Università
degli Studi
della Campania
Luigi Vanvitelli

CORSO DI LAUREA IN TECNICHE DI RADIOLOGIA MEDICA
PER IMMAGINI E RADIOTERAPIA

CORSO DI: INFORMATICA
Lezione N°9

Anno Accademico 2017/2018

Dott. Silvio Pardi

Sicurezza Informatica

La sicurezza informatica è quella branca dell'informatica che si occupa di valutare il rischio, le minacce e i metodi di protezione dei dati e dei software presenti sui calcolatori.

Con lo sviluppo delle reti informatiche sulle quali viaggiano dati sensibili e sistemi di pagamento, tale tematica è diventata sempre più cruciale.

La sicurezza abbraccia numerosi aspetti.

Obiettivi della Sicurezza Informatica

Salvaguardare l'integrità dell'informazione

- Ridurre il rischio che i dati possano essere cancellati/modificati a seguito di interventi non autorizzati o fenomeni non controllabili e prevedere adeguate procedure di recupero delle informazioni

Salvaguardare la riservatezza dell'informazione

- Ridurre a livelli accettabili il rischio che un'entità possa accedere ai dati senza esserne autorizzata. t

Salvaguardare la disponibilità dell'informazione

- Ridurre il rischio che possa essere impedito alle entità autorizzate l'accesso alle informazioni a seguito di interventi non autorizzate o fenomeni non controllabili

Backup dei dati

Con il termine Backup si indica il processo di replicazione di dati su un supporto generico di memorizzazione che può essere un HD, un CD o un DVD, un sistema a nastro.

Esso consente di avare una copia di riserva dei dati in questione utile per il recupero di essi a seguito di una perdita o di una modifica dovuta a cause accidentali o dolose.

L'organizzazione del backup dei dati è una delle prime azioni di sicurezza informatica necessarie per la salvaguardia dell'integrità dell'informazione.

Il piano di Backup

L’organizzazione del Backup di dati importanti è una attività che ha diversi gradi di complessità in funzione della quantità dei dati da tenere al sicuro e della velocità con cui essi vengono prodotti.

Esempi:

- Backup delle immagini prodotte da un centro di radiologia
- Backup delle informazioni dei pazienti di un ospedale
- Backup delle informazioni dei dipendenti di un centro di radiologia

Chiamiamo **piano di backup** il processo di definizione di cosa salvare (dischi, database, cartelle, utenti, macchine, volumi, ecc.), frequenza, ora di avvio, supporto e percorso di archiviazione, tipo di backup (completo, differenziale, incrementale), modalità di compressione, tipo di log e messaggistica da esporre, tipo di verifica integrità, e molte altre opzioni a seconda della complessità del sistema.

Backup delle immagini mediche

Nei primi sistemi PACS le immagini venivano archiviate immediatamente su memoria locale ad accesso veloce (on-line) per poi essere spostate dopo 3 - 6 mesi, su DVD all'interno di un «juke-box», da dove potevano essere richiamate in automatico in caso di necessità senza intervento umano (near-line), ma con tempi di risposta notevolmente superiori.

I DVD più vecchi venivano quindi rimossi dal sottosistema near-line e immagazzinati in armadi ignifughi (off-line): in caso di necessità, gli esami potevano essere immessi nuovamente nel sistema.

Con la diminuzione dei costi delle memorie di massa e con la diffusione di tecnologie Cloud, è diventata prassi mantenere tutte le immagini nella memoria ad accesso immediato secondo il paradigma (everything-on-line) cioè su hard-disk; questo, assieme alle crescenti velocità delle reti, permette un tempo di accesso alle informazioni dell'ordine dei secondi per una singola immagine.

BUG e PATCH

Con il termine BUG si intende generalmente un errore nella scrittura del codice di un software.

I BUG possono affliggere tutti i tipi di software, compresi i sistemi operativi, i browser, o programmi utilità in generale.

Tali errori possono causare semplici malfunzionamenti del programma, o nei casi più gravi rendere il sistema vulnerabile ad attacchi informatici.

Con il termine PATCH si intende un codice creato ad hoc per risolvere o mitigare gli effetti di un BAG di un software.

Esempi di BUG

Millennium bug, è il nome di un errore di progettazione di molti software degli anni 90. Per rappresentare le date venivano utilizzate solo due cifre decimali per memorizzare l'anno; tali cifre potevano assumere i valori compresi da "00" a "99", dando per sottintesa, come base di partenza, l'anno 1900. In questo modo, al raggiungimento dell'anno 2000, le conseguenze sarebbero state imprevedibili. Per risolvere questo BUG furono prodotte delle PATCH per i maggiori sistemi operativi e software.

Allo scoccare del 1º gennaio 2000, il millennium bug non fece danni apocalittici:

- Negli Stati Uniti, i sistemi informatici del United States Naval Observatory riportarono la data 1º gennaio 19100 e un centinaio di slot machine andarono in tilt;
- In Giappone alcuni sistemi di raccolta informazioni di volo rilevarono diverse falle e la centrale nucleare di Onagawa ebbe problemi di raffreddamento;
- In Australia il sistema di convalida dei biglietti degli autobus non funzionò
- In Spagna e Corea del Sud si ebbero diversi problemi con tribunali che riportavano documenti con data impostata al 1900
- Nel Regno Unito vi furono problemi di transazione del denaro con alcune carte di credito.

Esempi di BUG

- Sonda spaziale USA (1962)

La sonda automatica Mariner 1 invece di dirigersi verso Venere, subito dopo il lancio punta verso il basso. **La NASA e' costretta a farla esplodere in volo** per evitare che causi danni precipitando sulla terra. Il rapporto pubblicato in seguito dalla NASA ammette che la causa dell'errore e' un singolo trattino mancante da una riga di codice Fortran del programma di guida automatica della sonda.

- Nave da guerra USA va in crash grazie a Windows (1997)

Nel settembre del 1997, l'incrociatore lanciamissili USS Yorktown, comandato da un avanzatissimo sistema di gestione computerizzata basato su Windows NT, va in crisi per un buffer overflow che costringe la nave a restare paralizzata in mare per due ore.

Esempi di BUG

Meltdown è una vulnerabilità hardware che colpisce microprocessori Intel e ARM, che permette a programmi e potenziali haler di accedere ad aree protette di memoria di un computer.

Spectre è una vulnerabilità hardware che consente ai processi dannosi di accedere al contenuto della memoria mappata di altri programmi.

La patch sviluppata per questi BUG rallenta la velocità dei processori di una percentuale significativa!

Malware

Con il termine Malware (malicious software) si indica un qualsiasi software usato per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata.

Il principale modo di propagazione del malware consiste di frammenti di software parassiti che si inseriscono in codice eseguibile già esistente.

Tipi di Malware

Virus: sono parti di codice che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto. Si trasmettono da un computer a un altro tramite lo spostamento di file infetti ad opera degli utenti.

Worm: Sono codici che modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet. Per indurre gli utenti ad eseguirli spesso sfruttano dei difetti (Bug) di alcuni programmi per diffondersi automaticamente. Il loro scopo è rallentare il sistema con operazioni inutili o dannose.

Tipi di Malware

Trojan horse: Malware con istruzioni dannose nascosto all’interno di programmi con delle funzionalità lecite o utili per indurre l'utente ad utilizzarli. Non possiedono funzioni di auto-replicazione, quindi per diffondersi devono essere consapevolmente eseguiti dall’utente. Il nome deriva dal famoso cavallo di Troia.

l**Backdoor:** Sono dei programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione. Tipicamente si diffondono in abbinamento ad un trojan o ad un worm, oppure costituiscono una forma di accesso lecita di emergenza ad un sistema, inserita per permettere ad esempio il recupero di una password dimenticata.

Tipi di Malware

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

Hijacker: questi programmi si appropriano di applicazioni di navigazione in rete (soprattutto browser) e causano l'apertura automatica di pagine web indesiderate.

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

Tipi di Malware

Malvertising: malicious advertising, sono degli attacchi che originano dalle pubblicità delle pagine web

Keylogger: I Keylogger sono dei programmi in grado di registrare tutto ciò che un utente digita su una tastiera o che copia e incolla rendendo così possibile il furto di password o di dati che potrebbero interessare qualcun altro. La differenza con gli Adware sta nel fatto che il computer non si accorge della presenza del keylogger e il programma non causa rallentamento del pc, passando così totalmente inosservato

Tipi di Malware

Ransomware: Virus che cripta tutti i dati presenti su un disco, secondo una chiave di cifratura complessa; poi, per ottenerla e decrittografare il computer, bisogna pagare il cracker che ha infettato il pc e quindi ottenere la chiave di cifratura per "tradurre" i dati.

Software Antivirus

Un Antivirus è un software che ha l'obiettivo di individuare ed eliminare virus da un calcolatore.

Poiché gli Antivirus sono in grado di identificare diversi tipi di malware si fa spesso confusione rispetto alla classificazione fatta nelle slide precedenti.

Nell'accezione moderna un Antivirus è quindi un sofware utilizato per individuare ed eliminare diversi tipi di malware.

Software Antivirus

Gli antivirus esaminano i file e la memoria del computer alla ricerca di «pattern» conosciuti, ovvero alla ricerca di codici già noti come software malevoli.

Per fare questo gli antivirus si appoggiano a database esterni che devono essere sempre aggiornati.

L'attività di analisi da parte degli antivirus è detta SCANSIONE e può richiedere anche molto tempo.

La scansione può essere fatta anche on-line in maniera proattiva su ogni file che viene ricevuto dalla rete.

Software Antivirus

Esistono due grandi famiglie di Antivirus

- Per Personal Computer: Per eseguire la scansione sul disco fisso di un PC o su una penna USB o su qualsiasi dispositivo locale
- Per Server o sistemi enterprise: Ad esempio per individuare software malevoli inviati su sistema di posta elettronica o per individuare messaggi di SPAM

Attacco informatico

Un Attacco informatico o Cyber Attack è un tentativo illegale di ottenere informazioni da un computer.

Sono generalmente classificati in

- Web-based attack
  - Attacchi informatici svolti ai danni di un sito web o di una applicazione web
- System-based attack
  - Attacchi informatici che hanno l'obiettivo di compromettere il sistema operativo di un computer o la rete

Injection attack

Un Injection attack consiste nell'inserimento di dati all'interno di un server web al fine di manipolare le informazioni di un sito o eseguire codice malevolo.

Gran parte dei siti web utilizzano dei database di supporto, una delle tecniche di attacco è inserire dati all'interno di questi database sfruttando dei bug o degli errori di progettazione di un sito. Si parla in questo caso di SQL Injection. L'obiettivo e far eseguire al server che ospita il sito web dei codici e ottenere l'accesso ad informazioni in maniera non autorizzata.

File inclusion attack

Un attacco di tipo File Inclusion viene eseguito su dei sistemi che offrono una particolare vulnerabilità

Cross-Site Scripting (XSS)

E’ un tipo di attacco che consiste nello scrivere un codice malevolo in un javascript di una pagina web. I javascript sono dei codici che verranno eseguiti dal client, ovvero dal browser dell’utente.

DNS Spoofing

È un tipo di attacco svolto sul servizio chiamato DNS (Domain Name Resolution) Tale servizio ha il compito di redirigere l’utente verso il server che contiene la pagina web cercata. Un attacco di tipo DNS Spoofing consiste nel modificare il servizio DNS redirigendo gli utenti verso server non corretti o malevoli

Denial of Services (DoS)

E’ un tipo di attacco che ha l’obiettivo di rendere un servizio o una pagina web non accessibili per gli utenti (es. servizio di posta)

E’ generalmente svolto affollando il servizio obiettivo con un grosso numero di richieste.

DDoS (Distributed DoS) è un attacco DoS che viene eseguito da più sistemi contemporaneamente, distribuiti sulla rete al fine di rendere difficile l’individuazione della sorgente del traffico malevolo.

Gli attacchi DoS sono classificati in

- Volume Based Attacks
  - Si ottiene occupando la rete che connette la pagina web alla rete
- Protocol Attacks
  - Ha l’obiettivo di saturare le risorse del server che offre il servizio
- Application Layer Attacks
  - L’obiettivo è ottenere il crash del server che offre il servizio

Web-Based Attack

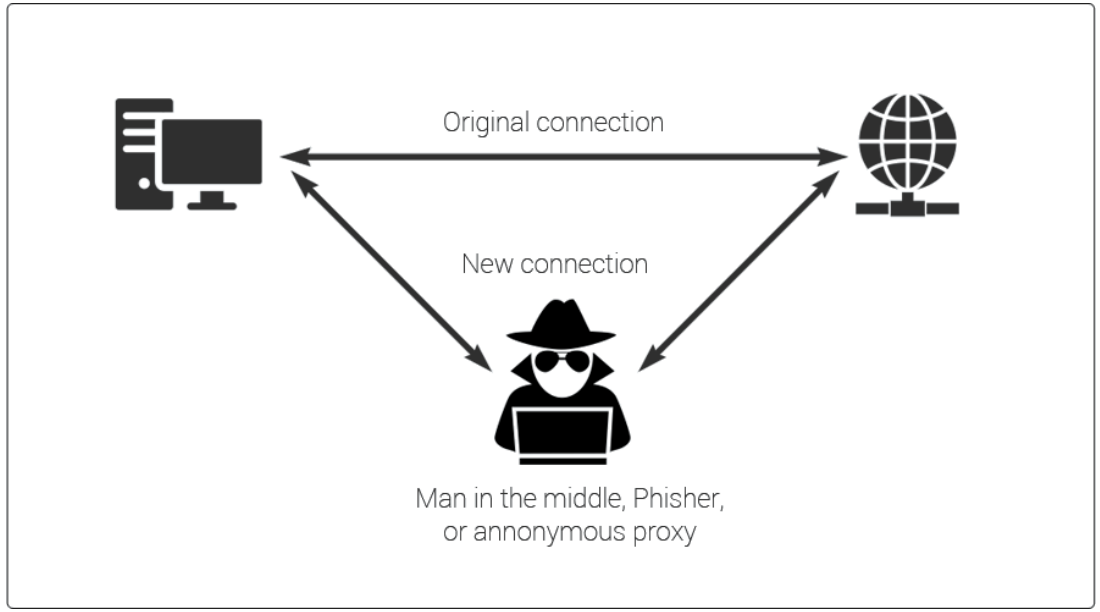
- Brute Force
  - È un metodo basato su tentativi
  - Si prova ad accedere a un servizio con le credenziali di un utente provando un grande numero di password create in maniera random
- Dictionary Attack
  - E’ come un brute force, ma anziché generare password random utilizza un dizionari di parole largamente utilizzate come password.
- Buffer overflow
  - Si ottiene costringendo un programma a memorizzare più dati di quanti possa gestire.

Web-Based Attack

Man in the middle:

In questo tipo di attacco, l'agente malevolo intercetta la connessione tra un client ed un server, quindi risponde al client fingendo di essere il servizio richiesto.

Mediante questo attacco è possibile quindi intercettare password o informazioni fornite in maniera ignara dall'utente che crede di interagire con il servizio corretto



Web-Based Attack

Phishing: L’obiettivo è quello di ottenere informazioni sensibili come password o PIN di sistemi bancari, bancoposta, email, paypal.

La tecnica consiste nella creazione di siti web identici a quelli dei siti ufficiali.

Successivo invio di email con richieste di accesso o di cambio password tramite i link indicati, che indirizzano verso le pagine web malevoli.

Firewall

Il firewall è una componente di rete che ha il compito di assicurare una connessione sicura sulla rete.

Il firewall può essere una componente hardware o software o una combinazione dei due.

L'obiettivo di un firewall è quello di proteggere le informazioni confidenziali e difendere il sistema da attacchi informatici provenienti da fuori o innescati da software malevoli.

I firewall possono difendere un intera rete oppure il singolo sistema

Firewall

Una delle tecniche più utilizzate dai firewall per proteggere il sistema da attacchi è il Packet filtering

Packet Filtering: Controlla i pacchetti ricevuti e inviati verificando i destinatari le sorgenti e il contenuto. Le informazioni ottenute possono essere analizzate e confrontate con database.

Un firewall può ad esempio bloccare un attacco DoS individuando la sorgente del traffico eccessivo o l'attvità di un WARM bloccando il traffico in uscita verso un sito malevolo.

Lo SPAM

Lo SPAM chiamato anche UCE (Unsolicited Commercial Email) è un attività che consiste nell'invio di messaggi verso moltissimi destinatari contemporaneamente.

Fenomeno cresciuto esponenzialmente a partire dagli anni 90

Gli obiettivi dello SPAM sono

- Invio di pubblicità
- Marketing (sistemi piramidali)
- Catene
- Messaggi Politici
- Frodi e attacchi informatici

Oggi si ritiene che oltre l'80% delle email inviate siano email di SPAM