L'IMPORTANZA DELLA SICUREZZA

TUTELA DELLA PRIVACY E SICUREZZA INFORMATICA

L'impiego dei sistemi di rete in strutture dalla più piccola alla più complessa presenta problematiche tecniche e normative di notevole rilevanza; in particolare vanno tenuti presente gli adempimenti derivanti dalla ***legge 675/96*** (dati personali) in materia di sicurezza ed integrità dei dati, le responsabilità per danni derivanti da accesso abusivo a sistemi informatici e relativo furto di informazioni, le responsabilità contrattuali per inadempimento provocato da un blocco dei sistemi.

Affrontare questi problemi richiede specifiche competenze professionali effettivamente certificate.

Gli esperti che si occupano di questa problematica sono professionisti iscritti all'albo degli ingegneri nel Settore dell'Informazione, ciò consente oltre ad una più precisa individuazione di problemi e soluzioni, anche il rilascio di attestazioni di conformità, verbali di collaudo e certificazioni (eventualmente asseverate dal tribunale) che hanno validità giuridica piena.

Non va infatti sottovalutata l'importanza di poter certificare l'assetto tecnico raggiunto in funzione di eventuali partecipazioni a gare d'appalto, attuazione di certificazioni di qualità, gestione di controversie giudiziarie.

Tutti i servizi offerti sono orientati ad elevare i livelli di sicurezza dei sistemi informatici proteggendoli dall'aggressione di virus, blocco dei sistemi, furto di informazioni ed accessi abusivi.

Completa l'offerta la possibilità di fornire, a richiesta, corsi di formazione specifici, anche presso la sede del cliente sull'operatività delle soluzioni applicate.

TIPOLOGIA DEI SERVIZI DI SICUREZZA INFORMATICA

- **Controllo e stesura delle politiche di sicurezza**
  Non è possibile implementare un sistema di sicurezza se non esistono delle regole sull'uso delle risorse informatiche. Ecco quindi l'esigenza di controllo delle politiche di sicurezza informatica presenti nell'apposito documento, se esistente, ed eventuali adattamenti alla normativa vigente.

- **Consulenza sulla normativa sul trattamento dati personali (L. 675/96 e D.P.R. 318/99)**
  Facendo riferimento alle specifiche esigenze, saranno affrontati i temi previsti sia dalla L. 675/96 (Privacy) che dal D.P.R. 318/99 (attuazione misure minime).
  In particolare:
  - controllo del rispetto della normativa vigente,
  - stesura o adeguamento del documento Misure Minime,
  - analisi dei rischi nel trattamento di dati personali,
  - rilevazione di eventuali debolezze e/o carenze nel trattamento di dati personali,
  - stesura del Documento Programmatico (se necessario),
  - pianificazione delle azioni correttive per la messa a norma.

- **Consulenza sul rispetto delle norme sul diritto d'autore (L.248/00)**
  - Presentazione delle norme vigenti in tema di diritto d'autore.
  - Esame di eventuali specifiche esigenze (conteggio licenze ed eventuale regolarizzazione).
  - Eventuale necessità e modalità di utilizzo del bollino SIAE sui vari tipi di supporti informatici.

- **Messa in sicurezza della Rete Aziendale**
  - Analisi della rete dall'esterno – esecuzioni di controlli sia manuali che con appositi strumenti software sulle possibili vulnerabilità, note alla data, del software presente su server (web e firewall compresi). Verrà steso un resoconto per ciascun server esaminato evidenziando in ordine di gravità le vulnerabilità riscontrate ed i rispettivi correttivi se esistenti.
  - Analisi della rete dall'interno - esecuzioni di controlli sia manuali che con appositi strumenti software sulle possibili vulnerabilità, note alla data, del software presente sia su server sia su posti di lavoro (eventualmente a campione se il numero dovesse essere elevato). Verrà steso un resoconto per ciascun server e/o posto di lavoro esaminato evidenziando in ordine di gravità le vulnerabilità riscontrate, comprensivo anche dei principali pacchetti software (Office, ecc...) e i rispettivi correttivi se esistenti.
  - Identificazione di eventuali rischi causati da un uso improprio delle risorse aziendali.

- **Ricostruzione delle modalità utilizzate in caso di attacco a sistemi informatici**
  - Analisi di sistemi attaccati e/o violati alla ricerca delle tracce lasciate da malintenzionati.
  - Stesura di un dettagliato resoconto di tutte le tracce trovate, delle tecniche usate da malintenzionati, cercando di fornire tutti gli elementi possibili al fine di individuare i responsabili.

- **Controllo ed eventuale messa in sicurezza del sistema di accesso RAS**
  - Controllo delle politiche d'accesso alla rete interna tramite modem e ricerca di eventuali vulnerabilità del sistema RAS (Remote Access System).
  - Stesura di un resoconto evidenziando gli eventuali interventi correttivi sia dal punto di vista tecnico che delle politiche d'accesso.

- **Controlli sul server di posta elettronica**
  - Controllo anti-relay (uso improprio del server di posta) e anti-spam (posta non richiesta, tipicamente pubblicità) del server di posta.
  - Stesura di un resoconto in cui saranno proposte politiche anti-relay (impedire a chi non ne ha il diritto di usare il server di posta per inviare e-mail) e politiche anti-spam sia passive (ridurre il rischio che il proprio indirizzo e-mail finisca in liste di spammer) che attive (limitare la quantità di spam ricevuta).

- **Installazione di reti e loro protezione**
  - Progettazione e installazione di reti con client Windows o Linux e server Windows o Linux.
  - Connessione della rete a Internet (sia in dedicata che in commutata) mediante un gateway Linux con Firewall (sistema di protezione per gli accessi) ed eventuali altri servizi (posta elettronica, web server, ecc...).
  - All'atto dell'installazione verranno particolarmente curati gli aspetti di sicurezza onde ridurre al minimo possibili problemi in particolare nella connessione verso la rete Internet.

- **Servizio di gestione delle problematiche di sicurezza delle reti locali**
  - Gestione delle problematiche di sicurezza dei PC della rete, con particolare attenzione all'eventuale connessione verso Internet, all'antivirus e al server di posta.
  - Monitoraggio dei sistemi in gestione al fine di prevenire sia malfunzionamenti che intrusioni.
  - Sui sistemi in gestione verranno installate le eventuali correzioni, a mano a mano che queste verranno rilasciate dai fornitori al fine di ridurre i rischi connessi alla sicurezza ed i malfunzionamenti.

- **Redazione di collaudi, perizie (anche giurate) e certificazioni di qualità**

- **Formazione sull'utilizzo sicuro delle risorse informatiche e telematiche**
  - Posta elettronica
  - Uso antivirus
  - Navigazione sicura
  - Impiego di sistemi crittografici
  - Esecuzione di backup e copie di riserva
  - Distruzione di informazioni