La Sicurezza Informatica

In questa breve presentazione vi mostreremo vari aspetti che riguardano il ramo della "*Sicurezza Informatica*" :

1) *Sicurezza Informatica* »»»

2) *Tipi di sicurezza* »»»

3) *La sicurezza nelle aziende* »»»

4) *La sicurezza dei programmi* »»»

5) *Le principali tecniche di attacco & le principali tecniche di difesa da tali attacchi* »»»

La sicurezza informatica

Che cos'è la sicurezza informatica ?

La "*Sicurezza informatica*" è quella branca dell'informatica che si occupa della salvaguardia dei sistemi informatici da potenziali rischi o violazioni dei dati. I principali aspetti di protezione del dato sono l'integrità e la disponibilità

I due pilastri su cui si basa la protezione dagli attacchi informatici

La protezione dagli attacchi informatici viene ottenuta agendo su due livelli: innanzitutto a livello fisico e materiale, ponendo i server in luoghi il più possibile sicuri, dotati di sorveglianza e di controllo degli accessi; anche se questo accorgimento fa parte della sicurezza normale e non della "sicurezza informatica" è sempre il caso di far notare come spesso il fatto di adottare le tecniche più sofisticate generi un falso senso di sicurezza che può portare a trascurare quelle semplici. Il secondo livello è normalmente quello logico che prevede l'autorizzazione di un'entità che rappresenta l'utente nel sistema

I tipi di sicurezza

Sulla base delle osservazioni finora fatte è chiaro che quando si parla di "Sicurezza Informatica" spesso si distinguono i concetti di "*Sicurezza Passiva*" e "*Sicurezza Attiva*"

Che cosa si intende per "Sicurezza Passiva"?

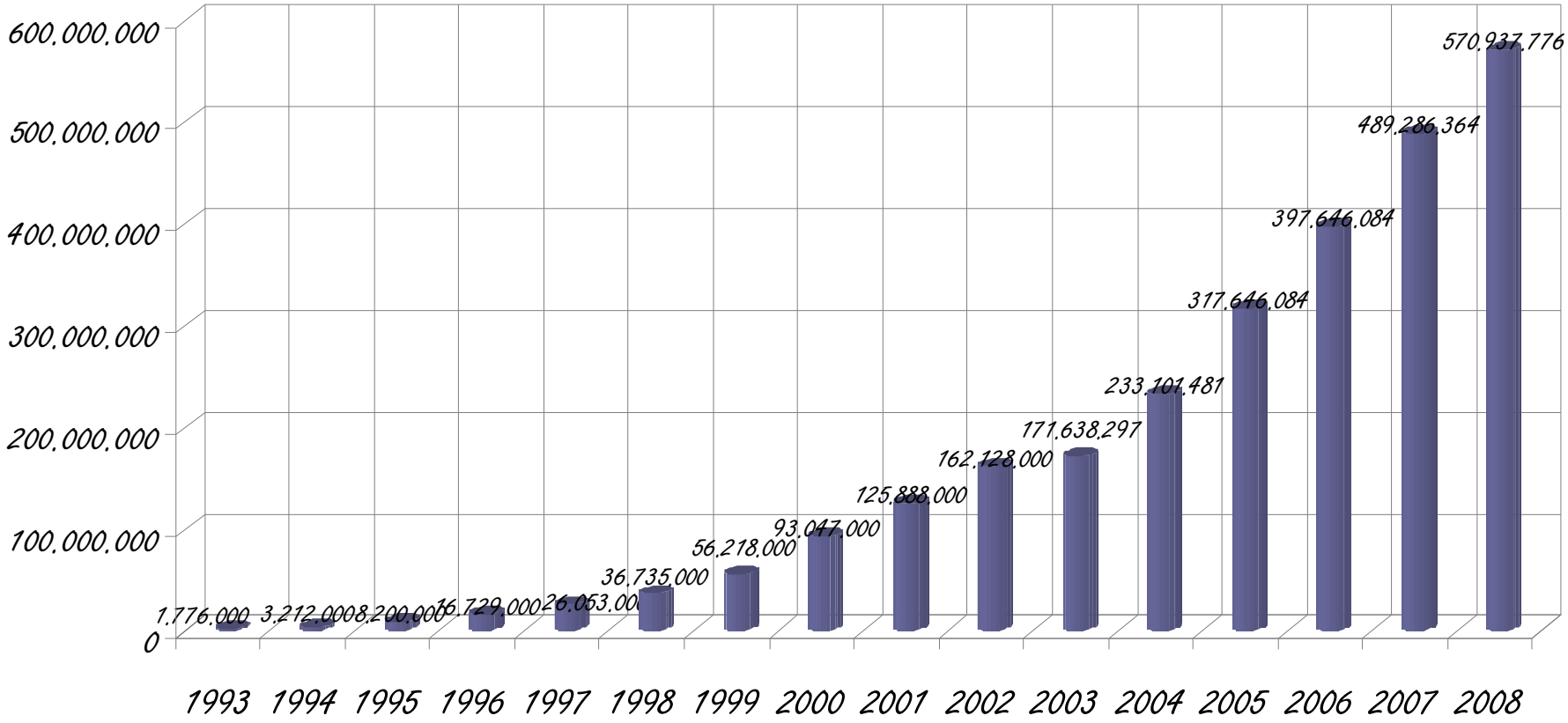
Per *sicurezza passiva* normalmente si vuol intendere le tecniche e gli strumenti di tipo *difensivo*, cioè quell'insieme di soluzioni che hanno come obiettivo l'impedimento agli utenti non autorizzati di accedere a risorse, sistemi, informazioni e dati di natura riservata. Quindi il concetto di sicurezza passiva è molto generale: ad esempio, per l'accesso a locali protetti, l'utilizzo di porte di accesso blindate, congiunti all'impiego di sistemi di identificazione personale, sono da considerarsi componenti di sicurezza passiva

Che cosa si intende per "Sicurezza Attiva"?

Per *sicurezza attiva* intendiamo, invece, le tecniche e gli strumenti mediante i quali le informazioni e i dati di natura riservata sono resi sicuri, proteggendo gli stessi sia dalla possibilità che un utente non autorizzato possa accedervi, sia dalla possibilità che un utente non autorizzato possa modificarli o danneggiarli.

È evidente ,quindi, che la sicurezza passiva e quella attiva sono tra loro complementari ed entrambe indispensabili per raggiungere il desiderato livello di sicurezza di un sistema

La crescita di Internet



Internet consente alle aziende di:

1. Effettuare commercio elettronico
2. Fornire un miglior servizio ai clienti
3. Ridurre i costi di comunicazione
4. Accedere facilmente alle informazioni

...Tuttavia...

Espone i computer delle aziende all'azione di attacchi da parte di malintenzionati, infatti :

1. Il numero di incidenti a causa di tali attacchi aumenta ogni anno
2. Le perdite finanziarie dovute a questi attacchi hanno raggiunto livelli misurabili in Miliardi di dollari

Indagine svolta dal FBI

Nel 2004, su 494 intervistati (aziende, agenzie governative, università ecc…)

1. Il 90% ha riportato incidenti legati alla sicurezza
   - I danni più seri riguardano il furto d'informazioni delicate e le frodi finanziarie
2. Il 75% ha subito solo un danno economico
   - Solo il 47% è stato in grado di quantificare l'ammontare del danno subito
3. Il 74% ritiene che la connessione ad Internet costituisca il maggior punto d'attacco
4. Solo il 34% ha denunciato gli incidenti subiti

Come si difendono le aziende ?

Dal momento che l'informazione è un bene che aggiunge valore all'impresa, e che ormai la maggior parte delle informazioni sono custodite su supporti informatici, ogni organizzazione deve essere in grado di garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento. Per questo esistono, a carico delle imprese che trattano i dati personali con strumenti elettronici, precisi obblighi in materia di privacy, tra cui quello di aggiornare annualmente uno specifico documento chiamato "documento programmatico sulla sicurezza"(documento con il quale si attesta la corretta adozione delle procedure che riguardano il trattamento dei dati personali). È stato anche approvato a livello internazionale il nuovo Standard ISO 27001:2005 finalizzato alla standardizzazione delle modalità adatte a proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponobilità.

Qual è l'intento degli attacchi ?

Le tecniche di attacco sono molteplici, perciò è necessario usare contemporaneamente diverse tecniche difensive per proteggere un sistema informatico, in modo da realizzare più barriere fra l'attaccante e l'obiettivo.
Spesso l'obiettivo dell'attaccante non è il sistema in sé, ma piuttosto i dati in essi contenuti, quindi la sicurezza informatica deve preoccuparsi di impedire l'accesso ad utenti non autorizzati, ma anche a soggetti con autorizzazione limitata a certe operazioni, per evitare che i dati appartenenti al sistema informatico vengano copiati, modificati, danneggiati o cancellati. Per prevenire le violazioni si utilizzano strumenti hardware e software.

Le principali tecniche di attacco

Le principali tecniche di attacco che possono recare danno al software e al sistema stesso sono molteplici, ne elencheremo solo alcuni:

1) Exploit [codice che sfrutta una vulnerabilità di un software per acquisire i privilegi di un computer]
2) Cracking [la modifica di un software per rimuovere la protezione dalla copia, oppure per ottenere accesso ad un'area altrimenti riservata; si intende anche la violazione di sistemi informatici collegati ad Internet, allo scopo di danneggiarli, di rubare informazioni oppure di sfruttare i servizi telematici della vittima (es. connesione ad Internet, traffico voce, sms, accesso a database ecc..) senza la sua autorizzazione]
3) Backdoor [in informatica sono paragonabili a *porte di servizio* (cioè le porte del retro) che consentono di superare in parte o in tutto le procedure di sicurezza attivate in un sistema informatico sono usate per consentire ad un utente esterno di prendere il controllo remoto della macchina senza l'autorizzazione del proprietario]

4) Sniffing [svolge l'attività di intercettazione passiva dei dati che transitano in una rete telematica(intercettazione fraudolenta di password o altre informazioni sensibili)]
5) Trojan [o **trojan horse** (dall'inglese Cavallo di Troia), Deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice *trojan* nascosto; esso è composto generalmente da 2 file: il file server, che viene installato nella macchina vittima, ed un file client, usato dall'attaccante per inviare istruzioni che il server esegue]
6) Virus Informatici [è un software, che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, generalmente senza farsi rilevare dall'utente. I virus possono essere o non essere direttamente dannosi per il sistema operativo che li ospita, ma anche nel caso migliore comportano un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso. In generale un virus danneggia direttamente solo il software della macchina che lo ospita, anche se esso può indirettamente provocare danni anche all'hardware, ad esempio causando il surriscaldamento della CPU, oppure fermando la ventola di raffreddamento]

Da chi vengono usate queste tecniche d'attacco

Le tecniche di attacco che abbiamo appena preso in considerazione vengono usate da individui che vengono classificati con il nome di Hacker.
L'Hacker non è altro che una persona che ama esplorare i dettagli dei sistemi informatici e i modi con cui estenderne la capacità, contrariamente alla maggioranza degli utenti, che impara solo lo stretto necessario.
Di Hacker possiamo dare anche quest'altra definizione ovvero una persona che programma con entusiasmo o che preferisce programmare piuttosto che discutere sulla programmazione

Classificazione

Gli Hacker si possono suddividere in 7 categorie principali:

1.Cracker: Programmatori specializzati nell'infrangere sistemi di sicurezza per sottrarre o distruggere dati.
2.Script Kiddie: Cracker che utilizzano script scritti da altri non essendo capaci di produrli da se.
3.Phracher: Rubano programmi che offrono servizi telefonici gratuiti o penetrano computer e database di società telefoniche.

4. Phreaker: Utilizzano informazioni telefoniche [es. numeri telefonici] per accedere ad altri computer.
5. Black Hat: Hacker "cattivo" che sfrutta le proprie abilità per delinquere.
6. White Hat: Hacker che si ritiene moralmente e legalmente onesto.
7. Grey Hat: È una via di mezzo tra Black e White Hat; non gli si può dare una definizione specifica.

Degli Hacker si deve fare un ulteriore distinzione, ovvero li si può distinguere in 2 insiemi:

1.Tipo positivo:

- Studente che ha come ideale rendere la tecnologia accessibile a tutti e creare soluzione a eventuali problemi legati all'informatica.

2.Tipo negativo:

- Individuo che sfrutta gli eventuali buchi nella sicurezza informatica per sottrarre dati, informazioni per utilizzarle a suo piacimento

La sicurezza dei programmi

Come ci possiamo difendere ?

Questa domanda si è posta all'attenzione degli sviluppatori di software come conseguenza della sensibile crescita dell'uso degli strumenti informatici e di internet. Per quanto riguarda la produzione di software "protetti" possiamo partire col definire il concetto di sicurezza come “l'assenza da condizioni conflittuali capaci di produrre danni mortali o irreparabili ad un sistema”. Nella progettazione di software è quindi fondamentale raggiungere il compromesso più funzionale tra l'efficienza d'uso del programma in questione e la sua capacità di "sopravvivenza" ad attacchi esterni e ad errori più o meno critici

Quali sono le caratteristiche della sicurezza ?

Due caratteristiche fondamentali esplicano il concetto di sicurezza:

- Safety (sicurezza): una serie di accorgimenti mirati ad eliminare la produzione di danni irreparabili all'interno del sistema;
- Reliability (affidabilità): prevenzione da eventi che possono produrre danni di qualsiasi gravità al sistema.

Un software (o programma) è tanto più sicuro quanto minori sono le probabilità di successo di un guasto e la gravità del danno conseguente al guasto stesso. Possiamo ora vedere, in ordine crescente, i possibili effetti dei guasti in cui può incorrere un software:

1) Nessun effetto
2) Rischio trascurabile
3) Rischio significativo
4) Rischio elevato
5) Rischio catastrofico

Gli errori di un programma

L'IEEE (Institute of Electrical and Electronics Engineers) ha catalogato gli errori nel software in tre diverse voci a seconda della natura degli errori stessi. Esse sono:

- Error: è un errore umano verificatosi durante il processo di interpretazione oppure durante il tentativo di risoluzione di un problema
- Failure: è un comportamento del software imprevisto ed incongruo rispetto alla funzionalità del programma stesso
- Fault: è un difetto del codice sorgente.

Gli errori di programma non nocivi, come ad esempio gli "spyware" ed il "buffer overflow" hanno la caratteristica di non modificare i file di sistema e non recare danno alle caratteristiche del sistema stesso.

Il controllo della sicurezza di un programma

Una volta prodotto il software si procede alla verifica del suo comportamento, in modo tale da effettuare una ricerca estesa dei difetti presenti, per passare poi alla loro eventuale eliminazione. Esistono diversi modelli di sicurezza per il controllo dei programmi basati su due metodi differenti:

Per essere efficace un programma deve essere controllato e deve essere privo di difetti nel codice, a questo fine viene effettuato un controllo del programma e delle prestazioni correlate all'affidabilità, in secondo luogo viene analizzata ogni parte di codice e funzione del sistema.

Tecniche di difesa

Quali sono le tecniche per difenderci dagli attacchi informatici ?

Ora vi mostreremo le principali tecniche di difesa che si possono adottare per difenderci al meglio dai vari attacchi informatici

1) Antivirus: consente di proteggere il proprio pc da software dannosi conosciuti come virus. Un buon antivirus deve essere costantemente aggiornato e deve avere in continua esecuzione le funzioni di scansione in tempo reale. Per un miglior utilizzo l'utente dovrebbe avviare con regolarità la scansione dei dispositivi del PC (dischi fissi, CD, DVD e dischetti floppy), per verificare la presenza di virus. Per evitare la diffusione di virus è inoltre utile controllare tutti i file che si ricevono o che vengono spediti tramite posta elettronica facendoli verificare dall'antivirus
2) Antispyware: software facilmente reperibile sul web in versione freeware, shareware o a pagamento. È diventato utilissimo per la rimozione di "file spia", gli spyware , che sono in grado di ottenere informazioni riguardanti le attività on-line dell'utente ed inviarle ad un'organizzazione che le utilizzerà per trarne profitto.
3) Firewall: installato e ben configurato garantisce un sistema di controllo degli accessi verificando tutto il traffico che lo attraversa. Protegge contro aggressioni provenienti dall'esterno e blocca eventuali programmi presenti sul computer che tentano di accedere ad internet senza il controllo dell'utente

4) Firma digitale, Crittografia: è possibile proteggere documenti e dati sensibili da accessi non autorizzati utilizzando meccanismi di sicurezza specifici quali: la firma digitale e l'utilizzo di certificati digitali per identificare l'autorità di certificazione.
5) Intrusion Detection System (IDS): è un dispositivo software e hardware (a volte la combinazione di tutti e due) utilizzato per identificare accessi non autorizzati ai computer. Gli IDS vengono utilizzati per rilevare tutti gli attacchi alle reti informatiche e ai computer. Un IDS è composto da quattro componenti principali:

1. Uno o più "sensori" utilizzati per ricevere le informazioni dalla rete o dai computer
2. Una "console" utilizzata per monitorare lo stato della rete e dei computer
3. Un "motore" che analizza i dati prelevati dai sensori e provvede a individuare eventuali falle nella sicurezza informatica
4. Il "motore di analisi" si appoggia ad un database ove sono memorizzate una serie di regole utilizzate per identificare violazioni della sicurezza.

Lavoro svolto dalla classe IV° G

Da

Amato Gaetano

Si ringrazia per la collaborazione

Arpaia Aniello

Mainardi Alfonso

Fine Presentazione