



Data Security

Soluzioni per l'e-Security

Data Security
Divisione di Swisstech Srl
swiss⁺tech
Piazza del Cristo 12
33170 Pordenone PN
P. IVA: 01569950932
REA: PN87022
<http://www.datasecurity.it>

Laboratorio e Ricerca
Via Leopardi 3
33085 Maniago PN

Telefono 0434 28500
Fax 0434 1851018



Indice

1.	PROFILO DI DATA SECURITY	3
1.1	MISSION	4
1.2	INIZIATIVE CULTURALI	4
1.3	I NOSTRI PARTNER	5
2.	ISPE - INFORMATION SECURITY PROCESS ENHANCEMENT	6
3.	I SERVIZI DI E-SECURITY CONSULTING	7
3.1	REDAZIONE E AGGIORNAMENTO DPS	8
3.2	SECURITY POLICY E PROCEDURE OPERATIVE	11
3.3	SECURITY CHECK-UP	13
3.4	RISK ASSESSMENT	13
3.5	PROCESS SECURITY REVIEW	14
3.6	BUSINESS CONTINUITY E DISASTER RECOVERY PLANNING	14
3.7	BUSINESS IMPACT ASSESSMENT	14
4.	FORMAZIONE E-SECURITY	15
4.1	E-SECURITY WORKSHOP	16
4.2	PRIVACY E SICUREZZA PER LA PUBBLICA AMMINISTRAZIONE	18
4.3	CORSI SULL'OPEN SOURCE	20
4.4	E-SECURITY TUTORIAL	20
5.	MANAGED SECURITY	22
6.	INTERNET SECURITY	23
6.1	OTTIMIZZARE L'ACCESSO A INTERNET	23
6.2	PROTEGGERE IL WEB	24
7.	SICUREZZA DELLE RETI	25
7.1	PROTEZIONE PERIMETRALE	26
7.3	SECURITY TEST	27
7.4	NETWORK SECURITY AUDIT	28
8.	AUTENTICAZIONE E CONTROLLO DEGLI ACCESSI	29
9.	DISASTER RECOVERY	30

1. Profilo di Data Security

Data Security è una società formata da un team di esperti di e-Security e di problematiche organizzative e tecnologiche che si occupa di gestione della sicurezza a 360 gradi, a partire dall'analisi del rischio fino all'implementazione di sofisticate soluzioni tecnologiche.

- Ciò che distingue in maniera significativa Data Security è la capacità di padroneggiare e integrare le componenti organizzative, normative, tecnologiche e di processo per realizzare soluzioni realmente efficaci e in sintonia con l'organizzazione e i sistemi aziendali.
- Una corretta gestione del rischio informativo richiede infatti una serie di analisi approfondite e lo studio di soluzioni il cui effetto può essere garantito solo da consulenti esperti. Queste analisi, correlate a progetti di ambito prettamente informatico, consentono di adottare le soluzioni più adeguate alle esigenze del cliente e di mitigare l'impatto sui processi produttivi già in atto.
- Analisi del rischio informatico e studio delle priorità di intervento.
- Test e Certificazione dei Sistemi e delle procedure di Sicurezza.
- Consulenza legale, tecnica e organizzativa su Sicurezza, Privacy, Autenticazione, Firma Digitale e Business Continuity.
- Formazione qualificata e sensibilizzazione sulle problematiche della sicurezza di personale e dirigenti.
- Audit e Assessment di Sicurezza.
- Test di vulnerabilità dei sistemi informatici dall'esterno e dall'interno della rete.
- Definizione delle politiche per la Sicurezza delle informazioni.
- Consulenza dedicata alla Pubblica Amministrazione per la redazione e l'aggiornamento del Documento Programmatico sulla Sicurezza, per lo sviluppo del sistema di gestione della sicurezza e per l'implementazione di Firma Digitale, Carta del Cittadino e Carta di identità elettronica.
- Progettazione di sistemi di Storage, Disaster Recovery e Business Continuity.

Oltre a ciò Data Security è in grado di fornire, attraverso i suoi partner, le migliori soluzioni tecnologiche per la Sicurezza informatica e di integrarle con i sistemi esistenti.

1.1 Mission

Data Security offre ai propri clienti un insieme di servizi per il miglioramento della sicurezza che comprendono:

- Attività di Consulenza per identificare in modo analitico la dimensione e la tipologia dei rischi e le priorità di intervento;
- Studi di Fattibilità per soluzioni di sicurezza;
- Implementazione di soluzioni di sicurezza informatica integrate con i sistemi informatici esistenti;
- Test e Certificazione dei sistemi di sicurezza;
- Formazione altamente qualificata sia per il personale tecnico che per il management.

Questo approccio consente di rispondere con competenza e professionalità anche alle esigenze di sicurezza più specifiche e personalizzate, rispettando al contempo le esigenze aziendali di ottimizzazione delle risorse e di rispetto di tempi e costi.

1.2 Iniziative culturali

Per la crescita dell'importanza e dell'affidabilità delle attività che fanno uso di Internet è importante la creazione e la diffusione di una vera e propria cultura della sicurezza.

La conoscenza delle problematiche di e-Security, la formazione di professionisti e un'informazione puntuale e obiettiva a tutti i livelli sono le chiavi per far comprendere agli operatori l'importanza strategica della sicurezza digitale e far crescere nel tempo le possibilità di operare in rete con maggiore tranquillità.

Data Security costituisce un punto di riferimento non solo per le aziende che si avvalgono dei suoi servizi, ma anche per il mondo accademico e culturale, grazie alla continua attività di formazione e informazione, quali la collaborazione con Istituti di ricerca universitari, l'organizzazione di eventi e convegni sui temi della e-Security, la sponsorizzazione di progetti che si propongono di diffondere la cultura della sicurezza.



Tra questi, di particolare rilievo è la collaborazione con il prestigioso **SANS Institute** con il quale, nell'ottica di una diffusione capillare della cultura e dei temi cardine che riguardano la sicurezza informatica, Data Security ha curato la versione italiana del fondamentale documento su "**Le venti vulnerabilità più critiche della sicurezza in Internet**".

Data Security, inoltre, ha sponsorizzato il progetto **Security Flop**, che si occupa di rilevare e segnalare le violazioni e le intrusioni compiute ai danni dei siti Web.

SecurityFlop è utile a tutti coloro che operano nell'e-business per ottenere informazioni sempre aggiornate riguardo le novità nel settore della sicurezza digitale e per verificare quotidianamente il rischio che corrono tutti i siti web e i sistemi collegati ad Internet, in particolare quelli che non dispongono di sistemi di sicurezza adeguati ad affrontare gli attacchi sempre nuovi che arrivano dalla rete mondiale.

1.3 I nostri partner

Chi si occupa di sicurezza informatica sa bene che il campo in cui si opera è così vasto e complesso che per offrire soluzioni realmente efficaci è necessario integrare tecnologie diverse, combinando in modo intelligente i migliori prodotti e le migliori soluzioni disponibili sul mercato. Per questa ragione Data Security ha stretto una serie di partnership strategiche con alcuni leader mondiali nel campo della sicurezza informatica, quali:

**Trust Italia – VeriSign**

Leader mondiale per la certificazione digitale;

**Ubizen**

Uno dei più importanti produttori di soluzioni e-Security e nella gestione in outsourcing di servizi di sicurezza;

**GemPlus**

Primi al mondo nello sviluppo di applicazioni basate su tecnologia Smart Card;

**nCipher**

Azienda leader nei sistemi di protezione crittografica;

**Nayatek**

Messaging Security, Management e Archiving solutions

**Qualys**

leader mondiale nei sistemi di security audit e nei test di sicurezza.

**Astaro**

Firewall - Virus Protection - VPN Content Filtering -
Intrusion Protection - Spam Protection

Grazie all'apporto dei propri partner e alla competenza dei suoi esperti, le tecnologie di protezione e i sistemi organizzativi proposti da Data Security sono sempre all'avanguardia fra le soluzioni di sicurezza disponibili sul mercato.

2. ISPE - Information Security Process Enhancement

Sviluppato da Data Security assieme ai propri partner tecnologici, ISPE è il modello di riferimento per la progettazione e la gestione dei processi di miglioramento della sicurezza informatica nella media e nella grande azienda.

Studiato come processo ciclico, ISPE si articola in sei moduli che permettono la gestione completa del problema sicurezza, dall'analisi dei rischi fino all'implementazione di soluzioni tecnologiche e organizzative.

I clienti che si avvalgono della metodologia ISPE sono sempre affiancati dagli esperti di Data Security, che forniscono un supporto immediato a partire dalle fasi iniziali, in modo da identificare le priorità e indirizzare le azioni e le scelte che verranno fatte successivamente.

Grazie all'approccio ISPE, le aziende che si affidano a Data Security hanno la certezza del fatto che i loro investimenti saranno integrati in un progetto organico di miglioramento della sicurezza, che consente:

Un supporto puntuale nella fase decisionale in materia di e-Security;

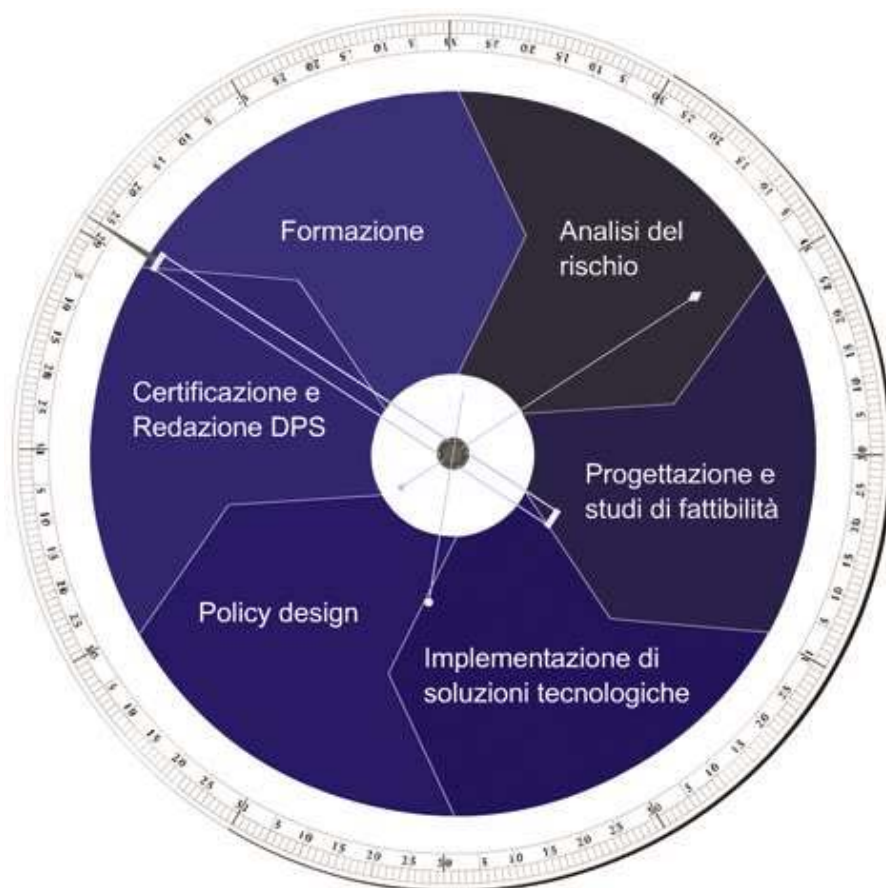
L'ottimizzazione degli interventi, con notevoli risparmi di costo;

La corretta integrazione di prodotti e tecnologie provenienti da diversi vendor;

La possibilità di monitorare costantemente il proprio livello di sicurezza e di programmare con criteri analitici gli investimenti;

Una copertura a 360 gradi di tutte le problematiche della sicurezza informatica;

La certezza di lavorare con un solido interlocutore di fiducia, oggi e domani.



3. I servizi di e-Security Consulting

I servizi di e-Security Consulting rispondono alla necessità di analizzare e valutare in maniera professionale le varie situazioni aziendali nei confronti della sicurezza, al fine di individuare e mettere in pratica le soluzioni più adeguate.

Spesso le soluzioni più efficaci non sono costituite da componenti esclusivamente tecnologiche, ma richiedono l'implementazione e il coordinamento di componenti organizzative, tecnologiche e di processo.

Per questo Data Security ha creato i servizi di e-Security consulting, mettendo a disposizione professionisti che assieme alle competenze tecnologiche specifiche possiedano la capacità di "pensare per processi" e di interagire con tutti i livelli dell'organizzazione aziendale.

Per valutare la natura e l'entità del rischio a cui è soggetta l'azienda, per stabilire quali siano i punti maggiormente critici del sistema informativo e dei processi aziendali, per determinare con quali strumenti organizzativi, tecnologici e di processo è possibile indirizzare tali criticità, sono necessarie attente analisi condotte da consulenti esperti e preparati.

Il team di consulenti di Data Security ha sviluppato una serie di competenze per rispondere a queste problematiche e individuare in maniera efficiente le soluzioni più adeguate. L'utilizzo di metodologie, tecniche e strumenti collaudati e consolidati assicura un approccio al tempo stesso pragmatico e rigoroso.

- **Redazione e aggiornamento DPS**
Per la stesura o l'aggiornamento del Documento Programmatico sulla Sicurezza introdotto dall'articolo 6 del DPR 318/99, un'attività che richiede esperienza e competenze specifiche, senza le quali si corre il rischio di ridurre l'operazione ad un'inutile attività burocratica.
- **Redazione di Security policy e procedure operative**
Nella maggioranza dei casi per accrescere la sicurezza di un sistema informatico non è sufficiente un intervento di tipo tecnologico, ma è necessario realizzare o aggiornare le policy organizzative.
La competenza di Data Security e l'esperienza anche a livello di ricerca universitaria acquisite dal suo staff permettono di disegnare policy efficaci, che al tempo stesso non appesantiscono i processi e la gestione delle informazioni nell'azienda.
- **Security check-up**
Una serie di analisi per individuare rapidamente le aree di macro-criticità e di maggior rischio per indirizzare e gestire tempestivamente le situazioni più critiche e focalizzare eventuali analisi successive.
- **Risk assessment**
Per individuare analiticamente tutte le aree di criticità proponendo per ciascuna un ventaglio di raccomandazioni e di soluzioni.
- **Process Security review**
Una serie di analisi che permettono di individuare analiticamente le aree e gli aspetti di criticità nell'ambito di un ben preciso processo aziendale.
- **Business Continuity planning**
Per prevenire e limitare le interruzioni alle normali attività di business a fronte di eventi particolari.

- **Business Impact Assessment**
Analisi per l'identificazione delle risorse critiche, l'assegnazione delle priorità ai processi di business e la stima delle eventuali perdite in termini quantitativi e qualitativi dovuta a interruzione dei processi critici.

3.1 Redazione e aggiornamento DPS

Il 1° Gennaio 2004 è entrato in vigore il nuovo codice sulla Privacy che richiede l'implementazione delle Misure minime di sicurezza, ovvero quelle misure disposte dal nuovo codice che differiscono dalle indicazioni del vecchio Dpr. 318/99.

Le nuove misure sono molto più stringenti di quelle previste dalla vecchia normativa, in particolare nei confronti dei profili di autorizzazione, dei sistemi di autenticazione, delle procedure di ripristino dell'accesso ai dati in caso di danneggiamento degli stessi e delle regole organizzative e della formazione degli Incaricati.

Con le nuove norme, il DPS diventa un obbligo per tutte le organizzazioni, pubbliche e private, che trattano dati sensibili con l'uso di strumenti elettronici, anche se questi ultimi non sono collegati a una rete pubblica. Il che significa che è sufficiente che dei dati sensibili risiedano su un singolo PC, anche se questo non è collegato ad alcuna rete, perché il DPS diventi obbligatorio.

Viene inoltre fissato una scadenza per la redazione e l'aggiornamento, che devono essere effettuati entro il 31 marzo di ogni anno.

Il punto 19 del Disciplinare tecnico prescrive che il DPS debba contenere idonee informazioni riguardo:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

- Oltre ad essere un obbligo di legge, il DPS ha anche una importante funzione interna di guida alla adozione ed al miglioramento delle misure di sicurezza: è quindi opportuno concepirlo come un vero e proprio piano per la sicurezza, estendendo il suo contenuto a tutti gli aspetti legati a tale problematica, che vanno anche oltre gli elementi obbligatori prescritti dal disciplinare tecnico.

Il DPS costituisce, inoltre, il punto di partenza per definire interventi e strategie per la sicurezza dei dati, perché permette di verificare il livello della sicurezza informatica e quindi di identificare subito le aree maggiormente a rischio. La specificità delle strutture nei diversi soggetti fanno sì che il DPS non sia un documento uguale per tutti, ma il frutto di una valutazione specifica da parte delle singole aziende, congiuntamente ai propri consulenti.

Certo è che la stesura del Documento Programmatico sulla Sicurezza è un'attività che richiede esperienza e competenze specifiche, senza le quali si corre il rischio di ridurre l'operazione ad un'inutile attività burocratica. Data Security, grazie alla competenza dei suoi consulenti e a una esperienza consolidata in decine di DPS in aziende e enti pubblici, può garantire il supporto in tutte le fasi di redazione, aggiornamento e certificazione del Documento Programmatico sulla Sicurezza.

E se, come spesso accade, nella fase di verifica viene riscontrata la necessità di provvedimenti urgenti, Data Security è attrezzata a fornire soluzioni chiavi in mano in grado di assicurare a pieno il rispetto dei requisiti di legge e gli standard internazionali per la sicurezza informatica.

L'ORGANIZZAZIONE DELLA PRIVACY

La prima e più urgente misura di sicurezza è quindi quella di carattere organizzativo. Il processo della sicurezza richiede infatti che, prima ancora di pensare all'adozione delle misure concrete, vengano definite una serie di compiti e procedure che regolino gli aspetti organizzativi del trattamento dei dati personali effettuato dall'Azienda.

È quindi necessario procedere preventivamente alla definizione di ruoli, compiti e responsabilità per la gestione di tutte le fasi del trattamento dei dati personali, con particolare riferimento alla necessità di garantire la loro sicurezza e alla adozione di specifiche procedure, che vadano a completare e rafforzare le contromisure tecnologiche adottate.

I consulenti Data Security possono affiancare i responsabili dell'organizzazione per la privacy all'interno dell'azienda per tutte le procedure di nomina, di approntamento di regolamenti, per la redazione di convenzioni per la comunicazione dei dati ad altre aziende private e ad enti pubblici e per stabilire le più adeguate policy di sicurezza.

LA FORMAZIONE

Il nuovo Codice sulla Privacy sancisce ancora una volta l'obbligatorietà di interventi formativi per gli incaricati del trattamento dei dati personali, già prevista dalla legge 675/96, dal D.P.R. 318/99 e dalle altre disposizioni in materia di privacy.

La legge prescrive di effettuare corsi per:

- informare gli incaricati del trattamento sui rischi che possono compromettere la sicurezza e la privacy dei dati;
- descrivere le misure di sicurezza disponibili per prevenire eventi dannosi;
- rendere edotti gli incaricati dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività;
- approfondire le responsabilità che ne derivano e le modalità per aggiornarsi sulle misure minime adottate dal titolare.

Questa formazione dovrebbe essere programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento di dati personali.

A questo scopo Data Security ha messo a punto e collaudato in diverse realtà, pubbliche e private, un **Corso per gli Incaricati del Trattamento dei dati personali** che illustra le responsabilità legate alle proprie funzioni, i rischi che minacciano i dati, le misure di sicurezza necessarie e i provvedimenti che tutte le aziende devono adottare.

Gli interventi formativi, sempre personalizzati per essere realmente coerenti con le prassi specifiche adottate in azienda, aiutano le diverse figure a conoscere meglio i rischi tipici nella gestione di dati personali e sensibili e le misure da adottare per ridurre i rischi e per ottenere un ragionevole livello di sicurezza e di privacy.

Oltre che per gli incaricati, infatti, la formazione sui temi della sicurezza e della privacy è utile anche per i Responsabili del trattamento dei dati, per i Dirigenti e gli Amministratori dell'azienda. Per queste figure sono a disposizione sessioni formative personalizzate che si focalizzano maggiormente sulle responsabilità specifiche dei ruoli dirigenziali.

3.2 Security Policy e Procedure Operative

Nella maggioranza dei casi per accrescere la sicurezza di un sistema informatico non è sufficiente un intervento di tipo tecnologico, ma è necessario realizzare o aggiornare le policy organizzative.

La competenza di Data Security e l'esperienza anche a livello di ricerca universitaria acquisite dal suo staff permettono di disegnare policy efficaci, che al tempo stesso non appesantiscono i processi e la gestione delle informazioni nell'azienda.

La pianificazione delle Policy è un'attività complessa che riguarda la definizione delle procedure di sicurezza, dei regolamenti e delle linee guida che le aziende o gli enti pubblici adottano per disciplinare al suo interno l'utilizzo di strumenti aziendali e le procedure delle diverse funzioni aziendali.

Vi sono Policy generali, rivolte cioè a tutto il personale, e Policy specifiche dedicate a regolare precisi ambiti aziendali o un numero ristretto di addetti.

La stesura di questi regolamenti deve naturalmente accordarsi con le leggi vigenti; particolare attenzione va rivolta in tal senso al rispetto delle normativa nel campo del diritto del lavoro, della regolamentazione sulla privacy e delle leggi che sanzionano i reati informatici.

Tutte le realtà pubbliche e private dovrebbero munirsi di policy adeguate per la salvaguardia della sicurezza informatica: se è vero, infatti, che l'attenzione ai rischi informatici in azienda viene il più delle volte rivolta all'esterno nei confronti dei di hacker e virus, è inconfutabile che i maggiori danni economici e in termini di immagine derivino molto più spesso da leggerezze o errori umani del personale interno dell'azienda.

Diverse ricerche hanno inoltre messo in evidenza come la mancata regolamentazione nell'utilizzo delle risorse informatiche aziendali possa comportare un innalzamento dei costi particolarmente rilevante, sia in termini di mancata produttività, sia in termini di crescita delle spese di manutenzione e di utilizzo delle risorse.

E' sufficiente fornire qualche dato per chiarire la dimensione del fenomeno e stimolare le giuste riflessioni:

- Diverse ricerche effettuate a livello internazionale hanno rivelato che, in mancanza di regole e/o strumenti tecnologici di filtraggio, una percentuale tra il 30% e il 40% del tempo impiegato on line dal dipendente viene utilizzato per fini diversi da quelli aziendali.
- Una recente indagine di Vault.com evidenzia che il 25,1% dei lavoratori dipendenti dichiara di navigare per fini personali dal posto di lavoro da 10 a 30 minuti al giorno, il 22,4% da 30 minuti ad 1 ora, l'11,9% da 1 ora a 2 e ben il 12,6% oltre 2 ore. Solo il 27% dichiara di navigare meno di 10 minuti al giorno.
- Un'indagine interna dell'Internal Revenue Service, l'ente che negli Stati Uniti si occupa delle entrate fiscali, ha rivelato che la navigazione o l'utilizzo di e-mail da parte dei lavoratori per scopi personali rappresentava il 51% del totale del tempo dedicato ad attività on line. (IRS marzo 2001)
- Più del 70% di tutto il traffico generato dai siti pornografici viene generato durante l'orario d'ufficio. (Fonte: SexTracker)
- Il 32,6% dei lavoratori che accedono ad Internet durante l'orario di lavoro dichiarano di farlo senza nessuna specifica finalità. (Fonte: eMarketer.com 2001)

E' piuttosto facile pertanto stimare quanto questi abusi nell'utilizzo aziendale di Internet costino alle imprese.

Oltre al danno patrimoniale causato dalla perdita di produttività, l'utilizzo improprio delle risorse aziendali può anche comportare problemi di carattere legale per l'azienda o per l'ente pubblico in cui si verifica. Si pensi alla violazione delle legge sul diritto d'autore, nel caso i dipendenti scarichino software o musica pirata dalla rete, o ancor peggio se le risorse dell'azienda vengono utilizzate per archiviare immagini o filmati pedo-pornografici. In questi casi il rischio legale è accresciuto nel caso che l'Autorità Giudiziaria, per condurre le proprie indagini, sia costretta a sequestrare le macchine, creando di fatto un grave pregiudizio alla regolare continuazione dell'attività dell'azienda.

Oltre alle motivazioni di carattere generale sopra elencati vi possono essere da parte dell'Azienda altre ragioni molto specifiche per dotarsi di policy aziendali per l'utilizzo delle risorse informatiche.

Di seguito ne elenchiamo alcune, così come sono state raccolte in occasione del disegno delle policy dei clienti Data Security:

- Necessità da parte dell'Azienda di prevedere e regolare l'accesso alla posta elettronica dei dipendenti senza previo assenso in determinate situazioni (ferie, emergenza, dimissioni, ecc.).
- Esigenza di informare i dipendenti sull'attività di monitoraggio del traffico di rete.
- Desiderio di accrescere l'immagine aziendale in termini di attenzione alla sicurezza e di impegno ad incentivare comportamenti premianti all'interno dell'azienda.
- Necessità di risolvere tensioni o problemi aziendali amplificati ad un utilizzo improprio della comunicazione e-mail (uso improprio delle funzioni di Carbon Copy, proteste, insulti o rivendicazioni inviati a molteplici destinatari, ecc.).
- Necessità di limitare e regolare le prerogative dell'Amministratore di Sistema per quanto concerne il monitoraggio e l'accesso ai dati personali archiviati o comunicati attraverso il sistema informatico aziendale.
- Desiderio di fornire ai dipendenti un testo semplice in cui sintetizzare i concetti e le linee guida essenziali per un uso sicuro delle risorse informatiche aziendali.

Laddove queste regole già esistano e siano attuate informalmente, la loro formalizzazione in un documento scritto e reso pubblico all'interno dell'Azienda può essere il sistema più efficace per razionalizzare l'uso di queste applicazioni, diminuendo il rischio di problemi tecnici o, peggio ancora, di abusi ed illeciti.

L'adozione di una policy scritta sull'uso delle applicazioni informatiche che consentono la comunicazione di dati personali è, inoltre, un modo per adeguarsi alle prescrizioni della legge sulla privacy, che richiede l'adozione di misure organizzative, logistiche e procedurali per garantire l'integrità e la riservatezza dei dati trattati mediante elaboratori elettronici.

3.3 Security Check-Up

Alla base di qualsiasi intervento, tecnologico o organizzativo, che miri a migliorare la sicurezza delle informazioni, si pongono una serie di analisi che individuino rapidamente le aree di macro-criticità e di maggior rischio, per indirizzare e gestire tempestivamente le situazioni più critiche e focalizzare analisi più specifiche.

L'obiettivo del servizio di Security check-up è proprio quello di individuare rapidamente (mediamente il tempo richiesto non supera una o due settimane) le aree di macro-criticità e di non-conformità, al fine di ottenere in breve tempo un primo quadro della situazione e pianificare razionalmente gli interventi e le eventuali analisi successive.

L'analisi e la valutazione del rischio viene fatta considerando una serie di parametri standard di riferimento, "pesati" tenendo conto di una serie di fattori di valutazione, tra cui il livello di sicurezza medio dell'industria alla quale appartiene l'azienda (es. banking, telecomunicazioni, industria, grande distribuzione, pubblica amministrazione, etc.).

L'output principale del servizio di Security check-up è costituito da una **quantificazione oggettiva del livello di rischio** (o di non-conformità) rispetto ai parametri standard di riferimento, con l'evidenziazione degli aspetti e delle motivazioni di maggiore criticità.

Oltre al fatto di essere breve ed efficace, il servizio di Security check-up presenta l'ulteriore vantaggio di richiedere un coinvolgimento ridotto delle risorse dell'azienda, sia in termini di tempo che di quantità di persone da intervistare: mediamente è sufficiente intervistare non più di cinque persone per produrre un'analisi significativa e sufficientemente dettagliata.

3.4 Risk Assessment

Il Risk Assessment è un'analisi approfondita che individua analiticamente le aree e gli aspetti di maggiore criticità, le aree di vulnerabilità e di non conformità agli standard di sicurezza del sistema informativo, analizzando l'adeguatezza del piano di sicurezza, delle difese perimetrali e della sicurezza applicativa.

Le analisi e le raccomandazioni sono raggruppate secondo tre dimensioni fondamentali di intervento: organizzativa, applicativa e di rete.

Durante la fase di analisi vengono precisate le caratteristiche dell'ambiente da esaminare e precisamente hardware installato, struttura delle reti, meccanismi di sicurezza, tipologia dei servizi erogati, software utilizzato.

L'output principale del servizio di Risk Assessment è costituito dal documento Security Master Plan, composto da una prima sezione che comprende una serie di report che dettagliano l'entità e la tipologia dei rischi relativi alle risorse aziendali da proteggere, e da una seconda sezione che comprende una sintesi delle criticità e delle raccomandazioni associate.

In alcuni casi l'output può comprendere una o più ipotesi di modifica/integrazione dell'architettura di rete, al fine di aumentare il livello globale di sicurezza.

3.5 Process Security Review

La Process Security Review è costituita una serie di analisi che permettono di individuare analiticamente le aree e gli aspetti di criticità nell'ambito di un ben preciso processo aziendale.

Nel corso dell'analisi sono identificati, in primo luogo, gli asset e i flussi di dati che fanno parte dei processi oggetto dell'analisi; questi vengono inseriti in uno schema che identifica e ne chiarisce le interdipendenze.

Andranno identificate quindi le minacce che possono mettere a rischio i processi e determinati gli impatti di eventuali compromissioni della confidenzialità, dell'integrità e della disponibilità dei dati in oggetto.

Per ciascuna criticità individuata vengono proposte una o più raccomandazioni, assieme ed eventuali ipotesi di modifica/integrazione dell'architettura di rete.

La Process security review permette di concentrare gli sforzi e le risorse sugli aspetti (processi) prioritari, e spesso fornisce degli spunti per la rivisitazione del processo, non solo in termini di sicurezza.

3.6 Business continuity e Disaster recovery planning

La continuità del servizio anche in situazioni critiche e il ripristino delle capacità di comunicazione e di elaborazione delle informazioni sono oggi più che mai importanti.

Il servizio di Business Continuity e di Disaster Recovery planning è tipicamente costituito da una serie di piani di intervento e di misure di contingenza da adottare in situazioni di emergenza o comunque anomale.

3.7 Business Impact assessment

Il Business Impact Assessment è una analisi finalizzata alla identificazione delle risorse critiche, all'assegnazione delle priorità ai processi di business e alla stima delle eventuali perdite in termini quantitativi e qualitativi dovuta a interruzione dei processi critici. Consiste nella valutazione del livello e della tipologia di rischi rispetto al settore di business e all'organizzazione delle attività condotte in azienda.

L'attività può venire svolta avendo come ambito l'intera azienda oppure uno specifico processo di business.

Molto frequentemente le analisi e le raccomandazioni prodotte nel corso della Business Impact Analysis servono come input per una successiva attività di **Business Continuity planning** e di **Risk assessment**.

4. Formazione e-Security

La formazione e il continuo aggiornamento sono elementi fondamentali per qualsiasi attività di miglioramento della sicurezza informatica.

Data Security prevede ogni anno investimenti continui per mantenere sempre aggiornata la preparazione del proprio personale a tutti i livelli.

Se l'importanza della formazione è universalmente riconosciuta, perché questa sia realmente efficace e abbia un impatto reale nei processi aziendali è importante determinare, di volta in volta, le metodologie più adatte alla realtà in cui si opera.

Data Security ha sviluppato un insieme di metodologie e di moduli formativi per rispondere a queste domande ed aiutare l'azienda ad accrescere il proprio livello educativo nel campo della sicurezza informativa e dell'organizzazione aziendale.

Il team di Data Security per la formazione conta su docenti con lunga esperienza accademica e di attività di formazione aziendale. Gli esperti che interverranno nella vostra azienda sono gli stessi che partecipano come relatori ai più prestigiosi Convegni e Workshop sulla sicurezza informatica in Italia e nel Mondo.

- **e-Security workshop**

Il corso sviluppato da Data Security rivolto a tutto il personale che utilizza gli strumenti informatici che prevede una formazione intensiva sui concetti guida della sicurezza e sulle metodologie da adottare limitare i rischi in azienda.

Suddiviso in diversi moduli per incontrare le esigenze di realtà aziendali di qualsiasi dimensione, e-Security Workshop prevede anche strutturazioni specifiche per dirigenti e IT manager.

- **Privacy e sicurezza nella Pubblica Amministrazione**

Nell'ambito delle iniziative legate alla Sicurezza, e in ottemperanza a quanto prescritto a termini di legge dal nuovo codice sulla Privacy, la formazione è strumento fondamentale per una corretta gestione delle tematiche legate alla sicurezza e alla privacy.

Data Security ha sviluppato diversi moduli formativi per il personale della Pubblica Amministrazione che forniscono la preparazione adeguata alla mansione, al ruolo e alla responsabilità di ciascuna figura dell'ente.

- **Corsi sull'Open Source**

Molte realtà pubbliche e private stanno valutando l'opportunità di adottare software Open Source come possibile soluzione per una significativa riduzione dei costi e della complessità gestionale.

Di fronte a questo scenario, chi debba fare investimenti e scelte strategiche in merito all'adozione di piattaforme IT, si trova di fronte al dilemma di come approfittare delle opportunità senza compromettere la qualità dei servizi erogati.

Perché se è vero che l'utilizzo di Unix e del software open source può rappresentare una svolta, è altrettanto vero che vi sono numerosi casi di fallimenti e delusioni, in cui alla fine i costi totali, così come la complessità applicativa e gestionale, sono aumentati.

- **e-Security Tutorial**

Il modulo e-Security Tutorial risponde all'esigenza diffusa di creare programmi per la crescita della percezione del rischio informatico in azienda.

Si tratta di un modulo di autoapprendimento e di verifica che può essere implementato su un supporto multimediale (Cd-Rom, DVD) o, meglio ancora, come modulo da inserire nella Intranet aziendale esistente.

Oltre a corsi elencati, Data Security sviluppa anche programmi di awareness mirati alle specifiche esigenze dell'azienda, effettuando anche valutazioni analitiche sul livello di conoscenza e di vigilanza preesistente in azienda.

4.1 e-Security Workshop

Il corso sviluppato da Data Security rivolto a tutto il personale che utilizza gli strumenti informatici che prevede una formazione intensiva sui concetti guida della sicurezza e sulle metodologie da adottare limitare i rischi in azienda.

Suddiviso in diversi moduli per incontrare le esigenze di realtà aziendali di qualsiasi dimensione, e-security workshop prevede anche strutturazioni specifiche per dirigenti e IT manager.

E-security workshop è un corso introduttivo il cui target è volutamente molto ampio; si spazia dal responsabile dei sistemi informativi al manager al capo progetto. Per il taglio allargato e introduttivo della trattazione, i partecipanti non devono essere necessariamente limitati al settore Information Technology, ma possono includere rappresentanti delle più disparate funzioni aziendali (ad esempio: Affari legali, Gestione frodi, Responsabili outsourcing, Direzione acquisti, Affari generali, Human resources, etc.).

Il corso mira a creare consapevolezza aziendale in merito alla problematica della sicurezza, introducendo una serie di tematiche chiave e collegandole il più possibile alla specifica realtà aziendale, in modo da suscitare interesse e curiosità. Far capire come la sicurezza non sia un optional, ma sia una necessità ed una priorità aziendale. Far capire come la sicurezza non sia semplicemente uno strumento, ma un processo trasversale da gestire nella sua globalità e nelle sue implicazioni organizzative, normative e tecnologiche.

E' accertato infatti che il livello complessivo della sicurezza informatica in un'azienda, proprio come in una catena, è condizionato dal grado di resistenza dell'anello più debole. Le vulnerabilità dell'intero sistema non dipendono solo da inadeguatezze di tipo tecnologico, ma più spesso derivano da scarsa preparazione degli utenti o dalla difficoltà degli amministratori dei sistemi nel riuscire a trovare il tempo e allocare le risorse umane necessarie ad affrontare le urgenze quotidiane create dalle nuove vulnerabilità scoperte o dalle esigenze dei propri utenti.

Il corso di **e-Security workshop** permette di:

- accrescere le conoscenze di base del management nel campo della sicurezza informatica;
- ridurre il carico di lavoro degli amministratori di sistema grazie alla mole minore di richieste di supporto da parte degli utenti;
- minimizzare i rischi di attacchi di tipo social engineering;
- aumentare il livello di consapevolezza dell'importanza della sicurezza informatica nell'universo aziendale;
- favorire il passaggio a nuove tecnologie di protezione delle informazioni, facendo in modo che tutto il personale partecipi alla transizione;

- comprendere le molteplici implicazioni legali e relative responsabilità connesse alla sicurezza informatica.

Suddiviso in diversi moduli per incontrare le esigenze di realtà aziendali di qualsiasi dimensione, e-Security Workshop prevede anche strutturazioni specifiche per dirigenti e IT manager.

e-Security Workshop per dirigenti

L'e-Security Workshop per dirigenti si articola in una serie di sessioni di lavoro organizzate con la finalità di analizzare le specifiche problematiche di sicurezza a livello macro-aziendale e di vagliare le differenti opzioni in termini di strategie organizzative.

I quattro obiettivi principali del workshop sono:

- Consentire al dirigente di capire il livello di rischio del proprio patrimonio informativo. L'intento è di far emergere quelle aree grigie di rischio - che comunemente interessano tutte le aziende medio grandi in Italia - quali i rischi di furto o diffusioni non autorizzate di informazioni, spionaggio industriale, frode contabile, utilizzo abusivo delle risorse informatiche, furti di hardware e software, ecc.
- Discutere i diversi modelli di organizzazione della sicurezza informatica (outsourcing/organizzazione interna/mix) e fornire gli strumenti per la razionalizzazione ed organizzazione della security in campo informatico. L'obiettivo è di fornire una rassegna dei modelli di e-Security più diffusi e di evidenziarne potenzialità e limiti in base alle specificità dell'azienda cliente.
- Consigliare una metodologia per la scelta dei manager chiave della sicurezza IT e per l'acquisto di nuovi sistemi di sicurezza informatici. La selezione degli uomini chiave della sicurezza informatica, ancora prima della scelta delle tecnologie, risulta un fattore fortemente strategico che come tale va opportunamente pianificato.
- Fornire al dirigente un supporto per colmare il gap conoscitivo con i tecnici responsabili della sicurezza IT. Un ultimo obiettivo, ma non meno importante, è di permettere ai dirigenti di riappropriarsi del proprio ruolo organizzativo anche nel settore ultra specialistico come quello della e-Security, attenuando, per quanto possibile, il gap conoscitivo esistente tra essi ed i tecnici responsabili per la sicurezza.

Il corso di e-security per dirigenti permette quindi di:

- stimare il valore delle informazioni per capire l'importanza dei principi di integrità, autenticità, confidenzialità e non ripudiabilità;
- conoscere i principali modelli organizzativi esistenti per la gestione del rischio informatico;
- individuare i rischi informatici in base alla probabilità che si verifichino e alla gravità delle conseguenze;
- prevenire degli illeciti informatici e dei danneggiamenti dovuti ad azioni imprudenti;
- riconoscere il ruolo fondamentale di ogni utente nel preservare la sicurezza informatica dell'azienda: le 10 azioni da ricordare e le 10 condotte da evitare;
- creare policy aziendali per la sicurezza informatica;

- colmare, almeno in parte, il gap tecnologico fra tecnici e manager per gestire al meglio i processi di miglioramento nel campo della sicurezza informatica;
- identificare responsabilità precise e individuare i responsabili;
- individuare i molteplici aspetti legali connessi alla sicurezza informatica;
- identificare e prevenire gli attacchi di social engineering;
- affrontare in maniera corretta degli incidenti e delle procedure di disaster recovery;
- gestire i rapporti con l'autorità pubblica in caso di reati informatici.

e- Security workshop per IT manager

L'e-security workshop per IT manager è un corso tecnico il cui target è rappresentato dal personale del settore ICT, con particolare riguardo ai responsabili della sicurezza informatica.

Il workshop è infatti organizzato per approfondire sia dal punto di vista tecnico che da quello criminologico ed organizzativo le tematiche riguardanti le violazioni della sicurezza informatica.

L'intento è fornire uno scenario quanto più dettagliato possibile per permettere agli IT manager di comprendere quali siano le evoluzioni presenti nel mondo della sicurezza IT e di orientarsi di conseguenza in termini di organizzazione interna e di acquisto di nuove tecnologie di protezione.

Gli obiettivi del workshop sono quindi di rendere i partecipanti in grado di:

- possedere una conoscenza approfondita sul fenomeno della criminalità informatica con particolare riferimento alla individuazione di trend e futuri profili di rischio. Conoscere le tecnologie e le soluzioni di sicurezza che si stanno imponendo sul mercato e le più recenti innovazioni tecnologiche del settore; conoscere le più diffuse e pericolose tecniche di hacking;
- effettuare analisi che tengano conto del rapporto costi/benefici nell'ambito delle soluzioni di sicurezza informatica da adottare. In particolare, viene proposto un modello di valutazione e stima dei progetti di sicurezza informatica utile a determinare e spiegare l'utilità e il valore di un progetto di miglioramento della sicurezza in un Consiglio di Amministrazione;
- conoscere le migliori ed affidabili risorse informative disponibili in rete;
- apprendere l'uso delle metodologie di Risk Assessment;
- essere in grado di comunicare in modo semplice e di convincere il management sulle reali necessità dell'IT department in termini di sicurezza;
- conoscere i processi di verifica e di certificazione della sicurezza informatica.

Il programma dettagliato del workshop è concordato di volta in volta in accordo con le specifiche esigenze del cliente.

4.2 Privacy e sicurezza per la Pubblica Amministrazione

Il nuovo Codice sulla Privacy sancisce ancora una volta l'obbligatorietà di interventi formativi per gli incaricati del trattamento dei dati personali, già prevista dalla legge 675/96, dal D.P.R. 318/99 e dalle altre disposizioni in materia di privacy, identificando la formazione come

strumento fondamentale per una corretta gestione delle tematiche legate alla sicurezza e alla privacy.

Data Security ha sviluppato diversi moduli formativi per il personale della Pubblica Amministrazione che forniscono la preparazione adeguata alla mansione, al ruolo e alla responsabilità di ciascuna figura dell'ente.

Nel corso delle sessioni formative vengono trasmessi e condivisi alcuni concetti fondamentali riguardanti:

- i rischi tipici che si possono presentare, in termini di sicurezza e privacy, nella gestione di dati personali operata da un Ente pubblico;
- le misure da adottare per ridurre al minimo i rischi e per ottenere un ragionevole livello di sicurezza e di privacy, in ottemperanza con quanto prescritto dalla normativa vigente;
- le norme legislative del nuovo codice Privacy (responsabilità delle diverse figure introdotte dalla legge, regolamenti di attuazione, provvedimenti giuridici) e dell'allegato B "Disciplinare tecnico in materia di misure minime di sicurezza";
- indicazioni su PKI, firma digitale, sistemi di e-government.

Con la collaborazione dell'Ente vengono individuate le tipologie di risorse da formare in funzione delle diverse tipologie di risorse che si differenziano per responsabilità, mansioni e ruolo all'interno dell'ente.

Ciascuna di queste figure presenta esigenze ben precise di formazione, dovute principalmente a:

- differenti livelli di responsabilità;
- differenti livelli di coinvolgimento operativo nel processo di trattamento dei dati personali;
- differenti livelli di visibilità della struttura organizzativa e dei processi dell'Ente.

4.3 Corsi sull'Open Source

Molte realtà pubbliche e private stanno valutando l'opportunità di adottare software Open Source come possibile soluzione per una significativa riduzione dei costi e della complessità gestionale.

Di fronte a questo scenario, chi deve fare investimenti e scelte strategiche in merito all'adozione di piattaforme IT, si trova di fronte al dilemma di come approfittare delle opportunità senza compromettere la qualità dei servizi erogati.

Perché se è vero che l'utilizzo di Unix e del software open source può rappresentare una svolta, è altrettanto vero che vi sono numerosi casi di fallimenti e delusioni, in cui alla fine i costi totali, così come la complessità applicativa e gestionale, sono aumentati.

Per questo Data Security ha deciso di organizzare una serie di corsi destinati al personale con responsabilità manageriali e tecniche delle aziende private e degli enti pubblici che hanno la necessità di valutare le opportunità - ed i rischi - connessi con l'adozione di sistemi operativi aperti e di software open source.

I corsi offrono il supporto e le conoscenze necessarie per effettuare con la giusta consapevolezza scelte potenzialmente rischiose e difficilmente reversibili, per le quali è necessario avere un quadro ragionevolmente completo delle possibili opzioni, con indicazioni chiare di che cosa convenga - e non convenga - fare per ridurre al minimo i rischi di insuccesso.

Per soddisfare sia le esigenze di inquadramento teorico e strategico, tipiche di ruoli con responsabilità manageriali e di spesa, che le esigenze di comprensione dettagliata dei comandi e dei pacchetti, tipiche del personale tecnico e degli amministratori di rete, di sistema e della sicurezza, Data Security ha predisposto i moduli:

- **Opportunità e rischi del software aperto**
per fornire al personale manageriale delle aziende private gli strumenti per compiere le scelte strategiche;
- **Open Source nella Pubblica Amministrazione**
diretto specificatamente a coloro che negli enti pubblici si occupano degli investimenti nel settore IT;
- **Sicurezza in ambiente Unix e Linux**
diretto prevalentemente a personale tecnico, per illustrare in pratica le applicazioni open source nel settore della sicurezza.
Nel corso delle sessioni tutte le nozioni introdotte teoricamente sono illustrate anche in pratica, utilizzando server, client e infrastrutture di comunicazione messe a disposizione da Data Security.

4.4 e-Security Tutorial

Con e-Security Tutorial, Data Security vuole fornire uno strumento interattivo per aumentare la consapevolezza di tutte le risorse aziendali in merito alla problematica della sicurezza.

E' stato pensato come modulo di autoapprendimento e di verifica che può essere implementato su un supporto multimediale (Cd-Rom, DVD) o meglio ancora come modulo da inserire nella Intranet aziendale esistente.

Questo garantisce a tutte le risorse aziendali che accedono alla Intranet e che quotidianamente utilizzano il sistema informatico aziendale di iniziare un percorso tra una serie di tematiche chiave della sicurezza informatica attinenti il più possibile alla specifica realtà aziendale, in modo da suscitare interesse e curiosità.

Il modulo si pone come strumento interattivo per l'avvio, il monitoraggio e il perfezionamento del processo di awareness, costituendo un agile e valido supporto alle attività di formazione e di prevenzione.

E' costituito da diverse sezioni che possono essere personalizzate a piacere, in accordo con le specifiche esigenze dell'azienda:

- Sezioni informative e documentali, che costituiscono un archivio continuamente aggiornabile di risorse per la formazione e l'autoformazione. Abbracciando in particolare gli argomenti introduttivi alla sicurezza informatica aziendale, segnalano casi pratici che si rapportano all'esperienza quotidiana di ciascun utente, divulgano, spiegano e commentano le policy per la gestione della sicurezza;
- Le sezioni interattive, che comprendono i test di autovalutazione, costituiscono un valido strumento per la verifica dei risultati nel processo di consapevolezza degli utenti;
- Le sezioni di servizio offrono la possibilità di segnalare tempestivamente le anomalie al responsabile per la sicurezza e di svolgere sondaggi, test e verifiche sul livello di awareness e sull'impatto dei piani di sicurezza nei confronti degli utenti.

5. Managed Security

La gestione della sicurezza della rete aziendale, la protezione della posta elettronica da virus e spam, gli strumenti per regolare l'utilizzo di Internet in azienda sono le esigenze più diffuse e più urgenti anche tra le PMI e gli studi professionali.

Le soluzioni offerte tradizionalmente dal mercato prevedono l'acquisto di costose infrastrutture e la disponibilità di personale qualificato che si occupi delle problematiche di gestione e aggiornamento, oneri che storicamente hanno frenato l'adozione di misure di sicurezza che, oltre ad essere esplicitamente previste per legge, sono di fondamentale importanza per migliorare la produttività e garantire la continuità del business.

Adottare soluzioni in full outsourcing con una struttura specializzata significa alleggerire la struttura aziendale di tutti i tempi, le procedure e i costi di gestione, mantenimento e aggiornamento; significa affidare un compito delicato a chi possiede l'esperienza e le competenze specifiche per svolgerlo al meglio, mantenendo al contempo il controllo su tutta la rete locale.

Per questo Data Security consiglia una serie di servizi di Security che risolvono le problematiche di sicurezza a costi contenuti:

- **Web Security**, che agisce come monitoraggio e filtro delle attività da e verso Internet: consente l'impostazione di restrizioni per l'accesso ad Internet da parte di utenti e gruppi a 60 categorie di siti classificati in più di 2 milioni di siti web e di stabilire quali categorie non rendere visibili in assoluto o nei giorni e negli orari stabiliti:
 - **Spyware Protection** blocca spyware, adware ed altre applicazioni maligne interrompendone l'azione.
 - **Virus Protection** difende i computer dai virus nascosti nei download e nelle mail web-based.
- **E-Mail Security**, che grazie ad un sistema di verifica che agisce tramite la scansione di tutto il traffico di corrispondenza tra la rete interna e quella esterna, agisce da:
 - **Virus Protection per la posta**, bloccando i virus presenti nel traffico mail SMTP e POP3 ed in tutti gli allegati, anche se compressi.
 - **Spam Protection**, utilizzando 9 tecniche differenti per filtrare lo spam senza bloccare il normale traffico.
 - **Phishing Protection**, bloccando tutte le mail che tentino illegalmente di acquisire informazioni confidenziali di utenti.
- **Network Security**, il sistema di protezione e blocco di ogni tipo d'intrusione sempre attivo che sorveglia e protegge tutto il traffico in entrata e uscita dalla LAN:
 - **Intrusion Protection**, identifica e blocca le intrusioni e gli attacchi application based utilizzando tecniche di individuazione pattern-based, euristiche e anomaly detection.
 - **Firewall**, controlla il traffico Internet in ingresso ed uscita tramite stateful raket inspection ed application level proxy.
 - **Virtual Private network Gateway**, permette connessioni e comunicazioni secure con uffici remoti, filiali e utenti in mobilità.
- **Online Monitor**, monitoraggio e supporto 24 ore su 24 per componenti critiche di sicurezza, firewall, sistemi di Intrusion detection e VPN, con servizio garantito dall'applicazione di rigidi Service Level Agreement.

6. Internet Security

Ormai tutte le aziende e gli Enti pubblici utilizzano Internet come fondamentale strumento di lavoro.

Ma se la rete Internet permette un immediato accesso a risorse in tutto il mondo, porta con sé anche alcuni inconvenienti quali i rischi di attacchi da parte di hacker e virus, la perdita di produttività dovuta all'abuso della connessione al Web durante l'orario di lavoro e l'aumento dei costi di connessione a banda larga, oggi necessaria per accedere ad applicazioni Web sempre più sofisticate.

Per eliminare questi inconvenienti è necessario ripensare le modalità di connessione per **ottimizzare l'accesso a Internet** sia in termini di utilizzo delle risorse di banda, sia in termini di sicurezza.

Oltre a proteggere e a monitorare la connessione degli utenti aziendali, è importante garantire anche la **sicurezza delle applicazioni Web** attraverso le quali l'azienda garantisce la propria presenza in Internet.

Non basta aggiornare i Web server con le relative patch. L'attività di continuo aggiornamento del software, oltre a essere complessa ed estremamente dispendiosa in termini di risorse (ogni giorno vengono scoperte nuove vulnerabilità), risolve il problema solo temporaneamente: il sistema è protetto solo fino alla scoperta della prossima vulnerabilità, e la divulgazione del problema e il rilascio delle patch relative avvengono quando i danni sono già stati causati.

Anche Virus e Worm dagli effetti disastrosi come Code Red e Nimda, che possono mettere in ginocchio un'intera Intranet nel giro di pochi minuti, sfruttano i problemi di sicurezza dei Web Server. Il solo Nimda ha causato in pochi giorni danni per 800 miliardi di dollari.

6.1 Ottimizzare l'accesso a Internet

L'introduzione delle nuove tecnologie nel mondo del lavoro ha incrementato la produttività e la qualità delle aziende, provocando però anche fenomeni meno rallegranti: navigare su Internet per scopi non professionali durante l'orario di lavoro arreca danno all'azienda sia dal punto di vista della produttività, sia per quel che riguarda il flusso dei dati, ostacolando o intasando la capacità di banda a disposizione, sia per la sicurezza dei sistemi stessi, con il pericolo sempre presente di aprire le porte a virus e hacker.

La visita di siti Internet illegali può inoltre essere dannosa per la reputazione dell'azienda e comportare addirittura conseguenze legali.

Per affrontare correttamente questa problematica è consigliabile percorrere due strade parallele: regolamentare l'utilizzo delle risorse informatiche attraverso un sistema di **policy** e allo stesso tempo impiegare misure tecniche di ottimizzazione e protezione del collegamento a Internet che, se non possono garantire la sicurezza assoluta, riducono di molto i possibili rischi.

Oltre alle classiche misure tecniche di protezione dei dati come i programmi **antivirus**, la predisposizione di una efficiente politica di **backup** e l'utilizzo di **firewall**, può essere utile migliorare e rendere più sicure le connessioni a Internet attraverso l'utilizzo di proxy e di sistemi di content filtering.

Il Proxy Web serve per ottimizzare l'accesso a Internet: in caso di frequente accesso alle medesime pagine, il server ne memorizza una copia locale da restituire ai client della rete aziendale, evitando così di doverle reperire direttamente su Internet.

Alcuni proxy sono dotati anche di funzionalità di content restriction, ovvero possono essere configurati per impedire o permettere il reperimento delle diverse risorse sulla base dell'Url o dei contenuti.

Le soluzioni di Content Filtering aiutano l'azienda ad utilizzare in maniera produttiva l'accesso a Internet, monitorando e gestendo il traffico generato dai propri collaboratori.

Queste soluzioni permettono, infatti, di filtrare indirizzi che possono rilevarsi improduttivi per l'attività aziendale. Attraverso il database raggruppato per categorie e costantemente aggiornato, permettono di discriminare la visibilità o la non visibilità di siti internet.

6.2 Proteggere il Web

Oltre a proteggere e a monitorare la connessione degli utenti aziendali, è importante garantire anche la sicurezza delle applicazioni Web attraverso le quali l'azienda garantisce la propria presenza in Internet.

Malintenzionati scoprono ogni giorno nuove vulnerabilità dei Web Server e delle applicazioni Web e le sfruttano per ottenere il controllo del sistema e, nella migliore delle ipotesi, modificare il contenuto dei siti Web. Le violazioni commesse ai danni dei sistemi informatici vengono di regola perpetrate sfruttando vulnerabilità ed exploit, e possono comportare conseguenze disastrose.

Ad aggravare questa situazione vi è il fatto che la scoperta e lo sfruttamento di questo genere di vulnerabilità sono oggi alla portata di tutti.

Le conseguenze di questi attacchi possono essere disastrose:

- danni d'immagine dovuti ad atti di vandalismo sulle pagine Web;
- furto, cancellazione o modifica di informazioni sensibili;
- mancato guadagno dovuto all'interruzione del servizio;
- spese ingenti di ripristino dei sistemi.

Le attività dei pirati informatici e il diffondersi dei virus possono comportare danni ben più gravi della temporanea interruzione del servizio dei siti. Nella maggior parte dei casi si assiste ad atti di vandalismo, quale la modifica dei contenuti delle pagine Web o la cancellazione del contenuto dell'intero sito, con conseguenti danni d'immagine per l'azienda; furto di informazioni sensibili concernenti l'organizzazione, la configurazione di rete oppure la clientela o gli utenti; uso dell'host come base per lanciare attacchi contro altri sistemi (attacchi D.D.O.S - Distributed Denial of Service); installazione di strumenti per il monitoraggio del traffico di rete e la cattura di informazioni di autenticazione (sniffing).

Ad aumentare il pericolo c'è il fatto che i server Web spesso rappresentano delle vere e proprie porte di accesso alla rete interna, nella quale sono custodite informazioni aziendali, dati sul personale, sulla clientela, dati di rilevanza economica e legale.

7. Sicurezza delle reti

Connettere la propria rete aziendale ad Internet è oggi una scelta spesso irrinunciabile, tuttavia non priva di rischi. Nuove tecniche di intrusione e nuove vulnerabilità vengono scoperte di giorno in giorno, esponendo a forti rischi i dati e la privacy aziendale.

Le informazioni che un intruso potrebbe ricavare da un'incursione effettuata con successo all'interno della rete o di un sito Internet potrebbero avere un impatto commerciale gravissimo (si pensi ad informazioni riservate trasmesse a un concorrente), senza contare il danno di immagine per l'azienda.

Per questo è necessario dotarsi di sistemi che proteggano adeguatamente la propria rete, come i dispositivi firewall, in grado di controllare l'accesso alle reti intercettando tutte le comunicazioni in entrata e in uscita. A seconda della configurazione e della tipologia, i firewall permettono di specificare quali dati, da che nodi e quali utenti possono accedere alla rete.

Il **firewall** separa e protegge la rete interna, definendo e rafforzando le policy di rete. I computer esterni alla rete devono attenersi a una specifica procedura per ottenere l'accesso alle risorse, agli host e a tutte le altre informazioni. Se l'accesso viene autorizzato l'utente può passare, a patto che si attenga alla procedura definita dal firewall.

Una parte importante di qualsiasi architettura di network security è inoltre l'**Intrusion Detection System (IDS)**, che monitorizza il traffico di rete per rilevare le attività sospette e registra i casi in cui individua traffico potenzialmente ostile.

Per le reti che integrano server pubblici accessibili da Internet (es. Web server o server di posta) è consigliabile predisporre una zona demilitarizzata (DMZ), aggiungendo un ulteriore livello di protezione e segmentando la rete interna.

L'utilizzo di soluzioni tecnologiche dedicate alla protezione del sistema informatico quali i firewall e gli IDS spesso non sono sufficienti ad assicurare un adeguato livello di protezione: basta infatti che anche solo una di tali componenti non sia configurata correttamente per mettere a rischio la sicurezza di dati, applicazioni ed infrastrutture.

Per questo motivo è necessario eseguire periodicamente una serie di test dall'esterno e dall'interno della rete, simulando una serie di attacchi e verificando in pratica se il sistema è sicuro.

Data Security realizza analisi di sicurezza e attività di Risk & Vulnerability assessment in grado di evidenziare i difetti e le debolezze di un sistema informatico: i **Security test** permettono di effettuare analisi approfondite e test di penetrazione che offrono un'immagine immediata e sintetica dello stato di sicurezza del vostro sistema; i **Network security audit** permettono di analizzare la rete dall'interno, rilevando le possibili vulnerabilità che, per dolo o distrazione, potrebbero causare danni ai dati e alle infrastrutture di rete.

7.1 Protezione perimetrale

I firewall sono elementi software o hardware/software destinati a costituire la prima linea di difesa della rete aziendale. La loro funzione è di filtrare tutti i pacchetti in entrata e in uscita per individuare e bloccare tentativi di intrusione ed accessi non autorizzati da parte di utenti non autorizzati.

Una efficace difesa perimetrale della propria rete informatica non si riduce però alla semplice installazione di un firewall. Per quanto il firewall sia ben progettato, se viene semplicemente collegato ad una rete con una configurazione base e abbandonato alla propria sorte, nel giro di pochissimo tempo diventa niente più che una suppellettile.

Per questo è necessario dotarsi di soluzioni firewall adatte alla propria attività e che prevedano un costante aggiornamento, sia esso in modalità full outsourcing come nella soluzione **Security Protection**, sia, per le reti con esigenze di firewalling più complesse, grazie a funzionalità di aggiornamento automatico come in Astaro Security Linux.

Astaro Security Gateway è una soluzione software integrata che fornisce ottime prestazioni in un firewall all-in-one in grado di affrontare le necessità di sicurezza di qualsiasi rete. Con un sistema operativo consolidato, una scansione ed ispezione dei pacchetti dello stack (stateful packet inspection), la protezione antivirus, il filtro dei contenuti, proxy applicativi e una soluzione per VPN in standard IPSec, Astaro Security Linux rappresenta una soluzione completa delle esigenze di sicurezza.

7.3 Security Test

Al di là di tutte le analisi che possono venire condotte sulla carta, seppur importanti, la determinazione delle effettive vulnerabilità di un sistema informatico e di una infrastruttura di comunicazione rimane l'attività più importante per evidenziare, e quindi per rimuovere, le vulnerabilità stesse.

L'utilizzo di soluzioni tecnologiche dedicate, quali ad esempio i firewall e gli IDS (Intrusion Detection System) per proteggere il sistema informatico non sono sufficienti per assicurare un adeguato livello di protezione: basta infatti che anche solo una di tali componenti non sia configurata correttamente, per mettere a rischio la sicurezza di dati, applicazioni ed infrastrutture. Per questo motivo è necessario eseguire una serie di security test, simulando una serie di attacchi e verificando in pratica se il sistema è sicuro o meno.

Data Security mette a disposizione delle aziende un servizio di Security Test, che mediante una serie di attacchi e di test permette di rilevare tutte le vulnerabilità prima che queste possano venire sfruttate da criminali informatici.

I test sono effettuati tramite Internet dall'esterno della rete aziendale, e rilevano i servizi raggiungibili e verificano le possibili vulnerabilità dallo stesso punto di vista che avrebbe un criminale informatico che volesse penetrare illegalmente nella vostra rete.

Per essere efficaci ed esaustivi, i test devono essere continuamente aggiornati per tenere conto delle nuove vulnerabilità che continuamente vengono scoperte nei sistemi operativi, software di base ed applicativi.

Per questo Data Security dispone di un Centro di Ricerca sulla Sicurezza Informatica, con personale altamente specializzato che aggiorna costantemente le base dati delle vulnerabilità e realizza i programmi e gli script necessari per individuare le vulnerabilità stesse.

Oltre al servizio di Security Test, Data Security mette a disposizione delle aziende il servizio di Security Audit, che risponde all'esigenza di determinare le debolezze e le vulnerabilità dall'interno dell'azienda: è infatti dimostrato che la maggior parte delle intrusioni e degli accessi non autorizzati avvengono dall'interno dell'azienda, non dall'esterno. Questo perché spesso dipendenti e collaboratori sono a conoscenza dell'architettura e delle contromisure di sicurezza adottate, nonché di user-ID e di password, quindi sono in grado potenzialmente di sferrare gli attacchi più insidiosi.

Per questo motivo è necessario tenere costantemente sotto controllo quali attacchi è possibile effettuare dall'interno dell'azienda, oltre che dall'esterno.

Poiché ogni realtà aziendale è caratterizzata da esigenze e peculiarità che la rendono spesso unica, il servizio di Security Audit risponde anche all'esigenza di effettuare una attività di auditing sulla sicurezza informatica ritagliata sulle esigenze della specifica realtà aziendale.

Tutti i test sono eseguiti sempre da personale esperto e con procedure che prevedono il massimo rispetto della riservatezza dei dati e dei risultati. Durante tutta l'attività di test il nostro staff di tecnici sarà sempre a vostra disposizione per affrontare prontamente qualsiasi problema.

Di seguito si riporta una sintesi delle varie tipologie di test che compongono il Security Test.

- Raccolta informazioni sul sistema:
Identificazione delle informazioni sul sistema rilevabili dall'esterno;
Scansione delle porte e dei servizi;
- Rilevamento delle vulnerabilità:
Security Scanner;
Ricerca vulnerabilità per le diverse tipologie di servizi presenti sul server.
- Analisi delle vulnerabilità e rimedi proposti:
Distribuzione percentuale dei livelli di rischio;
Specifiche tecniche delle vulnerabilità riscontrate;
Riferimento alla documentazione ufficiale in Internet sulle vulnerabilità rilevate.
- Altre caratteristiche del test:
Disponibilità di un responsabile tecnico per ogni test;
Programmazione della data di effettuazione del test;
Controllo costante dell'andamento dei test da parte di un nostro tecnico;
Possibilità di interrompere il test in corso;
Opzione test da eseguirsi in orario notturno o in giorni festivi.

7.4 Network Security Audit

La sicurezza dei sistemi informatici e dei dati in essa trattati comporta a chi si occupa del settore responsabilità nei confronti della propria organizzazione, di terze parti e della Legge. Diventa quindi indispensabile per le aziende programmare periodiche verifiche della propria struttura informatica avvalendosi della consulenza di personale altamente qualificato.

Il servizio di Network Security Audit rappresenta idealmente il primo passo da compiere sulla strada della protezione perimetrale della propria rete da attacchi e/o tentativi di intrusione non autorizzati.

Si tratta di una analisi che viene effettuata dall'interno delle rete, in quanto presuppone una indagine approfondita della architetture di rete, dei componenti della rete stessa, della configurazione dei diversi computer presenti in rete e del software installato.

Al termine dell'attività viene prodotto un report in cui sono descritte le vulnerabilità riscontrate e sono indicate le misure correttive per ottenere un grado adeguato di sicurezza.

8. Autenticazione e controllo degli accessi

Le soluzioni sviluppate da Data Security nel settore dell'autenticazione e del controllo degli accessi partono dalla convinzione che le tecnologie debbano supportare e facilitare delle scelte organizzative e che solo attraverso delle correzioni a livello organizzato si possono ridurre alcune vulnerabilità dei sistemi informatici.

Per questa ragione Data Security propone la giusta soluzione tecnologica solo dopo aver individuato le forme organizzative più adatte alla vostra attività e avervi consigliato gli eventuali correttivi.

Esistono diversi metodi di autenticazione, la cui opportunità è condizionata da diversi fattori quali l'importanza delle informazioni da proteggere, l'usabilità, la scalabilità ed il costo del sistema di autenticazione che si intende implementare.

In base al tipo di autenticazione che l'analisi di questi fattori identifica come quella ideale, possono venir realizzate soluzioni che si basano di volta in volta su un semplice sistema di password/user id, su una doppia autenticazione, su sistemi legati al GSM, sui certificati digitali, su metodi di riconoscimento biometrici o su combinazioni di questi sistemi.

Qualunque sia il sistema di autenticazione che si intende adottare, è comunque necessaria a monte della decisione una attenta analisi costi-benefici per individuare la soluzione che meglio coniughi per ciascuna situazione sicurezza, semplicità d'uso, costi di implementazione e di gestione.

Anche un sistema di autenticazione che utilizza solo user id e password può essere adeguato in molti casi, a patto che l'organizzazione che lo utilizza si organizzi implementando una **password policy** efficace.

Sistemi di autenticazione più sicuri si hanno con metodi che prevedono la doppia autenticazione, in quanto l'utente deve conoscere il proprio PIN e deve essere in possesso del dispositivo di autenticazione (sia esso un token, una Smart Card o un telefono GSM) per essere abilitato all'uso delle risorse.

Un ottimo metodo di autenticazione è anche quello che prevede l'utilizzo di Certificati Digitali, a patto che questi siano utilizzati in una struttura PKI, che permetta di uniformare e centralizzare tutte le strutture di autenticazione ed identificazione degli utenti e di accesso alle risorse.

La crittografia e la firma digitale, come è noto, non servono solo a garantire l'identità degli utenti, ma consentono anche un elevato livello di confidenzialità delle comunicazioni e mettono al riparo dai rischi di ripudio nelle transazioni. L'introduzione della firma digitale è stata in molte realtà un'occasione per un riordino di funzioni e permessi che hanno consentito di migliorare l'organizzazione del lavoro e di ridurre il rischio di comportamenti anti-aziendali o di rivelazioni inconsapevoli di informazioni riservate.

Un ulteriore metodo di autenticazione è quello biometrico, che si basa sul riconoscimento di caratteristiche uniche di ogni individuo quali la retina, l'impronta digitale o la voce. Combinando un sistema di autenticazione biometrico con l'utilizzo di un certificato su smart card il livello di sicurezza ottenuto è virtualmente inviolabile.

9. Disaster Recovery

Quanto tempo impiegherebbe la vostra azienda a riprendere il lavoro se il vostro CED venisse distrutto? Riuscireste a far ricominciare la vostra attività in tempi ragionevoli?

Per mettere l'azienda al riparo dai rischi connessi a impreviste interruzioni dell'ambiente che ospita gli strumenti informatici necessari al proprio business o proteggere un ente pubblico da interruzione di pubblico servizio dovuta ad eventi imprevedibili, per evitare perdite di dati, applicazioni e informazioni critiche, è importante attivare un piano di **Disaster Recovery e di Business Continuity** e dotarsi delle strutture e degli strumenti necessari a reagire a questo tipo di eventi.

L'identificazione della soluzione ottimale alle problematiche di Disaster Recovery richiede una corretta analisi di costi e benefici, attraverso un piano che definisce gli obiettivi principali in termini di dati da salvaguardare e la conseguente stesura di un Disaster Recovery Plan. Data Security aiuta i propri clienti a individuare i sistemi, le infrastrutture e le procedure più adatte a costruire i piani di Disaster Recovery più adatti alla propria attività, supportandoli dalla fase di studio a quella di pianificazione, dall'implementazione del piano ai test sulle procedure e sui sistemi.