroniche: legge di delega e decreto legislativo

Direttiva 2002/58/Ce modificata dalla Direttiva 2009/136/Ce sul settore delle comunicazioni elettroniche

Rientra nelle cinque direttive comunitarie del C.d. Pacchetto Telecom sul settore delle comunicazione elettroniche

Quali sono le novità introdotte all'art. 4? Quando entrano in vigore? La scadenza della legge di recepimento è prevista entro 25 maggio 2011

- Obbligo di Notificare la violazione dei dati personali per i Fornitori di servizi di comunicazione elettroniche
- Presupposti notificazione all'interessato
- Presupposti comunicazione alla sola Autorità Garante (Autorità competente)

DDL 2322
Legge comunitaria 2010

Il disegno di legge è stato depositato al Senato ed è all'esame della commissione.

Sono previsti i termini di approvazione del decreto legislativo (art. 1 e 10):

- **due mesi anteriori alla scadenza di recepimento** (i termini previsti nella direttiva 25 maggio 2011)
- in caso di lungo iter, meramente eventuale tre mesi dall'entrata in vigore del decreto delegato (se la legge entra in vigore dopo il 25 maggio 2011)

Ddl 2322

Art. 10 comma 3:

- Definizione dei profili di competenza tra Garante privacy e Direzione Nazionale Antimafia – DNA (lett. i)
- Riparto di attribuzioni tra Agicom e Garante privacy (lett.q)
- Riassetto dell'impianto delle sanzioni amministrative (anche depenalizzazione) del CCE (d.lgs. 259/2003), legge 109 del 1991 e C.d.P. (d.lgs.196/2003) – lett. r)

Depenalizzazione e revisione impianto sanzionatorio

Evitare che ogni violazione dei dati attivi un processo penale nell'ambito del Codice delle Comunicazioni elettroniche e del Codice della Privacy

Bilanciare la sicurezza dei dati e degli utenti con esigenze di non inflazionare in carico giudiziario penale

Revisione degli illeciti e sanzioni nelle materie disciplinate, tra cui la violazione dei dati personali, comunicazioni indesiderate, eccetera, anche mediante depenalizzazione

Definizione di Violazione dei dati personali

Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico nella Comunità

Analisi della definizione

Delitti informatici e violazione dei dati			
	Ogni azione che accidentalmente comporta: la distruzione, la perdita, la modifica dei dati personali, la rilevazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati, o comunque elaborati dal fornitore	**Ogni azione che in modo illecito comporta la distruzione, la perdita, la modifica dei dati personali**	**Ogni azione che in modo illecito comporta rilevazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati, o comunque elaborati dal fornitore**
Errore materiale dell'operatore informatico	**Sì**	**No**	**No**
Errore non voluto o non intenzionale	**Sì**	**No**	**No**
Effetto di qualunque condotta non accidentale che produca la distruzione, la perdita, la modifica di dati personali	**No**	**Sì**	**No**
L'effetto consistente in un accesso abusivo/ non autorizzato, Cessione di dati personali ad altri	**No**	**No**	**Sì**

Analisi della definizione

Non tutti i delitti informatici costituiscono una violazione dei dati			
	Accesso abusivo al sistema informatico art. 615 ter	**Accesso abusivo al sistema informatico art. 615 ter**	**Frode informatica (p.e. phishing)**
Banca dati contenenti informazioni personali	**Sì**	**No**	**Sì**
Esistenza Violazione dei dati	**Sì**	**No**	**Sì**

D.lgs. N.231/2001 resp. amministrativa degli enti estesa anche ai crimini informatici: corporate governance

Inoltre, il titolare del trattamento risponde secondo la normativa privacy sia per la violazione dei dati, sia per l'omessa adozione delle misure dei sicurezza, allo stato, le sanzioni amministrative e penali sono cumulabili

Obbligo di notificazione presupposti:

In caso di violazione dei dati personali il fornitore deve comunicare l'evento all'Autorità Garante

Il fornitore deve dimostrare di avere utilizzato le "opportune misure tecnologiche di protezione", tali misure devono essere applicate ai dati interessati dalla violazione altrimenti l' "incidente" verrà notificato anche all'interessato/abbonato

Requisiti delle misure di protezione: devono rendere i dati incomprensibili ai terzi non autorizzati ad accedervi

Separazione dati identificativi da altri dati o criptazione?

Ulteriori presupposti della notificazione della violazione dei dati personali:

L'Autorità Garante (Autorità Competente): potrà estendere l'obbligo di notificazione anche tenuto conto delle "presumibili ripercussioni negative della violazione"
- Poteri discrezionali

Obbligo di notificazione all'interessato/abbonato ha due principali scopi:

Premere sull'esigenza di tutela dell'immagine aziendale;

Creare un forte incentivo per le aziende ad investire in sicurezza ed adottare le "Misure opportune di protezione".

Come verranno recepite nella normativa nazionale le “misure opportune di protezione”?

Il Codice accoglie principalmente due tipologie di misure di sicurezza:

Le misure idonee/adeguate e le misure minime di sicurezza

Le misure idonee sono connesse al progresso tecnico

- ✓ *I dati personali oggetto del trattamento devono essere custoditi in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, nonché di accesso non autorizzato o di trattamento non consentito e non conforme alle finalità di raccolta.*

✓*A tale scopo, tutti i titolari del trattamento, devono predisporre tutte le idonee misure di sicurezza in relazione alle conoscenze acquisite in base al progresso tecnico (STATO DELL'ARTE), alla natura dei dati e alle specifiche caratteristiche del trattamento.*

Scelta del legislatore “Opportune misure tecnologiche di protezione”?

Misure minime di sicurezza

↓

Valutazione dell’efficacia minima (art. 33 e 169 TU)

↓

Sanzioni penali

Misure idonee

↓

Valutazione della piena efficacia (artt.31 e 15 TU)

↓

Sanzioni civili

Fornitore
(Art. 32 C.d.P.)

Fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta ai sensi dell'art. 31 **idonee misure di sicurezza e organizzative adeguate al rischio esistente**

Sicurezza del servizio e dei dati e la sicurezza della rete

In caso di mancanza di accordo tra i due fornitore – Agicom

Fornitore di servizio di comunicazione elettronica informa gli abbonati e gli utenti se sussiste un particolare **rischio di violazione dei sicurezza della rete** (notificazione di violazione di sicurezza della rete già presente nel C.d.P.) – informatica al Garante privacy e Agicom

Risk Analysis

L'analisi dei rischi è necessaria per adottare in modo cosciente e formale le decisioni organizzative in osservanza dei requisiti legali cogenti.

Questa attività è necessaria sia per individuare un corretto livello di contromisure sia per dare prova di un adeguato livello di diligenza da parte del Titolare del trattamento

Risk Analisys

- Determinare quali beni sono critici
- Identificare e valutare le contromisure
- Identificare le minacce possibili
- Determinare le vulnerabilità
- Calcolare le perdite previste
- Raccomandare le azioni correttive

Estensione Servizi interessati

La presente direttiva si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche nella Comunità, comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati (RFID)

Parere Gruppo europeo dei Garanti, 19 gennaio 2005, WP 105
Provv. Garante 09 marzo 2005, in Bollettino n. 59

Recepimento dei principi della tutela della privacy nella fase di progettazione della tecnologia RFID – Privacy by Design

Rispetto dei principi di necessità, finalità , proporzionalità

Informazione e indicazione segnaletica dei dispositivi

Rilascio del consenso al trattamento con riferimento la rimozione (Tag disabler) o attivazione dei tag

Impiego di sistemi di autenticazione per l'accesso ai dati e tecniche di cifratura applicate alla trasmissione

Quadro normativo comunitario

GEPD (10.4.08) - WP 150 (15.5.08)

Esiste una reale esigenza di estendere l'obbligo di notificazione anche a rete privati di comunicazione?

Soluzione suggerita dal GEPD (Parere del 10.4.08) ed accolta anche dal Gruppo europeo dei Garanti art. 29 (Parere WP 150 del 15.5.08):

Estensione della nozione di fornitore – reti private e semiprivate: università, uso privato delle email aziendali, servizi internet in alberghi, residence internet Cafè, servizi relativi alle banche dati sanitarie on line (rif. Provv. Amministratori di sistema)

Notifica delle violazione di sicurezza estesa (obbligo stabilito dalla Commissione europea) ai fornitori di servizi della società dell'informazione

Case Study in tema di security breach notification

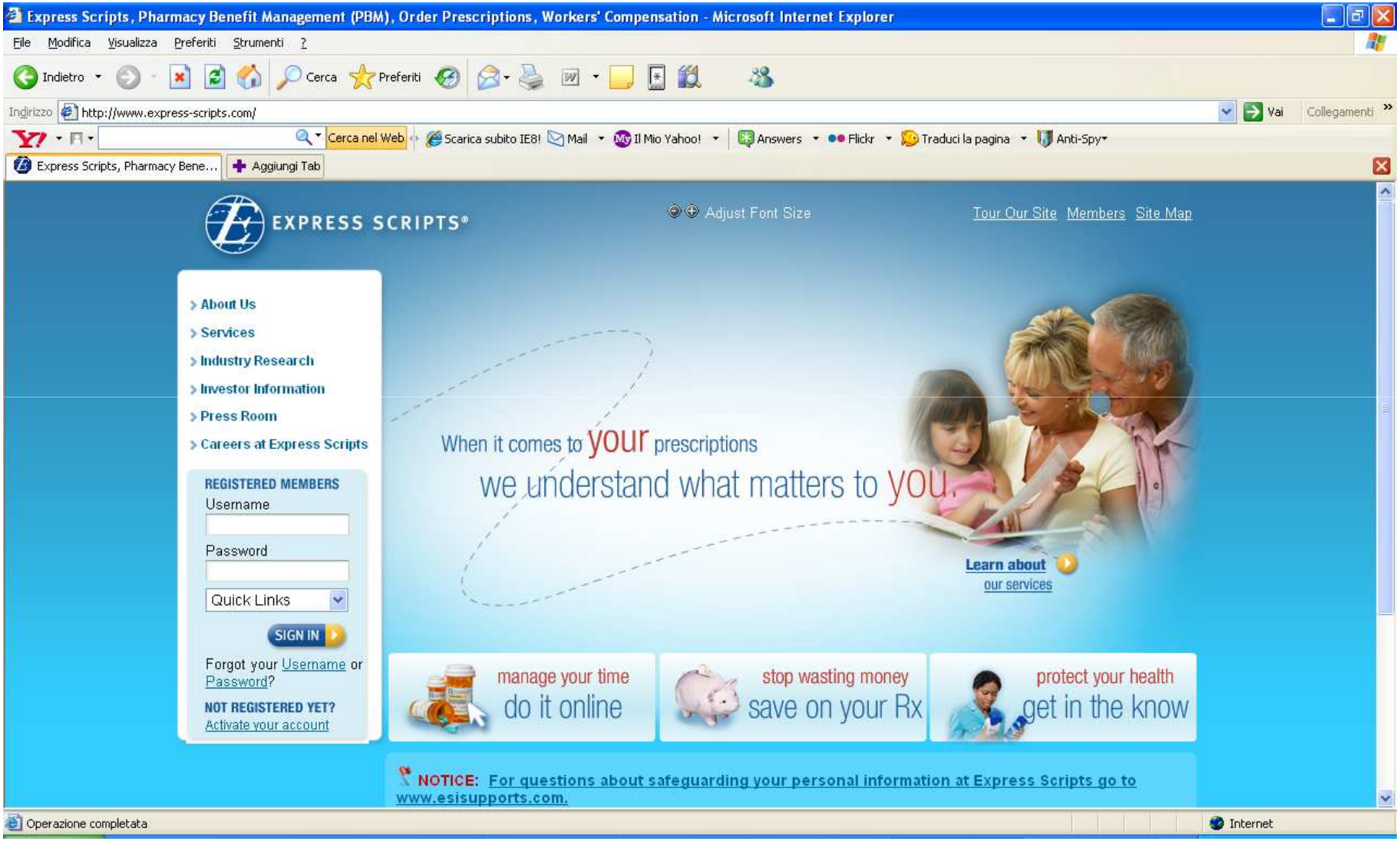
Express Script

Security Breach Notification

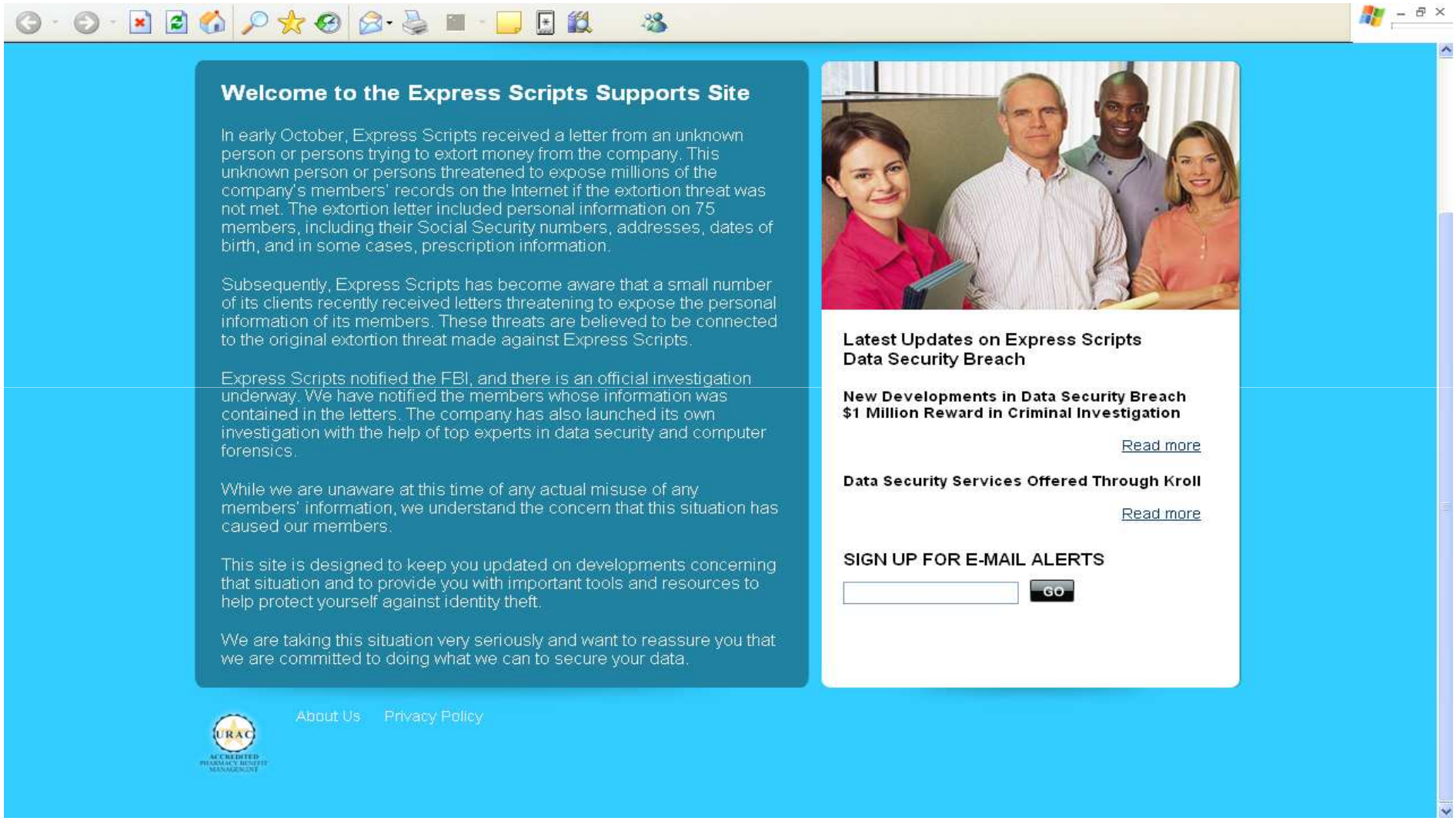
Estensione oltre l'ambito dei Fornitori di comunicazioni elettroniche?

Fonti attendibili parlano del coinvolgimento di più di 700.000 pazienti nella violazione dei dati

CASO EXPRESS SCRIPT



EXPRESS SCRIPT E IL RICATTO PER SALVAGUARDARE I DATI SANITARI



Prospettive di rischio e future riforme

Il mercato ICT e il diffuso utilizzo delle soluzioni tecnologiche sono in continuo evoluzione, la legislazione stenta a stare al posso, infatti la direttiva comunitaria 2009/136/Ce non ancora recepita dagli Stati Membri, è stata appena approvata, ma sono già presenti prospettive di riforma future

Garante Europeo – Peter Hustinx

"I welcome the many improvements in the protection of privacy in the revised ePrivacy Directive.

"But it is now crucially important to broaden the scope of the security breach provisions to all sectors and further define the procedures for notification."

Garante Europeo – Peter Hustinx

"Examples of such circumstances would include those where the loss could result in identity theft, fraud, humiliation or damage to reputation. The notification will include recommended measures to avoid or reduce the risks. The data breach notification framework builds on the enhanced provisions on security measures to be implemented by operators, and should stem the increasing flood of databreaches"

"social networking was one area where individuals were more exposed than ever to data loss."

"The emergence of such services makes it more likely that an extension of data breach notifications beyond telecoms providers will be needed"

"We have seen this in Germany recently where sensitive data was illegally collected from one of the biggest German social networks, Schueler VZ"

"data breaches cannot be limited to electronic communications networks alone – but may need to be addressed in new EU rules which cover **ONLINE SERVICES** as well"

Riepilogo conclusivo

Il titolare è il responsabile per l'esercizio dei poteri di direzione e controllo-reazione – anche qualora vi siano deleghe penali – due deligence

Convergenza verso una IS Governance

Ambito di impatto della Security Breach Notification

La analisi dei rischi e la classificazione degli asset passo fondamentale per la protezione delle informazioni

Scenari futuri di riforma della normativa comunitaria

FABIO DI RESTA
SPECIALISTA LEGALE PRIVACY E DIRITTO DELLE NUOVE TECNOLOGIE
ISO 27001 ICT SECURITY AUDITOR - LLM
STUDIO LEGALE DI RESTA – WWW.STUDIOLEGALEDIRESTA.IT
INFO@STUDIOLEGALEDIRESTA.IT