4 Mercati e tendenze

4.3 Le regole da seguire per la sicurezza dei dati

di *Daniele Ferraioli**

ESTRATTO. *Abbiamo tecnologie avanzate, in grado di monitorare ogni comportamento lecito e illecito di raccolta ed elaborazione di informazioni; non solo abbiamo una legge che disciplina il trattamento delle informazioni, tutelando la libertà di espressione, ma anche il diritto alla propria privacy. Ma noi, nel nostro piccolo, che cosa possiamo fare per rendere i nostri dati più sicuri?*

Dopo aver trattato, nel numero precedente della rivista, dei legami e talvolta delle contraddizioni tra privacy e nuove tecnologie, forniremo ora alcune indicazioni sui comportamenti da adottare nel trattamento dei dati, sia con strumenti tradizionali sia con strumenti elettronici. Tali indicazioni rientrano in buona parte tra le misure minime previste dall'Allegato tecnico al D.Lgs. 196/2003 per tutti coloro che trattano nell'ambito professionale dati personali, sensibili o giudiziari. Questo articolo, pur senza avere la pretesa di assolvere quanto prescritto dal Codice della privacy, intende fornire ai lettori una sorta di "tavola delle leggi" legata alla sicurezza, informatica e non.

La sicurezza delle informazioni

Che cosa intendiamo per sicurezza delle informazioni? Abbiamo almeno tre requisiti necessari per dichiarare sicuri i dati che trattiamo:

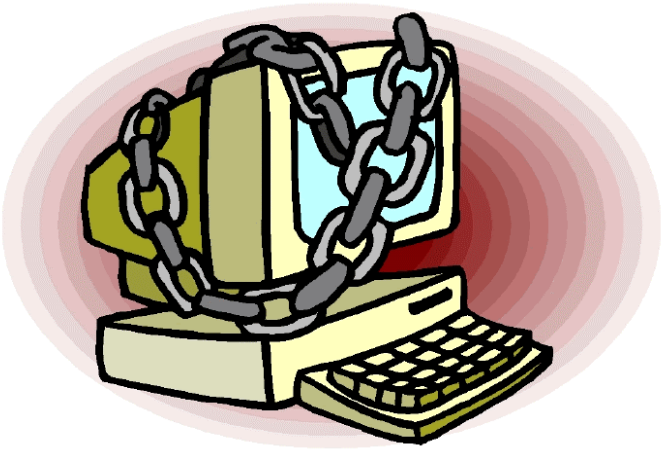
- dal punto di vista della **riservatezza**, le informazioni trattate devono essere protette da occhi indiscreti;
- da quello dell'**integrità**, le informazioni non devono poter essere accidentalmente o intenzionalmente alterate;
- infine, dal punto di vista dell'**immunità ai disastri** (*disaster recovery*), i sistemi tecnologici e logistici che ospitano i dati devono essere protetti da incidenti e guasti imprevisti.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche opportuni meccanismi organizzativi. Non è sufficiente aver adottato misure tecniche, per quanto sofisticate, se tali misure vengono poi usate impropriamente.

Facciamo due esempi pratici: un archivio cartaceo in un'azienda tradizionale e un *data base* su un server di una rete informatica aziendale. Supponiamo che l'archivio sia stato dotato di un sistema di accesso mediante tesserino magnetico individuale di riconoscimento. Il personale che chieda e ottenga per comodità di poter utilizzare una tessera *passepartout* collocata nelle vicinanze, vanifica gli sforzi per impedire l'accesso a un estraneo non autorizzato; inoltre gli accessi degli stessi addetti ai documenti in archivio non possono essere monitorati in alcun modo. In un sistema informativo aziendale si suppone che l'accesso alla base di dati avvenga tramite riconoscimento dell'utente che deve digitare il suo identificativo e la password: gli utenti, per comodità, hanno segnato la password su un *post it* attaccato al monitor, così da permettere l'accesso ai colleghi anche in caso di loro assenza.

Se ci prendiamo la briga, illegittima, di curiosare un po' in molte amministrazioni pubbliche, vedremo che questa seconda supposizione non è molto lontana dalla realtà! Cerchiamo allora di individuare una serie di comportamenti utili al fine di rendere la vita difficile, se non impossibile, alle persone un po' troppo curiose.

Le regole da seguire



Per prima cosa, chiudete le porte!

Il primo livello di protezione di qualunque sistema è quello fisico: una porta chiusa può non bastare, ma pone un primo ostacolo e richiede comunque uno sforzo per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti sulla scrivania. Quindi chiudete a chiave il vostro ufficio alla fine della giornata e riponete i documenti a chiave nei cassetti ogni volta che potete, in particolare se contengono dati sensibili e/o giudiziari.

Quando vi spostate dalla postazione di lavoro bloccate il computer. Se è vero che lasciare un computer acceso non crea problemi al suo funzionamento, anzi, velocizza il successivo accesso, occorre però ricordarsi di bloccarne l'uso (nei sistemi

operativi Microsoft Windows mediante la combinazione di tasti CTRL + ALT + TAB e scegliendo poi Blocca computer).

Evitate di lasciate lavori incompiuti sullo schermo. Chiudete sempre il programma che state utilizzando quando vi allontanate dal posto di lavoro, anche perché alcuni programmi non consentono l'attivazione automatica del blocco del computer. Potreste rimanere lontani più del previsto e un documento presente sullo schermo è ovviamente vulnerabile.

Conservate i vostri dati in un luogo sicuro. I documenti contenenti dati personali e ancor più sensibili e giudiziari non possono rimanere sulla scrivania dell'utente, ma devono essere riposti in cassetti, schedari o armadi solidi e chiusi a chiave. Le chiavi non dovrebbero rimanere appese, ma dovrebbero essere conservate personalmente dagli utenti incaricati dei trattamenti. Per i dischetti si applicano gli stessi criteri validi per i documenti cartacei, con l'aggravante che il loro smarrimento o furto potrebbe passare più facilmente inosservato. Soprattutto se contengono informazioni sensibili, riponeteli in luoghi sicuri non appena avete finito di usarli.

Una regola importante, specie per chi condivide stampanti o utilizza stampanti di rete, è di **maneggiare con cura le stampe di documenti riservati**. Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania, recatevi quanto prima a ritirare le stampe. I dispositivi distruggi documenti sono ormai diffusi e a buon mercato; distruggete personalmente le stampe quando non servono più.

Quando cancelliamo un file da un *floppy disk*, i dati cancellati non vengono effettivamente rimossi dal supporto, ma soltanto marcati come non utilizzati e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei vostri dati; solo l'utilizzo di un programma apposito garantisce che sul dischetto non resti traccia dei dati precedenti. Quindi **non riutilizzate i dischetti per affidare a terzi i vostri dati**; è meglio usare un dischetto nuovo.

Non fate usare il vostro computer a estranei, a meno di non essere sicuri della loro identità. In ogni caso, non fornitegli password.

Spesso capita di trovare programmi in versione non ufficiale o non originali; **di sicuro, se la loro provenienza è incerta, non sono autorizzati, quindi non installateli!** Oltre alla possibilità di trasferire involontariamente un virus, va ricordato che la maggior

parte dei programmi è protetta da *copyright*; la loro installazione può essere illegale.

Vi è mai capitato di perdere un file importante al quale avevate dedicato tanto lavoro? Se si, avrete già adottato **il sistematico salvataggio dei dati e il loro periodico *back up***. Molti programmi applicativi, per esempio quelli di videoscrittura, salvano automaticamente il lavoro a intervalli fissi, in modo da minimizzare il rischio di perdita accidentale dei dati. Imparate comunque a salvare manualmente il vostro lavoro con una certa frequenza, in modo da prendere l'abitudine di gestire voi stessi i dati e non fare esclusivo affidamento sul sistema. Quanto al *back up* su CD o DVD, oppure su un secondo *hard disk* o su una memoria *flash*, si tratta di un'eccezionale misura di sicurezza anche nel caso di rotture accidentali del disco principale. L'importante è eseguire il *back up* con frequenza.

Volete mettere un "lucchetto elettronico" al vostro personal computer? Allora **proteggete il vostro pc con una password.** La maggior parte dei computer offre la possibilità di impostare una password all'accensione, oltre che quella di riconoscimento da parte del sistema operativo o della rete. Questa caratteristica offre un buon livello di riservatezza.

Inoltre **non fatevi spiare quando state digitando la vostra password o altri codici di accesso.** Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state digitando anche se avete buone capacità di dattiloscrittura.

Altro stratagemma che andrebbe accuratamente evitato è l'uso di promemoria per le password, quali post-it, foglietti o altro. **Custodite la vostra password in un luogo sicuro, la memoria!**

Ecco alcuni semplici accorgimenti:

- non scrivete la vostra password, meno che mai vicino alla vostra postazione di lavoro;
- non dite a nessuno la vostra password;
- non scegliete password che si possano trovare in un dizionario. Esistono programmi che "provano" automaticamente come password tutte le parole contenute in un dizionario, anche in lingue straniere;
- non usate il vostro nome utente, né parole che possano in qualche modo essere legate a voi come, per esempio, quello dei vostri cari, degli animali domestici, date di nascita, numeri di telefono o altri dati comuni, perché sono le password più facili da indovinare;

- usate password abbastanza lunghe (alcuni sistemi richiedono almeno otto caratteri) con un misto di lettere, numeri e punteggiatura, se consentita;
- non utilizzate la stessa password per l'accesso alle varie procedure;
- cambiate la password a intervalli regolari.

Le regole da seguire per evitare i virus informatici

I virus sono particolari programmi con intenti distruttivi o comunque dannosi per i nostri dati e per i pc che li ospitano. Come per le reali infezioni si propagano per contagio, un elemento "intruso", normalmente un file infetto, viene a contatto con il nostro pc e, più o meno lentamente, inizia a contagiare i nostri file.

Vediamo come combattere il fenomeno virus, tenendo presente che i virus hanno preso piede anche nella telefonia mobile, grazie agli invii di file a contenuto multimediale tipici dei telefonini dell'ultima generazione.

- Per prima cosa dovete avere un buon *software* antivirus installato sul pc;
- dovete provvedere al costante aggiornamento delle impronte virali; in pratica, quasi ogni giorno. I produttori di antivirus aggiornano i *data base* dei virus informatici, in modo che il vostro antivirus riconosca i file "infetti"; di norma tale aggiornamento avviene collegandosi al sito Web del produttore di antivirus;
- usate soltanto programmi provenienti da fonti fidate;
- ogni programma o file deve essere sottoposto alla scansione da parte del programma antivirus prima di essere installato;
- un veicolo di infezione, specie nel passato, era costituito dai giochi copiati o "sprotetti", cioè da quei giochi che alcuni pirati informatici erano riusciti a rendere giocabili anche senza licenza originale. Se siete giocatori accaniti, usate postazioni isolate che non contengano dati utili e che possano essere eventualmente infettate senza che questo comporti un danno;
- assicuratevi di controllare il dischetto o il CD Rom di avvio, se non sono originali, prima di avviare il vostro computer in questa modalità. Se il supporto fosse infetto, il virus potrebbe trasferirsi nella memoria RAM e diffondersi ad altri file;
- proteggete i vostri dischetti da scrittura quando possibile. È il più efficace mezzo di prevenzione. I virus non possono rimuovere la protezione meccanica;
- non diffondete messaggi di provenienza dubbia. Se ricevete messaggi che avvisano di un nuovo virus pericolosissimo, prendetelo con le dovute cautele. Molte *mail* di questo tipo non sono veritiere;
- non partecipate a "catene di S. Antonio" e simili; tutti i messaggi che vi invitano a diffondere la notizia "quanto più possibile" potrebbero avere scopi molto simili a quelli dei

virus, cioè utilizzare indebitamente le risorse del sistema informativo e, magari, mandarlo in crisi.

Conclusioni

Come avete visto, molte delle indicazioni sono applicabili a situazioni della vita di tutti i giorni. Affidereste la vostra auto al primo sconosciuto? Lascereste ritirare la vostra cartella clinica a una persona che conoscete poco? Siete soliti digitare il PIN del vostro bancomat davanti a occhi indiscreti e curiosi? Parlate di argomenti delicati che riguardano la vostra famiglia in presenza di estranei? Lo stesso vale per dati e informazioni che trattiamo per motivi professionali. Non si tratta di diventare paranoici e maniacali, ma solo di adottare alcune regole comportamentali che, dopo qualche tempo, diventeranno parte integrante del nostro vivere.

** Titolare dello Studio di Ingegneria Ferraioli – consulente ICT (Information & Communication Technology)*