



D.Lgs. 231/2001

Sicurezza in ambiente aziendale:

I reati informatici

Verona, 20 IX 2010

Ing. Giacomo Pesce

Consulente di direzione e amministratore &Co Srl

www.and-co.net

www.viversicura.it



Campagna straordinaria di formazione per la diffusione
della cultura della salute e della sicurezza
Art. 11, comma 7 – D.Lgs. 81/08 DGR n. 277 del 09/02/2010





Il Computer Crime



Il Computer Crime è un fenomeno criminale che si caratterizza nell'abuso della tecnologia informatica.

Tutti i reati informatici sono accomunati da:

- ✓ L'utilizzo della tecnologia informatica per compiere l'abuso;
- ✓ L'utilizzo dell'elaboratore nella realizzazione del fatto.



Il Computer Crime



Definizioni:

REATO INFORMATICO

Reato commesso per mezzo di sistemi informatici e/o telematici e/o per cui vi siano prove in formato elettronico (*“Convenzione di Budapest”*)

SISTEMA INFORMATICO

Qualsiasi apparato in grado di svolgere funzioni autonome di elaborazione, anche se minime

SISTEMA TELEMATICO

Gruppo di apparecchiature interconnesse, una o più delle quali, per mezzo di un programma, compiono l'elaborazione automatica di dati (*“Convenzione di Budapest”*)



Il Computer Crime



Definizioni:

Figure che accedono abusivamente a rete informatica:

hacker: accede al sistema solo per dimostrarne la violabilità

cracker: vi accede per danneggiarlo o utilizzarlo indebitamente



Il Computer Crime



Definizioni:

Tipologie di accesso abusivo:

a) Accesso a sistema interconnesso a rete (Lan, WAN, Internet) cui **NON si è autorizzati**

- ✓ **caso hacker:** “traccia imbarazzante” per IT, che ripristina / tende a nascondere il fatto
- ✓ **caso cracker:** come hacker, ed inoltre presenza di danno, talvolta di difficile valutazione, meno nascondibile

b) Accesso a sistema di cui si dispone validamente delle credenziali, ma **per funzioni diverse dall'accesso effettuato** normalmente può essere un dipendente o collaboratore infedele

- ✓ frequentemente: è “impersonamento” di collega autorizzato, conoscendone illecitamente le credenziali
- ✓ è restare all'interno di un sistema contro la volontà (“policy”) del responsabile (amministratore IT)

In ogni caso esiste un'insufficiente protezione all'accesso (tecnica o pratica) oppure dolo dall'“interno”, che ha rivelato/facilitato le modalità di accesso



Il Computer Crime



Collocazione dei reati:

falsità: riferita ai documenti informatici

violazione di domicilio: accesso abusivo, detenzione/diffusione di codici di accesso, diffusione di hardware/software atti a danneggiare/interrompere sistemi informatici/telematici

inviolabilità dei segreti: intercettazione, interruzione, impedimento di comunicazioni informatiche/telematiche, installazione di apparecchiature di intercettazione

danneggiamento: di informazioni, dati, sistemi informatici e telematici, “semplici” e di “pubblica utilità”

truffa: frode informatica, effettuata alterando/operando su informazioni, dati sistemi informatici/telematici frode informatica del certificatore di firma elettronica



Il Computer Crime la normativa



Il Panorama Europeo

L'esigenza di punire i crimini informatici, emerse già alla fine degli anni '80, tanto che, il 13 Settembre 1989, il Consiglio d'Europa ha emanato una '**Raccomandazione sulla Criminalità Informatica**' dove venivano discusse le condotte informatiche abusive. I reati vennero divisi in due liste: facevano parte della prima lista detta '**lista minima**' quelle condotte che gli Stati sono invitati a perseguire penalmente quali:

- ✓ la frode informatica che consiste nell'alterare un procedimento di elaborazione di dati con lo scopo di procurarsi un ingiusto profitto;
- ✓ il falso in documenti informatici;
- ✓ il danneggiamento di dati e programmi;
- ✓ il sabotaggio informatico;
- ✓ l'accesso abusivo associato alla violazione delle misure di sicurezza del sistema;
- ✓ l'intercettazione non autorizzata;
- ✓ la riproduzione non autorizzata di programmi protetti;
- ✓ la riproduzione non autorizzata di topografie.



Il Computer Crime la normativa



Facevano invece parte della seconda lista detta **'lista facoltativa'** condotte 'solo eventualmente' da incriminare, quali:

- ✓ L'alterazione di dati o programmi non autorizzata sempre che non costituisca un danneggiamento;
- ✓ Lo spionaggio informatico inteso come la divulgazione di informazioni legate al segreto industriale o commerciale;
- ✓ L'utilizzo non autorizzato di un elaboratore o di una rete di elaboratori;
- ✓ L'utilizzo non autorizzato di un programma informatico protetto, abusivamente riprodotto.

Nel Settembre 1994 il Consiglio d'Europa ha aggiornato la precedente Raccomandazione ampliando le condotte perseguibili penalmente, inserendo:

- ✓ **Il commercio di codici d'accesso ottenuti illegalmente;**
- ✓ **La diffusione di virus e malware.**



Il Computer Crime la normativa



La legge 18/03/2008 n. 48 “Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno” ha introdotto nel D.Lgs. 8/06/2001 n 231 il nuovo

art. 24-bis

**Delitti informatici e trattamento
illecito di dati quali reati
presupposto**



D.Lgs. 231/01

Art. 24-bis. c.1



Tre categorie di reati

c.1 delitti di accesso abusivo

- ✓ accesso abusivo a sistema informatico o telematico,
- ✓ intercettazione illecita,
- ✓ impedimento,
- ✓ interruzione illecita di comunicazioni informatiche o telematiche,
- ✓ installazione di apparecchiature atte a intercettare comunicazioni informatiche o telematiche,
- ✓ danneggiamento di informazioni dati programmi sistemi informatici o telematici.



D.Lgs. 231/01

Art. 24-bis. c.1



c.1 delitti di accesso abusivo

Sanzioni

✓ Sanzione pecuniaria da 100 a 500 quote

In caso di condanna si prevede altresì l'applicazione delle sanzioni

✓ Interdizione all'esercizio dell'attività

✓ Sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali

✓ Divieto di pubblicizzare beni e servizi

Secondo il D.Lgs. 231/01, art. 11, co. 2, *"l'importo della quota è fissato (dal giudice) sulla base delle condizioni economiche e patrimoniali dell'ente, allo scopo di assicurare l'efficacia della sanzione"*. In base al Decreto (art. 10, co. 2) *"La sanzione pecuniaria viene applicata per quote in un numero non inferiore a cento nè superiore a mille"*.

Es. per un'azienda di ridotte capacità economiche e patrimoniali la quota potrebbe valere € 258,23 la sanzione potrebbe essere da € 25.823,00 a 129.115,00



D.Lgs. 231/01

Art. 24-bis. c.2



Tre categorie di reati

c.2 illeciti di detenzione

- ✓ detenzione abusiva di codici di accesso
- ✓ diffusione abusiva di codici
- ✓ installazione di apparecchiature (...) atte a interrompere e danneggiare – sistemi informatici e telematici

Sanzioni

- ✓ Sanzione pecuniaria fino a 300 quote
- In caso di condanna si prevede altresì l'applicazione delle sanzioni
- ✓ Sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali
 - ✓ Divieto di pubblicizzare beni e servizi



D.Lgs. 231/01

Art. 24-bis. c.3



Tre categorie di reati

c.3 delitti di falsità e frode informatica

- ✓ falsità relative a documento informatico
- ✓ frode del certificatore ossia del soggetto che presta servizi di certificazione di firma elettronica

Sanzioni

- ✓ Sanzione pecuniaria fino a 400 quote
- In caso di condanna si prevede altresì l'applicazione delle sanzioni
- ✓ Divieto di contrattare con la pubblica amministrazione
 - ✓ L'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi
 - ✓ Divieto di pubblicizzare beni e servizi



I reati informatici

Il codice penale



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



I reati informatici e il D.Lgs. 231: analisi



REATO

Art. 615-ter “Accesso abusivo ad un sistema informatico o telematico”

Art 617-quater CP, Art.617-quinquies CP, Art. 635-bis CP, Art. 635-ter CP, Art 635-quater CP, Art. 635 quinquies CP

CONDOTTA

Punisce la condotta di chi si introduce abusivamente, ossia eludendo una qualsiasi forma, anche minima, di barriere ostative all’accesso, in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà di chi a diritto di escluderlo.

IPOTESI DI REATO

Soggetti che si introducono nel sistema informatico della società per effettuare operazioni che portino un interesse o vantaggio per la società (diminuzione del credito dei clienti, maggiorazione dei costi dei servizi erogati, fatturazione di servizi non richiesti).

Soggetti si introducono abusivamente in sistemi informatici esterni al fine di procurare un interesse o vantaggio alla società. Ad esempio:

- ✓ Accesso abusivo nel sistema informatico di un concorrente al fine di conoscere l'offerta economica presentata per la partecipazione alla gara di appalto o il portafoglio clienti.
- ✓ Accesso abusivo nel sistema informatico di un concorrente al fine di conoscere i dati riservati.



I reati informatici e il D.Lgs. 231: analisi



REATO

Art. 615-ter “Accesso abusivo ad un sistema informatico o telematico”

Art 617-quater CP, Art.617-quinquies CP, Art. 635-bis CP, Art. 635-ter CP, Art 635-quater CP, Art. 635 quinquies CP

PROTOCOLLI DI CONTROLLO

- ✓ Definizione di politiche di sicurezza delle informazioni - gestione e uso delle password, modalità di effettuazione dei log-in e log-out, uso della posta elettronica, modalità di utilizzo dei supporti rimovibili, l'uso dei sistemi di protezione (antivirus, spam, phishing, spy)
- ✓ Inventario aggiornato dell'hardware e del software in uso agli utenti
- ✓ Procedure formali per l'assegnazione di privilegi speciali (ad es. amministratori di sistema, super-user)
- ✓ Tracciamento degli accessi degli utenti alla rete aziendale
- ✓ Controlli sugli accessi agli applicativi effettuati dagli utenti
- ✓ Tracciamento e monitoraggio degli eventi di sicurezza sulla rete



I reati informatici e il D.Lgs. 231: analisi



REATO

Art. 615-quater “Detenzione e diffusione abusiva di codici di accesso ai sistemi informatici o telematici” Art. 615-quinquies CP

CONDOTTA

Punisce la condotta di chi 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 in questo senso, allo scopo di procurare a sé o ad altri un profitto, o di arrecare ad altri un danno.

IPOTESI DI REATO

Soggetti si procurano codici di accesso ai sistemi informatici al fine di accedere al sistema interno ed effettuare operazioni che portino interesse o vantaggio per la Società.

Soggetti si procurano codici di accesso di sistemi informatici al fine di accedere a sistemi esterni e procurare un interesse o vantaggio alla Società.



I reati informatici e il D.Lgs. 231: analisi



REATO

Art. 615-quater “Detenzione e diffusione abusiva di codici di accesso ai sistemi informatici o telematici” Art. 615-quinquies CP

PROTOCOLLI DI CONTROLLO

- ✓ Definizione di politiche di sicurezza delle informazioni - gestione e uso delle password, modalità di effettuazione dei log-in e log-out, uso della posta elettronica, modalità di utilizzo dei supporti rimovibili, l'uso dei sistemi di protezione (antivirus, spam, phishing, spy)
- ✓ Creazione, modifica e cancellazione di account e profili
- ✓ Procedure formali per l'assegnazione di privilegi speciali (ad es. amministratori di sistema, super-user)
- ✓ Adozione di meccanismi di segregazione delle reti
- ✓ Gestione delle credenziali fisiche (badge, pin, codici di accesso, token authenticator, valori biometrici, ecc.)
- ✓ Tracciamento e monitoraggio degli eventi di sicurezza sulla rete
- ✓ Sicurezza fisica dei siti ove risiedono i sistemi IT



I reati informatici e il D.Lgs. 231: analisi



REATO

Art. 491-bis “Falsità di documenti informatici”

Art. 640-quinquies CP

CONDOTTA

Punisce chi integra uno dei reati relativi alle falsità in atti, se alcuna delle falsità previste dal Libro II, Titolo VII, Capo III Codice Penale, riguarda un documento informatico pubblico o privato, avente efficacia probatoria.

Di seguito si riportano alcune delle tipologie delittuose rilevanti, a titolo esemplificativo:

- ✓ falsità materiali commesse da un pubblico ufficiale o da un incaricato di pubblico servizio in atti pubblici e documenti ad essi assimilabili;
- ✓ falsità materiali in scrittura privata;
- ✓ falsità ideologiche in documenti pubblici commesse da un pubblico ufficiale, da un incaricato di pubblico servizio ovvero dal un privato;
- ✓ uso di atto falso (qualora l'autore materiale non sia precedentemente concorso nella falsificazione del documento);
- ✓ soppressione, distruzione e occultamento, parziale o totale, di atti veri.



I reati informatici e il D.Lgs. 231: analisi



REATO

Art. 491-bis “Falsità di documenti informatici”

Art. 640-quinquies CP

IPOTESI DI REATO

Soggetti integrano il reato al fine di modificare un documento informatico ad interesse o vantaggio della Società.

PROTOCOLLI DI CONTROLLO

- ✓ Politica per l'uso di controlli crittografici per la protezione delle informazioni
- ✓ Procedura a governo del processo di generazione, distribuzione ed archiviazione delle chiavi
- ✓ Procedure che regolamentano la digitalizzazione con firma digitale dei documenti, disciplinando il/i responsabile, livelli autorizzativi, utilizzo dei sistemi di certificazione, eventuale utilizzo e invio dei documenti, modalità di storage
- ✓ Procedura per la gestione delle chiavi a sostegno dell'uso delle tecniche crittografiche da parte della società

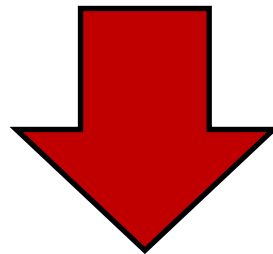


Modelli, best practice e strumenti di controllo



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

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



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

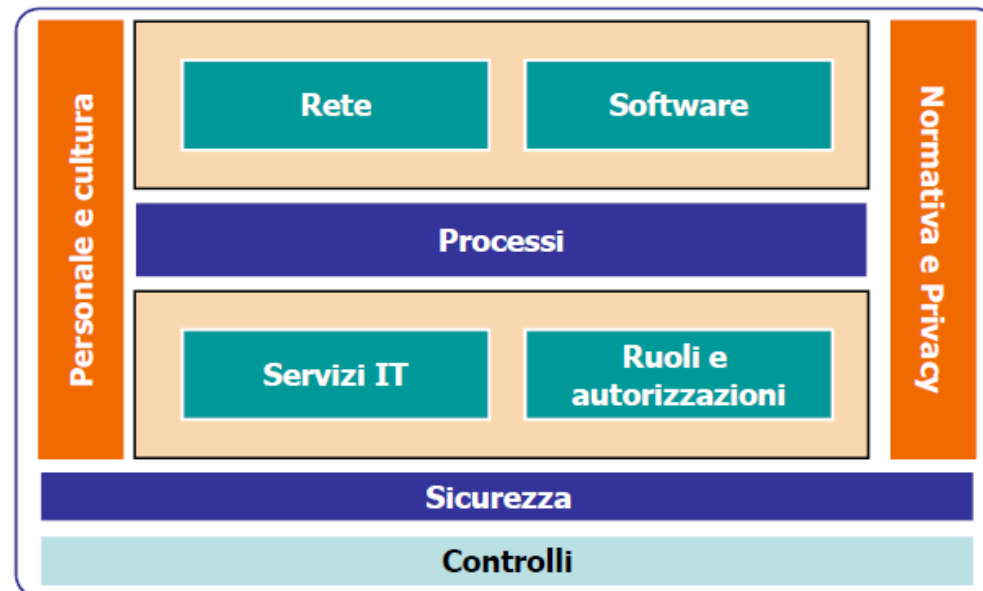


Modelli, best practice e strumenti di controllo



Esistono diversi standard, best practice e normative che supportano e spingono verso la definizione, implementazione, valutazione e monitoraggio di un Sistema di controllo IT che sia in grado di mitigare i rischi legati ai reati informatici

La normativa volontaria Internazionale propone la UNI EN ISO 27001:2005





Modelli, best practice la UNI EN ISO 27001



La norma **ISO 27001** è un “**code of practice**” rivolto a ogni tipo di organizzazione per la gestione dell’Information Security. Essa fornisce una serie di indicazioni per costituire una base all’implementazione di un sistema organizzativo orientato alla sicurezza informatica (da affiancare e integrare con il modello organizzativo 231), ossia al complesso di procedure per il governo della sicurezza attuato e mantenuto dall’organizzazione per garantire nel tempo il soddisfacimento della politica della sicurezza.

Essa, mediante l’implementazione del SGSI (Sistema di Gestione della Sicurezza delle Informazioni)

- ✓ suggerisce i controlli e le misure da adottare per assicurare che i rischi siano ridotte ad un livello minimo accettabile;
- ✓ una volta individuati i provvedimenti ed i controlli necessari, consente di definire adeguati strumenti di controllo per monitorarli (ad es. log);
- ✓ permette di gestire e mantenere i provvedimenti organizzativi adottati verificandone periodicamente l’efficacia.



Modelli, best practice



Alcuni spunti di riflessione:

La normativa Privacy (**D.Lgs. 196/2003**) interessa l'intera attività aziendale e, se implementata correttamente e mantenuta costantemente, offre strumenti utili per prevenire, reprimere, circoscrivere e provare gli illeciti di cui alla disciplina del D.Lgs. 231/2001 ancorchè la privacy regolamenta solo i dati personali.

L'applicazione delle misure di sicurezza richieste dalla normativa Privacy è fondamentale per l'adeguamento al sistema 231 per poter gestire una serie di rischi:

- ✓ distruzione o perdita anche accidentale di dati
- ✓ accesso non autorizzato
- ✓ trattamento non consentito
- ✓ trattamento non conforme alle finalità della raccolta



Modelli, best practice



Punti di attenzione:

- ✓ Identificazione e mappatura delle attività sensibili
- ✓ Modello di valutazione dei rischi:
 - Valutazione dei rischi di sicurezza
 - Valutazione delle attività di controllo
- ✓ Modelli di controllo per i crimini informatici
 - Processi
 - Policy e Procedure
 - Controlli di sicurezza da implementare/monitorare



Modelli, best practice cosa fare



Bisogna:

- ✓ inserire nel Codice Etico-Comportamentale basato sul modello organizzativo 231/2001 principi e valori per l'utilizzo della strumentazione informatica nello svolgimento della sua attività;
- ✓ recepire nel Codice Etico-Comportamentale, almeno come richiamo, le modalità di utilizzo e le linee-guida di impiego degli strumenti informatici contenute nel Documento di Policy Aziendale sull'informatica
- ✓ inserire nei contratti con "esterni" l'impegno al rispetto del Codice Etico

In particolare occorre

- I. definire e regolamentare affidamento/custodia degli strumenti informatici;
- II. definire e regolamentare i limiti di utilizzo degli strumenti informatici (di norma solo per attività lavorative e non per personali)
- III. disporre regole sull'utilizzo di dispositivi e di credenziali di accesso e loro utilizzazione, compreso l'uso delle aree dei *server* aziendali;
- IV. definire e regolamentare le modalità di produzione della documentazione, anche in forma cartacea, e della loro custodia;
- V. definire e regolamentare l'impiego della rete internet e della posta elettronica



Modelli, best practice cosa fare



Definire dei protocolli penal-preventivi:

- ✓ definizione e pubblicizzazione di specifiche deleghe nelle varie aree aziendali (in particolare, nell'area Informatica), con precisa specificazione di poteri e responsabilità dell'amministratore di sistema e dei suoi collaboratori;
- ✓ proceduralizzazione delle attività informatiche, nonché delle altre attività da considerarsi a rischio-reato, svolte con strumenti informatici;
- ✓ definizione di un processo continuo di informazione e di formazione generalizzato su commissibilità di reati informatici presupposti, e relative misure di prevenzione

Introdurre limitazioni all'uso degli strumenti informatici tramite strumenti tecnici:

- ✓ limiti navigazione internet, via proxy, firewall, filtri accesso siti web
- ✓ blocco chat e messaging, programmi social network
- ✓ impedire installazione programmi da parte utenti (nb "licenze")
- ✓ registrazione delle attività (Log) cfr. provvedimento Garante Privacy del 27/11/2008 (Misure ... prescritte ai titolari dei trattamenti ... circa ... attribuzione funzioni a amministratori di sistema)



Modelli, best practice cosa fare nello specifico



Controllo accessi

- ✓ attribuzione e gestione credenziali di accesso ai programmi, applicazioni, archivi
- ✓ creazione, modifica e cancellazione di account e profili;
- ✓ procedure formali per l'assegnazione di privilegi speciali (ad es. amministratori di sistema, super-user);

Monitoraggio

- ✓ sistemi di monitoraggio e log (registrazione eventi, rilevazione e avviso di anomalie);
- ✓ verifica sul tracciamento e monitoraggio degli eventi di sicurezza sulla rete;

Policy e organizzazione

- ✓ definizione ed organizzazione degli Information Systems Security Officers (ISSO);
- ✓ definizione dei ruoli degli utilizzatori, loro profili di utilizzo e poteri;
- ✓ verifica atto di nomina Amministratore di Sistema.
- ✓ definizione policy di uso dei dati aziendali (gradi di riservatezza e ambiti);
- ✓ definizione di politiche di sicurezza delle informazioni, gestione e uso delle password, modalità di effettuazione dei log-in e log-out, uso della posta elettronica, modalità di utilizzo dei supporti rimovibili, l'uso dei sistemi di protezione (antivirus,
- ✓ accertamento circa l'attività di controllo sull'operato degli Amministratori di Sistema in conformità alle policy aziendali.



Modelli, best practice cosa fare nello specifico



Privacy

- ✓ programma di informazione/formazione periodica dell'incaricato in ambito privacy
- ✓ Individuazione di ruoli e responsabilità in ambito privacy ed osservanza delle procedure aziendali in materia.
- ✓ controllo redazione o aggiornamento del Documento Programmatico sulla Sicurezza (DPS).
- ✓ verifica circa l'avvenuta menzione nella relazione accompagnatoria al bilancio della società dell'avvenuto o meno aggiornamento del DPS;
- ✓ controllo in merito alle attività di verifica compiute circa il rispetto delle misure minime di sicurezza privacy (i.e., controlli periodici IT);
- ✓ controllo a campione degli atti di nomina dei ruoli e delle responsabilità in ambito privacy (i.e., incaricati, responsabili, ecc.) e della documentazione rilevante in materia (i.e., informativa ex art. 13 per ogni categoria di interessati).



Modelli, best practice cosa fare nello specifico



Sicurezza fisica

- ✓ protezione fisica dei sistemi e relativi locali (hardware, software, lan, accessi esterni);
- ✓ Uso di proxy, firewall, reti private virtuali
- ✓ gestione delle credenziali fisiche di accesso (badge, pin, codici di accesso, token authenticator, valori biometrici, ecc.);
- ✓ sistemi di continuità, salvataggio e archiviazione;
- ✓ adozione di meccanismi di segregazione delle reti;
- ✓ Verifica della sicurezza fisica dei siti ove risiedono i sistemi IT;

Sicurezza logica

- ✓ sistemi di protezione logica di dati e documenti (integrità, riservatezza, autenticità, non ripudio, firma digitale);
- ✓ adottare una politica per l'uso di controlli crittografici per la protezione delle informazioni;
- ✓ adottare una procedura a governo del processo di generazione, distribuzione ed archiviazione delle chiavi crittografiche da parte della società;
- ✓ Uso di proxy, firewall, reti private virtuali



Modelli, best practice cosa fare nello specifico



Documenti informatici

✓ adottare procedure che regolamentino la digitalizzazione con firma digitale dei documenti, disciplinando i responsabili, i livelli autorizzativi, l'utilizzo dei sistemi di certificazione, l'eventuale utilizzo e invio dei documenti e le modalità di storage

Posta elettronica messaging

✓ adottare procedure che regolamentino la digitalizzazione con firma digitale dei documenti, disciplinando i responsabili, i livelli autorizzativi, l'utilizzo dei sistemi di certificazione, l'eventuale utilizzo e invio dei documenti e le modalità di storage

✓ Introdurre limiti alla navigazione internet, con uso di proxy, firewall, filtri accesso siti web

✓ Bloccare salvo profili autorizzati l'uso di programmi di chat, messaging e social network

✓ Impedire l'installazione programmi da parte di utenti non autorizzati

Software e applicazioni

✓ Disponibilità di ambienti separati di test, collaudo, produzione

✓ Impedire l'installazione programmi da parte di utenti non autorizzati

✓ Definire, attuare e verificare l'applicazione di procedure di debugging e aggiornamento software e applicazioni



GRAZIE PER L'ATTENZIONE !

Ing. **Giacomo Pesce**

Consulente di direzione e amministratore &Co Srl

www.and-co.net

www.viversicura.it

 Powered by Edulife

Campagna straordinaria di formazione per la diffusione
della cultura della salute e della sicurezza
Art. 11, comma 7 – D.Lgs. 81/08 DGR n. 277 del 09/02/2010

