Un progetto di

RegioneLombardia

unioncamerelombardia
camere di commercio lombarde

Realizzato da

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

WEB SISTEMA FIREWALL INFORMATICO RISCHI DOWNLOAD

LA SICUREZZA DELLE INFORMAZIONI

STRUMENTI E SOLUZIONI PER LE PMI

PRIVACY COMPUTER VIRUS PASSWORD TECNOLOGIA INFORMAZIONI

Camera di Commercio Como
Camera di Commercio Mantova
CAMERA DI COMMERCIO MILANO
CAMERA di COMMERCIO MONZA BRIANZA
Camera di Commercio Pavia
CAMERA DI COMMERCIO INDUSTRIA ARTIGIANATO AGRICOLTURA DI VARESE

LA SICUREZZA DELLE INFORMAZIONI
STRUMENTI E SOLUZIONI PER LE PMI

"Iniziativa realizzata nell'ambito dell'Accordo di Programma per la Competitività tra Regione Lombardia e Sistema Camerale lombardo"

PER CONTATTI:

REGIONE LOMBARDIA
DC Programmazione Integrata, Struttura Università e Ricerca - Piazza Città di Lombardia, 1 - 20124 Milano
Fax +39 02 67656882
e-mail: universita_ricerca@regione.lombardia.it

UNIONCAMERE LOMBARDIA
Via Ercole Oldofredi, 23 - 20124 Milano
Tel./Fax +39 02 6079601
e-mail: semplificazione@lom.camcom.it

ASSINTEL
Corso Venezia, 47 - 20121 Milano
Tel. +39 02 7750.231/235
e-mail: info@assintel.it

PREMESSA DI ALBERTO CAVALLI

Sottosegretario del Presidente all'Università e alla Ricerca di Regione Lombardia

Regione Lombardia ritiene la ricerca e l'innovazione fattori determinanti per lo sviluppo economico e sociale.

Soprattutto nella fase attuale: dalla crisi uscirà più velocemente chi saprà far crescere la competitività e l'attrattività investendo in innovazione. È l'innovazione, infatti, il vero motore della crescita e lo strumento decisivo di competitività fra i Paesi.

Creare un contesto in cui gli attori economico-sociali possano produrre innovazione con facilità, catturandone il valore, e creando crescita e benessere sono degli impegni che il Presidente Formigoni e Regione Lombardia hanno messo al centro delle politiche dei prossimi anni.

La chiave di volta per creare un ambiente attrattivo e competitivo è proprio la diffusione dell'ICT sull'intero territorio regionale, oggi incompleta.

A partire dalle iniziative infrastrutturali tra loro complementari di Regione Lombardia per estendere ai suoi cittadini un servizio di tipo ADSL con velocità minime garantite a partire da 2Mbit al secondo per utente fino a velocità di picco pari a 20Mbit al secondo, che coinvolge 140 comuni privi di infrastrutture telematiche adeguate.
In secondo luogo, il progetto Banda Ultra Larga (Bul), promosso dal Presidente Formigoni lo scorso maggio, può costituire un'eccellente occasione per fare della Lombardia uno dei territori più attrattivi e avanzati d'Europa: le dimensioni di questo progetto sono infatti superiori a qualsiasi altra iniziativa simile in Europa. La banda ultra larga garantisce infatti una connettività ad Internet a velocità superiori a 20Mbit per secondo ad utente ed entrerà nelle case di 4,2 milioni di cittadini lombardi, circa la metà della popolazione presente sul territorio, coinvolgendo 167 comuni.

Il valore complessivo dell'investimento è pari a 1 miliardo e 200 milioni di euro e la sua realizzazione è prevista in un arco temporale di 6 anni. Un progetto ambizioso che sarà in grado di cambiare le sorti di servizi che incidono sulla qualità della vita dei cittadini, sulla produttività, l'efficienza e la competitività agevolando al tempo stesso lo sviluppo culturale del Paese.

Oltre all'ICT, Regione Lombardia considera altresì strategiche e su cui investire fortemente per dare un forte impulso al proprio sistema economico e scientifico, aree tematiche quali Biotecnologie, Nuovi materiali o materiali avanzati, Agroalimentare, Aerospazio, Edilizia Sostenibile, Automotive, Energia, fonti rinnovabili e assimilate e i distretti di storica tradizione: Moda e design, Meccanica di precisione e metallurgia. Tali settori sono stati riconosciuti dal Ministero dell'Istruzione, dell'Università e della Ricerca quali distretti tecnologici: per sostenerli a presto sarà lanciato un bando congiunto di Ministero e Regione per il finanziamento di progetti di ricerca.

Naturalmente rafforzare l'ICT significa più contatti, più relazioni e più opportunità di crescere, ma anche una più forte necessità di sicurezza. Sotto questo profilo dunque sottolineo la validità del progetto "E-security per le PMI".

Attraverso la realizzazione del progetto, cofinanziato da Regione Lombardia e Unioncamere nell'ambito dell'accordo camerale in modo paritetico per un totale complessivo pari a 232.000 €, si intendono dunque promuovere metodologie innovative e la diffusione di un uso più sicuro e più consapevole della cultura della sicurezza informatica (e-security).

L'e-security non come un problema ma come un'opportunità. Secondo questa logica, si intende focalizzare l'attenzione delle piccole e medie imprese non solo sulla gestione delle emergenze, quanto sull'utilità della prevenzione dei rischi; evidenziando quindi gli aspetti organizzativi, metodologici e tecnici che devono essere pianificati e implementati per proteggere e mantenere affidabile il sistema aziendale.

Di qui il supporto all'individuazione di soluzioni – seconda finalità del progetto – mediante la predisposizione di strumenti concettuali e operativi che assistano l'imprenditore nell'autovalutazione del livello di sicurezza esistente e nell'identificazione delle eventuali misure di potenziamento.
L'obiettivo finale è quindi di porre le PMI nelle condizioni di saper determinare autonomamente il tipo di investimento in e-security necessario al proprio business e Regione Lombardia riconosce proprio alle PMI una priorità assoluta per uno sviluppo duraturo e dinamico.

Alberto Cavalli

PRESENTAZIONE DI FRANCESCO BETTONI

Presidente di Unioncamere Lombardia

È con convinzione e piacere che le Camere di commercio lombarde, coordinate dall'Unione regionale, hanno accolto e finanziato il progetto "E-security per le PMI" all'interno dell'Accordo di Programma per la Competitività siglato con Regione Lombardia.

Si tratta infatti di un investimento finalizzato a produrre strumenti di concreto ed efficace supporto al sistema delle micro e piccole imprese in tema di sicurezza informatica. Un tema, questo, spesso sottovalutato dalle imprese o sul quale, per mancanza di adeguata informazione, si investono risorse "sproporzionate" alle proprie necessità.

L'informatica e la telematica entrano sempre più in ogni impresa, in ogni ufficio pubblico o privato, in ogni casa.
E la crescente infrastrutturazione della Lombardia in tema di Banda Larga e Ultra Larga non potrà che incrementare e velocizzare ulteriormente tale processo.
Grazie alla rete non si trasferiscono solo "informazioni", pur determinanti nello sviluppo economico e nella crescita della competitività internazionale, ma sempre più anche "servizi" e possibilità di operazioni "on line" anche complesse e di forte rilevanza giuridica (le imprese stesse "nascono" telematicamente) od economica (operazioni bancarie, acquisti e vendite,...).

Da qui l'assoluta necessità di "sicurezza" in tutte le sue componenti: dalla garanzia di rispetto delle norme in materia, alla protezione dei dati sensibili propri e di terzi, fino alla garanzia di non essere esposti a ingerenze esterne.
Molto è da fare anche in materia di rischi "fisici" degli strumenti informatici: troppe micro e PMI non hanno adeguati sistemi di salvataggio del proprio patrimonio informativo.

Il pregevole ed analitico lavoro curato da Assintel per supportare le PMI sulla tematica della "e-security" è anche una conferma di come le Camere di commercio lombarde si muovono in materia di servizi alle imprese: stimolare e favorire nuovi servizi generati dal mercato e dal mondo associativo, anziché caricarsi dell'erogazione diretta di tali servizi.

Una concreta pratica di sussidiarietà, che lascia al "mercato" e ai soggetti che vi operano ciò che il mercato sa fare, limitandosi a intervenire – in funzione stimolatrice – dove invece ancora mancano servizi e attività.

E ciò che è stato particolarmente apprezzato nel progetto "E-security per le PMI" è la sua fase finale. Quella che si svilupperà concretamente "dentro" le piccole e medie imprese, accompagnandole nel percorso e verificando con loro stesse l'effettiva adeguatezza delle metodologie e degli strumenti proposti.
Da questa esperienza sul campo nasceranno ulteriori stimoli ed integrazioni per perfezionare la metodologia da proporre all'universo delle micro e piccole imprese.

Francesco Bettoni

INDICE

1

LA SICUREZZA DEI SISTEMI INFORMATIVI

In questo primo capitolo saranno fornite le nozioni utili per la comprensione dell'intero fascicolo, definendo cos'è un sistema informativo, cosa s'intende per sicurezza delle informazioni e perché le informazioni sono un bene primario per le aziende.

1.1 COSA S'INTENDE PER SISTEMI INFORMATIVI

Un sistema informativo comprende tutte le informazioni utilizzate dall'azienda, inclusi i supporti che le contengono, gli strumenti che permettono di crearle, modificarle, cancellarle o trasmetterle, e le persone, che sono sempre "fonti di informazioni" e contemporaneamente i gestori del sistema stesso.

Una buona parte del sistema informativo è composta dal sistema informatico, ossia quella parte del sistema informativo che fa uso di tecnologie informatiche come i computer, i programmi, Internet, ecc.

Un sistema informativo comprende però, anche tutte le informazioni che risiedono su altri supporti, come ad esempio gli archivi cartacei, i fax, le fotocopie, le stampe, ecc.

Quando si parla di sistema informativo, quindi, deve intendersi un sistema per la gestione delle informazioni in senso molto ampio, che comprenda tutte le informazioni a prescindere dagli strumenti, tecnologici e non, con cui gestirle.

Quando pensate alla sicurezza delle informazioni prendete in considerazione quelle contenute su supporti cartacei come le stampe, i fax o le fotocopie? ?

Un sistema informatico è solo una parte di un sistema informativo. !

1.2 COSA S'INTENDE PER SICUREZZA DELLE INFORMAZIONI

Porre in sicurezza delle informazioni significa tutelarne la riservatezza, l'integrità e la disponibilità.

Garantire la **riservatezza** (R) significa evitare che persone, volontariamente o involontariamente, possano accedere a una o più informazioni senza che ne abbiano l'autorizzazione. È il caso ad esempio del dipendente che, non avendo l'autorizzazione, accede a informazioni aziendali molto riservate; o è il caso del fornitore/cliente che accedendo ai locali aziendali vede documenti riservati non custoditi o abbandonati sulle scrivanie.

Garantire l'**integrità** (I) delle informazioni vuol dire invece evitare che queste possano essere modificate, cancellate o spostate. In ogni caso, cioè, ove si possa verificare una perdita di consistenza rispetto alla versione "originale", che è quella di cui ci si fida. È il caso ad esempio della perdita d'informazioni dovuta a un virus, al deterioramento di un apparato tecnologico o all'errore di un dipendente, oppure è il caso della modifica "postuma" di una fattura o di una posta di bilancio fatta fraudolentemente.

Garantire la **disponibilità** (D) delle informazioni significa invece garantire che esse siano sempre disponibili quando c'è la necessità.
Un virus o un dipendente che cancellano le informazioni sono anche un problema di disponibilità, oltre che d'integrità, qualora queste informazioni siano necessarie per svolgere le attività.

Tabella 1

Esempi di problematiche legate ai tre parametri di sicurezza delle informazioni:	R	I	D
Un cliente che accede ai locali aziendali e vede un listino prezzi fatto per un altro cliente.	X		
Un dipendente operativo che accede a dati riservati della direzione.	X		
Un criminale informatico che entra nei computer aziendali,	X		
cancella o modifica alcune informazioni,		X	
rendendole non disponibili o non disponibili in forma esatta quando sono necessarie.			X
La memoria di un computer che si guasta irreparabilmente.		X	X
La fuoriuscita di informazioni riservate (es. dati di bilancio, strategie aziendali, progetti per prodotti o servizi innovativi).	X		
L'interruzione prolungata di corrente elettrica.			X
Un furto di un computer.	X	X	X

Quando penso al concetto di sicurezza delle informazioni in azienda, ho chiari i tre parametri di sicurezza: integrità, disponibilità e riservatezza?

?

Un problema di sicurezza delle informazioni può coinvolgere uno o più dei parametri appena descritti. È il caso ad esempio della cancellazione non voluta di un'informazione. Ci si trova di fronte, infatti, sia a un problema d'integrità sia di disponibilità. Qualora poi la perdita d'informazioni fosse dovuta a un accesso non autorizzato, sarebbe anche un problema di riservatezza.

!

1.3 IL VALORE DELLE INFORMAZIONI PER L'AZIENDA

Ogni azienda dipende e vive grazie alle informazioni a prescindere dalla dimensione e dal mercato in cui opera. Senza informazioni un'azienda non potrebbe vendere il proprio prodotto o erogare il proprio servizio, non potrebbe richiedere i pagamenti o pagare i propri dipendenti, non avrebbe un know-how, un sito aziendale con cui farsi conoscere, ecc.

Il primo passo da compiere per proteggere il proprio patrimonio informativo è di imparare a conoscere la propria realtà anche sotto questo aspetto, individuando le informazioni presenti in azienda e associandole alle attività per cui sono rilevanti.

Successivamente sarà utile suddividerle per grado d'importanza, per poi dare loro la giusta tutela. Non tutte le informazioni, infatti, sono importanti in egual misura e sebbene tutte debbano essere tutelate, il minor o maggiore grado di protezione deve dipendere da un'analisi attenta della loro criticità.

La prima cosa da fare per compiere una valutazione corretta è definire quindi il giusto grado di criticità delle informazioni, avendo sempre ben presente i tre parametri di sicurezza visti nel paragrafo precedente: riservatezza, integrità e disponibilità.

In base a quanto detto, le domande che mi devo porre per definire quanto un'informazione è critica per la mia azienda sono:

- Che cosa succederebbe se quella particolare informazione fosse accessibile a chi non è autorizzato? (riservatezza)
- Che cosa succederebbe se quell'informazione fosse modificata o cancellata? (integrità)
- Che cosa succederebbe se non fosse più disponibile? (disponibilità)

E sulla base delle risposte date, definire un valore di criticità per l'azienda, anche semplicemente su una scala di valori basso, medio alto. Ad esempio, così (*Tabella 2*):

Tabella 2

Identifico l'informazione	***Associo l'attività per cui tale informazione è rilevante***	***Identifico un valore di criticità***	
INFORMAZIONE TIPO	**ATTIVITÀ**	**VALORE CRITICITÀ**	**PERCHÉ ...**
Fatture dei fornitori	Amministrazione/ Contabilità	Bassa	Una fattura di un fornitore qualora fosse letta da una persona non autorizzata non creerebbe particolari problematiche nell'erogazione del servizio, o nella fornitura del prodotto. Inoltre, anche nel caso sia modificato l'importo, esistono naturali strumenti di controllo sui pagamenti affinché si riesca ad accorgersene per tempo. Qualora la perdessi, inoltre, e non fosse più disponibile, potrei sempre richiederla al fornitore una seconda volta senza sollevare gravi problematiche.
Buste Paga	Gestione Personale/ Amministrazione	Media	Una busta paga letta da altri potrebbe sollevare problemi nel rapporto con i dipendenti. Anche la mancata disponibilità delle stesse potrebbe non garantire i pagamenti nelle date prefissate creando malcontento e disagio, oltre che un danno all'immagine.
Nuovi disegni di un prodotto innovativo o informazioni riguardanti un servizio innovativo	Progettazione	Alta	La fuoriuscita di documentazione strategica potrebbe creare un grave danno per lo sviluppo dell'azienda e la sua competitività sul mercato. Inoltre una modifica non autorizzata a un progetto complesso, o la non disponibilità d'informazioni legate a esso, potrebbe creare ritardi nei tempi di sviluppo e/o consegna, con una ripercussione economica oltre che d'immagine.

Ho mai riflettuto sull'importanza delle informazioni nella mia azienda?
Ho mai classificato le informazioni in base alla loro criticità?

?

Uno degli errori più grandi che si possono commettere in azienda è di percepire il valore delle informazioni solo nel momento in cui non siano più disponibili.
Il furto di un portatile ne è un esempio. Non è il valore dell'oggetto ciò a cui bisogna pensare.
Sono i dati in esso contenuti che dovrebbero essere stati protetti in modo adeguato, sia per evitare di non averli più disponibili e quindi di non per poterci più lavorare, sia per evitare che possano essere visti, utilizzati, o addirittura venduti da chi ha rubato l'oggetto.

!

2

COME VALUTARE I RISCHI

Nel capitolo precedente abbiamo definito il concetto di sistema informativo e di sicurezza delle informazioni, inoltre abbiamo compreso l'importanza delle informazioni stesse e imparato a classificarle in base alla loro criticità.
In questo capitolo vedremo da cosa è necessario difendersi per tutelare il patrimonio informativo, parleremo dei punti deboli e dei possibili danni ai sistemi informativi.

2.1 QUALI SONO LE MINACCE E I PUNTI DEBOLI CHE POSSONO COLPIRE IL SISTEMA INFORMATIVO DELLA NOSTRA AZIENDA?

Le **minacce** sono entità (individui, eventi, ecc.) capaci di causare un danno.

Una minaccia da sola non può produrre alcun danno, per farlo deve sempre sfruttare una vulnerabilità, ossia un **punto debole del sistema**.

I punti deboli possono provenire da qualunque parte o essere il risultato di qualunque circostanza, ma nella maggior parte delle ipotesi riguardano o difetti nella progettazione di un programma (cosiddetti "bug") oppure il fattore umano.

Normalmente le minacce sono suddivise in minacce di tipo **informatico, fisico o organizzativo** e a queste tre categorie vengono associate via via delle vulnerabilità (punti deboli).

Minacce Informatiche

Tra le minacce informatiche sicuramente la più famosa è il virus, ormai termine sostituito più propriamente dalla parola "*malware*", in italiano "*codice maligno*", per comprendere tutte le possibili varianti ed evoluzioni di questa particolare minaccia diffusasi negli anni.

Ma i virus, o meglio i "*malware*", sono solo una parte delle minacce informatiche.

Una minaccia informatica può anche essere:

- un malfunzionamento o un guasto dei programmi o dei personal computer;
- un'interruzione delle linee di comunicazione;
- una trasmissione o una ricezione errata di dati;
- un accesso alla rete o al sistema da parte di persone non autorizzate;
- una mancanza di aggiornamento dei sistemi operativi;
- ecc.

Minacce Fisiche

Le minacce fisiche toccano le risorse fisiche dell'azienda e le informazioni contenute su tali supporti fisici.

Esempi di minacce fisiche sono:

- incendi;
- allagamenti;
- disastri naturali;
- furti di estranei o di personale interno;
- deterioramento dei supporti di memorizzazione;
- accesso non autorizzato alle informazioni contenute su supporti cartacei;
- accesso non autorizzato ai locali aziendali;
- ecc.

Minacce Organizzative

Riguardano principalmente eventi legati al non rispetto di buone prassi, tentativi criminosi di terzi o errori del personale. Esempi di minacce organizzative sono:

- una persona (interna o esterna all'azienda) che ha accessi a informazioni, servizi o programmi che non è in grado di gestire o che non dovrebbe gestire;
- errori nella manutenzione delle apparecchiature;
- errori dei dipendenti;
- utilizzo di programmi non autorizzati;
- frodi aziendali;
- ingegneria sociale, ossia la tecnica di carpire informazioni direttamente dagli individui mediante raggiri;
- divulgazione d'informazioni riservate volontaria o involontaria;
- mancato rispetto di procedure;
- ecc.

Tabella 3: Riassunto delle Minacce Informatiche, Fisiche e Organizzative

Minaccia ***Informatica***	***Punto debole*** ***(vulnerabilità)***	***Descrizione***
Virus Malware	Navigazione su siti web inappropriati o download di file pericolosi. Poca dimestichezza nell'uso degli strumenti informatici.	Un virus per diffondersi sfrutta o un difetto di progettazione di un software, oppure la scarsa conoscenza di aspetti di sicurezza informatica di una persona, forzandola, anche tramite raggiri, a ricevere tale "infezione". Il più grande canale di diffusione di tali minacce è sicuramente Internet, inclusa la posta elettronica. Ecco perché è importante prestare attenzione ai siti che si visitano e ai file che si scaricano.
Malfunzionamento dei programmi o dei personal computer	Mancato aggiornamento dei programmi o del personal computer.	Ogni programma o computer, come ogni strumento può essere soggetto a malfunzionamenti. Per tanto deve essere sottoposto a manutenzione ordinaria. Nel caso dei programmi basta aver cura di installare eventuali aggiornamenti quando richiesto. Per quanto riguarda la parte elettronica e meccanica del personal computer (hardware) è utile controllarla periodicamente o quantomeno alle prime avvisaglie di malfunzionamento.
Minaccia ***Fisica***	***Punto debole*** ***(vulnerabilità)***	***Descrizione***
Incendio	Locale senza dispositivi anti incendio.	Ogni locale, ivi compresi gli uffici, è fisiologicamente a rischio d'incendio.
Furto	Accessi non controllati ai locali aziendali.	Devo tenere presente che quando subisco un furto di un'apparecchiatura (es. personal computer) non perdo solo questa ma anche la riservatezza, l'integrità e la disponibilità delle informazioni in esso custodite.

Deterioramento dei supporti di memorizzazione	Vecchie attrezzature.	Tutto invecchia e nell'invecchiare necessariamente vengono a mancare prestazioni e affidabilità. Questo, nel caso di un supporto di memorizzazione, può comportare la perdita, non solo del supporto stesso, ma anche di tutte le informazioni in esso contenute.

Minaccia ***Organizzativa***	***Punto debole*** ***(vulnerabilità)***	***Descrizione***
Persona che accede a informazioni cui non dovrebbe avere accesso	Non vengono definite procedure per gli accessi alle informazioni.	È il caso ad esempio del dipendente operativo che accede a dati riservati dell'amministrazione, della direzione. Oppure è il caso dell'ex-dipendente che porta con sé codici e informazioni per accedere ai dati della sua ex-azienda.
Errori nella manutenzione delle apparecchiature	Rivolgersi a fornitori non qualificati o non competenti.	Gli strumenti di lavoro che contengono le informazioni indispensabili per erogare i servizi o per fornire prodotti sono importanti per l'azienda. Come tali non devono essere soggetti a manutenzioni improvvisate da persone che non hanno le giuste competenze.
Non rispetto delle buone prassi di sicurezza delle informazioni	Mancanza di controllo e sensibilizzazione sul rispetto delle regole o mancata formazione.	È il caso dell'azienda che definisce delle buone prassi per la gestione della sicurezza delle informazioni e poi o non vigila sul controllo delle stesse o non forma il personale.

Ho mai fatto un'analisi delle possibili minacce per la mia azienda?
Ho mai preso in considerazione altre minacce che non fossero virus informatici?
Ero a conoscenza di minacce di tipo organizzativo?
Ho mai fatto un'analisi dei possibili punti deboli della mia azienda?

?

Le minacce che attentano a un sistema informativo non sono solo i virus. Le categorie sono molto più ampie. Conoscere bene le minacce e i propri punti deboli è il **secondo** *passo per ottenere una giusta protezione.*
Il **primo**, *l'analisi delle criticità, lo abbiamo visto nel capitolo precedente.*

L'anello più debole della catena della sicurezza è da sempre il fattore umano. Una corretta sensibilizzazione sull'importanza delle informazioni, siano esse contenute su supporti elettronici, cartacei o trasmesse oralmente è un fattore indispensabile per garantire la sicurezza delle informazioni.

!

2.2 QUALI POTREBBERO ESSERE I DANNI PROVOCATI DAL PRODURSI DI QUESTE MINACCE?

Quando una minaccia ha sfruttato con successo un punto debole, si produce un danno. Prima di vedere degli esempi è opportuno identificare almeno due tipologie di danno. Brevemente:

danni diretti - è il danno dovuto all'azione diretta della minaccia. Nel caso ad esempio della rottura di un computer, è il danno materiale legato all'apparecchio più il danno immateriale legato alle informazioni che contiene.

danni indiretti - è il danno dovuto all'azione indiretta della minaccia, ad esempio: la perdita di profitto dovuta a inattività, la perdita di competitività, i danni derivanti da cause legali o dalla perdita d'immagine, ecc.

Devono essere sempre considerate entrambe le tipologie per identificare in modo completo il danno potenziale. Chiarito quest'aspetto, vediamo degli esempi (*Tabella 4*):

Minaccia		*Danno*
TIPO	**DESCRIZIONE**	
Tecnologica	**Virus/Malware**	Perdita delle informazioni contenute nel computer, danno dovuto al recupero di tali informazioni e alla ripresa della piena operatività, fuga di riservatezza di potenziali dati sensibili o informazioni riservate con ripercussioni sull'immagine aziendale e/o sulla competitività, mancanza delle disponibilità di tali informazioni, ecc.
Tecnologica	**Malfunzionamento dei programmi o dei personal computer**	Danni materiali agli apparati, danni legati alla perdita di: operatività, integrità e disponibilità delle informazioni, di profitto per mancata erogazione del servizio o del prodotto, soddisfazione da parte del cliente, competitività, ecc.
Fisica	**Furto (anche interno ad opera di un dipendente)**	Danno materiale legato alla perdita dell'apparato, danno legato alla perdita di: informazioni contenute nel computer, operatività, riservatezza con possibili ripercussioni sull'immagine e la competitività, ecc.
Fisica	**Incendio**	Perdita delle informazioni custodite nei locali aziendali, danni fisici alle persone, danni strutturali, danni materiali legati alla perdita di apparati e attrezzature, ecc.
Organizzativa	**Errori nella manutenzione delle apparecchiature**	Danni materiali agli apparati, danni legati alla perdita di: operatività, integrità e disponibilità delle informazioni, di profitto per mancata erogazione del servizio o del prodotto, soddisfazione da parte del cliente, competitività, ecc.
Organizzativa	**Non rispetto delle buone prassi di sicurezza delle informazioni**	Il mancato rispetto delle buone prassi può portare a una tipologia di danni molto ampia, di fatto assimilabile alla somma di tutti i danni visti in precedenza.

Ho preso in considerazione sia i danni diretti che i danni indiretti? Quando subisco un danno a un supporto contenente informazioni, tengo in considerazione anche le informazioni contenute su tale supporto? ?

La stima di un danno è un procedimento ampio che comprende sia i danni diretti sia i danni indiretti. !

3

COME GESTIRE I RISCHI

Nei paragrafi precedenti sono stati analizzati i rischi legati alla sicurezza delle informazioni, in questo capitolo si cercherà di fornire metodologie e consigli pratici per gestirli.

3.1 COME AFFRONTARE I RISCHI

Il rischio che una minaccia, sfruttando una vulnerabilità, possa procurare un danno può essere gestito in diversi modi, ossia tramite: prevenzione, contenimento del danno, cessione a terzi, e accettazione.

Prevenzione:
Prevenire, significa cercare di ridurre le probabilità che un determinato evento dannoso accada, o meglio, che una minaccia riesca a sfruttare un punto debole.

In base ad alcuni degli esempi precedenti (*Tabella 5*):

Tabella 5

Vulnerabilità	*Prevenzione*
VIRUS/MALWARE	
Navigazione su siti web inappropriati o download di file pericolosi.	Aggiornare periodicamente i programmi e le applicazioni per evitare che un virus possa sfruttare delle vulnerabilità dovute a difetti di programmazione.
Poca dimestichezza nell'uso degli strumenti informatici.	Formare adeguatamente il personale sulle buone prassi da seguire nella gestione dei propri computer, delle applicazioni, della posta elettronica, di Internet, ecc.
INCENDIO	
Locale senza dispositivi anti incendio.	Eliminare dai locali aziendali oggetti potenzialmente infiammabili.
ERRORI NELLA MANUTENZIONE DELLE APPARECCHIATURE	
Rivolgersi a fornitori non qualificati o non competenti.	Provvedere alla manutenzione periodica degli strumenti avvalendosi di una lista di fornitori qualificati in precedenza valutandone a monte competenze e affidabilità.

Contenimento del danno:
Significa minimizzare le conseguenze di un danno prodottosi dopo che una minaccia ha sfruttato con successo una vulnerabilità.

In base agli esempi precedenti:

Tabella 6

Vulnerabilità	*Contenimento*
VIRUS/MALWARE	
Navigazione su siti web inappropriati o download di file pericolosi.	Verificare che i computer della propria azienda abbiano installato un antivirus (e/o che periodicamente sia aggiornato).
Poca dimestichezza nell'uso degli strumenti informatici.	Prevedere sempre delle copie di sicurezza ("backup") delle informazioni nel caso queste a causa di un virus non fossero più integre o disponibili.
INCENDIO	
Locale senza dispositivi anti incendio.	Predisporre i locali aziendali con dispositivi per spegnere gli incendi.
ERRORI NELLA MANUTENZIONE DELLE APPARECCHIATURE	
Rivolgersi a fornitori non qualificati o non competenti.	Prevedere delle apparecchiature di riserva che possano sostituire in breve tempo quelle danneggiate, e prevedere copie di sicurezza delle informazioni critiche per il business.

Cessione a terzi:
Si può anche decidere di cedere il rischio a terze parti, affidandosi a compagnie di assicurazione e a polizze specifiche. Erroneamente si pensa di poter cedere il rischio anche trasferendo un determinato processo a un fornitore esterno (cosiddetto "outsourcing"). Sebbene quest'atteggiamento possa tutelare l'azienda da danni materiali, non la tutela da tutti quelli immateriali dovendo, in definitiva, rispondere lei ai propri clienti e al mercato.

Accettazione (ritenere il rischio):
Ritenere un rischio, significa accettare il verificarsi di un evento dannoso e delle sue conseguenze.

Di norma si ritiene un rischio in due occasioni:

- quando la probabilità che un evento si verifichi è prossima allo zero;
- quando i danni prodotti dal manifestarsi di un evento sono di lieve entità;
- quando, dopo aver implementato idonee misure di sicurezza, ritengo che i costi d'introduzione di nuove e più stringenti misure superino i benefici attesi.

Ho fatto un'analisi in azienda dei possibili rischi? Ho definito in che modo gestirli? ?

La gestione del rischio deve essere un processo continuo e periodico. Le aziende cambiano perché cambiano i loro processi, le persone, le tecnologie. Oltre alle aziende cambiano anche le minacce. È quindi fondamentale definire dei periodi con cadenza almeno annuale in cui valuto nuovamente se, come e quanto gestire un rischio. !

3.2 GARANTIRE LA DISPONIBILITÀ DELLE INFORMAZIONI

Qualora abbia perso un'informazione, ad esempio contenuta in un file, utile per svolgere delle attività, sarà necessario recuperarla.

Per farlo ci si affida di norma a delle copie di sicurezza, dette anche copie riserva o "Back-up". La creazione di copie di sicurezza è un aspetto fondamentale nella corretta gestione delle informazioni e assicura che in caso di guasti, manomissioni, furti, errori dei dipendenti, virus, ecc., l'informazione sia sempre disponibile, garantendo, inoltre, la continuità delle attività in azienda. Tali copie di sicurezza sono ottenibili duplicando le informazioni su altri supporti, come memorie esterne (hard disk esterni, CD, DVD, chiavi USB, ecc.).

Il processo di duplicazione può essere gestito sia manualmente sia automaticamente, per tutte le informazioni o solo per una parte di esse. Inoltre le copie possono essere custodite nello stesso luogo nel quale risiede l'originale o in un luogo differente.

La copia di sicurezza custodita nella stessa sede dell'originale ha un limite, non protegge l'in-

formazione nel caso si verifichi un evento che colpisca direttamente il luogo in cui tali informazioni sono custodite, come ad esempio un intero ufficio. I casi più comuni sono incendi ed allagamenti.

Per evitare che in questi casi si perda la disponibilità, non solo degli originali ma anche delle copie di sicurezza, è necessario che queste risiedano:

- o in un'altra sede, affidandosi magari a fornitori specializzati nella custodia di tali dati,
- o in un ambiente più sicuro, come ad esempio un armadio ignifugo.

Quanto alla frequenza con cui fare copie di sicurezza, questa dipende da diversi fattori e non può essere univoca per tutte le aziende. È buona prassi quantomeno fare una copia di tutte le informazioni una volta alla settimana e una volta al giorno dei file (o cartelle) su cui si è lavorato durante il giorno.

Inoltre è necessario controllare periodicamente che il back up sia stato fatto completamente e che i dati copiati siano integri. Per farlo di norma vengono fatti degli specifici test di recupero in cui si simula la perdita dei dati e si prova a recuperarli utilizzando le copie di sicurezza.

Per concludere è necessario dire che le copie di sicurezza garantiscono la disponibilità delle informazioni in una moltitudine di casi (un dipendente che cancella per sbaglio un file, la memoria di un computer che si rompe, una manomissione volontaria, un furto di un portatile, ecc.) ma non tutti.
Basti pensare all'interruzione di corrente elettrica. Per quanto abbia delle copie di sicurezza, queste non saranno disponibili se non ho modo di accedervi per mancanza di corrente. Per risolvere questo problema, posso affidarmi a dei gruppi di continuità. Un gruppo di continuità fornisce corrente elettrica per un lasso di tempo necessario a che il problema sia risolto o quantomeno, per il tempo necessario a spegnere correttamente i sistemi affinché non si danneggino a causa di uno spegnimento irregolare.

Faccio copie di sicurezza delle informazioni? ?

Controllate periodicamente, soprattutto quando il processo è automatizzato, le copie di sicurezza per verificarne la completezza e l'integrità. !

3.3 AGGIORNARE I SISTEMI

Un criminale informatico od un virus sfruttano difetti di programmazione delle applicazioni o dei sistemi operativi per arrecare danni ai sistemi informativi. Gli aggiornamenti eliminano questi punti deboli mano a mano che vengono scoperti.

Tra tutti i programmi, alcuni meritano un'attenzione maggiore e più scrupolosa negli aggiornamenti:

- **sistema operativo**: è il software sul quale si appoggiano gli altri software e che permette di far funzionare tutti i dispositivi. I sistemi operativi sono programmi complessi, e la loro complessità rende fisiologica la presenza di errori di programmazione. Un esempio di sistema operativo è Windows, ma si stanno diffondendo altri sistemi operativi come ad esempio quelli per computer Apple (Mac OS);
- **programmi per la navigazione in Internet:** consentono di visualizzare i contenuti delle pagine dei siti web e di interagire con essi permettendo all'utente di navigare in Internet. Sono la porta di accesso alla rete e viceversa, ecco perché è importante che sia ben presidiata e non abbia punti deboli. Tra i più usati: Internet Explorer, Mozilla Firefox, Google Chrome, ecc.;
- **antivirus**: data la velocità con cui nascono e si propagano nuovi virus, l'aggiornamento quantomeno giornaliero deve essere la prassi;
- **applicazioni**: sebbene di norma siano software meno complessi di un sistema operativo, contengono comunque errori di programmazione (SAP, Zucchetti, Microsoft Office, ecc.).

Aggiornare tutti i programmi con costanza è difficoltoso ma è fondamentale per la sicurezza delle informazioni.

Per agevolare le attività è opportuno, ove possibile, impostare gli aggiornamenti automatici in modo che si scarichino e si installino automaticamente appena disponibili.

Aggiorno sistemi operativi e programmi ogni volta che un nuovo aggiornamento è disponibile?

?

Fate attenzione a versioni di programmi molto vecchie, le aziende che li sviluppano dopo diversi anni non garantiscono più gli aggiornamenti.

!

3.4 PROTEGGERSI DAI "CODICI MALIGNI"

Come accennato nel paragrafo relativo alle minacce tecnologiche, parlare di soli virus oggi è riduttivo.

Parlare di codici maligni ("malware"), macro categoria di cui i virus fanno parte, è sicuramente più corretto. Un codice maligno è un software creato con l'unico scopo di causare danni o al computer su cui viene eseguito o indirettamente all'utente che usa tale computer.

Per proteggersi da queste minacce è assolutamente necessario che sia presente sui sistemi e che sia costantemente aggiornato, quello che viene definito per storicità "**antivirus**" ma che sarebbe più sensato definire "**anti-codice maligno**".

Oltre che aggiornare gli antivirus ogni volta che è richiesto è buona prassi procedere **ad una scansione** (azione che può compiere il programma per rilevare un codice maligno dai sistemi) veloce del sistema ogni giorno e ad una più approfondita con cadenza settimanale.

Per proteggersi da codici maligni, in sintesi, si deve:

- installare un antivirus e aggiornarlo ogni volta che sia disponibile un nuovo aggiornamento;
- fare una scansione veloce giornalmente;
- fare una scansione approfondita una volta a settimana;
- installare e configurare un firewall (muro tagliafuoco), ossia un dispositivo, che analizza i dati applicando delle regole che contribuiscono alla sicurezza;
- può succedere che qualora uno o più virus abbiano "infettato" il PC, il sistema operativo possa essere irrimediabilmente compromesso, in questo caso può essere "preferibile" ripristinare completamente il sistema, reinstallando il sistema operativo con tutte le sue applicazioni;
- oltre a misure di sicurezza tecnologiche, ci si può proteggere dai malware adottando buone prassi durante la navigazione su Internet o nell'uso della posta elettronica e dei personal computer in generale. Vedremo questi aspetti nei paragrafi successivi.

Ho installato un antivirus? Aggiorno l'antivirus almeno quotidianamente? Faccio una scansione approfondita almeno una volta a settimana?

?

Per una protezione efficace le misure tecnologiche devono essere sempre affiancate da buone prassi (aggiornamenti, corretti principi di navigazione, di uso della posta elettronica, degli strumenti informatici, ecc.)

!

3.5 COME GESTIRE LA NAVIGAZIONE SUL WEB

Come accennato nel paragrafo relativo alle minacce tecnologiche, parlare di soli virus oggi è riduttivo.

Internet è oggi la fonte più prolifera di minacce e come vedremo anche nel capitolo delle frodi, non esclusivamente tecnologiche.
Questo comporta che oltre ai sistemi di protezione visti nel capitolo precedente, potrebbe essere necessario prendere ulteriori misure di sicurezza.

Si può ad esempio decidere di inibire totalmente l'accesso a Internet, o anche solo parzialmente, andando a definire siti non sicuri su cui non sarà concessa la navigazione. Oppure consentire la navigazione, ma inibire la possibilità di scaricare file da Internet o di eseguirli sul computer.

Si possono inoltre proteggere le comunicazioni che avvengono attraverso sistemi di messaggistica istantanea (Messenger, Skype, ICQ, ecc.)

con sistemi di tutela che proteggano i messaggi scambiati, da possibili intercettazioni di un criminale informatico.

A livello organizzativo si possono inoltre sensibilizzare gli utenti al corretto utilizzo di Internet, strumento indispensabile anche se pericoloso, raccomandando di non navigare su siti web non attinenti l'attività lavorativa o dai contenuti sospetti (ad esempio, siti che vi indichino come vincitori di improbabili concorsi a premi), di non partecipare a forum o chat o a social network, di non scaricare alcun tipo programma.

Data la loro forte diffusione è infine utile spendere qualche parola in più sul fenomeno dei social network on-line ossia, di tutte quelle reti sociali che nascono e si sviluppano su Internet, di cui la più famosa è Facebook.

I principali pericoli sono legati a:

- furti delle credenziali di accesso (nome utente e password), grazie alle quali un malintenzionato potrebbe appropriarsi sia delle informazioni della persona a cui ha rubato le credenziali, sia di altre persone fingendosi chi ha subito il furto;
- furti di identità, ossia persone che creano profili di altre persone, agendo in nome di queste;
- dati personali, visto che una volta inseriti appartengono all'impresa che gestisce il sito, in base al contratto di licenza d'uso accettato all'atto dell'iscrizione, e raramente letto per intero;
- danni all'immagine, per la diffusione di informazioni anche fuori dalla cerchia della rete sociale;
- frodi (si veda il capitolo successivo);
- ecc.

Per tutelarsi è necessario prima di tutto essere consapevoli dei rischi che comportano e:

- utilizzare password complesse e diverse per ogni servizio utilizzato (posta elettronica, social network, ecc.);
- limitare al massimo le informazioni disponibili a tutti, permettendo solo agli amici di visualizzare il profilo per intero;
- mai inserire dati come indirizzi, numeri di telefono, date di nascita, informazioni riservate sull'attività lavorativa o sulla famiglia;
- non inserire niente di cui ci si possa pentire in seguito, come oscenità o insulti;
- non rivelare informazioni personali, aziendali o finanziarie;
- non accettare le richieste di amicizia da persone sconosciute; ecc.

Nonostante abbia installato un antivirus e un firewall, continuo a subire attacchi informatici? ?

La sensibilizzazione del personale sull'uso di Internet è un fattore chiave per la sicurezza delle informazioni. !

3.6 COME GESTIRE LA POSTA ELETTRONICA

Anche la posta elettronica è un mezzo indispensabile per le aziende e contemporaneamente pericoloso se non gestito correttamente. È importante quindi impostare delle regole tecnologiche che definiscano:

- quanto può essere grande al massimo un allegato ad una mail, sia questa una mail da inviare o una da ricevere. Nel caso in cui un allegato sia quindi di una dimensione superiore a quella stabilita, i sistemi non permetteranno l'invio o la ricezione;
- che l'antivirus faccia sempre una scansione delle mail e relativi allegati;
- politiche di anti spam. Vale a dire definire un sistema di protezione della posta elettronica, che prevenga la ricezione massiccia di e-mail indesiderate e potenzialmente pericolose, lo spam appunto;
- linee guida comportamentali, ossia delle buone prassi per rendere consapevoli gli utenti dei pericoli, oltre che delle loro responsabilità.

Alcune linee guida contenute in un documento di "buone prassi", potrebbero essere:

- è vietato utilizzare la posta elettronica aziendale per scopi personali o per scopi

diversi dall'attività lavorativa;

- non aprire la posta elettronica proveniente da mittenti sconosciuti o il cui oggetto sia fuorviante;
- non scaricare file allegati alle e-mail se non si è certi che il contenuto sia sicuro. In caso di incertezze chiedere supporto all'assistenza;
- non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, forum non lavorativi, ecc.

Ho disposto delle linee guida comportamentali per l'utilizzo della posta elettronica? ?

La sensibilizzazione del personale sull'uso della posta elettronica è un fattore chiave per la sicurezza delle informazioni. !

3.7 EVITARE FRODI VIA INTERNET

Le frodi via Internet sono sempre più diffuse. Quella più famosa prende il nome di "phishing" e, attiva da diversi anni, si è evoluta assumendo nuove forme e appellativi: "pharming", "tabnapping", "smishing", ecc.

Il "phishing", e le sue evoluzioni, sono frodi informatiche finalizzate all'acquisizione di informazioni come dati personali, numeri di conto corrente, password, ecc. e sfruttano l'anello più debole della sicurezza: l'uomo.

A lato pratico, l'utente viene raggirato facendogli credere di interagire (via mail, via web, via sms) con un interlocutore fidato, come ad esempio il sito istituzionale della propria banca, quando invece sta comunicando i propri dati riservati ad un criminale. Non è raro imbattersi in questa truffa ricevendo mail di richiesta di numeri di carte di credito, da parte di malintenzionati che si fingono essere la vostra banca. Per difendersi da questi attacchi è necessario:

- verificare sempre l'indirizzo mail di chi vi manda la comunicazione;
- valutare il testo della mail stessa (errori ortografici, intestazioni generiche "Gentile Cliente", ecc.);
- diffidare sempre di chi vi chiede dati personali (una password, il numero della carte di credito, ecc.) tramite posta elettronica, nessuna istituzione seria lo fa;
- prima di inserire in un sito web qualsiasi tipo di dato riservato come per esempio nome utente e password per accedere al conto bancario o per fare un acquisto su Internet, assicuratevi che nell'indirizzo del sito (indicato nella barra degli indirizzi del programma per la navigazione) ci sia l'estensione "https" che significa connessione ad un'area protetta;
- aggiornare periodicamente i software di sicurezza;
- aggiornare i sistemi informatici;
- rimanere sempre aggiornati sulle nuove frodi (magari visitando periodicamente i siti specializzati) e formare il personale su questi aspetti.

Ho ricevuto mail in cui mi si richiedeva di comunicare dati personali? ?

Prima di inserire in un sito web qualsiasi tipo di dato riservato assicuratevi che nell'indirizzo del sito ci sia l'estensione"https" !

3.8 GESTIRE I PERSONAL COMPUTER DELL'AZIENDA

Ecco alcune regole pratiche per gestire la sicurezza dei personal computer della propria azienda.

Proteggete il computer con un nome utente e una password

Qualora ad un computer abbiano accesso più persone è necessario creare più utenti seguendo queste linee guida per la creazione di profili di utenza.

Un profilo di utenza permette ad una persona di accedere a determinate risorse (file, cartelle, applicazioni, ecc.) ed è di norma composto da un nome (nome utente o "user-id") e da una parola segreta (password).

Ad un nome e una password vengono associati dei permessi di accesso. L'insieme di queste tre componenti: nome utente, parola segreta e

associazione delle risorse, permette di definire in modo sicuro chi debba accedere a cosa e con che modalità.

A lato pratico è necessario per creare un profilo di utenza che:

- siano creati per ogni persona un nome utente identificativo della persona stessa (ad esempio, m.rossi);
- al nome utente (identificativo della persona) vengano assegnate le risorse (cartelle, programmi, file, ecc.) e quindi le informazioni, a cui può accedere. Questo può essere fatto per persona o per gruppi di persone con privilegi di accesso omogenei (ad esempio, m.rossi può accedere ai dati dall'amministrazione oppure m.rossi viene associato al gruppo "amministrazione" e in automatico gli vengono forniti gli accessi comuni a quel gruppo);
- al nome utente sia associata una parola segreta (password) permettendo al sistema di autenticare in modo univoco la persona e quindi di garantirle l'accesso alle risorse di cui ha bisogno, secondo le modalità che vedremo nel prossimo paragrafo.

Scelta e gestione delle password

Una password (parola segreta) per essere sicura deve avere delle caratteristiche:

- deve avere al minimo 8 caratteri alfanumerici, ossia deve contenere lettere e numeri (A,B,C ...,a,b,c ...,1,2,3...);
- non deve contenere il nome utente né deve riportare facili riferimenti ad esso. Ad esempio se il nome utente è "m.rossi" la password "mariorossi" non è da considerarsi sicura;
- deve essere cambiata (o meglio ancora scadere) ogni 90 giorni qualora si trattino solo dati personali e ogni 30 qualora si trattino dati personali sensibili (D.lgs. 196/2003, "legge sulla privacy"). Si veda a tale proposito il capitolo 4.1;
- quando la password viene cambiata si deve evitare di immetterne di sequenziali (xxyyzz01, xxyyzz02...);
- non deve essere comunicata a nessuno;
- non deve essere scritta su un foglio conservato all'interno del proprio ufficio;
- non deve essere salvata all'interno del computer o del cellulare in nessuna modalità;
- la prima password deve essere assegnata all'utente in modo automatico dal sistema, e il sistema deve obbligare l'utente a cambiarla al primo accesso;
- è meglio che i sistemi in automatico guidino l'utente ad inserire una password sicura, non permettendogli ad esempio di usarne una di quattro caratteri oppure che non scada mai.

Blocco del Computer

Quando ci si allontana dalla postazione di lavoro è importante bloccare sempre il computer (ctrl+alt+canc e poi "blocca computer" oppure tasto di windows +"L"). Il blocco del computer consente di proteggere il proprio accesso da persone non autorizzate.

Palmari, cellulari, smartphone, ecc.

Anche questi strumenti custodiscono informazioni importanti come le e-mail, gli allegati, la rubrica telefonica e il calendario degli appuntamenti, è pertanto buona norma estendere i principi e le protezioni visti in tutti i capitoli precedenti anche a questi dispositivi.

Abbiamo in azienda un computer utilizzato da più persone? Conosco gli obblighi del D.lgs. 196/03? ?

Attenzione che alcune regole di sicurezza non sono solo utili a proteggere i propri sistemi informativi ma sono veri e propri obblighi di legge. A tale proposito si faccia riferimento al D.lgs. 196/03. !

3.9 CREARE E GESTIRE LA RETE LOCALE E IL WIRELESS IN SICUREZZA

Una rete informatica è un insieme di apparecchiature connesse fra loro che consente di condividere risorse e informazioni. Una rete locale è una tipologia di rete informatica contraddistinta da un'estensione limitata, di solito ad un edificio.

Le misure di sicurezza più comuni sono:

- definire ed applicare una corretta profila-

tura degli utenti. Si veda a tale proposito il primo paragrafo relativo alla gestione dei personal computer;

- installare un firewall. Si può decidere di installare un firewall centralizzato nel caso di reti complesse o uno su ogni computer (personal firewall) nel caso di reti semplici;
- installare un gruppo di continuità per la gestione delle indisponibilità di corrente elettrica;
- installare un antivirus, prevedendone uno centralizzato nel caso di reti complesse o uno su ogni computer nel caso di reti semplici;
- mantenere i programmi sempre aggiornati. Anche gli aggiornamenti possono essere decisi ed effettuati centralmente;
- limitare i privilegi dei dipendenti sui loro computer. Questo significa che se non è necessario per le attività lavorative che un dipendente usi Internet, non vi possa accedere, oppure qualora non fosse necessario che inserisca chiavi USB o che installi nuovi programmi, sia inabilitato a farlo, ecc. In particolare limitare questi privilegi aiuta a tutelarsi anche da furti interni di informazioni, ossia furti di informazioni fatti dai dipendenti a danno dell'azienda che sono molto più diffusi di quelli esterni;
- predisporre dei Back-up automatici. Anche in questo caso possono essere definiti centralmente;
- gestire quotidianamente la rete, prevedendo dei controlli periodici sul suo funzionamento, inclusi gli aspetti di sicurezza.

Le reti wireless

Ormai sono largamente diffuse le reti senza fili (wireless) perché estremamente comode e facili da usare. Per connettersi ai computer, le reti wireless ricorrono a un collegamento radio invece che ai cavi.

Di conseguenza, chiunque si trovi all'interno del raggio di trasmissione radio è potenzialmente in grado di connettersi alle rete.

Per diminuire i rischi che una persona non autorizzata entri nella rete coperta dalle trasmissioni, è necessario utilizzare la funzione di crittografia (funzione di occultamento delle informazioni usata per precludere il tentativo di accesso non autorizzato) e di controllo dell'accesso fornita con l'apparecchiatura di rete wireless.

Al momento dell'installazione si deve avere cura di installare la tecnologia più recente, in modo da assicurarsi che anche le funzioni di crittografia siano all'avanguardia e al momento della scelta della chiave ("password del wireless") utilizzate i principi di definizione di una password sicura, visti nei capitoli precedenti.

Rispetto alle indicazioni ricevute come valuto la mia rete? (poco sicura, mediamente sicura, molto sicura). ?

Una rete sicura è una rete che è gestita giorno per giorno. !

3.10 L'ORGANIZZAZIONE DELLA SICUREZZA

A prescindere dalla dimensione dell'azienda, è fondamentale che gli aspetti di sicurezza delle informazioni siano tutt'uno con le normali attività aziendali diventando anch'esse parte del patrimonio culturale dell'azienda (know-how). Per far questo è utile disciplinare gli aspetti di sicurezza delle informazioni in apposite istruzioni rivolte agli utenti (anello debole della catena della sicurezza) affinché rispettino e preservino la sicurezza delle informazioni. A titolo esemplificativo, un set classico di istruzioni legate a questi aspetti potrebbe essere definito per:

La creazione, la modifica, la cancellazione dei profili d'utenza: definire delle linee guida per la corretta gestione dei profili di utenza andando anche ad individuare chi ha la responsabilità di approvare eventuali creazioni, modifiche e cancellazioni.
Esempi:

- solo la direzione può approvare la creazione di un utente, la modifica ai permessi e la sua cancellazione;
- qualora un utente si accorgesse di poter accedere a risorse che non attengono alla sua attività, è obbligo che comunichi l'anomalia al proprio diretto responsabile, ecc.

La creazione, l'utilizzo e la conservazione delle password: definire delle linee guida

per la corretta gestione delle password.
- una password deve avere almeno 8 caratteri alfanumerici;
- deve essere cambiata ogni 30 giorni, ecc.

L'utilizzo degli strumenti informatici (computer e programmi): fornire delle linee guida per il corretto utilizzo di questi strumenti identificando buone prassi, doveri e limiti.
Esempi:
- bloccare il computer ogni volta che ci si allontana dalla postazione;
- non provare ad aggiustare il computer da soli, ma chiamare sempre un tecnico, ecc.

L'utilizzo della rete Internet: definire le modalità di accesso, buone prassi nella navigazione, divieti, ecc.
- non scaricare file;
- non navigare su siti web non attinenti all'attività lavorativa, ecc.

L'utilizzo della posta elettronica: definire le modalità di utilizzo, identificare buone prassi, divieti e pericoli. Esempi:
- non scaricare allegati di dubbia provenienza;
- non utilizzare la casella di posta aziendale per scopi personali, ecc.

Gestione degli incidenti informatici: definire metodi di comportamento a seguito del rilevamento di un incidente informatico:
- non cercate di risolvere il problema da soli;
- contattate un tecnico, ecc.

Gestione di supporti cartacei: è utile disciplinare, ad esempio, come custodire, distruggere questo tipo di documentazione, come prevedere delle copie di sicurezza, ecc. Esempi:
- ritirare sempre i documenti una volta stampati dal cassetto della stampante;
- distruggere i documenti riservati con un distruggi documenti, ecc.

Gestione degli accessi fisici: Disciplinare su chi possa entrare in una determinata area e con che modalità. Esempi:
- gli ospiti hanno l'obbligo di registrarsi alla reception, indicando il motivo della visita, e devono essere sempre accompagnati da un referente interno;
- solo il personale autorizzato e provvisto dell'apposito badge può accedere agli uffici della direzione, ecc.

Creazione e Gestione delle copie di sicurezza: definire le modalità e tempi per la creazione di copie sicurezza.
Esempi:
- le copie di sicurezza dei file e delle cartelle su cui si è lavorato devono essere fatte ogni giorno prima di spegnere il computer;
- settimanalmente, ogni venerdì, le copie di sicurezza devono essere fatte su tutti i dati, ecc.

Ho disciplinato almeno gli aspetti di sicurezza più importanti in specifiche istruzioni? ?

La formalizzazione di istruzioni di sicurezza è importante per i dipendenti e per garantire la sicurezza delle informazioni. !

3.11 LA SICUREZZA FISICA

La sicurezza fisica riguarda:
- sia l'insieme di misure che prevengono e dissuadono persone non autorizzate (interne ed esterne) ad accedere a determinate aree e quindi alle risorse o alle informazioni in esse contenute;
- sia l'insieme di contromisure volte a salvaguardare tali risorse da eventi come incendi, allagamenti, furti, ecc.

Si gestisce la sicurezza fisica con, quindi:
- una serratura;
- un'istruzione per la gestione degli accessi fisici ai locali;
- un sistema di videosorveglianza;
- un sistema anti-incendio (rilevazione e spegnimento) nei locali;
- un allarme antifurto; ecc.

Nell'implementazione di contromisure di sicurezza fisica è necessario valutare sempre la tipologia di ambiente da proteggere e la criticità delle informazioni trattate.

Ho implementato misure di sicurezza fisica in linea con l'analisi di criticità delle informazioni trattate? ?

La sicurezza fisica è una condizione necessaria, anche se non sufficiente, per garantire la sicurezza delle informazioni. !

4

LE NORME VIGENTI IN MATERIA

Mettere in sicurezza i sistemi informativi, non è solo una buona prassi ma è anche un vincolo legislativo. Per questo motivo è fondamentale che l'azienda provveda a dare informazione e diffusione delle normative vigenti e della loro applicazione. Inoltre sarebbe auspicabile che sensibilizzasse sul rispetto delle regole e che periodicamente vigilasse sulla corrette applicazione delle stesse.

In particolare meritano di essere menzionate, e brevemente descritte, le seguenti norme:

4.1 "LEGGE SULLA PRIVACY"

Con questo termine si intende il D.lgs. 196/03, il cui titolo ufficiale è "Codice in materia dei dati personali". La norma, all'articolo 31, afferma che i dati personali oggetto di trattamento devono essere custoditi e controllati [...] mediante l'adozione di idonee e preventive misure di sicurezza [...]". All'articolo 33 si definiscono quali siano le **misure minime di sicurezza** da adottare.

Da un punto di vista informatico sono richieste l'identificazione e autenticazione degli utenti al sistema informatico, le copie di sicurezza per il recupero dei dati, e gli antivirus per i computer utilizzati per il trattamento dei dati personali.

Di particolare interesse è la richiesta di redigere un'autocertificazione in merito al trattamento di dati personali in osservanza delle misure minime di sicurezza previste dal codice della privacy e dal disciplinare tecnico riportato in allegato al codice stesso.

La normativa sulla privacy richiede a quasi tutte le aziende, l'adozione di un piano per la sicurezza delle informazioni, costringendole a rendersi consapevoli del proprio patrimonio informativo e delle proprie esigenze di sicurezza.

Il non rispetto della legge in questione comporta pesanti sanzioni civili e penali.

4.2 "LEGGE SUL COMPUTER CRIME"

La legge 547/93, ha introdotto, nel Codice Penale, una serie di crimini "informatici", quali: attentato a impianti informatici di pubblica utilità; falsificazione di documenti informatici; accesso abusivo a un sistema informatico o telematico; detenzione e diffusione abusiva di codici di accesso; diffusione di programmi diretti a danneggiare o interrompere un sistema informatico; violazione di corrispondenza telematica e intercettazione di e-mail; danneggiamento di sistemi informatici o telematici e frode informatica.

Notevole importanza riveste l'interpretazione delle responsabilità. In particolare, secondo alcune interpretazioni, non è possibile incriminare qualcuno nel caso in cui abbia compiuto uno degli atti elencati precedentemente, e la vittima non abbia messo in opera adeguate misure di sicurezza per contrastarli.

Da citare inoltre la Legge N°48 del 18 Marzo 2008 emanata per dare esecuzione alla *Convezione del Consiglio di Europa sulla Criminalità Informatica (2001)* che anch'essa ha modificato il nostro codice penale introducendo leggi che hanno permesso tra l'altro di armonizzare a livello internazionale gli interventi volti a combattere il crimine informatico.

4.3 DECRETO LEGISLATIVO 231/2001

Disciplina in merito "alla responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica [...]" e riguarda le sanzioni per illeciti penali che portano vantaggi ad una azienda. Tali illeciti comprendono tra altro la frode informatica in danno dello Stato (art.24) e delitti informatici e trattamento illecito dei dati (art.24 bis).

L'azienda può non rispondere dell'illecito se prova che: sono state adottate, prima della commissione del fatto, opportuni modelli di carattere organizzativo e gestionale, ossia di sicurezza, relative al flusso documentale; ha istituito una funzione di audit interna autonoma con il compito di vigilare sul funzionamento e l'osservanza delle misure e di curarne l'aggiornamento; le persone hanno commesso il reato eludendo fraudolentemente le misure di sicurezza; non vi è stata insufficiente vigilanza dell'audit.

In altre parole, l'azienda deve realizzare un sistema di sicurezza delle informazioni tale per cui nessuno possa commettere illeciti amministrativi per ignoranza delle direttive aziendali, o per errore.

Conosco i requisisti richiesti dalle norme vigenti in merito alla sicurezza dei sistemi informativi? ?

La sicurezza dei sistemi informativi è un obbligo di legge. !

5

IL PROGETTO DI RICERCA

"E-SECURITY PER LE PMI"

Nel corso dei mesi di Ottobre e Novembre 2010, 750 imprese lombarde sono state contattate al fine di rilevare puntuali informazioni ed opinioni circa la conoscenza e l'adozione di pratiche e soluzioni di sicurezza informatica.

Le interviste one-to-one sono state realizzate telefonicamente, attraverso la predisposizione di script strutturati appositamente per la tematica sottoposti ai Responsabili IT o loro capi funzionali.

Il progetto di ricerca è stato definito prevedendo specifiche scelte di numerosità e dimensione del campione, che da un lato rispecchia la struttura del mercato nelle provincie selezionate, rilevabile dai dati ISTAT, e dall'altro è funzionale agli obiettivi espressici, pertanto esclude le micro aziende (Aziende con un range di dipendenti <10 e di fatturato < 2 Milioni di Euro) così come le Top (Aziende con un range di dipendenti >500 e di fatturato > 250 Milioni di Euro).

I contenuti oggetto di analisi sono stati trattati seguendo un percorso logico che ha permesso di valutare il reale stato dell'arte della Sicurezza nelle PMI coinvolte nel progetto e la loro propensione ad ulteriori azioni nell'ambito della problematica.

Un particolare obiettivo dell'indagine è stato valutare come nel concetto di Sicurezza IT si comprendano tutte le misure informatiche atte a proteggere non soltanto il sistema informativo in quanto tale, ma anche l'attività che l'azienda conduce grazie al supporto del sistema informativo.

Si ritiene che questa precisazione sia doverosa in quanto il concetto di Sicurezza deve esulare dalle valutazioni di singoli prodotti o ambiti.

5.1 IL CAMPIONE DI IMPRESE

In relazione agli scopi prefissati per la nostra indagine, essa è stata svolta nell'autunno 2010 con interviste ai responsabili della Sicurezza IT di 750 imprese appartenenti a diversi settori d'attività distribuiti in modo da dare uno spaccato per quanto possibile rappresentativo delle PMI in Lombardia.

Nel dettaglio la composizione del nostro Panel rispecchia le seguenti specifiche:

TOTALE IMPRESE INTERVISTATE 750

CON SEDE NELLE PROVINCE DI:

- (26%) Milano
- (14%) Como
- (11%) Mantova
- (20%) Monza e Brianza
- (10%) Pavia
- (19%) Varese

OPERANTI NEL SETTORE DEL:

- (5%) Agricoltura
- (9%) Artigianato
- (21%) Commercio
- (31%) Industria
- (27%) Servizi
- (7%) Turismo

APPARTENENTI

51% **Piccole Imprese**
(10-50 dipendenti e 2-10 M€ di fatturato)

22% **Medio Piccole Imprese**
(50-100 dipendenti e 10-50 M€ di fatturato)

17% **Medie Imprese**
(100-250 dipendenti e 50-100 M€ di fatturato)

10% **Medio Grandi Imprese**
(250-500 dipendenti e 100-250 M€ di fatturato)

5.2 I RISULTATI DELLA RICERCA IN SINTESI

Come viene oggi percepita e gestita la Sicurezza Informatica dalle Aziende Lombarde? La risposta, in estrema sintesi, è che da parte delle imprese Lombarde traspare una maggiore consapevolezza nei confronti di questa tematica e che la sicurezza sta lentamente (e si spera inesorabilmente) iniziando a permeare anche i processi Aziendali. Anche nelle realtà di più piccole dimensioni.

Sia pure con luci e ombre, i dati emersi nel corso dell'indagine mostrano come la sicurezza sia un problema ben avvertito e in molti casi anche correttamente affrontato dalle imprese Lombarde. Il discorso però cambia quando dai modelli di approccio si passa all'effettiva diffusione delle soluzioni di sicurezza IT, che mostra lacune in taluni casi anche piuttosto ampie.
Infatti, mentre ad esempio i sistemi cosiddetti di prevenzione e difesa da virus, intrusioni e altre minacce provenienti dall'esterno, hanno un livello di diffusione decisamente elevato, le soluzioni che controllano l'accesso alle applicazioni e ai dati Aziendali, lo sono di meno, e ancor meno diffusi sono i sistemi di monitoraggio che permettono di prevenire i danni dovuti ad attacchi e intrusioni.

Certamente lo scenario che si prospetta a noi oggi è ben diverso da quello del recente passato: le Aziende Lombarde, seppur lentamente ed a fatica, si sono progressivamente sempre più impegnate sul fronte della Sicurezza Informatica.
Esse hanno innanzitutto introdotto regole e procedure di sicurezza alle quali vincolare tecnologie e utenti del Sistema Informativo ed inoltre hanno iniziato a ricorrere ad attività di Risk Assessment e ad attività specifiche per la gestione degli attacchi.
Tuttavia l'allargamento della visione della problematica della sicurezza ad aspetti e ad attività di natura non esclusivamente tecnologica non è ancora oggi completamente guidato e gestito da un comportamento pienamente consapevole delle Aziende, le quali, al contrario, appaiono in alcuni casi confuse sia sulle motivazioni sia sulle modalità.
Non a caso nel corso della nostra indagine emerge come la spinta ad affrontare investimenti in e-Security arrivi in modo preponderante da un potente driver, che si chiama "compliance". Gli altri motivi, dalla consapevolezza dei danni derivanti dalle vulnerabilità al fatto stesso di essere già stati colpiti e non voler ripetere l'esperienza, passano decisamente in secondo piano.

Analisi dei rischi

La Sicurezza Informatica, da cui dipende buona parte del know-how sviluppato dall'impresa e conservato sotto forma di dati digitali, è un aspetto ormai non più trascurabile dalle imprese di qualsiasi dimensione e di ciò sembrano esserne consapevoli anche le PMI Lombarde.

Infatti, questo è il dato principale emerso nel corso dell'indagine: le PMI Lombarde stanno rapidamente adeguando le procedure interne di gestione della Sicurezza Informatica sia in termini di rispetto delle normative sia in termini di adozione di strumenti e sistemi.

Questa attenzione è senz'altro motivata dal buon livello di consapevolezza maturata all'interno delle organizzazioni circa le conseguenze civili e penali derivanti dalla mancata adozione ad esempio delle "misure minime" previste dalla legge sulla Privacy.
Non è un caso dunque che circa il 99% degli intervistati dichiari che l'Azienda ha implementato tali misure così come che il 97% dichiari di essere consapevole anche delle disposizioni di legge in merito ai diritti di autore sulle licenze software.

Tra le Aziende che dichiarano di avere procedure documentate sul corretto uso degli strumenti informatici, di Internet e della posta elettronica sono emerse queste ulteriori evidenze:

- circa il 30% affermano che i propri dipendenti non sono informati del fatto che l'utilizzo delle risorse IT è ammesso esclusivamente per fini Aziendali;
- ben il 47% affermano che il proprio personale non è informato/formato circa i rischi derivanti dal non seguire le procedure di sicurezza previste in Azienda.

Dunque più o meno tutte le Aziende ricorrono alle policy di Sicurezza, ma emerge con chiarezza che solo una parte di loro le sa gestire correttamente: ciò è ancora più evidente se si prendono in considerazione le modalità di verifica della conoscenza delle policy sia successivamente al loro invio al personale dipendente sia periodicamente.

Emerge infatti che:

- *successivamente all'invio* - è solo il 15% delle Aziende a ricorrere a test di verifica della conoscenza delle policy, il 35% non fa nulla, sostenendo che è responsabilità dei dipendenti lo studio e la comprensione delle politiche, il 24% si limita a chiedere ai dipendenti se le abbiano lette e capite ed infine il 21% dichiara di procedere alla formazione dei soli dipendenti che affermino di non aver capito;
- *periodicamente* - il 50% delle Aziende dichiara di non effettuare alcun controllo periodico della conoscenza delle policy; il 30% procede a dei test di verifica ed il 12% a delle richieste di rilettura.

Sebbene i test di verifica siano l'unico strumento utile ad accertare con certezza la conoscenza e comprensione delle policy internamente all'Azienda, sono ancora poche le Aziende che vi ricorrono.

Al contrario è diffusa l'opinione che l'Azienda non debba preoccuparsi della verifica della conoscenza delle policy da parte dei dipendenti.

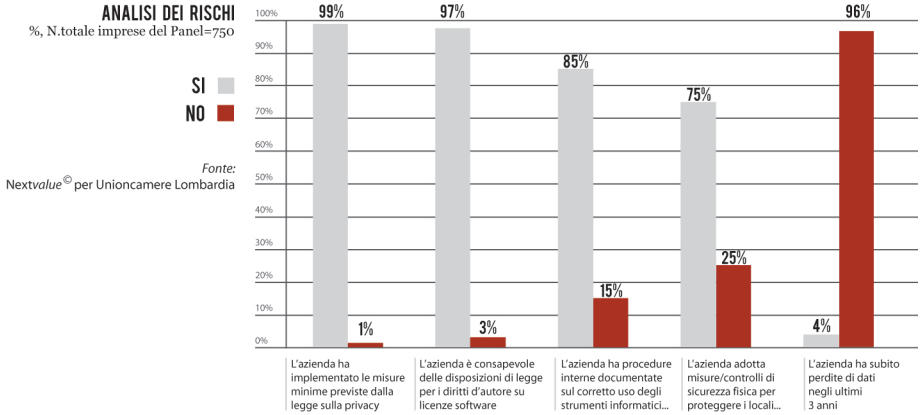
Viene al riguardo da domandarsi se tale atteggiamento sia motivato da una diffusa fiducia nel senso di responsabilità dei dipendenti oppure da una chiara sottovalutazione del problema: la distribuzione delle policy non è di alcuna utilità se ad essa non segue una fase di apprendimento guidato delle stesse ed un processo di verifica periodica della conoscenza di quanto appreso.

Inoltre, in seguito al verificarsi di attacchi palesemente provocati dal mancato rispetto delle policy, può risultare molto difficile per l'Azienda far ricadere la responsabilità di quanto accaduto sul solo dipendente in quanto quest'ultimo può sempre affermare di non aver ricevuto dall'Azienda il supporto necessario per la corretta comprensione di quanto dettato nelle policy.

La maggioranza delle Aziende è consapevole dell'importanza della Sicurezza Informatica, ma al tempo stesso il livello di "maturità" delle soluzioni adottate è ancora molto eterogeneo ed eterogeneo è il livello di sicurezza sui sistemi presenti all'interno di una stessa Azienda.

Se da un lato, ad esempio, è vero il fatto che le Aziende del Panel adottano sistemi antivirus per proteggere i propri sistemi, non altrettanto vero è il fatto che di essi siano dotati tutti i PC ed i Server aziendali (lo sono nel 58% dei casi) né tantomeno il fatto che essi vengano aggiornati regolarmente su tutti i sistemi su cui sono installati (lo sono nel 39% dei casi).

Grafico 1



Lo scenario di e-Security su cui si muovono le PMI Lombarde è dunque fatto di luci ed ombre.

Da un lato sono solo il 15% le imprese del nostro campione che non hanno ancora adottato procedure interne sul corretto uso degli strumenti informatici, così come solo il 25% dichiara di non aver adottato misure/controlli di sicurezza fisica per proteggere i locali in cui sono installati gli strumenti informatici e gli apparati comunicazione.

Dall'altro, le soluzioni adottate, soprattutto in ambito Risk Management sono spesso artigianali e sviluppate in casa, segno che mancano degli standard di riferimento con cui confrontarsi.

Inoltre, solo il 46% delle Aziende che dichiarano di adottare le misure minime di sicurezza previste dalla legge sulla privacy (L.196/2003) dispongono di dispositivi di protezione della rete Aziendale (firewall, proxy) così come solo nel 35% dei casi effettuano verifiche periodiche sulle misure minime di sicurezza tramite personale specializzato.

Nel 67% dei casi, tali Aziende hanno pianificato azioni su come comportarsi in caso di attacco, infezione da virus o perdita di dati mentre il restante 33% agisce al "momento" sulla base di non ben precisati criteri.

Nonostante ciò sono la maggioranza le Aziende che procedono alla log analysis, alla conservazione dei log e alla correlazione delle informazione generate dalla log analysis.

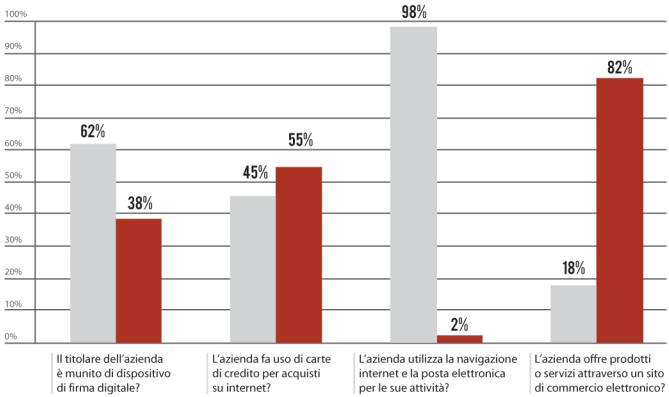
Questi risultati sembrerebbero dimostrare che le PMI Lombarde sono comunque consapevoli del fatto che Sicurezza non vuol dire solo prevenire gli attacchi, ma anche predisporre attività idonee alla loro gestione; in realtà lo scenario è meno roseo di quel che si potrebbe pensare in quanto in più della metà dei casi di svolgimento ad esempio dell'attività di log analysis, si procede in modalità manuale, fatto questo che vanifica l'utilità e l'efficacia dell'attività stessa.

Nonostante ciò emerge un dato estremamente positivo: solo il 4% del campione dichiara di aver subito perdite di dati negli ultimi 3 anni.

Resta da domandarsi se a fianco alla valutazione circa la perdita di informazioni legate ad "attacchi" da parte di soggetti terzi rispetto all'Azienda (come ad es. problemi di sicurezza del sistema informativo, violazione o interferenza con i diritti di privacy, furto di identità, divulgazione di informazioni personali) gli intervistati abbiano tralasciato di segnalare, volutamente o per "non conoscenza", quegli eventi direttamente imputabili alla scarsa attenzione del personale dipendente (perdita di PC, chiavi USB, ecc..), o se abbiano taciuto volutamente anche su determinati eventi per non compromettere la reputazione Aziendale.

L'UTILIZZO DI: FIRMA DIGITALE, INTERNET, POSTA ELETTRONICA E COMMERCIO ELETTRONICO

%, N.totale imprese del Panel=750



Fonte:
Next*value*© per Unioncamere Lombardia

Firma digitale, Navigazione Internet, Posta Elettronica, Commercio elettronico

Ciò che è emerso nel corso del Progetto di Ricerca è che le PMI Lombarde del Panel intervistato stanno anche aprendosi sempre di più al mondo Internet: ben il 98% del campione intervistato dichiara che l'Azienda utilizza la navigazione Internet e la posta elettronica per la gestione delle proprie attività, anche se solo il 18% utilizza la Rete non più solo per servizi quali la posta elettronica e il Web surfing, ma anche per promuovere e offrire prodotti e servizi attraverso un sito di commercio elettronico.

Così come cresce l'utilizzo della Rete per effettuare transazioni e dare disposizioni operative: il 62% dei titolari Aziendali è munito di dispositivo di firma digitale, che però in oltre la metà dei casi analizzati è custodita presso il commercialista, e ben il 45% delle Aziende del campione fa uso di carte di credito per effettuare acquisti su Internet; tali acquisti sono effettuati da personale abilitato e pienamente consapevole dei rischi connessi a tale attività secondo quanto riportato dal 95% degli intervistati.

Identificazione/Autenticazione

Quanto all'access management decisamente incoraggiante è la percentuale (96%) di Aziende intervistate che dichiarano di disporre di soluzioni di directory ovvero che per l'accesso al sistema informatico è necessaria l'autenticazione del singolo utente tramite login/password.

Sebbene rappresentino un ottimo punto di partenza, le soluzioni di directory non risolvono da sole il problema di garantire una gestione sicura dei sistemi informativi ma vanno integrate con sistemi specifici di gestione delle identità e degli accessi.

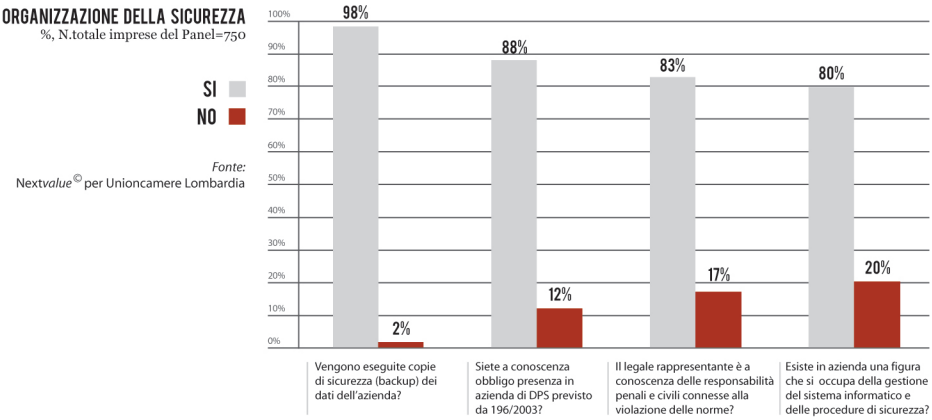
Approfondendo l'analisi su questo 96% di Aziende che utilizza soluzioni di directory, tra di esse solo il 26% dichiara che il proprio personale dipendente utilizza password scelte in base ai principi di sicurezza (codici alfanumerici, ecc..) e solo il 27% che esistono precise procedure di creazione/cancellazione/aggiornamento dei diritti di autenticazione per l'accesso al sistema.

Ciò è, ovviamente, un dato abbastanza preoccupante.

Conservazione dei dati

Passando invece all'analisi degli aspetti di IT Security connessi alla conservazione e gestione dei dati occorre sottolineare come a fronte di un 91% di Aziende che dichiarano di conservare e gestire i dati e le informazioni di valore all'interno dei propri sistemi informativi soltanto il 12% di esse dichiari l'esistenza in Azienda di un inventario dettagliato delle informazioni di valore e/o sensibili presenti all'interno della stessa.

Ciò la dice lunga sulla reale consapevolezza esistente in Azienda su come e dove sono conservati dati sensibili e/o di valore per l'Azienda così come sulla possibilità di monitorare il flusso di tali informazioni ed evitare il furto, la perdita, ecc.. delle stesse.



Organizzazione della sicurezza

In termini di organizzazione della sicurezza in Azienda nell'80% delle PMI Lombarde del Panel esiste una figura che in qualche modo si occupa della gestione del sistema informatico e delle procedure di sicurezza.

Tale figura, soprattutto nelle Aziende di più piccole dimensioni, è una figura esterna all'Azienda con un contratto di consulenza e vincolata da obblighi contrattuali volti a proteggere la sicurezza delle informazioni dell'Azienda e della rete.

Tale dato rivela che la Sicurezza Informatica è un importante elemento che gli imprenditori delle Aziende intervistate riconoscono possa essere tranquillamente delegato a specialisti. Consapevoli nell'83% dei casi delle responsabilità penali e civili connesse alla violazione delle norme. Lo specialista informatico conosce le disposizioni legali che devono essere rispettate ed è in grado di spiegare nel dettaglio tutte le sfaccettature della problematica.

All'imprenditore spetta poi la responsabilità di mettere la Sicurezza Informatica in cima alle priorità dell'Azienda ed egli ha il compito di sensibilizzare i propri collaboratori sui pericoli ed i rischi. Pertanto la Sicurezza Informatica è una questione che riguarda il "capo", ma il capo non deve essere necessariamente uno specialista informatico.

L'elevata percentuale di delega evidenziata nel campione (la sicurezza è affidata ad una figura consulenziale esterna all'Azienda nell'85% dei casi) porta necessariamente ad una gestione più attenta alla tematica rispetto al passato, sia in termini di conoscenza/adeguamento delle policy di sicurezza rispetto alle normative vigenti (l'88% dei responsabili IT intervistati dichiara infatti di essere a conoscenza dell'obbligo di avere in Azienda il Documento Programmatico sulla Sicurezza - DPS previsto dalla legge 196/2003), sia in termini pratico/operativi (il 98% delle Aziende del Panel esegue copie di sicurezza/Back-up dei dati dell'Azienda).

Sebbene il valore medio di Aziende che conoscono ed applicano tali obblighi di legge in Azienda è senz'altro molto alto (88%), approfondendo l'analisi con domande specifiche su come avviene ad esempio l'aggiornamento del DPS il quadro assume linee un po' meno marcate.
Innanzitutto posti di fronte alla domanda sulla frequenza di aggiornamento del DPS stesso solo il 36% delle Aziende ha dichiarato che esso viene redatto ed aggiornato annualmente a fronte di un 48% di Aziende in cui il DPS viene redatto solamente una volta, proprio in ragione dell'obbligatorietà di adempimento a tale "esercizio formale", a cui si somma un 16% di Aziende in cui viene addirittura prodotta soltanto l'autocertificazione.
È evidente dunque che una discreta percentuale di imprese considera in buona parte la Sicurezza Informatica ancora una "necessità": gli obblighi di legge impongono di adeguare, almeno in parte, i comportamenti e le abitudini Aziendali ma non impediscono alle imprese meno virtuose di "fare il minimo indispensabile".

Tant'è vero che solo nel 15% dei casi le PMI Lombarde rendono noti i riferimenti del personale a cui è possibile rivolgersi in casi di violazioni sulla sicurezza e solo nel 21% dei casi in Azienda sono stati erogati corsi per introdurre ai dipendenti le direttive della legge 196/2003 come abbiamo già precedentemente commentato.

Politiche di Back-up e Disaster Recovery

Dicevamo di come la quasi totalità delle Aziende del Panel dichiari di effettuare Back-up, analizzando nel dettaglio quelle che sono le reali azioni messe in pratica in merito alla gestione delle copie di sicurezza dei dati il primo dato che occorre commentare riguarda la frequenza di esecuzione delle copie di sicurezza. Solo il 3% del Panel dichiara di effettuarle giornalmente, il 78% lo fa settimanalmente, il 15% mensilmente e il restante 4% addirittura saltuariamente.

Non meno critico è il fatto che solo nel 13% dei casi analizzati l'utente di PC Portatili, organizer o PDA si assicura di effettuare con regolarità il Back-up dei dati salvati su tali dotazioni tecnologiche.

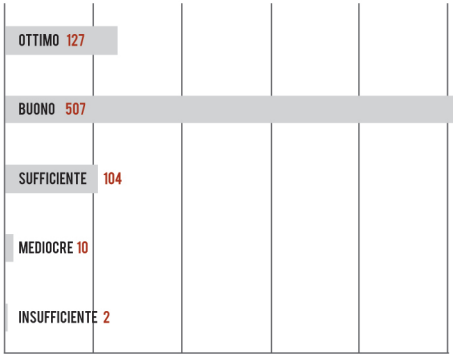
Inoltre, sono il 24% le Aziende cha hanno predisposto un piano per gestire situazioni di Disaster Recovery e il 35% quelle in cui i Back-up sono adeguatamente custoditi. Ed ancora, il margine di intervento in ambito e-Security è ancora molto ampio se solo una percentuale del 40% effettua prove di recupero dati dalle copie di sicurezza.

Grafico 4

AUTOVALUTAZIONE DEL LIVELLO DI E-SECURITY IN AZIENDA

Valori assoluti, N. totale imprese del Panel=750

Fonte: Next*value*© per Unioncamere Lombardia



Considerazioni conclusive

A prescindere da quanto resta ugualmente da fare, il quadro complessivo emerso dalle interviste è comunque decisamente confortante.

Ci troviamo di fronte a un atteggiamento sicuramente più maturo nei confronti delle soluzioni di Sicurezza Informatica, più consapevole delle logiche evolutive e di quanto ancora è necessario fare per migliorare la situazione.

Le PMI Lombarde, meglio rispetto al passato, guardano alla sicurezza non tanto come implementazione di un'infrastruttura statica basata su prodotti e tecnologie che proteggano l'impresa da attacchi esterni quanto, sempre di più, evidenziano la necessità di intendere la sicurezza come un processo continuo che coinvolge sì le tecnologie, ma soprattutto il controllo continuo del livello di sicurezza inteso come efficacia del complesso di tecnologie, politiche e procedure implementate.

Non è un caso dunque che gli stessi intervistati abbiano un'alta considerazione circa il livello di Sicurezza Informatica presente in Azienda.

Tuttavia la netta maggioranza delle Aziende ha definito regole e procedure di sicurezza che hanno generalmente per oggetto gli standard tecnologici e l'organizzazione nel suo complesso; è invece ancora relativamente poco diffusa la definizione di politiche di Sicurezza aventi per oggetto il comportamento del singolo individuo.

Ne consegue il permanere nelle Aziende italiane del convincimento che la sicurezza sia prevalentemente un problema di natura tecnologica, riguardante cioè il sistema informativo.

Inoltre le Aziende sembrano cogliere l'importanza di trattare la sicurezza a livello di Organizzazione, ma non anche a livello di singolo individuo, dimenticando che quest'ultimo è pur sempre un anello della catena organizzativa: permane dunque la sottovalutazione degli attacchi provenienti dall'interno, sia di quelli casuali sia di quelli volti a compiere atti fraudolenti.

GLOSSARIO

Antivirus	Applicazione utilizzata per l'identificazione e l'eventuale rimozione di codici maligni. *Paragrafo 3.3*
Applicazioni (o software applicativi)	Un programma o un insieme di programmi in grado di funzionare su un computer. *Paragrafo 3.2*
Back-up	Copia di riserva di un disco, di uno o più file o cartelle su supporti di memorizzazione diversi da quello in uso. *Paragrafo 3.1*
Codice maligno (malware)	Un codice maligno è un software creato con l'unico scopo di causare danni o al computer su cui viene eseguito o indirettamente all'utente che usa tale computer. *Paragrafo 3.3*
Danni diretti	È il danno dovuto all'azione diretta della minaccia. *Paragrafo 2.2*
Danni indiretti	È il danno dovuto all'azione indiretta della minaccia (es. danno di immagine). *Paragrafo 2.2*
Disponibilità	Uno dei tre parametri della sicurezza delle informazioni. Significa garantire che le informazioni siano sempre disponibili quando c'è la necessità. *Paragrafo 1.1*
Download	*In generale s'intende il trasferimento di dati dalla "rete" (locale o Internet) al computer locale. Paragrafo 2.1 e 3.1*
Firewall	Ossia un dispositivo, hardware o software che analizza i dati entranti ed uscenti da una rete o un computer e viceversa applicando delle regole che contribuiscono alla sicurezza. *Paragrafo 3.3*
https	Protocollo che viene utilizzato per garantire trasferimenti riservati di dati nel web, in modo da impedire intercettazioni dei contenuti. *Paragrafo 3.6*
Integrità	Uno dei tre parametri della sicurezza delle informazioni. Significa evitare che le informazioni possano essere modificate, cancellate o spostate. *Paragrafo 1.1*
Minaccia	Sono entità (individui, eventi, ecc.) capaci di causare un danno. Normalmente sono suddivise in minacce di tipo informatico, fisico o organizzativo. *Paragrafo 2.1*
Nome utente (username)	Definisce il nome con il quale l'utente viene riconosciuto da un computer, da un programma o da un server. *Paragrafo 3.7*
Password	È una sequenza di caratteri alfanumerici utilizzata per accedere in modo esclusivo ad una risorsa informatica. *Paragrafo 3.7*

Phishing ("pharming", "tabnapping", "smishing")	Tipologia di frode in cui l'utente viene raggirato facendogli credere di interagire (telematicamente) con un interlocutore fidato quando invece sta comunicando i propri dati riservati ad un criminale. *Paragrafo 3.6*
Riservatezza	Uno dei tre parametri della sicurezza delle informazioni. Significa evitare che persone, volontariamente o involontariamente, possano accedere a una o più informazioni senza che ne abbiano l'autorizzazione. *Paragrafo 1.1*
Scansione (antivirus)	Azione che può compiere il programma per rilevare un codice maligno dai sistemi. *Paragrafo 3.3*
Sistema Informatico	La parte del sistema informativo che fa uso di tecnologie informatiche come i computer, i programmi, Internet, ecc. *Paragrafo 1.1*
Sistema Informativo	Un sistema informativo comprende tutte le informazioni utilizzate dall'azienda, inclusi i supporti che le contengono, gli strumenti che permettono di crearle, modificarle, cancellarle o trasmetterle, incluse le persone, che sono "fonti di informazioni" e contemporaneamente i gestori del sistema stesso. *Paragrafo 1.1*
Sistema Operativo	È il software sul quale si appoggiano gli altri software e che permette di far funzionare tutti i dispositivi. *Paragrafo 3.2*
Social Network on-line	Reti sociali che nascono e si sviluppano su Internet, di cui la più famosa è Facebook. *Paragrafo 3.4*
Spam	È l'invio di grandi quantità di messaggi indesiderati (generalmente commerciali). Può essere messo in atto attraverso qualunque media, ma il più usato è Internet, attraverso l'e-mail. *Paragrafo 3.5*
UPS o gruppo di continuità	Un'apparecchiatura che si usa per mantenere costantemente alimentati elettricamente apparecchi elettrici. *Paragrafo 3.1*
Vulnerabilità	Punti deboli di un sistema che possono essere sfruttati dalle minacce per causare un danno. *Paragrafo 2.1*

BIBLIOGRAFIA

"Computer Crime"	Strano Marco, Apogeo, 2000
"ICT a tutela della persona. Un approccio giuridico ai reati informatici"	Emanuele Florindi, Franco Angeli, 2005
it.wikipedia.org	*per parte delle definizioni e il glossario*

RegioneLombardia

Ciò che differenzia positivamente la Lombardia rispetto alle altre regioni italiane è il suo primato nel settore della ricerca e innovazione. Leader nazionale del settore, conta 12 università, 1 scuola superiore universitaria e più di 600 centri di ricerca e trasferimento tecnologico registrati nel sistema regionale QuESTIO (www.questio.it).

Gli obiettivi dell'amministrazione di Regione Lombardia in questo settore comprendono la promozione della ricerca, dell'innovazione e del trasferimento tecnologico come fattori strategici per lo sviluppo di un sistema economico, competitivo e moderno al fine di favorire l'incontro tra la domanda di innovazione espressa dal mondo delle imprese e la risposta del sistema della ricerca.

Per attuare questa strategia, Regione Lombardia punta sulla ricerca e l'innovazione per attrarre e facilitare l'insediamento di attività produttive ad alto valore aggiunto, valorizzare le risorse umane e il reclutamento di giovani talenti e favorire gli investimenti delle imprese e enti di ricerca in innovazione e sviluppo in modo da creare un contesto favorevole e armonico che incoraggia lo scambio di tecnologie e coniuga la conoscenza, lo studio e l'intelligenza con la manualità e il saper fare, elemento alla base dello sviluppo di alte e innovative tecnologie non presenti sul mercato.

Principali azioni attivate da Regione Lombardia nel settore della Ricerca e Innovazione sono l'emanazione di bandi per sostenere la realizzazione di progetti di ricerca innovativi nei settori prioritari e strategici (individuati nell'allegato A alla DGR IX/1817 dell'8/6/2011) e di promozione della cooperazione scientifica tecnologica anche internazionale, il sostegno alla nascita di nuove imprese (es. fondo Seed e fondo Next), accordi in addizionalità di risorse con enti istituzionali e territoriali, organismi di ricerca e regioni italiane ed estere per favorire l'innovazione e la valorizzazione del capitale umano, oltre al sostegno alla realizzazione di centri di eccellenza, ecc.

L'Unione delle Camere di Commercio della Lombardia è l'organo che riunisce e rappresenta le 12 Camere di Commercio della regione, e quindi il sistema degli interessi generali delle imprese, con l'obiettivo primario di consolidare il ruolo di protagonista della Lombardia non solo all'interno dello scenario italiano, ma anche in una dimensione Europea.

La mission di Unioncamere Lombardia è infatti: "*Consolidare sul territorio lombardo – attraverso l'azione delle Camere di Commercio – politiche e prassi favorevoli alla crescita del sistema delle imprese al fine di consolidare la leadership della Lombardia nel processo di integrazione europeo*".

La Giunta Esecutiva è costituita da Francesco Bettoni, Presidente della Camera di Commercio di Brescia e da ottobre 2004 Presidente di Unioncamere Lombardia, affiancato dal Vice Presidente Vicario Paolo De Santis (Presidente Camera di Commercio di Como) e dai due Vice Presidenti Gian Domenico Auricchio (Presidente Camera di Commercio di Cremona) e Giovanni Paolo Malvestiti (Presidente Camera di Commercio di Bergamo).

Il sistema a rete

Unioncamere Lombardia è un nodo del sistema a rete del mondo camerale che collega in Italia:

- 105 Camere di Commercio provinciali,
- 19 Unioni Regionali,
- 144 Aziende speciali,
- 103 Camere di Conciliazione,
- 21 Laboratori chimico-merceologici,
- 74 Camere di Commercio italiane all'estero rappresentate da Assocamerestero,
- 32 Camere di Commercio italo-estere,
- 65 Eurosportelli,
- 38 Borse merci e sale di contrattazione.

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

Assintel è l'associazione nazionale di riferimento delle imprese ICT e aderisce a Confcommercio – Imprese per l'Italia.

Rappresenta le imprese associate presso autorità, enti ed istituzioni nazionali ed internazionali, ne tutela gli interessi e si fa portavoce delle loro esigenze.

Assintel rappresenta l'ICT sull'intero territorio nazionale attraverso accordi diretti con le associazioni territoriali di Confcommercio, per portare concretamente le iniziative e i servizi alle migliaia di piccole e medie aziende che operano nel settore.

A livello confederale, Assintel fa parte del Consiglio Generale di Confcommercio e ne presiede la Commissione Innovazione e Servizi.

L'associazione interpreta, traduce e comunica le esigenze dell'ecosistema di partnership composto da operatori globali e locali che operano su tutto il territorio nazionale e nei diversi segmenti del mercato ICT, ed è impegnata a mettere in contatto concretamente domanda e offerta, stimolando un approccio empatico alle esigenze del mercato e sollecitando una comunicazione adeguata al target di riferimento.

L'associato è al centro della mission di Assintel, l'anima e il motivo stesso di esistere dell'associazione: dall'associato e dalle sue esigenze nascono i programmi e i servizi di Assintel.

Fare parte di una associazione di categoria è strumento fondamentale per consentire all'azienda di entrare in un network di imprese con gli stessi obiettivi ed esigenze, di avere una posizione più forte sul mercato, di usufruire di canali privilegiati di accesso alle risorse e ai finanziamenti, di far sentire la propria voce sui tavoli di discussione più importanti del settore.

Cuore dell'offerta di Assintel sono la gamma di servizi per l'azienda - attraverso la collaborazione delle strutture territoriali - e soprattutto lo sviluppo di iniziative strategiche per il mercato ICT.
L'intensa attività eventistica, le ricerche e le analisi di scenario, gli incontri territoriali di networking, la presenza istituzionale a prestigiosi eventi e fiere di settore, i progetti in collaborazione con le Istituzioni, la formazione finanziata, le convenzioni, i gruppi di lavoro settoriali sono solo alcune delle iniziative che Assintel sviluppa per i propri associati.

LA SICUREZZA DELLE INFORMAZIONI

STRUMENTI E SOLUZIONI PER LE PMI