AUTOMOBILE CLUB RAVENNA

POLITICHE DI SICUREZZA

DELLE INFORMAZIONI

SOMMARIO

1 Premessa

Il Dlgs. N° 196/03 (Codice in materia di protezione dei dati personali), prevede un articolato sistema normativo finalizzato alla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

L'ambito di applicazione delle norme è estremamente ampio poiché riguarda trattamenti di dati da chiunque effettuati con la sola esclusione dei trattamenti espletati da persone fisiche per fini esclusivamente personali.

La tutela si concretizza sostanzialmente nel garantire che il trattamento dei dati sia svolto nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone con particolare riferimento alla riservatezza della identità personale.

Sostanzialmente tali norme sono rivolte sia al titolare che al responsabile del trattamento qualora nominato. L' A.C. di RAVENNA è titolare e responsabile dei dati trattati per proprio conto (fornitori, personale dipendente, ecc.).

Si ricorda che sia il titolare che il responsabile del trattamento dei dati sono destinatari di una serie di norme che si concretano in adempimenti per la gestione di dati personali, tra cui l'obbligo di garantire la ***sicurezza delle informazioni****.*

La sicurezza è fondata sul rispetto di misure minime di sicurezza la cui adozione garantisce preventivamente da accessi non autorizzati, da distruzioni, o perdita dei dati, da trattamenti non consentiti o non conformi alle finalità per cui sono stati raccolti.

2 La sicurezza delle informazioni

L‘informazione è una componente fondamentale per l‘attività di ogni istituzione e, conseguentemente, deve essere adeguatamente protetta. La sicurezza informatica protegge l‘informazione nei confronti di un‘ampia gamma di attacchi potenziali al fine di garantire la continuità dell‘attività e minimizzare i danni e le interruzioni di servizio.
La sicurezza delle informazioni è caratterizzata dai seguenti aspetti:

- **Confidenzialità**: garantisce che l‘informazione è accessibile solamente a coloro che hanno l‘autorizzazione ad accedervi;
- **Integrità**: garantisce l‘accuratezza e la completezza dell‘informazione e dei metodi di elaborazione;
- **Disponibilità**: garantisce che gli utenti autorizzati possano accedere all‘informazione quando vi è necessità.

La sicurezza delle informazioni è realizzata attraverso l‘attivazione di politiche specifiche, strutture organizzative, procedure, funzionalità software ed è completata da un sistema di controlli.

E‘ importante sottolineare un principio che deve stare alla base della sicurezza di ogni organizzazione: la corretta separazione dei ruoli fra i responsabili della gestione della sicurezza e gli utenti operativi.

2.1 DEFINIZIONE DEI REQUISITI DI SICUREZZA

La definizione dei requisiti di sicurezza deriva da:

- Valutazione del rischio cui possono essere esposti i beni dell‘amministrazione con i potenziali danni che ne derivano; tale valutazione consiste in un‘attività sistematica volta a considerare l‘impatto sulle attività istituzionali, derivante da carenze o violazioni del sistema di sicurezza in termini di perdita di confidenzialità, integrità o disponibilità del sistema informativo. I risultati della valutazione portano a definire le azioni e le priorità di intervento nelle fasi di realizzazione dei sistemi di sicurezza e dei relativi controlli;

- Quantificazione ed accettazione del cosiddetto “rischio residuo“ cioè il rischio non coperto dai sistemi di sicurezza o da strumenti/sistemi non tecnologici (es. norme, assicurazioni, ecc.);

- Individuazione dell‘insieme dei requisiti legali, regolamentari e contrattuali a cui l‘istituzione ed i suoi fornitori devono far fronte.

3 Politiche di sicurezza

Questo documento è una dichiarazione generale, prodotta dal **vertice** dell' A.C. RAVENNA che definisce le regole per la corretta realizzazione e gestione della stessa. Queste politiche di sicurezza costituiscono il blocco di partenza da cui raggiungere qualsiasi obiettivo di information security che sia realmente efficace e rappresentano quindi un indispensabile strumento di supporto alla gestione. Le politiche di sicurezza sono usate come un punto di riferimento per una vasta varietà di attività di information security che includono:

- progettazione di controlli interni alle applicazioni;
- definizione delle regole per il controllo degli accessi;
- esecuzione dell'analisi del rischio;
- formazione degli utenti per un corretto utilizzo degli strumenti a disposizione ed altro.

3.1 POLITICHE DI SICUREZZA DELL' A.C. DI RAVENNA

Gli obiettivi che si vogliono conseguire sono di garantire, in accordo con le leggi e le regole interne:

a) **per le risorse tecnologiche**:
   - la disponibilità del servizio in una forma adeguata, anche a fronte di eventi eccezionali, tramite la formulazione di appropriati piani di recupero delle funzionalità del sistema;
   - la continuità del servizio a copertura delle esigenze operative dell'ufficio.

b) **per i dati**:
   - la riservatezza delle informazioni;
   - l'integrità delle informazioni;
   - la correttezza delle informazioni ritenute critiche per le eventuali conseguenze derivanti da una loro alterazione;
   - la disponibilità delle informazioni e delle relative applicazioni.

Di seguito si riporta l'elenco di regole che devono essere adottate per garantire un livello di sicurezza modulabile:

- chiunque, dipendente o persona esterna, impieghi risorse informatiche dell'ufficio deve essere espressamente autorizzato da **un responsabile appositamente designato**;
- le autorizzazioni devono garantire che sulle informazioni possano intervenire solo le persone abilitate e ciascuna nei limiti delle proprie competenze;
- le autorizzazioni vengono definite in accordo con le leggi, le norme interne e il livello di riservatezza e importanza delle informazioni;
- chiunque autorizzi un dipendente o una persona esterna all'impiego di risorse informatiche dell'ufficio deve essere chiaramente individuabile;
- le informazioni sono protette in accordo con la loro criticità, sia nei sistemi ove risiedono, sia nei trasferimenti da un sistema ad un altro;
- le autorizzazioni per l'accesso ai dati e alle applicazioni sono di responsabilità del proprietario dell'informazione;

- le autorizzazioni per l'accesso alle risorse tecnologiche (hardware e software di base e di ambiente) sono in carico al **responsabile del trattamento dei dati**;
- le modalità di gestione delle autorizzazioni sono concordate dallo stesso con il proprietario dell'informazione;
- è consentita la delega delle operazioni di gestione delle autorizzazioni a condizione che siano definite ed implementate procedure organizzative e modalità tecniche che impediscano che il raggiungimento degli obiettivi di sicurezza venga compromesso;
- sono predisposte opportune procedure tecniche ed organizzative per il sollecito ripristino del servizio a fronte di guasti o malfunzionamenti.

Per risorse informatiche da considerare nell'ambito della sicurezza, ci si riferisce a:

- dispositivi tecnologici (computer, terminali, linee di comunicazione, ecc.) il cui danneggiamento fisico può comportare l'interruzione del corretto funzionamento e la conseguente sospensione del servizio;
- sistemi operativi o prodotti software la cui modifica, cancellazione o indisponibilità può comportare l'interruzione del funzionamento e la conseguente sospensione del servizio oppure può comportare la possibilità di accesso e manomissione di dati riservati da parte di personale non autorizzato
- programmi applicativi la cui modifica o cancellazione può compromettere l'esercizio di alcune funzioni del sistema informativo o alterarne le corrette caratteristiche di funzionamento;
- dati per i quali si richiedono riservatezza, integrità e disponibilità.

3.2 POLITICHE DI SICUREZZA FISICA

La Sicurezza fisica si realizza attraverso la protezione delle aree dedicate agli strumenti, specifici o di supporto, per l'elaborazione, la conservazione e la distribuzione delle informazioni.

Gli obiettivi che si vogliono conseguire sono:

- salvaguardare l'integrità fisica delle persone e l'integrità fisica e funzionale di apparati e locali;
- evitare che un'operazione non ammessa provochi un danno significativo per l' A.C. o per i soggetti che interagiscono con esso.

Le Politiche di Sicurezza Fisica sono espresse dalle seguenti norme:

- le caratteristiche dei locali utilizzati devono essere commisurate all'importanza delle risorse da proteggere;
- l'accesso ai locali deve essere limitato alle persone abilitate e deve esistere un sistema di monitoraggio degli accessi;
- nessuno può utilizzare una attrezzatura critica per la sicurezza se non autorizzato;

- nessuno può rimuovere od introdurre attrezzature o altri componenti informatici senza uno specifico documento di autorizzazione;
- devono esistere procedure che descrivano l'uso degli impianti ausiliari (condizionamento, alimentazione elettrica, antincendio, etc.) in condizioni normali ed in condizioni di emergenza; il personale deve essere istruito al riguardo gli impianti ausiliari devono essere periodicamente sottoposti a collaudo.

3.3 POLITICHE DI SICUREZZA LOGICA

La sicurezza logica si realizza attraverso la protezione del patrimonio informatico mediante soluzioni, sia hardware che software, rese operative dal sistema informatico stesso.

Gli obiettivi che si vogliono conseguire sono:

- controllo degli accessi alle risorse informatiche a salvaguardia da intrusioni ed attacchi interni ed esterni, sicurezza nella memorizzazione e trasmissione;
- disponibilità del servizio;
- disponibilità di informazioni che consentano di indagare su possibili violazioni;
- controllo del riutilizzo supporti.

Le Politiche di Sicurezza Logica sono espresse dalle seguenti norme:

- l'identità dell'utente deve essere certificata (User-id, Password);
- le modalità di strutturazione di user-id e password devono seguire, laddove la tecnologia lo permetta, ciò che viene impartito dalla normativa vigente (Art. 34, c. 1, lett. a) e regole da 1 a 11, Allegato B) tecnico in materia di protezione dei dati personali, Dlgs. N. 196/03)";
- ogni servizio richiesto viene reso disponibile solo se previsto dalle autorizzazioni dell'utente;
- si deve tenere opportuna traccia scritta delle operazioni individuate come critiche;
- tutti i dati critici devono essere memorizzati e trasmessi in modo sicuro;
- tutti i dati e le operazioni relativi alla gestione della sicurezza devono essere considerati critici;
- tutti i supporti riutilizzabili su cui sono stati memorizzati dati riservati devono essere opportunamente trattati prima del loro rilascio in modo che non si possano da essi desumere informazioni significative;
- il funzionamento delle applicazioni deve essere sempre ripristinabile a fronte di eventuali danneggiamenti.

3.4 RESPONSABILITÀ GENERALI

Le responsabilità, in termini di sicurezza, delle risorse informatiche sono suddivise nei seguenti termini generali:

- **Per quanto riguarda le strutture informatiche comuni (sistema di elaborazione centrale, reti di telecomunicazioni, server), le responsabilità fanno capo alla struttura deputata alla gestione dei sistemi informativi;**

- **Per quanto riguarda le risorse informatiche che fanno capo alle singole unità operative (es. personal computer), il capo di ogni unità operativa è individuato come responsabile delle proprie risorse.**

In entrambi i casi l'attuazione della protezione deve seguire le linee guida descritte negli specifici documenti di policy di sicurezza all'interno dell'organizzazione.

Ogni dipendente è responsabile dell'utilizzo delle risorse informatiche a lui assegnate ed utilizzate per l'espletamento della propria attività.

Le responsabilità nell'ambito della sicurezza dei sistemi informativi oltre che avere una valenza in termini di tutela del patrimonio ed in termini di tutela degli operatori e dei gestori, assume, alla luce del recente codice sulla privacy, anche una valenza giuridica.

4 Regole e Procedure

In questa sezione vengono illustrati i controlli per proteggere le informazioni in qualsiasi forma essi siano memorizzate, compreso posta elettronica, files su computer, programmi e documenti cartacei. In particolare, vengono definiti i controlli da attivare nel caso si trattino informazioni "critiche", ai fini della riservatezza e/o dell'integrità.

4.1 CLASSIFICAZIONE DELLE INFORMAZIONI

La classificazione delle informazioni costituisce l'attività basilare per la valutazione del rischio e quindi del potenziale danno che un loro non corretto utilizzo può apportare al patrimonio informativo dell'ufficio o di enti con cui essa interagisce.

La classificazione non deve essere riferita ai soli dati informatici, ma deve essere estesa a tutte le tipologie di informazioni e di documenti che li contengono oltre che ai programmi che li trattano indipendentemente dalla tipologia dei supporti su cui vengono memorizzati e registrati; per cui occorre prendere in considerazione anche le stampe, le linee di comunicazione, i documenti contenenti informazioni che non derivano direttamente da elaborazioni informatiche, ecc. E' perciò necessario prevedere un'opportuna classificazione delle informazioni sulla base del livello di riservatezza delle stesse.

Informazioni "critiche"

Nelle sue banche dati l'A.C. di RAVENNA mantiene informazioni relative ai Soci ACI (dati legali, piani di marketing, ecc.), nonché quelle che attengono alla sua gestione interna, per esempio:

- **Banca Dati Contabile dell'A.C..**
- **Banca Dati riferiti al personale.**

Queste informazioni consentono lo svolgimento dell'attività istituzionale dell' A.C.. Attraverso questi dati vengono svolte operazioni di marketing allo scopo di incrementare il potenziale associativo.
Tali informazioni "critiche" sono, quindi, molto importanti per il successo e gli affari presenti e futuri dell'Ente; l'accesso a tali informazioni da parte di persone non autorizzate porterebbe grave danno all'ufficio.

Responsabilità

Tutti i dipendenti sono responsabili di proteggere le informazioni "critiche" in loro possesso per motivi di lavoro.

La funzione aziendale che è preposta al trattamento dell'informazione o che la genera (titolare del dato) decide se questa è da considerarsi "critica" oppure no. Per decidere questo, la funzione aziendale fa una serie di considerazioni: il contenuto, il

valore dell'informazione, gli impatti contrattuali, gli impatti legali, ma soprattutto le indicazioni del Titolare dei Dati.
La classificazione di "critica" deve essere applicata solo alle informazioni che lo sono veramente e per il tempo strettamente necessario.

Anche le informazioni non classificate "critiche" possono avere valore per l'A.C. e quindi non devono essere divulgate a meno che l' Ente non ne autorizzi la diffusione, comunque in accordo con la legislazione italiana vigente.

Inoltre nessuna informazione deve essere divulgata alla stampa o agli organi di comunicazione o ad altri enti senza l'approvazione del vertice dell'Automobile Club di RAVENNA.

I **responsabili dei vari uffici** devono assicurarsi che le informazioni originate nella loro area siano correttamente classificate e che gli utilizzatori siano a conoscenza delle responsabilità definite in questo documento, sono responsabili, inoltre, di rendere indisponibili le informazioni "critiche" alle persone che non hanno più la necessità di esserne a conoscenza *(business need*).

Controlli per le informazioni "critiche"

- **Deve essere chiaramente indicata la classificazione "critica".**
- **Devono essere utilizzate solo dai dipendenti dell' Ente che ne hanno effettiva necessità.**
- **Devono essere custodite in modo da impedirne l'accesso a persone che non ne hanno la necessità.**

Tecnici di Società terze che intervengono sulla manutenzione dei PC in uso presso l'A.C., attraverso l'esportazione di dischi o supporti magnetici, devono necessariamente essere incaricati al trattamento dei dati automatizzati dal Titolare.

4.2 INCIDENTI E VIOLAZIONI

Devono essere attivate opportune procedure per minimizzare il rischio derivante da violazioni delle misure di sicurezza e per garantire un'adeguata e tempestiva segnalazione dei reali o sospetti incidenti o violazioni.
Un incidente, nell'ambito della sicurezza dei sistemi informativi, è un evento, un evento sospetto od una vulnerabilità tale da violare l'integrità, la confidenzialità o la disponibilità delle applicazioni o dei dati del sistema; nel caso di individuazione o di sospetto riguardante un incidente deve essere data immediatamente segnalazione alle strutture preposte.

4.3 GESTIONE DEGLI INCIDENTI

4.3.1 Premessa

E necessario stabilire le norme e le responsabilità per la denuncia, le indagini e la prevenzione di incidenti di sicurezza.

Sono considerati incidenti di sicurezza tutti quegli eventi che possono provocare un danno ai dipendenti, alle sedi o agli impianti dell' A.C., una perdita di beni o informazioni di valore per la Ente.
Sono anche considerati incidenti di sicurezza le violazioni alle leggi dello Stato, che si dovessero verificare nell'A.C. o che coinvolgano il proprio personale.

4.3.2 Incidenti gravi

Sono considerati "gravi" i seguenti incidenti:

1. Azioni violente o tentate azioni violente contro l'A.C. o il proprio personale (es: attentati alla sede, sequestro di persona, bombe, minacce di bombe).
2. Perdita o potenziale perdita di informazioni "critiche".
3. Qualsiasi incidente di sicurezza che possa portare al licenziamento o alla denuncia alle Pubbliche Autorità di un dipendente dell'A.C..
4. Ogni situazione che attivi un "Piano di Emergenza" per la sede.
5. Frodi, furti di denaro, tangenti, ecc. ai danni dell' Ente.
6. Perdite ricorrenti di proprietà, la cui ripetitività metta in evidenza possibili carenze di protezione.
7. Danni, distruzione di beni dell' Ente a causa di incidenti, disastri naturali o azioni ostili.
8. Utilizzo non appropriato o non corretto di informazioni e di beni dell'A.C..
9. Gravi violazioni di leggi italiane, nella sede dell'A.C. da parte di dipendenti della Ente.

4.3.3 Direttive

Ogni incidente di sicurezza deve essere immediatamente identificato e comunicato al proprio superiore diretto. Deve essere effettuata un'analisi dei fatti e devono essere prese le opportune azioni correttive.

Gli incidenti considerati "gravi" devono essere immediatamente comunicati al **Direttore dell'A.C. RAVENNA**.
E' compito del **Direttore dell'A.C. RAVENNA** coinvolgere le Pubbliche Autorità per gli eventuali adempimenti di legge.

Il rilascio di informazioni alla stampa o agli organi di informazioni deve essere dato solo dal **Direttore dell'A.C. RAVENNA** o da persona da lui esplicitamente delegata.

Ogni dipendente che ha subito sottrazioni di beni personali o sia stato vittima di reati durante la sua permanenza nei locali dell'A.C., ha comunque il diritto di tutelarsi mediante denuncia agli organi di Pubblica Sicurezza o di invocarne l'intervento.

Le informazioni relative agli incidenti di sicurezza sono da classificare “critiche” e quindi da trattare secondo quanto riportato nel capitolo “Sicurezza Logica” del presente Manuale.

4.3.4 Responsabilità

- **Direttore dell’A.C. RAVENNA**

Ogni capo, nella cui area di responsabilità si sia verificato un qualsiasi incidente di sicurezza, deve:

1. appurare lo svolgimento dei fatti, avvalendosi, se il caso lo richiede, della collaborazione di altre funzioni
2. redigere un rapporto dettagliato al **Direttore dell’A.C. RAVENNA**
3. definire gli eventuali provvedimenti per prevenirne il ripetersi.

4.4 PROGRAMMI E SOFTWARE PERICOLOSI (VIRUS INFORMATICI)

Per minimizzare i rischi derivanti dall‘introduzione di programmi (virus informatici) e/o software pericolosi, devono essere attivate e strettamente seguite le opportune misure di sicurezza al fine di individuare tempestivamente infezioni virali, eliminarne gli effetti e bloccarne la diffusione. Data la natura del fenomeno è fondamentale, oltre che attenersi alle norme operative diramate, dare immediata informativa alla struttura preposta alla gestione della sicurezza nel caso di individuazione o sospetto di casi relativi ad infezione da virus informatici

5 Il Sistema Informativo e i rischi connessi all'accesso alla rete Internet

5.1 PREMESSA

In questo paragrafo vengono elencati rapidamente alcuni dei rischi indotti dalla presenza di collegamenti alla rete internet. Vengono quindi individuate le più comuni contromisure tecniche adottabili per garantire l'operatività delle infrastrutture informatiche ed assicurare il livello di sicurezza minimo ritenuto adeguato alle proprie esigenze. Uno dei principi basilari da tenere in mente, nella definizione delle politiche di sicurezza e nella scelta degli strumenti tecnologici di supporto è quello relativo alla proporzionalità dei costi. In generale infatti la spesa per assicurare il necessario livello di protezione dovrebbe essere inferiore al costo da sostenere per il recovery dei danni a seguito di un attacco subito. In altre parole la spesa per la sicurezza ed i meccanismi adottati dovranno sempre essere attentamente dimensionati, evitando il ricorso a tecnologie troppo sofisticate, costose e difficili da amministrare. Vale la pena ricordare che nella quantificazione del potenziale danno vanno considerati, oltre al valore economico, anche elementi a volte trascurati come, ad esempio, la reputazione, l'affidabilità ed in genere l'immagine dell'Automobile Club.

I rischi sono stati suddivisi molto semplicemente in **esterni** ed **interni,** a seconda della provenienza della minaccia. Contrariamente a quanto ci si potrebbe aspettare è stato dimostrato che molto spesso gli attacchi più seri e dannosi provengono dall'interno e sono opera di soggetti che conoscono la struttura della rete e dei servizi su di essa veicolati ed hanno avuto accesso, magari per le funzioni ricoperte, ai principali sistemi di elaborazione.

5.2 RISCHI ESTERNI

- Accessi non desiderati: la connessione ad Internet sottopone alla possibilità di accessi alla rete interna da soggetti estranei e non autorizzati, esponendo le postazioni di lavoro e i dati in esse contenuti a rischio di manomissione o sottrazione;

- Virus: la navigazione Internet e ed il servizio di posta elettronica sono i principali veicoli di diffusione dei virus. I rischi connessi al contagio da virus informatico sono la perdita dei dati, l'accesso agli stessi da parte di soggetti estranei e non autorizzati, il blocco dei PC o di altri dispositivi connessi alla rete, il sovraccarico della stessa;
- E-MAIL Spamming: con questo nome si intendono le problematiche legate alla ricezione di un traffico di e-mail fasulle, non richieste e non sollecitate; tale rischio se non gestito può provocare :

    1. blocco dei server di posta elettronica
    2. aumento del traffico di rete e relativo sovraccarico con rallentamento delle applicazioni e relativi disservizi;

- Intercettazione dei dati: i dati trasmessi da un PC prima di giungere a destinazione attraversando la rete Internet, per definizione pubblica e non protetta, vengono gestiti da diversi apparati. Esiste quindi la possibilità che i dati vengano intercettati lungo il cammino e modificati oppure soltanto letti, con evidente violazione della privacy e dell'integrità degli stessi.

- Denial Of Service (DOS): utilizzando diverse tecniche, anche in coordinamento con altri soggetti attaccanti, è possibile per un malintenzionato far sì che un servizio, (come ad esempio il sito web istituzionale), divenga non più disponibile agli utenti autorizzati.

5.3 RISCHI INTERNI

- Trasmissione illecita di dati attraverso Internet: è possibile che chi ha ottenuto accesso a dati sensibili o riservati li possa trasmettere su Internet a soggetti non autorizzati a ricevere/manipolare quei dati;
- Navigazione su siti Internet con contenuti offensivi e/o forti o comunque non pertinenti con l'attività lavorativa: la navigazione libera su Internet dovrebbe essere sottoposta a filtraggio evitando che dalla rete interna si possano raggiungere siti con contenuti ritenuti non pertinenti;
- Traffico non consentito: la navigazione —libera" in Internet può interferire pesantemente con le attività istituzionali: lo scarico/scambio di immagini, di file musicali e video, (attraverso i così detti meccanismi di peer to peer), se non regolamentato finisce inevitabilmente col sovraccaricare la rete. Sono possibili politiche che vanno dal non consentire traffico al di fuori del necessario per l'attività lavorativa a politiche che restringano tali attività limitandole ad esempio a determinate fasce orarie o, più efficacemente adottando strumenti di partizionamento del traffico che, in modo automatico assegnano alle attività istituzionali la capienza di banda necessaria penalizzando gli accessi —liberi".
- Manomissione, danneggiamento di sistemi, apertura di back door. Qualora il personale deputato all'amministrazione dei sistemi lasci, per motivi di varia natura (quiescenza, ecc), l'ufficio sarà necessario revocare immediatamente tutte le autorizzazioni e provvedere alla generazione di nuovi account. In caso contrario eventuali malintenzionati potrebbero sfruttare le conoscenze acquisite, nello svolgimento delle attività lavorative, per acquisire il controllo dei sistemi dall'esterno o in generale per provvedere al loro danneggiamento o manomissione, compromettendone anche le informazioni contenute al loro interno.

5.4 L'ORGANIZZAZIONE PER LA SICUREZZA

Premessa

Prima di addentrarsi nell'esame degli strumenti tecnici a disposizione nell'ambito della sicurezza informatica è importante sottolineare, ancora una volta, la necessità di un cambiamento di tipo culturale e di un nuovo approccio alle problematiche poste

dall‘utilizzo di sistemi informativi connessi in rete. La consapevolezza dei rischi in gioco, ottenuta attraverso la sensibilizzazione ed il coinvolgimento di tutti gli utenti dei sistemi informativi, insieme con una corretta organizzazione che guardi prima ai processi e poi ai prodotti, costituiscono infatti le premesse indispensabili per ottenere buoni risultati. La tecnologia da sola non è sufficiente. Un importante punto di riferimento in materia è costituito dalla direttiva del Ministro per l‘Innovazione del 16 gennaio 2002 in materia di sicurezza. Essa prevede e descrive le attività per posizionarsi su di un livello di sicurezza individuato come —base minima“, da cui partire per ulteriori iniziative di miglioramento. La direttiva suggerisce inoltre un modello per la gestione della sicurezza, da adattare alla realtà di ogni amministrazione che prevede essenzialmente i seguenti passi:

- definizione delle strategie generali (politiche);
- formalizzazione delle procedure e delle regole;
- controllo del rispetto delle norme (auditing);
- gestione dei problemi di sicurezza (incident management);

5.5 LE CONTROMISURE DI TIPO TECNICO

Al fine di minimizzare i rischi e gli effetti di attacchi informatici sono oggi a disposizione svariate contromisure di tipo tecnico. Le contromisure sotto elencate sono coerenti con le politiche di sicurezza dell’Automobile Club di RAVENNA.

La tecnologia offre una vasta gamma di strumenti di sicurezza informatica mirati a contrastare ciascuna delle vulnerabilità o dei rischi legati all‘utilizzo di postazioni di lavoro in rete, (sia essa Intranet o Internet).

Di seguito si indicano alcuni degli strumenti e delle tecnologie più comuni.

5.5.1 Firewall

Il Firewall e' un sistema che va posto al "confine" tra la rete locale interna e la rete Internet, in modo che tutto il traffico entrante ed uscente dalla rete interna sia costretto a transitare attraverso il firewall stesso. In tal modo le singole unità di traffico, i pacchetti, possono essere esaminate applicando la politica di sicurezza più adeguata. Il firewall realizza quindi una specie di 'barriera telematica' contro qualunque accesso non autorizzato in modo da proteggere il sistema locale da ogni indebita intrusione.

Una delle tipologie più comuni di firewall e quella così detta “Packet Filtering“. In questa configurazione il firewall controlla ogni pacchetto che transita e lo confronta con le regole che ha memorizzate per consentirne o meno il passaggio. Tale filtraggio viene effettuato specificando, protocollo per protocollo, le regole di accettazione o di rifiuto dei pacchetti associati. Le regole possono essere definite in modo molto flessibile. E‘ ad esempio possibile inibire completamente il traffico proveniente da determinate sottoreti o soltanto da alcune macchine ben individuate;

sarà possibile bloccare o abilitare singoli protocolli di rete scegliendo anche la direzione consentita.

Ad ogni modo la policy implementata sul firewall deve rispondere ai seguenti principi generali:

- Tutto il traffico deve essere proibito ad eccezione di quello esplicitamente permesso attraverso la compilazione delle rispettive regole;
- Il traffico permesso deve essere lo stretto necessario per permettere la normale operatività;
- Gli indirizzi di rete dei personal computer sulla rete interna devono essere mascherati e resi invisibili all'esterno della rete, al fine di garantirne maggiormente la sicurezza;
- deve esistere la possibilità di cifrare il traffico di rete, laddove necessario, mediante l'utilizzo di opportuni protocolli;

L'apparato firewall va posizionato nel segmento di rete tra il router di accesso ad Internet e la rete interna in modo che possa verificare tutto il traffico destinato o proveniente da reti esterne (Internet).

Il firewall deve essere configurato per tenere traccia del traffico analizzato, tramite file di log, per successive indagini.

5.5.2 Antivirus Gateway

Permette di esaminare il traffico generato dalla navigazione internet e dalla posta elettronica alla ricerca di eventuali Virus Informatici. Il server Antivirus Gateway si posiziona all'interno della LAN, ed opera, per il riconoscimento, sulla base di un archivio contenente le firme dei virus correntemente identificati. In caso di positività viene in genere inviato un allarme all'amministratore della sicurezza e, opzionalmente, all'utente. In genere l'elemento pericoloso viene rimosso o, nel peggiore dei casi, il messaggio infetto viene cancellato.
L'aggiornamento delle firme dei virus o dei trojan deve poter essere effettuata in maniera automatica e preferibilmente senza la supervisione di un operatore.

5.5.3 Sistema Antivirus

Il sistema antivirus permette di contrastare l'infezione dei PC da parte di virus informatici e trojan. Il sistema, nella sua architettura più articolata, si compone di una componente software server e di una componente client. La parte server deve essere installata su hardware dedicato e permette la gestione centralizzata della parte client. La parte client deve essere installata sui PC della rete interna e deve proteggere lo spazio disco dei PC dall'infezione di virus conosciuti.

La postazione server deve permettere di individuare facilmente quali postazioni sono infette ed eventualmente tentare di rimuovere l'infezione. Inoltre deve essere possibile da questa postazione inviare in maniera automatica e programmata gli aggiornamenti alle stazioni di lavoro connesse in rete.

L‘aggiornamento del database delle firme dei virus sul server centrale deve essere automatico e provenire direttamente dal sito del produttore.

5.5.4 URL Filtering

Si tratta di soluzioni software che consentono il filtraggio delle pagine web richieste dall‘utente bloccando quelle che puntano a siti con contenuti ritenuti non idonei. L‘elenco dei siti non permessi, la così detta —black list“ di navigazione, viene generalmente suddiviso in categorie (ad es. cinema, news, contenuti per adulti, chat, ecc.) e deve essere aggiornato in maniera periodica.

Le categorie proibite o permesse potranno tener conto di diversi fattori legati alla sensibilità degli utilizzatori, all‘utilità e alla pertinenza dei contenuti con l‘attività svolta. Potrà essere lasciata facoltà a particolari gruppi di utenti di visitare categorie di siti proibite ad altri e viceversa. Questo meccanismo richiede quindi che il filtraggio sia basato anche sull‘identificazione dell‘utente che sta navigando.

5.5.5 VPN - (Virtual Private network)

Consente di cifrare e contrassegnare i messaggi in maniera elettronica in modo che siano inintelligibili a chi è estraneo alla comunicazione e che sia possibile rivelare eventuali manomissioni del messaggio. Grazie opportuni algoritmi è possibile identificare reciprocamente il mittente ed il destinatario della comunicazione. In generale non è difficile configurare una VPN tra due sistemi tramite l‘utilizzo del protocollo IPSEC, che va opportunamente configurato su entrambi gli host. Un‘alternativa all‘utilizzo di tale protocollo può essere il ricorso a prodotti di terze parti, basati solitamente su protocolli proprietari e venduti sotto forma di pacchetti software da installare sulle entità che devono comunicare o come componenti hardware.

Riferimenti legislativi

5.6 PROTEZIONE DEI SISTEMI INFORMATICI DA ATTACCHI ESTERNI (CRIMINALITÀ INFORMATICA)

La legge 547/93, ha modificato alcuni articoli del codice penale, introducendo nel nostro sistema una serie di "crimini informatici", che comportano a carico del reo, l'irrogazione di pene variabili fino ad un massimo di cinque anni di reclusione:

- *Attentato a impianti informatici di pubblica utilità (art. 420)*
- *Falsificazione di documenti informatici (art. 491bis)*
- *Accesso abusivo ad un sistema informatico o telematico (art. 615ter)*
- *Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615quater)*
- *Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615quinquies)*
- *Violazione di corrispondenza telematica (artt. 616-617sexies);*
- *Intercettazione di e-mail (art. 617quater)*
- *Danneggiamento di sistemi informatici e telematici (art. 635bis)*
- *Frode informatica (alterazione dell'integrità di dati allo scopo di procurarsi un ingiusto profitto) (art. 640ter)*

L'introduzione di queste figure di reato impone una riflessione sulle "conseguenze aziendali" di comportamenti penalmente rilevanti, tenuti da dipendenti dell'Ente o da terzi:

- *L'Ente dovrà adottare tutti i dispositivi di sicurezza necessari (password, codici di accesso, ecc.), per difendere i propri sistemi informatici da attacchi esterni, sia come misura di opportuna prevenzione, ma anche per consentire, nella malaugurata ipotesi che simili intrusioni si verificassero, l'incriminazione del soggetto attivo, con la conseguente richiesta di danni in sede civile;*
- *Dovranno essere posti in atto tutti gli interventi necessari a ridurre i rischi di coinvolgimento dell'Ente, nell'ipotesi che i reati siano commessi dai propri dipendenti che, utilizzando gli strumenti aziendali, si introducano abusivamente nei sistemi informatici di terzi.*

Ferma la responsabilità dell'autore del comportamento illecito, il nostro ordinamento penale prevede infatti la categoria dei cosiddetti "reati omissivi impropri" (art. 40 c.p.) che si concretizzano nella violazione di un generico obbligo giuridico di impedire determinati eventi dannosi. Per giurisprudenza e dottrina unanimi, tra le fonti di tale obbligo rientra sicuramente la posizione di controllo connaturata ad un rapporto di lavoro subordinato.

Nel caso dei "reati informatici" sebbene la condotta criminosa sia caratterizzata da un comportamento positivo da parte dell'autore, un coinvolgimento penale anche del datore di lavoro, a titolo di concorso nel reato commesso da un proprio dipendente, non può essere pertanto aprioristicamente escluso, qualora le circostanze concrete dimostrino, che il comportamento criminoso del dipendente sia stato agevolato dalla

mancata adozione, da parte del datore di lavoro, di idonee misure di prevenzione e controllo.

Considerazioni del tutto analoghe a quelle precedenti, valgono in relazione a possibili coinvolgimenti penali del datore di lavoro in relazione a comportamenti dei propri dipendenti che integrino la fattispecie di reato prevista dall'art. 171bis della legge 22 aprile 1941 n. 633, come modificata dalla Legge 18 agosto 2000 n. 248, in materia di abusiva duplicazione e/o commercializzazione di programmi per elaboratore
Un'altra ipotesi di reato, sanzionato con pene rilevanti, è il cosiddetto "trattamento illecito dei dati personali", che si estrinseca nell'uso dei dati personali per scopi diversi da quelli consentiti dalla legge e allo scopo di trarne profitto.

L'ipotesi di reato più interessante e innovativa è rappresentata dall'"Omessa adozione di misure necessarie alla sicurezza dei dati": "Chiunque, essendovi tenuto, omette di adottare le misure necessarie a garantire la sicurezza dei dati personali, in violazione delle disposizioni dei regolamenti [...], è punito con la reclusione fino ad un anno. Se dal fatto deriva nocumento, la pena è della reclusione da due mesi a due anni". Costituisce un trattamento sanzionatorio molto severo a carico del responsabile della sicurezza, se si considera che è prevista la punibilità anche del comportamento semplicemente colposo, per negligenza, imperizia o imprudenza.

- ***Legge 18 agosto 2000 n. 248***

"Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore". Integrato dal D.L. 15 marzo 1996 n. 205 e che sostituisce il precedente D.L. 518/92;

- ***Legge 23 dicembre 1993 n. 547***

"Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica";

- ***Direttiva UE 95/46/CE del 24 ottobre 1995***

La direttiva è "relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" L'art. 32 della Direttiva ne prevede il recepimento da parte degli Stati membri "al più tardi alla scadenza del terzo anno successivo alla sua adozione" (23 ottobre 1998);

- ***Dlgs. 196/03***

"Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" che recepisce la direttiva dell'Unione Europea del punto precedente.