

SECURITY & PRIVACY

Abstract: Un numero sempre maggiore di aziende adotta delle policy aziendali per l'utilizzo delle strumentazioni informatiche, di Internet e della posta elettronica.

Questo tipo di policy è vincolante nei confronti del dipendente?

Esiste nell'ordinamento italiano un divieto all'utilizzo di strumentazioni tecnologiche volte a proteggere l'azienda contro attacchi informatici o altre violazioni del loro sistema informativo?

Esistono nell'ordinamento italiano dei limiti o dei divieti al controllo dell'uso delle strumentazioni informatiche da parte dei lavoratori?

www.euroonesistemi.com

BY EURO ONE SISTEMI S.R.L. White Paper

Web Security: Implicazioni Legali

2

Indice:

Intervista 3

Scenario 1: Il dipendente utilizza Internet per mandare messaggi con contenuti diffamatori 5

- Inguria e diffamazione via Internet 5
- Le possibili soluzioni 6

Scenario 2: Il dipendente scarica sul suo computer o nelle sue cartelle server materiali (musica, filmati, immagini) protetti dalle legge sul diritto d'autore 7

- La normativa vigente 7
- La necessità di un'adeguata tutela all'interno dell'azienda 7

Scenario 3: Alcuni file contenenti materiali pedopornografici sono stati rilevati nel computer o nelle cartelle dei dipendenti. 9

- La detenzione di materiale pedopornografico 9
- Gli ulteriori comportamenti penalmente rilevanti 9
- Le responsabilità dell'impresa 10

Scenario 4: Il dipendente installa sul proprio computer aziendale del software pirata o software non autorizzato dall'azienda 11

Scenario 5: Un'azienda contamina un'altra azienda a causa di un virus o di spyware nel suo sito web 12

- I virus ed il codice penale 12
- Le conseguenze per l'azienda 12

Scenario 6: Il dipendente salva su una chiavetta USB informazioni coperte da segreto e le divulga a terzi. 13

- Le norme poste dal nostro ordinamento giuridico a protezione delle informazioni coperte da segreto 14
- Le contromisure da adottare in azienda 14

Scenario 7: Il dipendente incaricato dei rapporti con le banche subisce un attacco di phishing e comunica involontariamente a terzi le password di accesso al conto bancario on-line dell'azienda 15

- Il Phishing 16
- Il Phishing e le sanzioni previste 16
- Le possibili soluzioni 16

Scenario 8: Uno spyware s'insedia nel sistema informativo dell'azienda e viene rubata tutta la banca dati del personale. Uno spyware s'insedia nel sistema informativo di una azienda di e-mail - marketing e viene rubata la banca dati marketing di un cliente 18

- Le disposizioni del Codice in materia di protezione dei dati personali 18

SECURITY & PRIVACY

Scenario 9: I computer fanno parte all'insaputa dell'azienda di una Botnet che sferra un attacco del tipo Denial Of Service ad una terza società 20

- Le sanzioni a carico dei pirati informatici 20
- I rischi per l'azienda e la computer forensic 20

Scenario 10 - La moglie di un dipendente si collega da remoto con il computer portatile aziendale alla rete aziendale e causa la propagazione di un virus. 21

- Quali sono le possibili sanzioni a carico del dipendente nel caso sua moglie si sia collegata alla rete aziendale ed abbia causato involontariamente la propagazione di un virus? 21

Web Security: Implicazioni Legali

3

Intervista

EurOne Sistemi intervista l'Avv. Gabriele Faggioli, legale specializzato in Information Technology Law, docente dell'Area Sistemi Informativi della SDA Bocconi e Presidente di A.N.GA.P. (Associazione Nazionale Garanzia della Privacy).

E' autore di diversi libri e di numerosi articoli aventi ad oggetto il diritto dell'informatica.

Euro One Sistemi : Un numero sempre maggiore di aziende adotta delle policy aziendali per l'utilizzo delle strumentazioni informatiche, di Internet e della posta elettronica. Questo tipo di policy è vincolante nei confronti del dipendente?

Spetta all'azienda scegliere se adottare una policy per le strumentazioni informatiche vincolante o limitarsi ad adottare un documento non vincolante .

La policy di utilizzo delle strumentazioni informatiche per essere vincolante nei confronti del lavoratore deve però essere integrata nel regolamento interno dell'azienda e deve rispondere ad alcuni requisiti di legge.

Infatti ai sensi dell'articolo 7 dello Statuto dei lavoratori *"le norme disciplinari relative alle sanzioni, alle infrazioni in relazione alle quali ciascuna di esse può essere applicata ed alle procedure di contestazione delle stesse, devono essere portate a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti"*.

Pertanto il datore di lavoro dovrà provvedere a rendere nota mediante affissione la policy per l'uso delle strumentazioni informatiche.

Inoltre la policy dovrà fare riferimento sempre sulla base dell'articolo 7 dello Statuto dei lavoratori alle sanzioni disciplinari stabilite nel contratto collettivo di lavoro.

Euro One Sistemi : Esiste nell'ordinamento italiano un divieto all'utilizzo di strumentazioni tecnologiche volte a proteggere l'azienda contro attacchi informatici o altre violazioni del loro sistema informativo?

Non esiste nell'ordinamento italiano nessun divieto espresso all'utilizzo di tecnologie volte a proteggere l'azienda contro attacchi informatici.

Al contrario il Codice in materia di trattamento dei dati personali impone ai titolari del trattamento l'adozione di misure di sicurezza idonee volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Il Codice impone anche l'adozione di misure minime di sicurezza per il trattamento dei dati con strumenti elettronici.

In particolare il titolare del trattamento deve:

adottare un sistema di autenticazione informatica e un sistema di autorizzazione;

utilizzare idonei strumenti elettronici contro i rischi di intrusione e di diffusione di virus e altri software maligni
aggiornare periodicamente i software che prevengono le vulnerabilità dei sistemi e che ne correggono i difetti
provvedere al salvataggio dei dati.

L'azienda potrà inoltre adottare anche misure di sicurezza volte ad evitare o prevenire la commissione di reati da parte dei propri dipendenti quali ad esempio il download di file a contenuto pedopornografico o lo scambio di file audio o video protetti da diritto d'autore.

Euro One Sistemi: Esistono nell'ordinamento italiano dei limiti o dei divieti al controllo dell'uso delle strumentazioni informatiche da parte dei lavoratori?

Queste problematiche non sono state puntualmente disciplinate dal legislatore italiano. Sono infatti ancora fondamentali le norme stabilite dallo Statuto dei lavoratori. In base al primo comma dell'articolo 4, *è vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori*". Il secondo comma prosegue disponendo che *"gli impianti e le apparecchiature di controllo che siano richiesti da esigenze"*

SECURITY & PRIVACY

organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna". La giurisprudenza ha contribuito a interpretare tali principi; innanzitutto ha precisato che per *altre apparecchiature* non bisogna intendere macchinari esterni o separabili dagli strumenti di lavoro ma che invece è necessario considerare le funzioni che

Web Security: Implicazioni Legali

4

l'apparecchiatura possiede. Le *altre attività*, inoltre, non sono solo i comportamenti legati alla prestazione lavorativa ma anche quelli esulanti da tale attività, comunque in grado di caratterizzare il dipendente. Da queste norme si deduce che se un controllo intenzionale sul comportamento dei dipendenti è sicuramente vietato, uno indiretto e conseguente ad esigenze organizzative, produttive o di sicurezza è invece possibile a determinate condizioni. Vero quanto detto occorre considerare che i controlli sull'utilizzo delle strumentazioni informatiche comportano la raccolta di dati personali dei dipendenti. Il Garante per la protezione dei dati personali si è di recente pronunciato in materia di controllo dell'utilizzo di internet da parte di un lavoratore confermando le tesi già esposte dal Data Protection Working Party, organo della Comunità Europea istituito per monitorare e fornire alcuni pareri riguardo all'applicazione della direttiva europea sulla privacy. Il Garante ha ribadito la necessità di informare preventivamente i lavoratori sui controlli effettuati e sulle relative modalità e di rispettare il principio di proporzionalità che comporta l'adozione di misure di controllo adeguate alle possibili violazioni poste in essere dai dipendenti. In conclusione il provvedimento ha ribadito la legittimità di questa tipologia di controlli purché rispondente ai principi di trasparenza, di legittimità e di proporzionalità.

Web Security: Implicazioni Legali

5

Scenario 1: Il dipendente utilizza Internet per mandare messaggi con contenuti diffamatori

Accade sempre più frequentemente che i dipendenti per svolgere le mansioni loro assegnate, utilizzino le strumentazioni informatiche messe a loro disposizione dalle aziende. In particolare l'uso di internet è ormai in molti settori uno strumento lavorativo di primaria importanza in grado di accrescere la produttività individuale. Nonostante questo, attraverso le reti telematiche si possono porre in essere condotte certamente illecite in base alle norme contenute nell'ordinamento giuridico italiano.

Internet, infatti, non è solo uno strumento utile a reperire con grande facilità le informazioni, ma è soprattutto un mezzo di comunicazione che può essere sfruttato dagli individui per esprimere le proprie idee ed opinioni. Nella rete esistono infatti molti siti che permettono agli utenti di comunicare tra loro (p.e. chat, servizi di messaggistica, ecc.) e di manifestare il proprio pensiero (p.e. forum, newsgroup ecc.), spesso sotto l'apparente garanzia dell'anonimato.

Ingiuria e diffamazione via Internet

Quali sono le conseguenze, in termini legali, nel caso in cui un dipendente utilizzi Internet per inviare messaggi con contenuti diffamatori durante l'esercizio delle sue mansioni lavorative?

La libertà di espressione, ossia della manifestazione del proprio pensiero, è un diritto inviolabile garantito sia dalla Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali sia dalla Costituzione italiana. Tale libertà, tuttavia, non può spingersi fino ad offendere l'altrui reputazione ed il codice penale italiano contiene norme che sanzionano le condotte tese a tale scopo.

In particolare, l'articolo 594 del Codice Penale che disciplina il reato di ingiuria punisce con la reclusione fino a sei mesi o con la multa fino a cinquecentosedici euro chiunque offende l'onore o il decoro di una persona presente. **L'elemento caratterizzante di questo reato è dunque la presenza della persona offesa, caso che può verificarsi anche in un contesto virtuale come Internet, per esempio in una chat o in un sito di messaggistica istantanea.** Il codice penale inoltre prevede pene superiori nel caso in cui l'offesa consista nell'attribuzione di un fatto determinato (reclusione fino a un anno o multa fino a milletrecentadue euro)

SECURITY & PRIVACY

o sia commessa in presenza di più persone.

L'articolo 595 del codice penale che disciplina la diffamazione punisce, invece, con la reclusione fino a un anno o con la multa fino a milletrentadue euro chi, comunicando con più persone, offende l'altrui reputazione (la pena è della reclusione sino a due anni e della multa sino a duemilasesantacinque euro nel caso l'offesa consista nell'attribuzione di un fatto determinato). **La differenza rispetto al reato di ingiuria risiede nell'assenza della persona offesa che può verificarsi, per esempio, nel caso di contenuti diffamatori pubblicati all'interno di un forum o di un sito internet, o inviati via e-mail.**

Per sciogliere ogni dubbio circa la possibilità che i reati di ingiuria e diffamazione possano essere commessi anche attraverso le reti telematiche è utile citare una sentenza della Corte di Cassazione penale in base alla quale *"basterebbe pensare alla cosiddetta trasmissione via email, per rendersi conto che è certamente possibile che un agente, inviando a più persone messaggi atti ad offendere un soggetto, realizzi la condotta tipica del delitto di ingiuria (se il destinatario è lo stesso soggetto*

Web Security: Implicazioni Legali

6

offeso) o di diffamazione (se i destinatari sono persone diverse)" (Cass. sez. V penale, 27.12.2000, n. 4741) Nonostante in base ai principi generali del nostro ordinamento giuridico il dipendente risponderà personalmente dei reati commessi, tuttavia non mancano i riflessi negativi anche nei confronti dell'impresa. Innanzitutto in sede di indagine dell'autorità giudiziaria si vedrà per prima coinvolta dal momento che verrà rintracciato l'indirizzo IP del computer dal quale sono partiti i messaggi diffamatori. In tale circostanza l'azienda sarà tenuta a collaborare per favorire l'altrimenti difficile individuazione del dipendente realmente responsabile del comportamento illecito fornendo tutto il supporto necessario alla prosecuzione delle indagini.

In sede civile l'azienda potrà essere chiamata a risarcire i danni eventualmente cagionati a terzi dal comportamento illecito del dipendente in base all'articolo 2049 del codice civile (che prevede una responsabilità dei datori di lavoro per i danni arrecati dal fatto illecito dei propri dipendenti nell'esercizio delle incombenze cui sono adibiti). Da non sottovalutare, infine, il rischio che l'organizzazione subisca un danno all'immagine derivante dal fatto il reato di ingiuria e/o diffamazione è stato commesso utilizzando le proprie strumentazioni informatiche.

Le possibili soluzioni

Occorre quindi che le imprese adottino le necessarie misure sia sul piano regolamentare (policy sull'utilizzo delle strumentazioni informatiche da parte dei dipendenti), sia sul piano tecnico (p.e. filtri per la navigazione in internet) per limitare le spiacevoli conseguenze derivanti da comportamenti illeciti dei dipendenti quali la diffusione di messaggi diffamatori tramite internet.

Web Security: Implicazioni Legali

7

Scenario 2: Il dipendente scarica sul suo computer o nelle sue cartelle server materiali (musica, filmati, immagini) protetti dalle legge sul diritto d'autore

La diffusione delle strumentazioni informatiche e dell'accesso ad Internet, in assenza di una regolamentazione e di un controllo da parte del datore di lavoro, può essere causa di inefficienze dovute ad un loro uso estraneo all'attività lavorativa. Recenti statistiche confermano che molti dipendenti navigano in internet durante l'orario di lavoro per finalità personali. Non è raro, e ciò è spesso dovuto ad una cattiva conoscenza sulle effettive implicazioni giuridiche, che i dipendenti utilizzino la rete per reperire e scaricare abusivamente materiale protetto dalla legge sul diritto d'autore, come file musicali, immagini o film.

La normativa vigente

In Italia tali creazioni sono infatti protette quali opere dell'ingegno di carattere creativo dalla legge 22 aprile 1941, n. 633 (*"Protezione del diritto d'autore e di altri diritti connessi al suo esercizio"*) che attribuisce agli autori, oltre al diritto inalienabile alla paternità sulle opere sviluppate, anche i diritti esclusivi di utilizzazione economica (invece trasmissibili a terzi) sulle stesse. Sotto questo secondo aspetto solo all'autore, o all'eventuale cessionario dei diritti

SECURITY & PRIVACY

di utilizzazione economica, spetta il diritto di stabilire quali utilizzazioni dell'opera autorizzare a terzi, spesso dietro il pagamento di un determinato compenso. Logica conseguenza di questo assunto è che la duplicazione (ma anche la distribuzione, la modifica, l'esecuzione) di opere dell'ingegno senza l'autorizzazione da parte dell'autore o degli aventi diritto è da considerarsi sicuramente illecita. Dal punto di vista sanzionatorio il download abusivo da parte del dipendente di opere dell'ingegno protette dalla legge sul diritto d'autore costituisce un illecito amministrativo punito ai sensi dell'articolo 174 ter della stessa con la sanzione principale di € 154,00 e con quelle accessorie della confisca del materiale e della pubblicazione del provvedimento su un giornale quotidiano a diffusione nazionale (salvo sanzioni più elevate in caso di recidiva o di fatto grave).

Tuttavia è oggi molto diffuso anche il file sharing, ossia lo scambio di files attraverso piattaforme di condivisione peer to peer. Attraverso queste piattaforme gli utenti mettendo a disposizione della comunità i propri materiali digitali, hanno la possibilità di scaricare i files degli altri utenti che utilizzano il medesimo sistema. Il file sharing non è di per sé una pratica illegale, ma lo diventa quanto i files condivisi sono per esempio opere dell'ingegno per le quali non siano stati assolti i relativi diritti d'autore. L'articolo 171 comma 1 lettera a-bis) della legge sul diritto d'autore, recentemente modificato, punisce con la sanzione penale della multa da € 51,64 a € 2.065,82 chiunque mette a disposizione del pubblico, **immettendola in un sistema di reti telematiche**, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa. Tuttavia il trasgressore è ammesso a pagare, prima dell'apertura del dibattimento o dell'emissione del decreto penale di condanna, una somma corrispondente alla metà del massimo della pena stabilita (oltre alle spese del procedimento), e tale pagamento estingue il reato a suo carico. Pene molto più severe sono poi previste (la reclusione da uno a quattro anni e la multa da € 2.582,28 a € 15.493,70) nel caso in cui la comunicazione al pubblico mediante internet, sia stata effettuata per fini di lucro ossia per trarne un vantaggio economico diretto.

La necessità di un'adeguata tutela all'interno dell'azienda

Le aziende hanno comunque la necessità di tutelarsi da possibili coinvolgimenti scaturenti da violazioni della normativa sul diritto d'autore poste in essere dai propri dipendenti.

Si consideri preliminarmente che il materiale protetto illecitamente scaricato dal dipendente sarebbe comunque rinvenuto sulle strumentazioni informatiche aziendali e presso i locali di questa avverrebbe il sequestro ad opera della Guardia di Finanza. Inoltre la pubblicazione di provvedimento di condanna a carico di un dipendente su un giornale a diffusione nazionale avrebbe sicuramente effetti pregiudizievoli sull'immagine dell'azienda nei confronti dei terzi.

Con riferimento al file sharing, infine, in caso di illecita immissione file musicali, film o immagini sarebbe l'azienda a venir preventivamente identificata attraverso l'IP del computer che si è collegato alla rete, e solo in un momento successivo ed eventuale sarebbe possibile rintracciare il dipendente responsabile. Assolutamente da non sottovalutare, gli ulteriori profili risarcitori in sede di contenzioso civile attivati dai titolari dei diritti sulle opere violate.

Web Security: Implicazioni Legali

8

Il controllo a posteriori sulle opere protette dal diritto d'autore scaricate dai dipendenti sui computer e server aziendali è molto difficoltoso in quanto occorre valutare caso per caso se vi siano state violazioni o meno alla normativa esaminata (nel caso di download da siti autorizzati, per esempio, non è ravvisabile nessuna condotta illecita, per quanto il comportamento del lavoratore integri violazione del dovere di diligenza verso il datore di lavoro ex art. 2104 del codice civile). Le soluzioni migliori a disposizione dell'azienda sono probabilmente il divieto a livello regolamentare in capo ai dipendenti di scaricare o immettere nella rete materiale di qualsiasi genere non attinente all'attività lavorativa (o comunque di provenienza illecita) e l'adozione di forme di controllo sulla navigazione in internet che, per esempio, inibiscano l'accesso a determinati siti o impediscano il download o l'upload di files di grandi dimensioni.

Web Security: Implicazioni Legali

9

Scenario 3: Alcuni file contenenti materiali pedopornografici sono stati rilevati nel computer o nelle cartelle dei dipendenti.

I reati connessi alla pornografia minorile (pedopornografia), sicuramente tra i più infamanti tra quelli disciplinati dal codice penale italiano, sono aumentati in modo esponenziale in conseguenza della diffusione dell'utilizzo di internet e delle strumentazioni informatiche. Per contrastare l'espansione del fenomeno della pedopornografia il legislatore

SECURITY & PRIVACY

è intervenuto con la legge 3 agosto 1998 n. 269 (*"Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù"*) che inserendo gli articoli da 600 bis a 600 octies ha allargato l'elenco delle condotte penalmente rilevanti ed ha espressamente contemplato le reti telematiche quali mezzi di commissione dei reati legati alla pornografia minorile. Tali articoli hanno recentemente subito alcune modifiche per effetto della legge 6 febbraio 2006, n. 38 (*"Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet"*) che ha ulteriormente allargato la sfera delle condotte penalmente rilevanti.

La detenzione di materiale pedopornografico

Quali sono le conseguenze a cui va incontro un dipendente per aver scaricato sul proprio PC aziendale materiale pedopornografico? Indubbiamente, dopo la novella del 1998 tale condotta integra una condotta costituente reato. L'articolo 600 quater del codice penale (*"Detenzione di materiale pornografico"*) prevede infatti la sanzione della reclusione fino a tre anni e della multa non inferiore a € 1.549,00 per chi si procura o detiene materiale pornografico utilizzando minori degli anni diciotto (in seguito alla novella del 2006 il secondo comma di questo articolo prevede ora che le pene debbano essere aumentate in misura non eccedente i due terzi nel caso in cui il materiale detenuto sia di ingente quantità).

La giurisprudenza ha contribuito a circoscrivere l'ambito delle condotte sanzionabili sulla base di questo articolo, seppur nella precedente formulazione. Per esempio alcune sentenze hanno chiarito che ai fini della configurazione del reato di cui all'articolo 600 quater del Codice Penale occorre che il soggetto non si sia limitato a consultare un sito web ove siano visionabili immagini pedopornografiche, ma abbia volontariamente e consapevolmente scaricato sul proprio PC e salvato nella memoria tali immagini. Anche la collocazione delle immagini vietate in file temporanei che ne consentono la visione reiterata fino alla definitiva cancellazione è stata considerata integrare il reato di detenzione di materiale pedopornografico nel caso di utilizzatori esperti ed a conoscenza del funzionamento di tale tipologia di file. Al contrario la giurisprudenza ha escluso, per esempio, l'esistenza di profili di responsabilità in un caso nel quale il materiale rinvenuto costituiva la mera traccia di una trascorsa consultazione del web creata dai sistemi di salvataggio automatico sul personal computer.

Web Security: Implicazioni Legali
10

Gli ulteriori comportamenti penalmente rilevanti

Il reato sopra esaminato non punisce comportamenti tesi al coinvolgimento di minori in attività pornografiche, ma sostanzialmente i consumatori finali di queste ultime. Il Codice penale, infatti, prevede sanzioni più pesanti invece per chi non si limiti a fruire di materiale pedopornografico ma abbia un ruolo attivo nella sua divulgazione. In particolare l'articolo 600 del Codice penale ter (anch'esso modificato dalla legge 38/2006) punisce:

- con la reclusione da uno a cinque anni e con la multa da € 2.582,00 a € 51.645,00 chiunque con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde o pubblicizza materiale pedopornografico, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto (comma 3)
- con la reclusione fino a tre anni e con la multa da € 1.549,00 a € 5.164,00 chiunque, offre o cede ad altri, anche a titolo gratuito, materiale pedopornografico (comma 4)

Le norme sopra esaminate, quindi, sanzionano in particolare le condotte di diffusione (ad un numero indeterminato di persone) e di comunicazione (a soggetti determinati tenendo presente che è punibile la semplice offerta di materiale pedopornografico) di materiale pedopornografico. Ancora una volta la giurisprudenza ha contribuito nel tempo a chiarire e circoscrivere i concetti sopra delineati. Per esempio l'utilizzo di programmi di file sharing per la condivisione di materiale pedopornografico è stata considerata diffusione con conseguente applicazione della fattispecie di reato di cui al terzo comma dell'articolo 600 ter del Codice penale (in quanto chiunque può accedere alle cartelle condivise e prelevare il materiale vietato), a differenza della trasmissione diretta tra due utenti di una chat line invece rientrante nella previsione del quarto comma.

Come è facilmente intuibile, anche le condotte sopra esaminate possono essere realizzate anche da un dipendente che non si limiti, per esempio, a detenere materiale pedopornografico sul PC aziendale ma lo divulghi o diffonda in qualsiasi modo all'interno o all'esterno dell'organizzazione.

Le responsabilità dell'impresa

Come già chiarito nella trattazione degli scenari precedenti, regola generale dell'ordinamento giuridico italiano è la

SECURITY & PRIVACY

personalità della responsabilità penale; i dipendenti rimangono quindi i soli penalmente responsabili dei reati commessi. Una parte minoritaria della dottrina ritiene, invece, che anche il datore di lavoro possa essere chiamato a rispondere a titolo di concorso dei reati commessi dai dipendenti, nel caso in cui il loro comportamento criminoso sia stato agevolato dall'assenza in azienda di adeguate misure di controllo e prevenzione degli illeciti. Il secondo comma dell'articolo 40 del codice penale prevede infatti che *"non impedire un evento, che si ha l'obbligo giuridico di impedire, equivale a cagionarlo"* (reato omissivo improprio). Secondo questa corrente dottrinale discenderebbe dallo stesso rapporto di lavoro l'obbligo da parte del datore di lavoro di prevenire ed impedire la commissione di reati ad opera dei propri dipendenti

Indipendentemente dalla possibilità o meno di un coinvolgimento in sede penale del datore di lavoro, occorre considerare che il corpo del reato, ossia le immagini dal contenuto pedopornografico sarebbe trovato supporti informatici (hard disk, server, ecc.) di proprietà dell'azienda. In primo luogo la stessa potrebbe essere chiamata a dimostrare la propria estraneità nella commissione del reato da parte del proprio dipendente, dimostrazione sicuramente più agevole nel caso siano state precedentemente adottate le contromisure idonee a prevenire comportamenti illeciti di questo tipo. In secondo luogo l'azienda difficilmente potrebbe evitare il sequestro da parte dell'autorità giudiziaria delle strumentazioni informatiche contenenti immagini pedopornografiche.

L'impresa potrà invece essere tenuta a risarcire in sede civile i danni causati ai terzi dal comportamento illecito dei propri dipendenti. Occorre però non tralasciare i danni all'immagine che potrebbe subire l'azienda in conseguenza della commissione di un reato connesso alla pedopornografia, di sicuro impatto negativo sull'opinione pubblica ed in particolare sulla clientela, sempre più attenta anche agli aspetti etici del comportamento delle organizzazioni.

Web Security: Implicazioni Legali

11

Scenario 4: Il dipendente installa sul proprio computer aziendale del software pirata o software non autorizzato dall'azienda

Il software è stato inserito dal **decreto legislativo 29 dicembre 1992 n. 518** tra le opere dell'ingegno di carattere creativo, estendendo ad essi la protezione della legge sul diritto d'autore (legge 22 aprile 1941 n. 633) prevista per le opere letterarie. All'autore di un software spettano, oltre ai diritti morali, come quello alla paternità dell'opera, i diritti esclusivi di utilizzazione economica quali la riproduzione, la duplicazione, la vendita e l'elaborazione. Come avviene per le restanti opere dell'ingegno nessuna utilizzazione del programma per elaboratore è consentita in assenza di un'autorizzazione da parte dell'autore (o del soggetto al quale sono stati trasferiti i diritti esclusivi di utilizzazione economica).

La stessa legge 518 del 1992 aveva già previsto, sanzioni di carattere penale per la duplicazione abusiva di programmi per elaboratore, tuttavia tale condotta era punita esclusivamente se effettuata con finalità di lucro (ossia l'intenzionale perseguimento di un vantaggio economico, o, in altre parole, un immediato incremento patrimoniale). Tale limitazione non aveva mancato di suscitare feroci critiche da parte di numerosi interpreti che ritenevano tale previsione assolutamente insufficiente ad arginare il fenomeno della pirateria, ovvero della diffusione e duplicazione di software in assenza di autorizzazione da parte dell'autore

Proprio l'enorme dilagare a livello internazionale di tale fenomeno, favorito altresì dal crescente utilizzo delle reti telematiche, ha indotto il legislatore comunitario e successivamente quello italiano a prevedere una disciplina più rigida. Infatti, con la legge 18 agosto 2000 n. 248 è stato attribuito alla S.I.A.E. (Società Italiana degli Autori ed Editori) il compito di **apporre un contrassegno** su ogni supporto contenente programmi per elaboratore o multimediali **destinati ad essere posti in commercio o ceduti in uso a qualunque titolo a fine di lucro** (art. 181 bis l.d.a.). Il contrassegno deve essere apposto ai soli fini della tutela dei diritti relativi alle opere dell'ingegno previa attestazione da parte del richiedente di aver assolto gli obblighi previsti dalla normativa sul diritto d'autore e sui diritti connessi. Per i programmi per elaboratore il contrassegno può essere sostituito da un'apposita dichiarazione identificativa resa alla SIAE dai produttori o importatori. **E' quindi illecito qualunque software posto in commercio senza il contrassegno S.I.A.E. (o della dichiarazione identificativa).**

In secondo luogo la legge 248 del 2000 ha inasprito le sanzioni per l'illecita duplicazione di software (articolo 171 bis legge 633/1941) divenuta punibile se effettuata anche per finalità di profitto (e non solo di lucro). Come ha chiarito la giurisprudenza italiana il concetto di profitto è da considerarsi sicuramente più ampio di quello di lucro ed è comprensivo anche del semplice risparmio di costi. Le sanzioni sono molto severe e consistono nella **multa da €**

SECURITY & PRIVACY

2.582,28 a € 15.493,70 e nella reclusione da sei mesi a tre anni.

Viste le disposizioni esaminate appare assolutamente necessario che l'azienda ponga in essere delle misure volte a contrastare l'installazione di software pirata all'interno dei propri computer o server aziendali. Pur ribadendo che la responsabilità penale nel nostro ordinamento è personale, e che quindi l'azienda nella persona dei suoi amministratori non può essere ritenuta responsabile di un reato commesso dal dipendente (è opportuno ricordare che, secondo l'orientamento dottrinale esposto nel precedente scenario, nel caso di mancata applicazione di idonee misure di controllo e prevenzione degli illeciti, gli amministratori potrebbero invece rispondere a titolo di concorso nel reato commesso dal dipendente) tuttavia, nel caso di specie, vi sono ulteriori problematiche da tenere in considerazione.

Innanzitutto l'impresa, nel caso in cui la Guardia di Finanza (alla quale sono stati demandati i compiti di prevenzione, ricerca e repressione delle violazioni anche in materia di diritti d'autore) dovesse verificare la presenza di software pirata sui computer, non potrebbe evitare il sequestro degli stessi, con notevole intralcio allo svolgimento delle proprie attività. Inoltre, potrebbe essere tenuta a dimostrare che l'installazione del software da parte del dipendente non è stata autorizzata, cosa sicuramente difficoltosa nel caso in cui il lavoratore utilizzi il programma per elaboratore piratato per l'esercizio delle proprie mansioni. Residua inoltre la possibilità che l'azienda sia chiamata a risarcire sulla base dell'articolo 2049 del codice civile i terzi che eventualmente siano stati lesi dalla condotta illecita dei dipendenti (si veda a riguardo quanto esposto nello Scenario 1).

Web Security: Implicazioni Legali

12

Scenario 5: Un'azienda contamina un'altra azienda a causa di un virus o di spyware nel suo sito web

I virus ed il codice penale

I virus informatici, a livello generale, sono programmi per elaboratore appositamente sviluppati con la finalità di danneggiare un sistema informatico o di alterarne le funzionalità. I virus, sempre più numerosi e potenzialmente dannosi, rappresentano un problema molto rilevante per la sicurezza aziendale e comportano la necessità della predisposizione di adeguate contromisure sia dal lato tecnico che organizzativo.

La grande diffusione di questi programmi ed i conseguenti danni stessi causati ai sistemi informatici ha indotto il legislatore italiano a prevedere con Legge 23 dicembre 1993 n. 547 (*"Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"*), una fattispecie di reato relativa ai virus informatici.

L'articolo 615 quinquies del codice penale sanziona con la pena della reclusione sino a due anni e con la multa sino a € 10.329,00 la condotta di chi diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento. Come risulta evidente dalla lettura di questa norma, ai fini della configurazione del reato previsto non è necessario che il virus diffuso o comunicato abbia provocato dei danni al sistema informatico, essendo invece sufficiente la consapevolezza della dannosità dello stesso da parte dell'agente.

In ambito aziendale, la mancata protezione dei sistemi informatici dall'attacco di virus, è idonea non solo a danneggiare l'azienda stessa, ma anche soggetti esterni. E' sufficiente pensare, per esempio, ai danni provocati dalla propagazione di un virus o di uno spyware (un particolare tipologia di software maligno utilizzato prevalentemente per il furto di dati) nel sistema informatico di un'altra organizzazione o di un cliente che abbia visitato il sito internet dell'azienda sul quale era inconsapevolmente caricato.

Le conseguenze per l'azienda

Escludendo nel caso sopra esaminato la sussistenza dei requisiti per l'applicazione del sopra menzionato articolo 615 quinquies del codice penale nei confronti della persona fisica (per esempio un dipendente) responsabile della propagazione del virus (che sarebbero presenti esclusivamente nel caso di una intenzionale, ossia dolosa, diffusione del virus stesso) sono invece sicuramente ravvisabili profili di responsabilità in capo all'azienda titolare del sito web infetto.

L'articolo 2043 del codice civile, in primo luogo, prevede un obbligo generale di risarcimento per i danni causati a

SECURITY & PRIVACY

terzi da un comportamento negligente (cosiddetta responsabilità extracontrattuale). E' evidente, nel caso di specie, che la presenza di un virus informatico nel proprio sito web può essere dovuta ad una condotta negligente dell'azienda che non ha provveduto ad adottare tutte le misure necessarie per proteggere i propri sistemi informatici. Nell'eventualità dunque che i soggetti danneggiati dalla propagazione del virus riescano a dimostrare l'illegittimità del comportamento dell'azienda titolare del sito web, ne risulterebbe un obbligo in capo a questa di risarcire i danni provocati.

Da un altro punto di vista occorre considerare che le aziende sono tenute, in base al Codice in materia di protezione dei dati personali (d.lgs 196/2003, noto anche come Codice della Privacy), ad adottare determinate (minime e idonee) misure di sicurezza a protezione dei sistemi informatici nel caso trattino dati personali. La mancata adozione di tali misure, può essere fonte sia di responsabilità civile sia di responsabilità penale. In particolare l'allegato B del Codice della Privacy, contenente l'elenco delle misure minime di sicurezza, prevede che le aziende debbano proteggere i dati personali dall'azione di programmi di cui all'articolo 615 quinquies del codice penale (virus informatici) mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale. Nonostante l'adozione di tale misura sia sufficiente nel caso di specie ad escludere una responsabilità penale (la mancata adozione di anche una soltanto delle misure minime elencate è condotta integrante reato in base all'articolo 167 del Codice della Privacy), non esclude invece una responsabilità civile dell'azienda nei confronti degli interessati (ossia di coloro a cui i dati trattati si riferiscono) nel caso in cui il giudice chiamato a decidere sull'esistenza dei presupposti per il risarcimento del danno, la ritenga comunque inadeguata a prevenire il danno provocato. Il Codice, infatti, oltre alle misure minime di sicurezza (come visto obbligatorie) prevede in ogni caso l'adozione di idonee misure di sicurezza da valutarsi in base al progresso tecnico, alla natura dei dati personali

Web Security: Implicazioni Legali

13

trattati e alle specifiche caratteristiche del trattamento, volte a ridurre al minimo i rischi di distruzione o di perdita dei dati trattati.

Da quanto esposto emerge chiaramente l'esigenza da parte delle imprese di limitare i comportamenti dei dipendenti che possano essere causa di propagazioni di virus all'interno ed all'esterno delle aziende e di adottare ogni misura idonea, tra cui gli antivirus, a protezione dei sistemi informatici per evitare conseguenze giuridicamente rilevanti.

Web Security: Implicazioni Legali

14

Scenario 6: Il dipendente salva su una chiavetta USB informazioni coperte da segreto e le divulga a terzi.

L'evoluzione delle tecnologie informatiche impone alle imprese di affrontare problematiche sempre nuove e dalle conseguenze potenzialmente sempre più dannose. Si considerino, per esempio, i rischi connessi alla diffusione dei dispositivi informatici removibili di ultima generazione (quali le chiavette USB, Hard Disk portatili, ecc.) che permettono di archiviare facilmente grandi quantità di informazioni. Tali strumenti, nel peggiore dei casi, potrebbero essere utilizzati dai dipendenti e dai collaboratori per salvare un'enorme quantità di informazioni aziendali segrete allo scopo di danneggiare l'azienda attraverso la loro divulgazione a terzi (ed in primis ad una società concorrente). Allo scopo di valutare appieno la pericolosità di tali comportamenti, occorre altresì evidenziare la grande importanza che stanno assumendo per le organizzazioni gli asset immateriali, quali le informazioni e le conoscenze.

Le norme poste dal nostro ordinamento giuridico a protezione delle informazioni coperte da segreto

In primo luogo, il codice civile impone ai dipendenti di adottare un comportamento fedele nei confronti dell'azienda volto a tutelare il Know how della stessa. L'articolo 2105 del codice civile, in particolare, prevede che il prestatore di lavoro non debba trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio. La violazione dell'obbligo di fedeltà da parte del dipendente consente all'azienda (ai sensi dell'articolo 2106 del codice civile) di applicare sanzioni disciplinari, graduate secondo la gravità dell'infrazione.

Inoltre, le informazioni aziendali ricevono esplicita protezione anche dalla legislazione in materia di diritto industriale e nello specifico dal Codice della proprietà industriale, di recente approvazione. L'articolo 98 dello stesso prevede espressamente una tutela per le informazioni aziendali e le esperienze tecnico-industriali, comprese quelle commerciali, soggette al legittimo controllo del detentore ove tali informazioni:

- siano segrete, nel senso che non siano nel loro insieme, o nella precisa configurazione e combinazione

SECURITY & PRIVACY

dei loro elementi, generalmente note o facilmente accessibili agli esperti ed agli operatori del settore;

- abbiano valore economico in quanto segrete;
- siano sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete.

Diretta conseguenza della norma sopra esaminata è il divieto disciplinato dal successivo articolo 99 del Codice stesso di rivelare a terzi, oppure acquisire od utilizzare le informazioni e le esperienze aziendali oggetto di protezione.

Esistono, infine, nell'ordinamento italiano anche sanzioni penali a tutela della segretezza delle informazioni.

L'articolo 621 del codice penale punisce se dal fatto deriva nocimento, con la reclusione fino a tre anni o con la multa da € 103,00 a € 1.032,00 chiunque, essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, di altrui atti o documenti, pubblici o privati, non costituenti corrispondenza, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto. Ai fini dell'applicazione di questo articolo, nella nozione di documenti rientra anche qualunque supporto informatico contenente dati, informazioni o programmi.

L'articolo 623 codice penale, inoltre, prevede la sanzione della reclusione fino a due anni per chiunque, venuto a cognizione per ragione del suo stato o ufficio, o della sua professione o arte, di notizie destinate a rimanere segrete, in relazione a scoperte o invenzioni scientifiche o applicazioni industriali, le rivela o le impiega a proprio o altrui profitto.

Le contromisure da adottare in azienda

L'esistenza di norme poste a tutela della segretezza delle informazioni aziendali corredate da specifiche sanzioni a carico dei trasgressori non esonera l'azienda dall'adottare misure preventive atte a scongiurare questo tipo di comportamento da parte dei propri dipendenti.

Le organizzazioni da un lato possono tutelarsi con l'adozione (possibilità prevista dell'articolo 2125 del codice civile) di patti non di concorrenza nei confronti dei dipendenti per il tempo successivo alla cessazione del contratto di lavoro, dall'altro sfruttando le possibilità loro offerte dal diritto industriale, quali la protezione garantita ai marchi, ai brevetti o ai modelli industriali.

Web Security: Implicazioni Legali
15

Le aziende potrebbero inoltre decidere di dotarsi di un regolamento interno per l'uso delle strumentazioni informatiche o telematiche che contempli il divieto di utilizzare supporti removibili da parte dei dipendenti e preveda eventualmente sanzioni disciplinari nei confronti dei trasgressori. Da non sottovalutare, infine, l'adozione di tecnologie, oggi ampiamente disponibili, che consentono di inibire l'utilizzo delle porte USB dei computer aziendali per collegare qualsiasi tipo di memoria removibile (chiavetta USB, HD portatile ecc...). Queste soluzioni hanno sicuramente il vantaggio di limitare a priori i possibili comportamenti illeciti dei dipendenti, senza peraltro violare in alcun modo la loro riservatezza.

Web Security: Implicazioni Legali
16

Scenario 7: Il dipendente incaricato dei rapporti con le banche subisce un attacco di phishing e comunica involontariamente a terzi le password di accesso al conto bancario on-line dell'azienda

La diffusione nell'utilizzo della rete internet da parte di un sempre maggior numero di soggetti, spesso sprovvisti delle necessarie conoscenze informatiche di base, ha fatto crescere in modo esponenziale le condotte illegittime volte a sfruttare la loro disinformazione. Sono infatti in continuo aumento i furti d'identità, da intendersi come la raccolta abusiva di informazioni su un soggetto o organizzazione al fine di una loro successiva utilizzazione in attività illecite.

Il furto d'identità è quindi sovente il mezzo utilizzato per poter successivamente attuare condotte sicuramente illegittime quali lo spamming, la predisposizione di truffe o la sottrazione di fondi da conti correnti on-line.

Una delle ultime espressioni del furto di identità messa in atto dai pirati informatici è il phishing.

Il Phishing

Il phishing, è una attività fraudolenta, attuata nei confronti di un elevato numero di soggetti, solitamente attraverso l'invio di messaggi di posta elettronica, con lo scopo di entrare in possesso di informazioni personali degli stessi quali codici di identificazione, numeri di carte di credito, codici dispositivi per l'home banking ecc. Tali informazioni

SECURITY & PRIVACY

vengono successivamente utilizzate dal soggetto agente (Phisher) per effettuare a proprio vantaggio operazioni in sostituzione del legittimo titolare (quali operazioni bancarie, accesso a sistemi informatici).

Statisticamente, il phishing viene maggiormente utilizzato per carpire informazioni inerenti i numeri di carte di credito o i codici dispositivi al fine di entrare in possesso dei capitali delle vittime della truffa. Ovviamente anche le aziende possono essere danneggiate dal Phishing nel caso le informazioni recuperate siano di sua titolarità; è sufficiente pensare in tal senso all'eventualità che un dipendente rimanga vittima di un attacco e comunichi le password aziendali per l'accesso ai conti bancari on-line.

Il Phishing e le sanzioni previste

Gli attacchi di Phishing vengono sferrati attraverso metodologie molto simili e che si ripetono nel tempo. L'attacco inizia con l'invio ad una massa indistinta di destinatari (il cui indirizzo e-mail è stato carpito illecitamente) di un messaggio di posta elettronica che riproduce fedelmente la grafica e il logo utilizzati da un istituto bancario. Con il messaggio inviato il soggetto viene avvisato per esempio di alcuni problemi tecnici o di sicurezza che si sono verificati con il proprio conto corrente di home banking (in realtà il phisher non conosce se il destinatario della e-mail è o meno cliente di una data banca, tuttavia maggiore è il numero dei messaggi inviati maggiore è la probabilità di raggiungerne la clientela). Il "correntista" viene poi invitato con un apposito link a collegarsi ad un sito internet per potere risolvere questi problemi tecnici legati al proprio conto corrente (anche il sito internet è di regola in tutto e per tutto identico al sito originale dell'istituto di credito) e gli viene richiesto di autenticarsi inserendo la sua password ed il codice dispositivo. Questi dati vengono quindi carpiri dal phisher e successivamente utilizzati per compiere operazioni sul conto corrente del malcapitato (ad esempio trasferimenti di danaro).

Come accennato il Phishing è una condotta fraudolenta punibile ai sensi dell'articolo 640 codice penale relativo alla truffa che prevede la pena della reclusione da sei mesi a tre anni e della multa da € 51,00 a € 1.032,00 per chiunque, con artifici o raggiri, inducendo taluno in errore, procuri a sé o ad altri un ingiusto profitto con altrui danno.

In un attacco di phishing sono infatti presenti tutti gli elementi previsti dalla norma di cui sopra ed in particolare:

- gli "artifici o raggiri" costituiti dalla riproduzioni di e-mail e di siti internet appartenenti ad istituti bancari;
- l'induzione in errore del destinatario, che riteneva di fornire alla propria banca i dati relativi al suo conto corrente
- l'ingiusto profitto costituito per esempio dall'illecito prelievo effettuato sul conto del soggetto indotto in errore.

Le possibili soluzioni

Dal momento che un attacco di Phishing portato a termine nei confronti di un'azienda potrebbe causare perdita di fondi conservati nei propri conti correnti, il più delle volte difficilmente recuperabili, è assolutamente necessaria

Web Security: Implicazioni Legali

17

l'adozione di adeguate contromisure volte a ridurre tale pericolo. In primo luogo è indispensabile che i dipendenti siano informati su tali forme di truffa e sugli accorgimenti da porre in essere per riconoscerle (alcune norme potrebbero per esempio essere inserite nel regolamento interno per l'utilizzo delle strumentazioni informatiche aziendali). E' altresì possibile dotarsi di strumenti tecnologici che limitino la possibilità di essere destinatari di attacchi di phishing (quali filtri anti spam) o che avvertano l'utente della navigazione su siti non autentici.

Web Security: Implicazioni Legali

18

Scenario 8: Uno spyware s'insedia nel sistema informativo dell'azienda e viene rubata tutta la banca dati del personale. Uno spyware s'insedia nel sistema informativo di una azienda di email - marketing e viene rubata la banca dati marketing di un cliente

Gli spyware sono una tipologia di software maligni sviluppati per trasmettere all'esterno attraverso la rete internet le informazioni contenute nelle banche dati dei sistemi informatici nei quali sono stati caricati. I dati così sottratti e trasferiti vengono poi raccolti ed utilizzati all'esterno per compiere attività illecite e spesso con finalità di profitto. Ad accrescere ulteriormente i rischi connessi a tali tipologie di virus informatici è la facilità con cui gli stessi riescono ad insediarsi nei sistemi informatici; la semplice navigazione su particolari pagine web è talvolta sufficiente a rendere possibile un'infezione. Uno spyware potrebbe pertanto facilmente essere introdotto nel sistema informativo dell'azienda e ritrasmettere verso l'esterno tutte le informazioni contenute nelle sue banche dati.

Tra le informazioni conservate nei sistemi informatici aziendali vi sono sicuramente dati personali, da intendersi ai

SECURITY & PRIVACY

sensi del decreto legislativo 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali) come qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. Sono quindi dati personali le informazioni relative alla clientela, ai fornitori, ai dipendenti ecc...

Alcune banche dati possono contenere anche dati sensibili ovvero idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale. E' assolutamente probabile che nella banca dati del personale dell'azienda potrebbero essere registrati dati sensibili riguardanti i propri dipendenti (come quelli relativi all'appartenenza sindacale o allo stato di salute).

Come vedremo le aziende hanno degli obblighi di protezione dei dati personali trattati nell'esercizio delle proprie attività, accompagnati da sanzioni che nei casi più gravi sono di carattere penale.

Capita sempre più spesso, inoltre, a seguito della diffusione dei contratti di outsourcing, che le organizzazioni affidino all'esterno la gestione di dati personali. Si pensi per esempio al caso di un'azienda di e-mail marketing alla quale altre società abbiano affidato le proprie banche dati per procedere all'invio di messaggi pubblicitari. In tali casi occorre considerare che la perdita e/o la sottrazione di dati personali contenuti in una delle banche dati affidate alla società, dovuta per esempio all'azione di uno spyware, comporta una sua responsabilità al limite anche nei confronti dei interessati dei dati stessi (cioè le persone fisiche o giuridiche cui i dati si riferiscono) ma sicuramente verso i clienti (titolari del trattamento).

Le disposizioni del Codice in materia di protezione dei dati personali

L'azienda proprietaria dei dati, secondo quanto previsto dal Codice in materia di protezione dei dati personali è "titolare del trattamento dei dati" e, pertanto, le competono tutte le decisioni riguardanti le finalità, le modalità del trattamento dei dati personali. In particolare, spetta all'organizzazione decidere quali strumenti sono utilizzati per il trattamento dei dati e le misure di sicurezza che devono essere implementate.

Web Security: Implicazioni Legali

19

L'Articolo 31 del Codice prevede che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. L'idoneità delle misure di sicurezza deve essere valutata in relazione alla natura dei dati pertanto se l'azienda tratta dati sensibili dovrà adottare delle misure di sicurezza tali da scongiurare qualsiasi perdita di dati. L'idoneità deve altresì essere rapportata alle specifiche caratteristiche del trattamento.

In caso di perdita di dati l'azienda potrebbe dovere rispondere dei danni causati per effetto del trattamento ai sensi dell'articolo 15 del Codice se non prova di avere adottato tutte le misure idonee ad evitare il danno. Pertanto, l'idoneità o meno delle misure di sicurezza in questo caso è lasciata al libero convincimento del giudice, il quale potrebbe anche ritenere le stesse, nei singoli casi specifici, inadeguate rispetto ai rischi di perdita o alla natura dei dati (c.d. responsabilità per attività pericolose ex art. 2050 del codice civile che prevede il ribaltamento dell'onere

SECURITY & PRIVACY

della prova).

Ai sensi dell'articolo 33 del Codice i titolari del trattamento sono comunque tenuti ad adottare le misure minime volte ad assicurare un livello minimo di protezione dei dati personali come specificate nell'Allegato B al Codice che prevede tra l'altro:

- che i dati personali siano protetti contro il rischio di intrusione e di danneggiamento, mediante l'attivazione di idonei strumenti elettronici (quali ad esempio antivirus) da aggiornare con cadenza almeno semestrale;
- che siano effettuati almeno annualmente aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici ed a correggerne difetti (in caso di trattamento di dati sensibili o giudiziari l'aggiornamento deve essere invece almeno semestrale);
- che i dati sensibili o giudiziari siano protetti contro l'accesso abusivo mediante l'utilizzo di idonei strumenti elettronici (router, firewall).

La mancata applicazione delle misure minime di sicurezza è sanzionata penalmente ai sensi dell'articolo 169 del D.lgs 196/03 dove si prevede che: "*Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro*".

Web Security: Implicazioni Legali
20

Scenario 9: I computer fanno parte all'insaputa dell'azienda di una Botnet che sferra un attacco del tipo Denial Of Service ad una terza società

Avviene con sempre maggior frequenza che le reti aziendali siano abusivamente utilizzate da estranei per sferrare attacchi informatici o compiere altre tipologie di reati: è il fenomeno delle Botnet. Senza scendere nei particolari, i sistemi informatici aziendali collegati ad internet, a causa di inefficienze della sicurezza, possono essere infettati da particolari virus che consentono ai loro creatori di assumere il controllo degli stessi. I computer infettati entrano così a far parte di una rete sotto il controllo di soggetti esterni che li possono utilizzare, per esempio, per sferrare attacchi verso altri sistemi informatici del tipo Denial Of Service, ossia volti ad impedirne le funzionalità.

Le sanzioni a carico dei pirati informatici

Ovviamente, l'attività dei gestori di tali reti di computer infetti è da considerarsi sicuramente illecita e sanzionabile sulla base di alcune disposizioni contenute nel codice penale. In primo luogo l'articolo 615 quinquies del codice penale punisce con la sanzione della reclusione sino a due anni e con la multa sino a diecimilatrecentoventinove euro la diffusione di programmi diretti a danneggiare o interrompere un sistema informatico. E' evidente, infatti, sia che i virus utilizzati per la creazione delle Botnet siano idonei ad alterare le funzionalità dei sistemi informatici aziendali (consentendo a terzi non autorizzati di assumerne il controllo), sia che la condotta sia sorretta da dolo. Nel caso in cui i computer infettati siano, inoltre, a qualsiasi scopo utilizzati dai creatori dei virus, è altresì configurabile la condotta di accesso abusivo ad un sistema informatico di cui all'articolo 615 ter del codice penale. Tale norma prevede la sanzione della reclusione sino a tre anni per chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza. In base ad un orientamento consolidato della giurisprudenza, ai fini della configurazione del presente reato è sufficiente che il sistema informatico sia protetto da una qualsiasi misura di sicurezza, indipendentemente dalla sua idoneità o meno a prevenire l'illecita intrusione.

I rischi per l'azienda e la computer forensic

Come accennato, i computer aziendali facenti parte di una botnet, possono essere utilizzati per sferrare attacchi verso sistemi informatici di altre organizzazioni (condotta anch'essa punibile dal sopra esaminato articolo 615 ter del codice penale) o per compiere altre tipologie di reato. E' ovvio che in tali casi, in sede di indagine dell'autorità giudiziaria, l'azienda correrà l'altissimo rischio di vedersi direttamente coinvolta in quanto apparirà, in un primo momento, che gli attacchi informatici sono partiti dai suoi computer. Anzi è proprio questo lo scopo dei gestori delle botnet, che vogliono ostacolare le attività di indagine rendendo difficoltosa la propria individuazione.

Per queste ragioni l'azienda in primo luogo potrebbe subire un sequestro ad opera dell'autorità giudiziaria delle strumentazioni informatiche utilizzate per commettere il reato (le stesse contengono infatti elementi assolutamente necessari ai fini dell'individuazione del soggetto realmente responsabile). L'azienda stessa potrebbe inoltre essere chiamata a raccogliere attraverso indagini interne le necessarie prove informatiche al fine di dimostrare la propria estraneità alle condotte illecite poste in essere, a sua insaputa, utilizzando le proprie strumentazioni informatiche. Tuttavia le caratteristiche stesse delle prove digitali pongono il problema di una loro raccolta secondo tecniche e

SECURITY & PRIVACY

modalità che garantiscano una loro efficace produzione in sede processuale. Negli ultimi anni è nata una nuova disciplina la "computer forensic", il cui obiettivo principale è proprio la creazione di un protocollo di regole da seguire per la ricerca della prova informatica, per la sua acquisizione e per la sua conservazione con il fine di garantire che i risultati delle indagini abbiano valore anche in sede processuale. A tal fine l'azienda dovrebbe adottare idonee soluzioni sia sul lato organizzativo (attraverso una corretta formazione dei propri dipendenti volta a definire procedure da seguire nella raccolta di prove informatiche) sia sul piano tecnologico, utilizzando i software per la computer forensic attualmente disponibili.

Oltre a questo, dal momento che per entrare a far parte di una Botnet è solitamente necessario che il sistema informatico sia stato preventivamente infettato da un virus, l'azienda potrebbe essere chiamata a dimostrare di aver adottato le misure minime di sicurezza previste dal Codice in materia di protezione dei dati personali. I soggetti responsabili dell'applicazione delle misure minime potrebbero quindi venire coinvolti in un procedimento penale (peraltro con sanzioni molto elevate) che ha come antecedente un comportamento illecito da parte di terzi (gestori della Botnet)!

Web Security: Implicazioni Legali
21

Scenario 10 - La moglie di un dipendente si collega da remoto con il computer portatile aziendale alla rete aziendale e causa la propagazione di un virus.

Le aziende sempre di più attribuiscono ai loro dipendenti strumentazioni elettroniche portatili (cellulari, palmari, computer ...) che consentono loro di svolgere la propria attività lavorativa anche al di fuori della sede aziendale, sia in modo permanente (si pensi all'ipotesi del telelavoro) sia per esigenze sporadiche (ad esempio in caso di trasferta).

Emerge chiaramente che in tali situazioni dette strumentazioni possono essere alla portata non solo del dipendente ma anche di terzi quali ad esempio familiari o amici. E' quindi tutt'altro che remota la possibilità, dovuta ad un comportamento negligente del dipendente (ma a volte anche doloso), che un soggetto estraneo all'organizzazione aziendale si possa collegare da remoto alla sua rete informatica. In casi di questo tipo è superfluo evidenziare i rischi a cui va incontro l'azienda, che corre il pericolo di subire la compromissione dei propri sistemi informatici e dei dati in esso contenuti (è sufficiente immaginare gli effetti della propagazione di un virus).

Quali sono le possibili sanzioni a carico del dipendente nel caso sua moglie si sia collegata alla rete aziendale ed abbia causato involontariamente la propagazione di un virus?

Una delle principali cause che potrebbero consentire a terzi di utilizzare le strumentazioni aziendali messe a disposizione del dipendente è una cattiva gestione delle password che devono invece essere correttamente custodite e mantenute segrete. Vi sono alcune disposizioni normative riguardanti le password che possono astrattamente essere applicabili ai dipendenti che dolosamente o colposamente le abbiano comunicate a terzi. L'articolo 615 quater del codice penale punisce con la reclusione sino a un anno e con la multa sino a cinquemilacentosessantaquattro euro *"chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo"*. Ovviamente l'applicazione di questa norma richiederebbe la difficile dimostrazione di una volontà diretta del dipendente alla comunicazione della password (nel caso di specie alla moglie) per trarne un profitto o per arrecare un danno all'azienda.

Altre disposizioni sono inoltre contenute nel Codice in materia di protezione dei dati personali che, come visto negli scenari precedenti, impongono all'azienda di adottare quantomeno le misure minime di sicurezza (previste dall'articolo 33 ed elencate nell'Allegato B). In particolare il predetto allegato B obbliga i titolari del trattamento (le aziende) a fornire istruzioni agli incaricati (tra i quali i dipendenti):

- che prescrivano di adottare le necessarie cautele per assicurare la segretezza delle password e la diligente custodia dei dispositivi in loro possesso ed uso esclusivo (punto 4);
- che prescrivano di non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento (punto 9).

Come più volte ripetuto nei precedenti scenari l'articolo 169 del Codice in materia di protezione dei dati personali commina una sanzione di carattere penale per la mancata adozione delle misure minime di sicurezza.

SECURITY & PRIVACY

Nel caso in oggetto, ai fini di stabilire il responsabile della mancata applicazione delle misure di sicurezza concernenti le password occorre preventivamente valutare se l'azienda abbia o meno provveduto a fornire le istruzioni agli incaricati in merito alla gestione delle password e delle strumentazioni informatiche. In caso affermativo responsabile del reato di cui all'articolo 169 è il dipendente, che, in presenza di precise istruzioni dell'azienda, non ha provveduto ad applicare le prescritte misure di sicurezza.

Se le istruzioni di cui sopra sono state inserite nel regolamento interno per l'uso delle strumentazioni informatiche e telematiche al dipendente potrebbe essere applicata una sanzione disciplinare. Lo stesso è invece civilmente responsabile nei confronti dell'azienda per gli eventuali danni causati dalla sua condotta illegittima (per esempio dei danni provocati dal virus propagatosi all'interno dell'azienda per effetto della navigazione della moglie).