LA SICUREZZA INFORMATICA

Premessa.

Il problema della «sicurezza delle informazioni» è antico quanto l'Uomo, o almeno, quanto l'Uomo da quando può comunicare. Un tempo la «riservatezza» delle informazioni riguardava prettamente il settore militare: per migliaia di anni sovrani e generali hanno avuto il bisogno di comunicazioni efficienti per governare i loro paesi e comandare i loro eserciti, consapevoli delle conseguenze che avrebbe avuto la caduta dei loro messaggi in mano ostili.

In epoca moderna la segretezza delle informazioni, ha indotto le nazioni a creare dipartimenti di crittografia con il compito di garantire la sicurezza delle informazioni, escogitando e impiegando i migliori sistemi di scrittura segreta.

La «crittografia», cioè la scienza che si occupa di come codificare un messaggio e di come successivamente decodificarlo, ha avuto una progressiva evoluzione nel corso dei secoli, fino ai rapidi sviluppi teorici e tecnologici impressi dalla seconda guerra mondiale, che permisero la decifrazione dei codici giapponesi e tedeschi da parte degli alleati.

Nel V secolo a.C. era ben sviluppata la «steganografia», l'arte cioè di "coprire la scrittura". Gli spartani, ad esempio, inviavano gli ordini ai capi militari tramite messaggi scritti su una striscia di cuoio che, avvolta su un bastone (lo scitale) di un diametro ben preciso, permetteva di leggere il testo in chiaro lungo il bastone. Erodoto nelle "Storie" narra della pratica inventata da Istieo per comunicare l'ordine di ribellione ad Aristagora, di rasare la testa del più fidato degli schiavi, per incidervi poi il messaggio ed inviarlo al destinatario dopo che fossero ricresciuti i capelli (libro V) o ancora la tecnica di Demarato di raschiare la cera da una tavoletta doppia, incidervi il messaggio da recapitare e ricoprirlo nuovamente di cera (libro VII). Da Plinio il Vecchio (I secolo d.C.) ad Umberto Eco ("Il nome della rosa), la letteratura è disseminata di esempi di scrittura a base di limone o latice di titimabo, che appaiono invisibili, ma ricompaiono una volta che il testo venga esposto a una fonte di calore (cd. inchiostro simpatico).

Tuttavia il punto debole di quest'arte, la possibilità cioè di scoprire il messaggio, favorì lo sviluppo e l'evoluzione della crittografia, non solo scienza ma vera e propria arte di "nascondere il messaggio", più precisamente il suo significato rendendolo incomprensibile secondo un procedimento preconcordato dal mittente e dal destinatario. Si narra che lo stesso Giulio Cesare fosse solito cifrare i propri messaggi sostituendo ogni lettera con quella che nell'alfabeto segue di qualche posizione.

Con l'avvento della società dell'informazione, basata cioè sull'uso delle informazioni come parte integrante delle attività umane, la necessità di sicurezza delle informazioni è diventata una componente della sicurezza dei beni in generale, o *security*, e non si limita alle tecniche per nascondere il contenuto dei messaggi. Se, sotto quest'ultimo aspetto, i crittosistemi classici (disco cifrante, enigma) sono stati ormai soppiantati da un cifrario a doppia chiave di sicurezza, pubblica e privata, la sicurezza informatica si snoda su due livelli di protezione dagli attacchi informatici: a livello fisico e materiale, ponendo gli strumenti (pc, server) in luoghi sicuri possibilmente dotati di sorveglianza e di controllo degli accessi; a livello immateriale attraverso un sistema di autorizzazioni per l'accesso degli utenti quale baluardo per la tutela dei dati personali.

La nozione di sicurezza informatica.

L'importanza acquisita dalla protezione dei dati personali nella società dell'informazione porta alla necessità di garantire la sicurezza del contesto in cui gli stessi vengono trattati, e ciò ha contribuito

all'affermazione della sicurezza informatica quale snodo fondamentale nel percorso evolutivo della tutela della privacy.
La locuzione sicurezza informatica si connota di significati spesso ambivalenti e difficilmente sovrapponibili, tanto che non è possibile neppure individuarne una definizione univoca, se non astraendosi da qualsivoglia contesto e profilo di analisi.
In linea generale, infatti, con il termine sicurezza s'intende una situazione di affidabilità che induce qualsiasi soggetto a sentirsi protetto rispetto all'ambiente esterno e difeso da situazioni di pericolo e di aggressione che possano compromettere la sua sfera di azione.
Generalmente considerata come la branca dell'informatica che si occupa della salvaguardia dai potenziali rischi o violazione di dati, una delle principali definizioni esistenti in letteratura considera la sicurezza informatica quale "scienza che studia come proteggere le informazioni elaborate o trasferite elettronicamente da atti indesiderabili che possono avvenire accidentalmente o essere frutto di azioni colpose o dolose" (Perri, 2003).
Una definizione che tuttavia necessita di un'ulteriore specificazione di natura economica con la conseguenza che la sicurezza informatica deve considerarsi lo studio, lo sviluppo e l'attuazione delle strategie, delle politiche e dei piani operativi volti a prevenire, fronteggiare e superare eventi in prevalenza di natura dolosa e/o colposa, in grado di danneggiare le risorse materiali, immateriali e umane di cui l'azienda dispone e necessita per garantirsi un'adeguata capacità concorrenziale.
Ad ogni modo, ogni definizione evidenzia due aspetti fondamentali della sicurezza informatica: da un lato la prevenzione o protezione contro accesso, distruzione o alterazione di risorse ed informazioni da parte di utenti non autorizzati; dall'altro l'abilità del sistema adottato a proteggere non solo le informazioni e le risorse, ma anche il sistema stesso rispetto ai principi cardini della sicurezza informatica: confidentialità (confidentiality), integrità (integrity), autenticazione (authentication), controllo degli accessi (control access), non ripudio (non-repudiaton), disponibilità (availability), privatezza (privacy).
Dal punto di vista dei requisiti, di seguito meglio specificati, la sicurezza informatica può essere definita come l'insieme delle misure, di carattere organizzativo e tecnologico, atte a garantire l'autenticazione dell'utente, la disponibilità, l'integrità e la riservatezza delle informazioni e dei servizi, gestiti o erogati in modo digitale.

Sicurezza informatica attiva e passiva.

I due livelli di protezione, materiale e immateriale, propri della sicurezza informatica e le considerazioni fin qui svolte consentono di operare una distinzione tra i concetti di sicurezza attiva e passiva, tra loro complementari ed entrambe necessarie per raggiungere un ottimale livello di sicurezza del sistema informatico.
Per **Sicurezza Attiva** si intendono le tecniche e gli strumenti mediante i quali le informazioni e i dati di natura riservata sono resi sicuri, proteggendo gli stessi sia dalla possibilità che un utente non autorizzato possa accedervi, sia dalla possibilità che un utente non autorizzato possa modificarli o danneggiarli.
Per **Sicurezza Passiva**, invece, normalmente si vuol intendere le tecniche e gli strumenti di tipo difensivo, cioè l'insieme di soluzioni che hanno come obiettivo l'impedimento agli utenti non autorizzati di accedere a risorse, sistemi, informazioni e dati di natura riservata. Quindi il concetto di sicurezza passiva è molto ampio in quanto fa riferimento a svariate componenti quali l'accesso a

locali protetti, l'utilizzo di porte di accesso blindate, congiunti all'impiego di sistemi di identificazione personale.

I requisiti della sicurezza informatica.

1- CONFIDENZIALITA'**(confidentiality):** assicura che le informazioni non siano accessibili ad utenti non autorizzati;

2- INTEGRITA' **(integrity): a**ssicura che le informazioni non siano alterabili da persona non autorizzate (in maniera invisibile agli utenti autorizzati). Il sistema deve cioè impedire l'alterazione diretta o indiretta delle informazioni, sia da parte di utenti e processi non autorizzati, sia in seguito ad eventi accidentali. Inoltre, il sistema deve impedire e comunque rilevare alterazione dirette o indirette delle informazioni da parte di utenti o procedure non autorizzati o a causa di eventi accidentali; ovvero la riduzione a livelli accettabili del rischio di cancellazioni o modifiche di informazioni a seguito sia di fatti accidentali e/o naturali, che di atti dolosi di soggetti non autorizzati.
Il concetto riguarda altresì il grado di correttezza, coerenza e affidabilità sia delle informazioni, sia delle risorse informatiche. Per le prime rileva il fatto che esse non possano venire alterate, cancellate o modificate per errore o per dolo, e che all'interno di un database, per esempio, i dati siano tra loro coerenti. Con riferimento all'hardware, l'integrità si riferisce invece alla corretta elaborazione dei dati, alla garanzia di un adeguato livello delle prestazioni, al corretto instradamento dei dati in rete e così via. Quanto infine al software, ci si riferisce a fattori come la coerenza, la completezza e la correttezza delle applicazioni, la correttezza dei file di sistema, dei file di configurazione etc.

3- AUTENTICAZIONE **(athentication):** assicura che gli utenti siano effettivamente chi dichiarano di essere. I processi di «autenticazione» servono a verificare l'identità di chi sta accedendo ad un dato sistema, attraverso un procedimento che può essere di questo tipo:
a) esecuzione di test sull'identità dell'utente;
b) utilizzo di credenziali da parte dell'utente come prova della propria identità (password, certificato digitale, dispositivo biometrico, token);
c) successivamente all'autenticazione gli viene concesso l'accesso alle sole risorse per cui è autorizzato (ad es. mediante controlli di accesso, permessi, privilegi). L'Autorizzazione consiste nel diritto accordato all'utente (che può essere una persona, ma anche un software) di accedere ad un sistema e alle sue risorse, in base ad un dato profilo.

4-RISERVATEZZA (**privacy**): assicura che gli utenti possano controllare quali informazioni su di sé vengono raccolte, come vengono usate, chi le usa, chi le mantiene, e per quale scopo vengono usate. Nessun utente deve poter ottenere o dedurre dal sistema informazioni che non è autorizzato a conoscere.
La riservatezza consiste dunque nella riduzione a livelli accettabili del rischio di accesso improprio e dell'utilizzazione dell'informazione da parte di soggetti non autorizzati.
La riservatezza si può realizzare sia nella fase di archiviazione dell'informazione, sia nelle fasi di comunicazione.

5- CONTROLLO DEGLI ACCESSI (**access control**): consiste nell'assicurare che gli utenti abbiano accesso unicamente a tutte le risorse e a tutti i servizi cui sono autorizzati. Esso è strettamente connesso al canone dell'autenticazione.
6-NON RIPUDIO (**non-repudiation**): assicura che il mittente di un messaggio non possa negare il fatto di aver spedito il messaggio. Esso è strettamente connesso al canone dell'autenticità: il requisito del non ripudio consente di avere la certezza che una data informazione appartenga a chi dice di averla generata (autenticità), con la conseguenza che chi ha generato una data informazione non deve poter negare di averlo fatto (non ripudio).

7- DISPONIBILITA' (**availability**): assicura che un sistema sia operativo e funzionale in ogni momento (non deny-of-service); il sistema deve rendere disponibili a ciascun utente abilitato le informazioni alle quali ha diritto di accedere, nei tempi e nei modi previsti.
Nei sistemi informatici, i requisiti di disponibilità sono legati anche a quelli di prestazione e di robustezza: il sistema deve garantire la disponibilità delle informazioni a ciascun utente autorizzato nei modi e nei tempi previsti (politiche aziendali), ovvero la riduzione a livelli accettabili del rischio di impedimento agli utenti autorizzati di fruire del sistema informativo e di accedere e utilizzare le informazioni, sia a seguito di fatti accidentali e/o naturali che di atti dolosi di soggetti non autorizzati
Garantire la disponibilità delle informazioni significa far sì che queste siano accessibili agli utenti che ne hanno diritto, nel momento in cui essi lo richiedano. Questo significa che i sistemi, la rete e le applicazioni debbono fornire le prestazioni richieste e che in caso di malfunzionamento ovvero di eventi catastrofici esistano delle procedure, degli strumenti e delle persone, in grado di ripristinare la completa funzionalità dei sistemi in tempi accettabili (disaster recovery).
Si deve quindi: 1. preservare la disponibilità delle condizioni ambientali (energia, temperatura, umidità, etc.), utilizzando idonei sistemi di controllo, sistemi di climatizzazione e gruppi di continuità; 2. preservare la disponibilità delle risorse hardware e software anche a fronte di problemi di varia natura (guasti, errori, disastri, ecc.), utilizzando sistemi di backup (per gli archivi) e sistemi ridondanti (per l'hardware); 3. preservare i sistemi da attacchi esterni.

Le principali modalità di attacco al sistema informatico.
1) Exploit: codice che sfrutta una vulnerabilità di un software per acquisire i privilegi di un computer. Gli exploit vengono in genere pubblicati sui bollettini di sicurezza perché sono una "prova tangibile" dell'esistenza di un bug**.**

2) Cracking: la modifica di un software per rimuovere la protezione dalla copia, oppure per ottenere accesso a un'area altrimenti riservata; si intende anche la violazione di sistemi informatici collegati ad Internet, allo scopo di danneggiarli, di rubare informazioni oppure di sfruttare i servizi telematici della vittima (es. connessione ad Internet, traffico voce, sms, accesso a database, ecc.) senza la sua autorizzazione;

3) Backdoor: in informatica sono paragonabili a porte di servizio (cioè le porte del retro) che consentono di superare in parte o in tutto le procedure di sicurezza attivate in un sistema informatico. Sono usate per consentire ad un utente esterno di prendere il controllo remoto della macchina senza l'autorizzazione del proprietario.

4) Sniffing: svolge l'attività di intercettazione passiva dei dati che transitano in una rete telematica (intercettazione fraudolenta di password o altre informazioni sensibili);

5) Trojan o trojan horse: deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente installa ed esegue anche il codice trojan nascosto; esso è composto generalmente da 2 file: il file server, che viene installato nella macchina vittima, e un file client, usato dall'attaccante per inviare istruzioni che il server esegue;

6) Virus informatici: si tratta di un software che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, generalmente senza farsi rilevare dall'utente. I virus possono essere o non essere direttamente dannosi per il sistema operativo che li ospita, ma nel caso migliore comportano comunque un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso. In generale un virus danneggia direttamente solo il software della macchina che lo ospita, ma esso può indirettamente provocare danni anche all'hardware, ad esempio causando il surriscaldamento della CPU, oppure fermando la ventola di raffreddamento;

6) Worm: si tratta di malware che non hanno bisogno di infettare altri file per diffondersi, perché modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet. Per indurre gli utenti ad eseguirli utilizzano tecniche di ingegneria sociale, oppure sfruttano dei difetti (Bug) di alcuni programmi per diffondersi automaticamente. Il loro scopo è rallentare il sistema con operazioni inutili o dannose.

7) Spyware: software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato. Le informazioni carpite possono essere di vario tipo: dalle abitudini di navigazione fino alle password e alle chiavi crittografiche di un utente.

8) Dialer: questi programmi si occupano di gestire la connessione ad Internet tramite la normale linea telefonica. Sono malware quando vengono utilizzati in modo illecito, modificando il numero telefonico chiamato dalla connessione predefinita con uno a tariffazione speciale, allo scopo di trarne illecito profitto all'insaputa dell'utente.

9) Adware: programmi software che presentano all'utente messaggi pubblicitari durante l'uso, a fronte di un prezzo ridotto o nullo. Possono causare danni quali rallentamenti del pc e rischi per la privacy in quanto comunicano le abitudini di navigazione ad un server rem.

Possibili conseguenze degli attacchi:

1) alterazione/interruzione di processi nel trattamento dei dati. Si riferisce al possibile degrado o addirittura all'interruzione dei processi "di trattamento";
2) alterazione/interruzione del processo cui si riferisce il dato;
3) alterazione/interruzione di altri processi correlati. Si riferisce al fatto che il dato potrebbe essere condiviso da più processi che pertanto verrebbero parimenti compromessi da una sua perdita di disponibilità;

4) violazione delle norme di legge sulla criminalità informatica (L. 547/93). Si riferisce alle sanzioni penali qualora, nel caso di perdita di integrità del dato, si configuri uno dei reati previsti dalla legge citata (es. la diffusione di virus, anche se non dolosa, rientra in questa fattispecie);
5) violazione delle norme di legge sulla tutela del software (L. 518/92). Si riferisce alle sanzioni penali nel caso di violazione delle leggi citate. La perdita di integrità del dato in questo caso è prodotta dal suo utilizzo con software non autorizzato e/o non funzionante correttamente;
6) violazione obblighi di legge sulla conservazione dei dati. Si determina qualora il danneggiamento coinvolga dati che debbano essere conservati integri come indicato dalle varie norme in materia;
7) divulgazione di informazioni riservate con violazione di norme interne. Si manifesta quando vengano violate norme interne con accesso non autorizzato a dati sensibili e si riferisce alle sanzioni previste dalla legge per violazione alla segretezza dei dati sensibili;
8) alterazione di processi amministrativi. Si riferisce al fatto che la perdita di riservatezza in processi amministrativi può avere conseguenze rilevanti;
9) ricatti e/o minacce dall'esterno. Si concretizza in possibili azioni di rivalsa effettuate all'Amministrazione da soggetti esterni, venuti in possesso di informazioni riservate;
10) rivendicazioni interne. Si concretizza invece in azioni da parte di personale interno che utilizzi informazioni riservate per perseguire propri scopi.

Le principali tecniche di difesa dagli attacchi.

1) Antivirus: consente di proteggere il proprio pc da software dannosi conosciuti come virus. Un buon antivirus deve essere costantemente aggiornato e deve avere in continua esecuzione le funzioni di scansione in tempo reale. Per un miglior utilizzo l'utente dovrebbe avviare con regolarità la scansione dei dispositivi del PC (dischi fissi, CD, DVD e dischetti floppy), per verificare la presenza di virus. Per evitare la diffusione di virus è inoltre utile controllare tutti i file che si ricevono o che vengono spediti tramite posta elettronica facendoli verificare dall'antivirus. Gli Anti-virus non sono in grado normalmente di proteggere in maniera completa un sistema informatico, ma necessitano di essere abbinati ad altri software come gli Anti-Malware, Anti-spam, i Firewall, etc..

2)Antispyware: software facilmente reperibile sul web in versione freeware, shareware o a pagamento. È diventato utilissimo per la rimozione di "file spia", gli spyware, che sono in grado di ottenere informazioni riguardanti le attività-on-line dell'utente ed inviarle ad un'organizzazione che le utilizzerà per trarne profitto.

3) Firewall: letteralmente "muro tagliafuoco", è un componente passivo (fisico) di difesa perimetrale di una rete informatica, che può anche svolgere funzioni di collegamento tra due o più parti di rete. Se installato e ben configurato garantisce un sistema di controllo degli accessi verificando tutto il traffico che lo attraversa. Protegge contro aggressioni provenienti dall'esterno e blocca eventuali programmi presenti sul computer che tentano di accedere ad internet senza il controllo dell'utente.

4) Firma digitale, Crittografia: è possibile proteggere documenti e dati sensibili da accessi non autorizzati utilizzando meccanismi di sicurezza specifici quali la firma digitale e l'utilizzo di certificati digitali per identificare l'autorità di certificazione.

5) Intrusion Detection System (IDS): è un dispositivo software e hardware (a volte la combinazione di tutti e due) utilizzato per identificare accessi non autorizzati ai computer.
Gli IDS vengono utilizzati per rilevare tutti gli attacchi alle reti informatiche e ai computer. Un IDS è composto da quattro componenti principali:1. Uno o più "sensori" utilizzati per ricevere le informazioni dalla rete o dai computer; 2. Una "console" utilizzata per monitorare lo stato della rete e dei computer; 3. Un "motore" che analizza i dati prelevati dai sensori e provvede a individuare eventuali falle nella sicurezza informatica; 4. Il "motore di analisi" si appoggia ad un database ove sono memorizzate una serie di regole utilizzate per identificare violazioni della sicurezza.

6) Gli Anti-malware: (o più comunemente Anti-virus) sono dei software che hanno lo scopo di prevenire, rilevare ed eventualmente rendere inoffensivi i codici malware.

7) Anti-spam: lo spamming è l'invio di messaggi indesiderati (generalmente di tipo commerciale e pubblicitario) ed è noto anche col nome di «posta spazzatura». Lo spam viene inviato senza il permesso del destinatario ed è considerato altamente dannoso anche dagli Internet Service Provider, che vi si oppongono sia per i costi generati dal traffico indesiderato sia perché può costituire una violazione contrattuale della «Acceptable Use Policy» ed essere causa di interruzione dell'abbonamento da parte dell'utilizzatore. Gli antispam che analizzano la provenienza e/o il contenuto dei messaggi effettuano una azione di filtraggio.

8) Honeypot: letteralmente "barattolo del miele", è un sistema o componente hardware o software usato come «trappola» o "esca" a fini di protezione contro gli attacchi di pirati informatici. Normalmente è utilizzato per proteggere reti locali. Solitamente consiste in un computer dedicato o un sito web che «sembra» contenere informazioni importanti e preziose ma che in realtà non contiene informazioni sensibili.

Il ruolo della privacy.
L'evoluzione del concetto di sicurezza impone, alla luce dell'indissolubile legame tra i diritti sociali e i diritti di libertà, di riconsiderare i rapporti della stessa con la privacy, nel senso che non è più possibile concepire una contrapposizione degli stessi.
Il diritto alla sicurezza deve essere inteso come una delle molteplici espressioni del diritto di libertà che, al pari della riservatezza, è consacrato nella nostra Costituzione tanto da assumere la connotazione democratica .
Il ruolo della privacy e della sua legislazione assume in questo ambito un ruolo di garanzia e di controllo in funzione di quel giudizio di responsabilità che deve esistere affinché quest'apparente dicotomia si mantenga sempre nel giusto equilibrio.
Lo spionaggio, la sorveglianza e la conseguente aggressione alla privacy dei cittadini e di interi stati sovrani fa sempre più spesso notizia. Il concetto di sicurezza e di sorveglianza sono da decenni in totale evoluzione. La sicurezza è diventata una caratteristica costante e fondamentale del mondo moderno. Un mondo moderno che, per dirla come Bauman, è un mondo liquido. Si parla di modernità liquida come nuovo genere di modernità intendendola come individualizzata, privatizzata, incerta, flessibile, vulnerabile. Cittadini, lavoratori, consumatori, navigatori della Rete sono sempre in movimento, spesso privi di certezze, ma accettano il rischio che i loro movimenti

vengano monitorati, tracciati, localizzati e profilati. Anche l'esigenza di sicurezza e la necessità di privacy scivolano poco a poco in uno stato fluido. L'esigenza di sicurezza e l'aumento della capacità di sorveglianza sui dati personali dilaga. Un tempo la sorveglianza era solida, stabile, in qualche modo garantita da principi giuridici certi e da punti di riferimento indiscutibili. Oggi la sorveglianza tende a farsi liquida, soprattutto nei momenti in cui frammenti di dati personali, trattati per determinate finalità, divengono facilmente utilizzabili per altri scopi.

Ormai quando parliamo di privacy dei nostri dati abbiamo di fronte un concetto di riservatezza che si muove su un "doppio binario": da un lato, il trattamento dei dati dei consumatori, la profilazione delle nostre abitudini a fini di marketing e di studio del comportamento umano, e dall'altro il trattamento e la conservazione dei dati per finalità di accertamento, prevenzione e repressione dei reati nonché per esigenze di sicurezza nazionale.