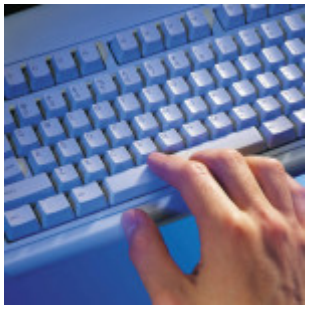
La nuova edizione della norma ISO 27002 (seconda parte)



In questo articolo (cfr. precedente articolo) passiamo ad esaminare la seconda parte della norma La norma UNI CEI ISO/IEC 27002:2014 – *Raccolta di prassi sui controlli per la sicurezza delle informazioni* (che sostituisce la ISO 27002:2005).

12 Sicurezza delle attività operative

Questa area comprende ben 7 categorie:

- **Procedure operative e responsabilità (12.1)**: devono essere predisposte procedure per documentare lo svolgimento di una serie di attività inerenti la sicurezza, occorre gestire i cambiamenti all'organizzazione e la capacità delle risorse (di *storage*, di banda, infrastrutturali ed anche umane), infine è necessario mantenere separati gli ambienti di sviluppo da quelli di produzione.
- **Protezione dal malware (12.2)**: un solo controllo in questa categoria (protezione dal malware) che prescrive tutte le misure di sicurezza da attuare contro il malware. Non solo antivirus per prevenire ed eliminare malware, ma anche azioni di prevenzione tecnica e comportamentali (consapevolezza degli utenti).
- **Backup (12.3)**: devono essere documentate ed attuate procedure di backup adeguate a garantire il ripristino dei dati in caso di perdita dell'integrità degli stessi e la continuità operativa (vedasi anche punto 17).
- **Raccolta di log e monitoraggio (12.4)**: devono essere registrati, conservati e protetti i log delle attività degli utenti normali e di quelli privilegiati (si ricorda che per apposita disposizione del Garante Privacy italiano i log degli accessi in qualità di Amministratore di Sistema devono essere mantenuti in modo "indelebile" per almeno 6 mesi), occorre inoltre mantenere sincronizzati gli orologi dei sistemi con una fonte attendibile.
- **Controllo del software di produzione (12.5)**: particolari attenzioni devono essere adottate nell'installazione ed aggiornamento del software di produzione (non solo per organizzazioni del settore ICT, banche o assicurazioni, ma anche per aziende manifatturiere!).
- **Gestione delle vulnerabilità tecniche (12.6)**: viene fornita dalla norma un'ampia guida attuativa sulla gestione delle vulnerabilità tecniche conosciute (occorre mantenere un censimento dell'hardware e del relativo software installato su ogni elaboratore, installare le *patch* di sicurezza in modo tempestivo, mantenersi aggiornati sulle vulnerabilità di sicurezza conosciute, ecc.), oltre alle

indicazioni sulla limitazione nell'installazione dei software (è opportuno, infatti, ridurre al minimo la possibilità per gli utenti di installare applicativi software autonomamente, anche se leciti come le utility gratuite che, a volte, possono essere il veicolo di *adware* o altre minacce alla sicurezza).
- **Considerazioni sull'audit dei sistemi informativi (12.7)**: gli audit sui sistemi informativi dovrebbero avere un impatto ridotto sulle attività lavorative e le evidenze raccolte dovrebbero essere raccolte senza alterare i dati dei sistemi (accessi in sola lettura) e dovrebbero essere mantenute protette.

Questi elementi nella precedente versione della norma erano in gran parte all'interno della sezione 10 "*Communications and Operations Management*" (ma la gestione delle vulnerabilità tecniche era, invece, al paragrafo 12.6, per puro caso lo stesso della versione attuale della norma), il quale comprendeva anche i controlli del punto 13 seguente.

13 Sicurezza delle comunicazioni

Questa sezione contiene due sole categorie:

- **Gestione della sicurezza della rete (13.1)**: occorre adottare alcuni accorgimenti per garantire la sicurezza delle reti interne (responsabilità, autenticazioni, ecc.); viene anche citata la ISO/IEC 27033 nelle sue parti da 1 a 5 sulla sicurezza delle reti e delle comunicazioni per ulteriori informazioni. Deve, inoltre, essere gestita la sicurezza dei servizi di rete, compresi i servizi acquistati presso fornitori esterni, e la segregazione delle reti (separazione delle VLan, gestione delle connessioni Wi-Fi, …).
- **Trasferimento delle informazioni (13.2)**: occorre stabilire ed attuare politiche e procedure per il trasferimento delle informazioni con qualsiasi mezzo (posta elettronica, fax, telefono, scaricamento da internet, ecc.), nel trasferimento di informazioni con soggetti esterni occorre stabilire accordi sulle modalità di trasmissione, le informazioni trasmesse tramite messaggistica elettronica dovrebbero essere adeguatamente controllate e protette (non solo e-mail, ma anche sistemi EDI, *instant messages*, *social network*, ecc.) e, infine, occorre stabilire e riesaminare periodicamente accordi di riservatezza e di non divulgazione con le parti interessate.

I 7 controlli di quest'area sono sicuramente molto dettagliati e migliorano, oltre ad aggiornare, la precedente versione della norma, includendo controlli (un po' sparsi nella versione 2005 della ISO 27002) che recepiscono le nuove modalità di comunicazione, tra cui i social network, professionali e non.

14 Acquisizione, sviluppo e manutenzione dei sistemi

Quest'area tratta la sicurezza dei sistemi informativi impiegati per le attività aziendali e comprende tre categorie:

- **Requisiti di sicurezza dei sistemi informativi (14.1)**: la sicurezza dei sistemi informativi- acquistati o sviluppati ad hoc – deve essere stabilita fin dall'analisi dei requisiti, deve essere garantita la sicurezza dei servizi applicativi che viaggiano su reti pubbliche (ad esempio attraverso trasmissioni ed autenticazioni sicure crittografate), infine occorre garantire la sicurezza delle transazioni dei servizi applicativi.
- **Sicurezza nei processi di sviluppo e supporto (14.2)**: devono essere definite ed attuate politiche per lo sviluppo (interno o esterno all'organizzazione) sicuro dei programmi applicativi, devono essere tenuti sotto controllo tutti i cambiamenti ai sistemi (dagli aggiornamenti dei sistemi operativi alle modifiche dei sistemi gestionali), occorre effettuare un riesame tecnico sul funzionamento degli applicativi critici a fronte di cambiamenti delle piattaforme operative (sistemi di produzione, database, ecc.) e si dovrebbero limitare le modifiche (personalizzazioni) ai pacchetti software, cercando comunque di garantirne i futuri aggiornamenti. Inoltre dovrebbero essere stabiliti, documentati ed attuati principi per l'ingegnerizzazione sicura dei sistemi informatici e per l'impiego di ambienti di sviluppo sicuri. Nel caso in cui attività di sviluppo software fossero commissionate all'esterno, dovrebbero essere stabilite misure per il controllo del processo di sviluppo esternalizzato. Infine dovrebbero essere eseguiti test di sicurezza dei sistemi durante lo sviluppo e test di accettazione nell'ambiente operativo di utilizzo, prima di rilasciare il software.
- **Dati di test (14.3)**: i dati utilizzati per il test dovrebbero essere scelti evitando di introdurre dati personali ed adottando adeguate misure di protezione, anche al fine di garantirne la riservatezza.

Nel complesso i 13 controlli di questa sezione sono molto dettagliati e comprendono una serie di misure di sicurezza informatica ormai consolidate che riguardano tutti gli aspetti del ciclo di vita del software impiegato da un'organizzazione per la propria attività. Alcuni principi vanno commisurati ad una attenta valutazione dei rischi, poiché una stessa regola di sicurezza informatica (ad es. l'aggiornamento sistematico e tempestivo del software di base) potrebbe non garantire sempre l'integrità e la disponibilità dei sistemi (ad es. errori o malfunzionamenti introdotti dagli ultimi aggiornamenti di un sistema operativo).

15 Relazioni con i fornitori

Questo punto di controllo tratta tutti gli aspetti di sicurezza delle informazioni che possono legati al comportamento dei fornitori. Sono state individuate due categorie:

- **Sicurezza delle informazioni nelle relazioni con i fornitori (15.1)**: è necessario stabilire una politica ed accordi su tematiche inerenti la sicurezza delle informazioni con i fornitori che accedono agli asset dell'organizzazione; tali accordi devono comprendere requisiti per affrontare i rischi relativi alla sicurezza associati a prodotti e servizi nella filiera di fornitura dell'ICT

(cloud computing compreso).

- **Gestione dell'erogazione dei servizi dei fornitori (15.2):** occorre monitorare – anche attraverso audit se necessario – e riesaminare periodicamente le attività dei fornitori che influenzano la sicurezza delle informazioni, nonché tenere sotto controllo tutti i cambiamenti legati alle forniture di servizi.

16 Gestione degli incidenti relativi alla sicurezza delle informazioni

L'area relativa agli incidenti sulla sicurezza delle informazioni (sezione 13 della precedente versione della norma) comprende una sola categoria (erano 2 nella precedente edizione):

- **Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti (16.1)**: devono essere rilevati e gestiti tutti gli incidenti relativi alla sicurezza delle informazioni (viene qui richiamata la ISO/IEC 27035 – *Information security incident management*), ma anche rilevate ed esaminate tutte le segnalazioni di eventi relativi alla sicurezza che potrebbero indurre a pensare che qualche controllo è risultato inefficace senza provocare un vero e proprio incidente e pure tutte le possibili debolezze dei controlli messi in atto. In ogni caso ogni evento relativo alla sicurezza delle informazioni va attentamente valutato per eventualmente classificarlo come incidente vero e proprio o meno. Occorre poi rispondere ad ogni incidente relativo alla sicurezza delle informazioni in modo adeguato ed apprendere da quanto accaduto per evitare che l'incidente si ripeta. Infine dovrebbero essere stabilite procedure per la raccolta di evidenze relative agli incidenti e la successiva gestione (considerando anche eventuali azioni di analisi forense).

17 Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa

In quest'area (corrispondente al punto 14 sella precedente versione della norma) viene trattata la ***business continuity*** in 5 controlli suddivisi in due categorie:

- **Continuità della sicurezza delle informazioni (17.1)**: la continuità operativa per la sicurezza delle informazioni dovrebbe essere pianificata a partire dai requisiti per la business continuity, piani di continuità operativa (*business continuity plan*) dovrebbero essere attuati, verificati e riesaminati periodicamente.
- **Ridondanze (17.2)**: per garantire la disponibilità (e la continuità operativa) occorre prevedere architetture e infrastrutture con adeguata ridondanza.

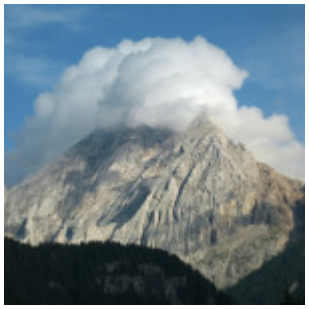
Naturalmente sull'argomento esiste la norma specifica UNI EN ISO 22301:2014 – *Sicurezza della società – Sistemi di gestione della continuità operativa – Requisiti.*

18 Conformità

Questo ultimo punto di controllo (era il punto 15 nella ISO 27002:2005) tratta la gestione della cosiddetta "*compliance*", ovvero la conformità a leggi, regolamenti ed accordi contrattuali con i clienti. Sono identificate due categorie:

- **Conformità ai requisiti cogenti e contrattuali (18.1)**: occorre innanzitutto identificare i requisiti cogenti, quindi attuare controlli per evitare di ledere i diritti di proprietà intellettuale, proteggere adeguatamente le registrazioni che permettono di dimostrare la conformità a tutti i requisiti cogenti, in particolare devono essere rispettati leggi e regolamenti sulla privacy (in Italia il D.Lgs 196/2003 in attesa del nuovo Regolamento Europeo, ma nella norma viene citata come riferimento la ISO/IEC 29100:2011 "*Information technology – Security techniques – Privacy framework*"). Infine occorre considerare eventuali limitazioni all'uso dei controlli crittografici vigenti in alcune nazioni.
- **Riesami della sicurezza delle informazioni (18.2)**: dovrebbe essere svolto periodicamente un riesame indipendente sulla sicurezza delle informazioni dell'organizzazione, i processi di elaborazione delle informazioni e le procedure dovrebbero essere riesaminate periodicamente per valutarne la continua conformità ed adeguatezza alla politica ed alle norme ed infine dovrebbero essere eseguite delle verifiche tecniche della conformità dei sistemi informativi a politiche e standard di sicurezza (ad esempio *penetration test* e *vulnerability assessment*). Su quest'ultimo controllo si fa riferimento alla ISO/IEC TR 27008 – *Guidelines for auditors on information security management systems controls*.

Cosa hanno in comune privacy, cloud computing e business continuity?



In precedenti articoli (Il cloud computing e la PMI, i sistemi di gestione della sicurezza delle informazioni, ISO 22301 e la business continuity, le novità sulla privacy) abbiamo affrontato tutti questi argomenti che, indubbiamente, hanno un unico filo conduttore.

Oggi molte aziende, fra cui anche numerose PMI, hanno dati "nel *cloud*", ovvero memorizzati in risorse fisiche non collocate all'interno dell'azienda, bensì su internet, magari senza rendersene conto. Infatti, oltre a veri e propri servizi

cloud erogati da fornitori specializzati, molte PMI utilizzano servizi di archiviazione gratuiti quali SkyDrive, Dropbox o Google Drive in maniera non strutturata, in quanto sono propri reparti o uffici o addirittura singoli collaboratori che, per praticità, hanno pensato di sfruttare suddetti *tool* di archiviazione remota.

In altri casi alcune organizzazioni utilizzano software via web che memorizzano i dati su server remoti, magari presso il fornitore del software (spesso si tratta di Saas, *Software as a Service*).

Tra i principali aspetti negativi che hanno generato diffidenza sull'archiviazione nel *cloud* c'è sicuramente la **sicurezza dei dati**, declinata in termini di **riservatezza**. Molti imprenditori, infatti, hanno la sensazione che alcuni dati riservati (informazioni commerciali, proprietà intellettuale relativa a progetti, ecc.) debbano rimanere in azienda per paura che qualcuno li possa consultare.

Normalmente una PMI, specialmente una piccola impresa, non effettua un'adeguata **valutazione dei rischi** che corre e, pertanto, valuta questo argomento a sensazione, piuttosto che con fatti concreti. Quali sono infatti i rischi reali?

In una logica di *Risk Assessment*, naturalmente, ogni impresa fa storia a se; bisogna conoscere quali dati vorrebbe mettere sul cloud, qual è il livello di riservatezz**a** che tali dati devono avere, se si tratta di dati sensibili, quali **procedure di backup** sono implementate, di che tipo di **connessione internet** si dispone e così via.

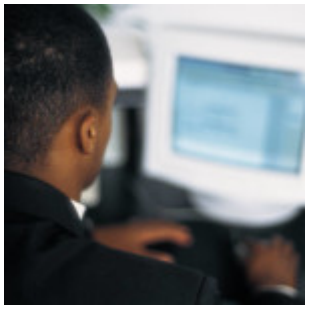
In linea generale parlare di dati poco sicuri nel *cloud* perché si teme che qualcuno possa "guardarci dentro" non ha molto senso: a parte che bisognerebbe valutare quale livello di sicurezza ci si aspetta per ogni tipo di dato (si veda il precedente articolo sulla valutazione dei rischi per la sicurezza delle informazioni), oggi molti *repository* di dati nel *cloud* forniscono ampie garanzie di sicurezza, soprattutto se sono gestiti da importanti player del settore, quali Microsoft, Google, Amazon, ecc.

Se, come al solito, decliniamo il termine **Sicurezza** in **Riservatezza**, **Integrità** e **Disponibilità** (ISO 27000 *docet*) e valutiamo nel complesso **il livello di rischio che incombe sui dati nel cloud**, vediamo che, a fronte di un **livello di riservatezza più che adeguato** (i dati di una PMI nel cloud normalmente sono sufficientemente protetti da sguardi indiscreti, grazie alle misure di sicurezza informatica che i fornitori più seri offrono ormai per *default*), certamente superiore a quello che si può ottenere all'interno dell'azienda stessa (dove potrebbero esserci soggetti interessati a curiosare dove non dovrebbero) la garanzia di **integrità dei dati** è più

che buona, ma sulla **disponibilità** degli stessi occorre fare qualche riflessione.

Su quest'ultimo aspetto incide non solo l'affidabilità del fornitore di servizi *cloud* e dell'infrastruttura di cui dispone, ma anche la **connessione internet** che, ancora ogg,i non è sicuramente adeguata in molte imprese italiane, sia per **velocità**, sia per **continuità del servizio**. È proprio questo l'anello di congiunzione con la **continuità operativa**, più elegantemente detta ***business continuity***.

Infine la **privacy**, ovvero la **protezione dei dati personali** con la relativa legge italiana (D.Lgs 196/2003) ed il **nuovo Regolamento Europeo** che sarà emanato probabilmente il prossimo anno. In questo ambito un Parere della Commissione Europea del 2012 ha per il momento fugato molti dubbi sulle garanzie legali che un'impresa dovrebbe richiedere al proprio fornitore di servizi cloud per essere tranquilla di non incorrere in pesanti problemi legali.



Probabilmente molti **contratti** che regolamentano la fornitura di servizi *cloud* (spesso mascherati sotto la fornitura di *software as a service*) non cautelano adeguatamente l'organizzazione che, non dimentichiamolo, è **titolare del trattamento dei dati** memorizzati in un server chissà dove. È prassi consolidata, infatti, di numerosi fornitori di SaaS di spostare i database dei propri clienti nello spazio web più conveniente per rapporto qualità/prezzo, non importa se in Canada o in Australia In tali situazioni le aziende non dovrebbero dimenticare che come titolari del trattamento sono i **responsabili di fronte alla legge su eventuali inosservanze del Codice della Privacy** e che "esportare" i dati personali fuori dalla Comunità Europea non è sempre possibile, come minimo occorre richiedere il consenso dell'interessato.

Dunque quali interrogativi deve porsi un'azienda coscienziosa prima di affidare i propri dati al *cloud*?

Vediamo i principali, fermo restando che solo dopo una precisa valutazione dei rischi si può determinare quali aspetti sono più critici in ogni singola realtà.

1. Il contratto con il fornitore mi garantisce adeguatamente rispetto alla normativa sulla privacy?
2. Il livello di riservatezza necessario sui dati è adeguatamente garantito da misure di sicurezza dichiarate contrattualmente dal fornitore?
3. La disponibilità dei dati garantita contrattualmente (SLA) è adeguata alle mie esigenze?
4. Posso rientrare in possesso dei miei dati quando voglio e senza costi eccessivi?
5. Il fornitore è sufficientemente affidabile? Si serve di subfornitori egualmente affidabili e resi noti contrattualmente?
6. In caso di perdita dei dati quali sistemi di *disaster recovery* mi garantiscono di rientrare operativo nel più breve tempo possibile? Tale tempo è coerente con

le mie esigenze operative?
7. So esattamente in quale stato o area geografica sono memorizzati i miei dati?
8. Ho considerato tutti i possibili fattori di rischio che possono incombere sulla mia continuità operativa?
9. Ho definito gli obiettivi di disponibilità del servizio e di *business continuity* in caso di situazione di crisi?
10. Sono in grado di monitorare il comportamento del fornitore ed eventualmente sottoporlo ad audit sul rispetto dei vincoli contrattuali?

Oggi esistono molti sistemi per garantirsi un futuro tranquillo con i dati nel *cloud*, ad esempio seguendo i principi ed i metodi indicati dalle **norme della famiglia ISO 27000** (ISO 27001 che riporta i requisiti di un **sistema di gestione della sicurezza delle informazioni** certificabile, ISO 27002 che riporta le *best practices*, ovvero i controlli che possono essere messi in atto, ISO 27005 che è la linea guida per il *risk assessment*, …) includendovi i requisiti cogenti per la privacy in vigore in Italia ed in Europa. Se il problema di mantenere una certa continuità operativa costituisce un fattore critico si può adottare la metodologia esposta nella ISO 22301 ed in altri standard e linee guida sull'argomento.

Mediante gli stessi sistemi ci si può garantire in modo adeguato nei confronti del fornitore, ad esempio esaminando il contratto con un supporto legale competente, verificare se il fornitore dispone di certificazioni ISO 9001, ISO 27001, ISO 22301 oppure dispone di un Report SSAE 16 ("*Statement on Standards for Attestation Engagements*" n. 16 , standard AICPA per il reporting sui controlli alle organizzazioni che forniscono servizi in outsourcing, richiesto dalle aziende soggette al *Sarbanes-Oxley Act* o SOX, Sezione 404).

Se ascoltiamo quello che ci raccontano gli esperti di sicurezza informatica che relazionano nei frequenti seminari o convegni sull'argomento non c'è certo da stare tranquilli nemmeno all'interno della propria azienda (tra *ransomware* e *data leakage* ogni tanto nascono minacce sempre più terrificanti per il futuro delle nostre imprese, senza dimenticare il comportamento dei collaboratori disonesti) e, quindi, un cloud consapevole può veramente essere una buona cosa.

Dall'altra parte la *software house* che fornisce applicazioni *web-based* con l'opzione di memorizzare i dati, anziché su un server interno all'azienda, su un server remoto (ovvero nel *cloud*) dovrebbe prendere in considerazione tutti gli aspetti sopra esposti, sia al fine di fornire un servizio pienamente conforme alle normative applicabili e di piena soddisfazione di tutte le esigenze del cliente, sia al fine di non incorrere in problemi legali nel caso in cui qualcosa andasse storto, anche solo a causa del proprio fornitore di servizi cloud. Dunque valutare quali tipi di dati verranno archiviati nel cloud dai propri clienti e quali garanzie forniscono i fornitori di spazio di archiviazione a cui ci si rivolge (le **caratteristiche di un data center sicuro** sono state esposte in un articolo apparso lo scorso anno sulla rivista INARCOS).

In conclusione, come per qualsiasi decisone o progetto strategico, le aziende (clienti e fornitori) dovrebbero valutare con adeguate competenze la situazione nel suo complesso ed i rischi che si potrebbe correre. Purtroppo tali competenze, informatiche, legali e gestionali spesso non sono presenti in piccole realtà poco strutturate che, quindi, rischiano di incorrere in problemi significativi e se poi trattano dati sensibili, in particolare dati sanitari, potrebbero veramente incorrere in perdite economiche e di immagine molto importanti.

Quando serve la perizia informatica contro i dipendenti disonesti?

Oggigiorno, con lo sviluppo delle tecnologie informatiche, le organizzazioni di ogni settore mantengono sempre più il loro know-how sui sistemi informatici, talvolta solo su di essi! Pensiamo a progetti di impianti e macchinari, programmi software, dati di clienti e fornitori, ecc..
Questo costituisce un rischio che spesso non viene valutato a dovere, infatti la perdita di tali dati o, peggio, la sottrazione di essi da parte di malintenzionati è sempre più frequente. Ma se il rischio di perdita dei dati dovuto ad incidenti informatici (danneggiamento dei supporti e dei sistemi) e non (incendi, allagamenti, terremoti, ecc.) spesso viene analizzato e più o meno adeguatamente gestito – almeno nelle organizzazioni più strutturate – il rischio di sottrazione di dati da parte di soggetti che operano dall'interno dell'azienda o dello studio professionale sovente non è analizzato in modo idoneo e, quindi, la perizia non serve se non è stata preceduta da adeguate misure preventive.

Le ricerche condotte da autorevoli organizzazioni operanti nel settore della sicurezza delle informazioni e le analisi delle autorità preposte alla difesa contro la criminalità informatica testimoniano che sempre più crimini informatici vengono commessi dall'interno dell'azienda.
Volendo sorvolare sulle possibili attività non lecite svolte dal dipendente dell'azienda quando è collegato ad internet (consultazione e scaricamento di materiale da siti pedofili, scaricamento di materiale coperto da diritti d'autore, ecc.), soffermiamoci sulla sottrazione con eventuale cancellazione di dati del dipendente o collaboratore che poi utilizza gli stessi dati per sviluppare un'attività concorrenziale oppure per rivenderli alla concorrenza.
Mentre da un lato tali azioni – svolte sempre più da gruppi organizzati piuttosto che da singoli – possono portare alla sottrazione e distruzione di dati su supporto

cartaceo con qualche difficoltà, l'asportazione e cancellazione di dati in formato elettronico è alquanto più agevole, anche grazie ai nuovi supporti di memorizzazione molto più capienti che in passato e facili da nascondere, per non parlare delle possibilità offerte dal *cloud* di trasferire in poco tempo alcuni gigabyte di dati tramite account personali gratuiti.
Il recupero di eventuali dati cancellati proditoriamente dal collaboratore disonesto potrebbe dare esiti incerti, infatti i risultati dipendono dalla scaltrezza di chi commette il reato, che potrebbe aver gettato documenti cartacei nel "distruggi documenti" oppure cancellato i dati informatici in modo irreversibile attraverso appositi programmi. Conoscendo le tecniche di backup dell'organizzazione anche i salvataggi potrebbero essere inutilizzabili in caso di impiego di metodi che non conservano le copie di documenti cancellati o sostituiti oppure se le copie di sicurezza sono accessibili al malintenzionato.
A questo punto l'organizzazione danneggiata potrebbe rivolgersi all'avvocato per far valere i propri diritti, ma questi dovrà sicuramente interpellare un esperto informatico per raccogliere le prove del reato e cercare di recuperare i dati cancellati.
Mentre per quest'ultima azione è fondamentale l'esistenza di un backup recente dei dati (sempre che tra i fuoriusciti non ci sia qualcuno del reparto EDP!), raccogliere prove da poter far valere in Tribunale non è facile. Spesso infatti il solo trascorrere del tempo fra il momento del presunto reato e l'intervento del perito informatico di parte o di quello nominato dall'Autorità Giudiziaria (detto anche CTU) comporta un deterioramento di eventuali prove. Infatti un PC o un Server non è esattamente nelle stesse condizioni nelle quali è stato perpetrato il reato già pochi minuti dopo, in quanto alcune operazioni di routine vengono attivate periodicamente dal sistema operativo e dai programmi e tali attività potrebbero inficiare le possibilità di recuperare dati cancellati o comunque di ricostruire lo "stato di fatto" del sistema informatico al momento in cui si sospetta sia avvenuta la sottrazione e cancellazione di dati.
Attualmente numerosi programmi sono in grado di recuperare file cancellati o perlomeno parte di essi, ma le continue riscritture del disco rigido possono vanificare l'attività di recupero. Dunque il consiglio è quello di "congelare" il disco sul quale erano contenuti i dati sottratti e cancellati. Non correte a vedere se c'è spazio nel vostro congelatore, intendo dire che bisogna estrarre l'hard-disk dal PC e riporlo in una custodia adeguata fino all'arrivo del perito informatico. Se il reato commesso è tale da valer la pena di intentare una causa per danni l'inutilizzo di qualche disco per un certo tempo sarà sicuramente un'operazione vantaggiosa. Tra l'altro le recenti modifiche al Codice Penale hanno introdotto alcuni reati informatici che solo una decina di anni fa non erano previsti, tra cui l'accesso abusivo ad un sistema informatico.
Naturalmente anche i supporti di backup che potrebbero dimostrare la presenza di file poi sottratti e cancellati andrebbero conservati senza riutilizzarli per successivi salvataggi.
Tutti i file di log dei sistemi informatici potrebbero poi essere utili per tracciare attività fraudolente, ma per dimostrare che una certa operazione (cancellazione, copia) è stata commessa da una certa persona è necessario provare

che l’operazione è stata effettuatada un determinato utente che si è autenticato nel sistema informatico attraverso una password segreta.
A questo proposito l’applicazione di tutte le prescrizioni previste dal codice della privacy (D.Lgs 196/2003) consente al titolare del trattamento di dimostrare di aver fatto di tutto per prevenire il danno e ciò è necessario anche per tutelarsi nei confronti di eventuali terzi danneggiati. Supponiamo infatti che il dipendente malintenzionato abbia sottratto progetti importanti svolti dall’azienda per un cliente che, a questo punto, vedrebbe informazioni riservate divenire di dominio di persone non autorizzate e che magari potrebbero essere vendute alla concorrenza! Tale cliente potrebbe rivalersi sull’azienda che ha subito la sottrazione di dati, ovvero oltre al danno anche le beffe!
Purtroppo nella maggior parte dei casi il perito, che deve operare in modo da alterare il meno possibile il corpo del reato, si trova a che fare con situazioni nelle quali è difficile dimostrare con ragionevole certezza un comportamento fraudolento. Questo spesso avviene a causa della stessa organizzazione che ha subito il danno, la quale non solo non ha intrapreso idonee misure preventive per proteggere i propri dati, ma ha anche agito in modo non corretto per salvaguardare le prove dopo che il fatto è stato commesso. Infatti, la mancata osservanza di alcune prescrizioni del Codice della Privacy – in particolare del disciplinare tecnico delle misure minime di sicurezza (allegato B del Codice) – oppure della disposizione relativa agli Amministratori di SIstema potrebbe creare all’organizzazione danneggiata più danni che benefici in Tribunale. Anche l’impiego non corretto di misure di sorveglianza quali videosorveglianza non autorizzata, sistemi di rilevamento presenze con sistemi biometrici o software di monitoraggio del comportamento degli utenti nei sistemi informatici potrebbero risultare vani di fronte ad una buona difesa del colpevole che potrebbe a sua volta contrattaccare conoscendo le vulnerabilità legali della sua (ex)azienda. In questi casi è opportuno chiedersi “a quanto” serve la perizia informatica, se vogliamo parafrasare il titolo di questo articolo.

In generale, dunque, l’organizzazione deve aver ben chiaro cosa proteggere, quali sono le informazioni più importanti ed in base ad una attenta analisi dei rischi ed una valutazione del costi di prevenzione, decidere come proteggersi.

In un convegno sulla sicurezza informatica di qualche tempo fa, ad esempio, è stato esposto che le suddette valutazioni hanno portato una importante azienda meccanica del bolognese a concludere che il rischio maggiore non è costituito dal fatto che un potenziale concorrente potesse sottrarre i progetti delle proprie macchine per crearne di proprie (i tempi ed i costi per mettere in piedi un’organizzazione con know-how adeguato sarebbero stati eccessivi), ma piuttosto poteva costituire un pericolo più consistente la sottrazione di informazioni finalizzate alla realizzazione di parti di ricambio, compresi i dati dei clienti.

Il problema del cosiddetto “*data leakage*“, considerato anche nella noma ISO 27002 “*Information technology security tecniques – Code of practice for information security management*“, ha portato alcune aziende ad ideare dei sistemi di protezione

della conoscenza che potrebbero prevenire furti di informazioni oppure renderli inoffensivi.

Ad esempio gli ormai noti sistemi di DRM (*Digital right Management*) che impediscono di ascoltare brani musicali, oppure di leggere ebook, acquistati via internet su un numero illimitato di dispositivi potrebbero essere applicati a codice sorgente di applicativi software o a progetti di impianti o macchinari.

In conclusione i passi per definire ed attuare un'adeguata strategia di protezione del know-how aziendale può essere riepilogata nei seguenti punti:

1. Determinare le informazioni da proteggere ed assegnarne dei livelli di priorità.
2. Effettuare una valutazione di rischi che si corrono
3. Stabilire ed attuare delle contromisure preventive per eliminare o ridurre i rischi più significativi.
4. Definire delle azioni di contenimento da attuare in caso di furto di informazioni con eventuale perdita delle stesse.

Seguendo queste regole l'intervento del consulente informatico – e la relativa perizia informatica – può risultare efficace e talvolta essere evitato.

Firma digitale: finalmente al via una nuova e più sicura versione

Le nuove regole sulla firma digitale sono entrate in vigore questa settimana. Le novità di legge obbligheranno gli utenti ad aggiornare il software del proprio sistema di firma per garantire un più elevato grado di affidabilità e sicurezza. La deliberazione n.45/2009 del CNIPA e le successive modifiche della determinazione commissariale n.69/2010 hanno infatti definito i nuovi standards tecnici di sicurezza per la firma digitale. Nella maggior parte dei casi, l'aggiornamento software si traduce semplicemente in una operazione eseguibile direttamente online, che consentirà di adeguare la propria smart card alle nuove funzioni di sicurezza definite nelle regole tecniche. In altri casi, ovvero per tutte quelle smart card il cui numero di serie inizia con la sequenza 1202, sarà invece necessario procedere ad una vera e propria sostituzione fisica della scheda. Purtroppo, tali schede non sono in grado di accogliere i formati e gli algoritmi previsti per le nuove specifiche di sicurezza e pertanto devono essere sostituite. In realtà, queste smart card sono quelle di prima emissione, che avrebbero raggiunto presto il limite di validità della carta. In virtù delle scadenze definite dalla normativa i certificatori accreditati dovranno rendere disponibili gli aggiornamenti dei dispositivi entro

prossimo 31 dicembre 2010, mentre gli utenti avranno modo di adeguare la propria firma entro il 30 giugno 2011. (Fonte CertineWs)

viaFirma digitale: finalmente al via una nuova e più sicura versione | Information Security.