SEMINARIO
IMPRESE DI SPEDIZIONE E CYBER SECURITY: ASPETTI LEGALI, ASSICURATIVI E TECNOLOGICI

FEDESPEDI

ALSEA

15 maggio 2018

REGOLAMENTO UE 679/2016 – MODIFICHE E NOVITA'

MODIFICHE

ruoli Titolare/Responsabile

informativa e consenso

esercizio diritti

data transfer

NOVITÀ

nuove definizioni

registro trattamenti

accountability

diritto all'oblio e portabilità dei dati

data breach

privacy by design – privacy by default

valutazione d'impatto

Data Protection Officer

estensione dell'ambito territoriale

sanzioni

REGOLAMENTO UE 679/2016 – DATA BREACH

Il GDPR amplia il novero dei business obbligati a notificare immediatamente, pena sanzioni elevate, alle Autorità e agli interessati i casi di *data breach* (violazione dei dati).

Occorre implementare monitoraggio dei sistemi critici e procedure di gestione in caso di evento.

Bisognerà fare in modo che la vostra organizzazione sappia esattamente cosa fare (individuazione, indagine, report, notifica) in caso di *data breach*.

REGOLAMENTO UE 679/2016 – ANALISI DEI RISCHI

Il Regolamento prevede l'obbligo di effettuare una valutazione dei Principali rischi per la sicurezza dei dati personali e dei principali rischi per i diritti e le libertà delle persone fisiche.

Il Titolare dovrà poi prevedere misure adeguate a limitare tali rischi.

L'art. 31 del d.lgs.196/2003 prevedeva un'analisi dei rischi derivanti da:

- distruzione o perdita dei dati (anche accidentale);
- Accesso non autorizzato;
- Trattamento non consentito o non conforme alla finalità della raccolta.

REGOLAMENTO UE 679/2016 – ANALISI DEI RISCHI

Articolo 32

*b) la capacità di assicurare su base permanente la **riservatezza, l'integrità, la disponibilità e la resilienza** dei sistemi e dei servizi di trattamento;*

resilienza: capacità di **reazione di un sistema** a fronte di eventi che mettono a rischio la sicurezza dei dati trattati dallo stesso.

*c) la capacità di ripristinare **tempestivamente** la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;*

Tempestivamente (al tempo giusto, nel momento opportuno, o, più spesso, in tempo utile) vs **non superiori a sette giorni**

punto 23 Allegato B al d.lgs.196/2003

*….. 23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e **non superiori a sette giorni……***

CYBER SECURITY & RIVOLUZIONE DIGITALE

DEFINIZIONI E CENNI STORICI

RIVOLUZIONE DIGITALE – CENNI STORICI

► Principali epoche in cui l'informatica viene identificata e divisa, cambiamenti delle tecnologie e rivoluzione digitale:

1960: Primi dispositivi elettronici - Sistemi centrali detti "***mainframe***";

1960-1970: Sistemi distribuiti - Mainframe e Terminali;

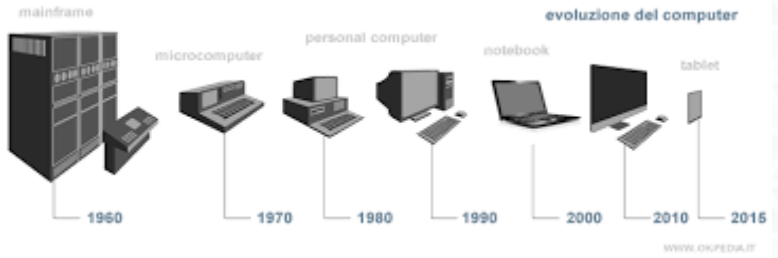
1980: Nascita del personal computer - Sistemi "**office**";

1980 ->: Sistemi in rete;

1990: Nascita di internet, cosidetto Web 1.0;

1990-2000: Ri-centralizzazione - ERP;

2000: Web 2.0 e nascita dei "**social network**".



RIVOLUZIONE DIGITALE – CENNI STORICI

CYBER SECURITY – DEFINIZIONE

- La ***Cyber Security*** rappresenta un insieme di **mezzi** e **tecnologie** tese alla protezione ed alla salvaguardia dei sistemi informatici, da potenziali rischi e/o violazioni di informazioni e dati.

  La crittografia risponde alle esigenze di sicurezza, in termini di:

  - confidenzialità: proteggere i dati dall'essere letti da persone non autorizzate;

  - integrità: proteggere i dati da modifiche non autorizzate;

  - autenticazione: verifica delle credenziali di accesso al sistema;

  - non ripudiabilità: il mittente non può disconoscere la paternità del messaggio.

- Coinvolgendo aspetti:

  - tecnici;

  - organizzativi;

  - giuridici;

  - umani.

CYBER SECURITY – NUMERI

- Negli ultimi quaranta anni sono stati compiuti molti passi riguardo la *Cyber Security* (**Sicurezza Informatica**), permettendo di definire adeguatamente sia la **materia** che **l'analisi** delle minacce e dei rischi ad essa correlati.

- A livello mondiale, il cybercrime è risultato la prima causa di attacchi gravi ai sistemi informatici nel 2017 (76% del totale) per un danno complessivo stimabile in **500 miliardi di dollari**.

CYBER SECURITY – NUMERI

Hacked companies 2011-2013

- **90%** of 600 companies suffered a computer hack in the past 12 months
- **77%** of companies were actually hacked multiple times
- The respondents reported having a very low confidence in their ability to prevent attacks
- Many believe they simply aren't prepared
- **53%** also believe they will experience an attack in the next 12 months.

CYBER SECURITY

ASPETTI TECNOLOGICI

CYBER SECURITY – ASPETTI TECNOLOGICI

Hacking:

- Accesso abusivo ad un sistema informatico finalizzato ad un uso della macchina non consentito;
- Richiede, di regola, che siano superate **almeno** le misure di sicurezza predisposte dall'amministratore di sistema;

- Comprende sia chi tenta di servirsi delle risorse di un computer non disponendo di **alcun tipo di autorizzazione**, sia il caso di chi, utente della macchina, dispone di un'autorizzazione **limitata a specifiche operazioni**.

CYBER SECURITY – ASPETTI TECNOLOGICI

- In termini generali, ogni sistema operativo, ogni software che gestisce un particolare servizio, nonché ogni protocollo che consente la trasmissione di dati possiede delle **debolezze intrinseche**;
- Esperti di sicurezza informatica e **hackers**, sono costantemente alla ricerca di tali falle;
- I primi tenteranno di **patcharle**, ossia di eliminarle, i secondi tenteranno invece di sfruttarle per i loro **progetti criminosi**.

CYBER SECURITY - ASPETTI TECNOLOGICI

- Essendo **l'informazione** una componente fondamentale per l'attività di ogni organizzazione, è necessario che sia adeguatamente protetta.

- La Sicurezza Informatica ha lo scopo di proteggere l'informazione nei confronti di un'ampia gamma di attacchi potenziali, al fine di garantire la continuità dell'attività e minimizzare i danni e le interruzioni di servizio.

- Laddove l'infrastruttura non sia **adeguatamente strutturata e protetta**, una possibile violazione potrebbe portare allo spegnimento di macchine e impianti, creando ingenti danni alle vittime degli attacchi.

CYBER SECURITY - ASPETTI TECNOLOGICI

- E' necessario individuare le **minacce**, le **vulnerabilità** ed i **rischi** associati a tutti gli asset informatici, al fine di proteggerli da possibili attacchi (**interni** o **esterni**) che potrebbero provocare danni diretti o indiretti di impatto superiore ad una deteminata soglia di tollerabilità.

- Ogni organizzazione deve dimostrare di 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 e costante aumento.

CYBER SECURITY

COME PROTEGGERSI

CYBER SECURITY - COME PROTEGGERSI

Physical security

Accesso fisico di utenti alle macchine

Operational/Procedural security

Policy di sicurezza

Personnel Security

…

System Security

Acl, log, …

Network Security

Firewall, IDS, Vpn, buon routing e filtri

Limitazione rischi

- Davvero serve una connessione permanente alla rete?

Uso di deterrenti

- Pubblicizzare strumenti di difesa e punizione.

Prevenzione

- Crittografia;
- Politiche;
- Antivirus.

Rilevamento

- Logging;
- Intrusion detection.

Reazione

- Intrusion management;
- System recovery;
- Tribunale.

CYBER SECURITY - COME PROTEGGERSI

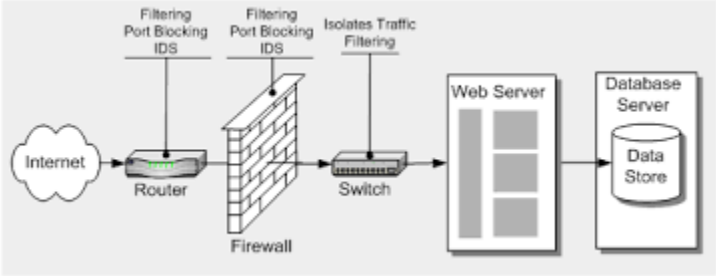
- Mettere in atto **puntuali strategie di protezione dei dati** è fondamentale per il successo di ogni azienda, in quanto i dati sono uno dei beni più preziosi per ogni business.

6 punti chiave:

1. Sapere quali sono i dati da proteggere (e dove sono);
2. Formare e sensibilizzare i dipendenti in termini di sicurezza;
3. Creare un elenco dei dipendenti che hanno accesso ai dati sensibili;
4. Effettuare un'analisi dei rischi;
5. Installare software di protezione affidabili e schedulare scansioni di sicurezza regolari;
6. Eseguire regolarmente il backup dei dati più importanti e sensibili.

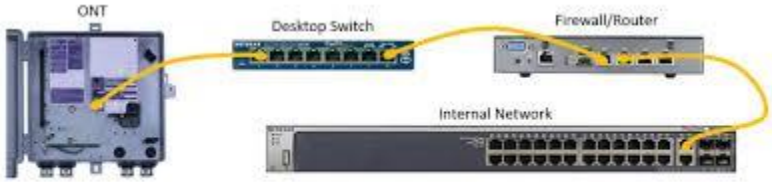
CYBER SECURITY - COME PROTEGGERSI

Metodi di protezione:



- Buona pianificazione della rete con hardware adeguato (**router**, **switch** ecc.) insieme alla divisione della rete in aree a livello di sicurezza variabile.

- Controllo dell'integrità delle applicazioni (**bugs free**) e verifica della correttezza delle configurazioni.



- Utilizzo di software che controllino e limitino il traffico di rete dall'esterno verso l'interno e viceversa (es. **firewall**, **router screening** ecc.)

CYBER SECURITY - COME PROTEGGERSI

- I **business leader** dovrebbero definire una strategia di sicurezza olistica a difesa dell'organizzazione;
- La conformità normativa non è sempre sufficiente;
- L'acquisto dei più recenti prodotti di sicurezza può prosciugare i budget senza migliorare la difesa complessiva;
- **<u>Un solido approccio alla cyber defense richiede un cambiamento di mentalità: l'organizzazione aziendale deve allearsi con il team responsabile della sicurezza;</u>**

CYBER SECURITY - COME PROTEGGERSI

- Utilizzo di applicazioni che integrino **algoritmi di crittografia** in grado di codificare i dati prima della loro trasmissione in rete (es. **PGP**, **SSH**, **SSL** ecc.)

- Aumentare la consapevolezza sulle minacce esistenti e illustrare le possibili misure a protezione di rete e produzione;

- E' necessario garantire la separazione dei ruoli fra i responsabili della gestione della sicurezza e gli utenti operativi.

CYBER SECURITY - COME PROTEGGERSI

- Le difese informatiche sono minacciate da avversari digitali fortemente motivati e che dispongono di grandi risorse;
- Gli hacker sono sofisticati professionisti che si avvalgono di tecniche all'avanguardia;
- I ladri informatici operano a livello transnazionale e raramente vengono perseguiti.

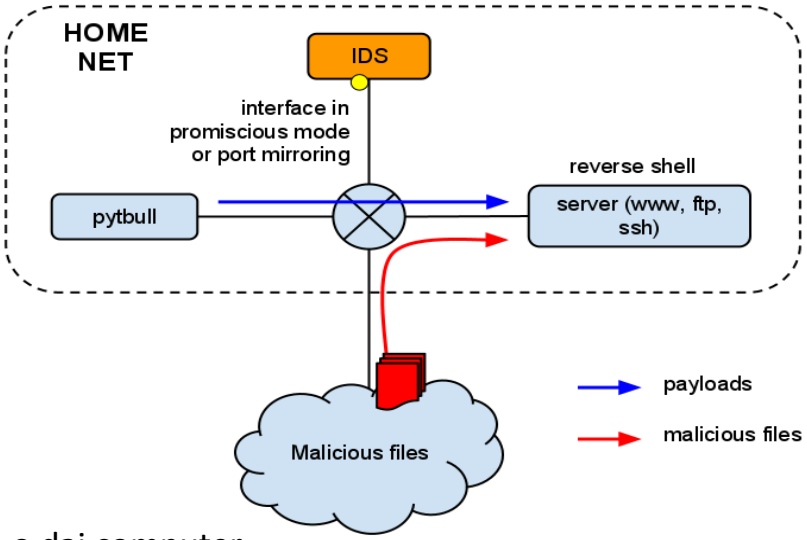
CYBER SECURITY - STRUMENTI DI DIFESA: FIREWALL

- Dispositivi **software** o **hardware** posti a protezione dei punti di interconnessione eventualmente esistenti tra una **rete privata** interna (ad es. una Intranet) ed una **rete pubblica** esterna (ad. es. Internet) oppure tra due reti differenti.

- La loro funzione principale è quella di agire come dei **filtri** controllando tutto il traffico di rete che proviene dall'esterno, nonché quello che viene generato dall'interno, permettendo soltanto quel traffico che risulta effettivamente autorizzato.

CYBER SECURITY - STRUMENTI DI DIFESA: IDS

- l'***Intrusion Detection System*** o IDS è un dispositivo software o hardware (o a volte la combinazione di entrambi, sotto forma di sistemi stand-alone pre-installati e pre-configurati) utilizzato per identificare accessi non autorizzati (**intrusioni**) ai computer o alle reti locali.



- Le intrusioni rilevate possono essere quelle prodotte da cracker esperti, da tool automatici o da utenti inesperti che utilizzano programmi semiautomatici.

- Un IDS è composto da **quattro** componenti:

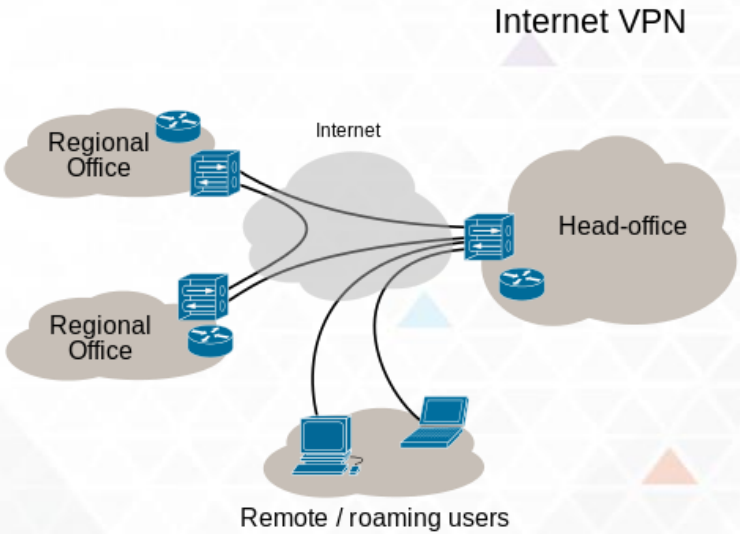
- Uno o più **sensori** utilizzati per ricevere le informazioni dalla rete o dai computer;
- Una **console** utilizzata per monitorare lo stato della rete e dei computer;
- Un **motore** che analizza i dati prelevati dai sensori e provvede a individuare eventuali falle nella sicurezza informatica;
- Un **database** cui si appoggia il motore di analisi e dove sono memorizzate una serie di regole utilizzate per identificare violazioni della sicurezza.

CYBER SECURITY - STRUMENTI DI DIFESA: VPN

- Una VPN (**Virtual Private Network**) è una rete di telecomunicazioni privata, instaurata tra soggetti che utilizzano, come tecnologia di trasporto, un protocollo di trasmissione pubblico e condiviso, come ad esempio la rete Internet.

- Il loro scopo è di offrire alle aziende, a un costo minore, le stesse possibilità delle **linee private a noleggio**, ma sfruttando reti condivise pubbliche.

- Può essere pensata anche come l'estensione a livello geografico di una **rete locale privata aziendale sicura** che colleghi tra loro siti interni all'azienda stessa variamente dislocati su un ampio territorio, equivalente a **un'infrastruttura fisica di rete dedicata**.



CYBER SECURITY - STRUMENTI DI DIFESA: SIEM

► **SIEM (Security Information and Event Management)**:
Ci si riferisce ad una serie di prodotti software e servizi che combinano/integrano le funzionalità offerte dai SIM (security information management) a quelle dei SEM (security event management);

► Il termine *security information and event management* è stato coniato da Mark Nicolett e Amrit Williams dell'azienda americana Gartner nel 2005.

Principali funzioni:

► Tracciare le autenticazioni attraverso i sistemi, individuando, se presenti, gli accessi non autorizzati;
► Rilevamento di malware e relative parti infette del sistema;
► Monitoraggio delle connessioni e del trasferimento dei dati;
► Rilevamento di connessioni sospette verso l'esterno;
► Violazione delle politiche interne del sistema;
► Tentativi di attacco e compromissione al corretto funzionamento delle applicazioni web.

CYBER SECURITY

SOCIAL ENGINEERING

CYBER SECURITY - SOCIAL ENGINEERING

- Non di soli malware vive l'hacker...
- I cyber criminali attraverso tattiche sofisticate tentano di accedere ai sistemi informatici delle loro vittime e trafugare dati e informazioni personali di ogni genere.
- Si tratta della cosiddetta **Social Engineering** (ingegneria sociale), ossia un insieme di tecniche a metà tra **psicologia** e **ingegneria**.

- L'hacker parte dallo studio dei **comportamenti delle vittime**, così da poter trovare un "**argomento comune**" di discussione e riuscire così a entrare nelle sue "grazie".
- E' approssimabile ad una **manipolazione psicologica** che induce chi ne è vittima ad assumere determinati comportamenti o rivelare informazioni personali senza rendersene realmente conto ed averne quindi realmente intenzione.

CYBER SECURITY - SOCIAL ENGINEERING

► Il cyber criminale deve studiare comportamenti, abitudini e preferenze della vittima, così da poter entrare in contatto con essa e **guadagnarne la fiducia**.

► Successivamente, saranno messe in campo **tecniche differenti** a seconda del profilo psicologico e sociale della persona da colpire.

► Per indurre l'utente ad agire secondo la propria volontà e i propri fini, l'hacker può mettere in campo l'autorevolezza (dimostrandosi, ad esempio, esperto di un determinato settore) oppure fare leva sulla paura o sul senso di colpa.

► **<u>Lo scopo principale dell'ingegneria sociale è ottenere informazioni e dati confidenziali in possesso della vittima, per poi portarla a fornire dati riservati oppure a installare autonomamente un malware</u>**.

CYBER SECURITY - SOCIAL ENGINEERING

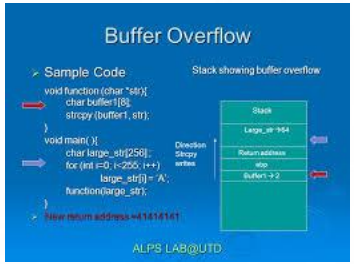
- Come difendersi dagli attacchi di ingegneria sociale?
- Il consiglio principale è quello di non fidarsi mai di nessuno su Internet;
- Quando uno sconosciuto ci contatta dobbiamo sempre essere diffidenti;
- E' necessario prestare particolare attenzione anche se l'interlocutore sembra gentile o riporta marchi e loghi famosi, come una banca, una grande azienda o si finge un conoscente;
- Attenzione alle e-mail che riceviamo dalle banche o da organi di polizia che ci chiedono di pagare multe o modificare i dati del nostro conto. Possono sembrare tentativi banali ma sono realizzati in maniera così verosimile da poter trarre in inganno anche persone solitamente attente alla sicurezza informatica.

CYBER SECURITY

TIPI DI ATTACCHI

CYBER SECURITY - TIPI DI ATTACCHI

- **Exploit:** Tipologia di *script*, *virus*, *worm* o binario che sfruttando una specifica vulnerabilità presente in un sistema informatico, permette l'esecuzione di codice malevolo su di esso, con lo scopo di far ottenere all'attaccante l'acquisizione dei privilegi amministrativi.



- **Buffer Overflow**: E' una condizione di errore che si verifica a runtime, quando in un buffer di memoria di una data dimensione, vengono scritti dati di dimensioni maggiori. Tale falla permette comportamenti imprevisti da parte del software e del sistema operativo, permettendo all'attaccante di prendere possesso della macchina.

- **Shellcode:** E' un programma in linguaggio assembly che tradizionalmente esegue una shell. Può essere utilizzato per sfruttare un bug mediante un exploit, consentendo di acquisire l'accesso alla riga di comando di un computer, o più in generale di eseguire codice arbitrario.

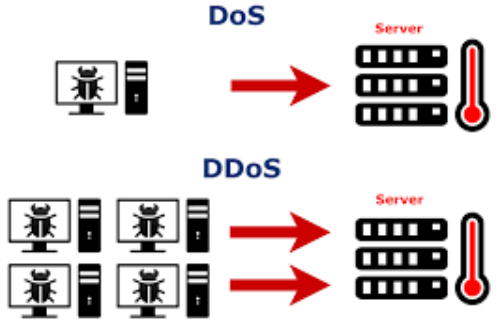
CYBER SECURITY - TIPI DI ATTACCHI

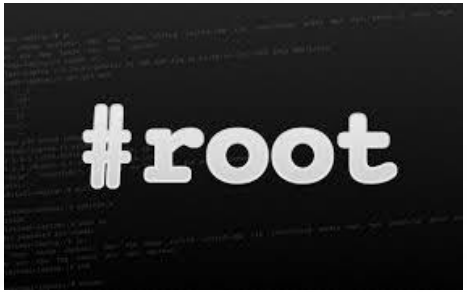
- **Cracking**: violazione di sistemi informatici collegati ad Internet o ad un'altra rete, allo scopo di **danneggiarli**, di **rubare informazioni** oppure di **sfruttare i servizi telematici** della vittima (connessione ad Internet, traffico voce, sms, accesso a database etc..) senza la sua autorizzazione.

- **Trojan:** Indica un tipo di malware, il quale nasconde il suo funzionamento all'interno di un altro programma apparentemente utile e innocuo. L'utente, eseguendo o installando quest'ultimo programma, in effetti attiva anche il codice del trojan nascosto.

CYBER SECURITY - TIPI DI ATTACCHI

- ***Dos/DDos** (Denial of Service) :* Lo scopo di questo tipo di attacco è **saturare deliberatamente le risorse** di un sistema che fornisce un servizio ai client, ad esempio un sito web su un web server, fino a renderlo **non più in grado di erogare il servizio** ai client richiedenti. Nell'attacco DDoS - (*Distributed Denial of Service*), il traffico in entrata che inonda la vittima proviene da **molte fonti diverse**. Ciò rende effettivamente impossibile fermare l'attacco semplicemente bloccando una singola fonte (***Botnet***).





- ***Escalating privilege**:* Inteso come sorpasso delle autorizzazioni, rappresenta lo sfruttamento di una falla, di un errore di progetto o di configurazione di un software applicativo o di un sistema operativo al fine di acquisire il controllo di risorse macchina normalmente precluse a un utente o a un'applicazione. Un'applicazione con maggiori autorizzazioni di quelle previste dallo sviluppo originale o fissate dall'amministratore di sistema può mettere in opera azioni impreviste e non autorizzate.

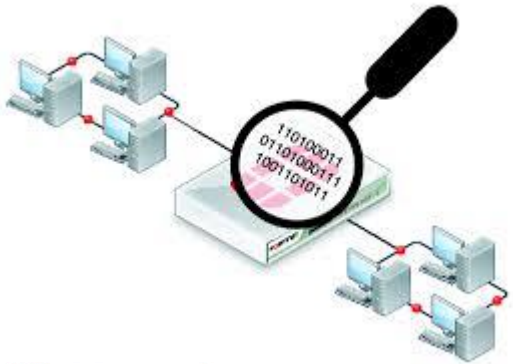
CYBER SECURITY - TIPI DI ATTACCHI

- ***Backdoor:*** è un metodo per **bypassare** la normale **autenticazione** in un sistema informatico, un crittosistema o un algoritmo, che può celarsi segretamente all'interno di un ignaro programma di sistema, di un software separato, o può anche essere un componente hardware malevolo.

- Sono spesso scritte in diversi linguaggi di programmazione e hanno la funzione principale di superare le difese imposte da un sistema, come può essere un firewall, al fine di accedere in remoto a un personal computer, ottenendo il completo o parziale possesso del bersaglio.

CYBER SECURITY - TIPI DI ATTACCHI

- ***Port Scanning:*** è una tecnica informatica progettata per sondare un server o un host al fine di stabilire quali **porte** siano in ascolto sulla macchina. Questa tecnica è spesso utilizzato dagli amministratori per verificare le politiche di sicurezza delle loro reti, e dagli hacker per identificare i servizi in esecuzione su un host e sfruttarne le vulnerabilità. Elaborando le risposte è possibile stabilire (anche con precisione) quali servizi di rete siano attivi su quel computer.



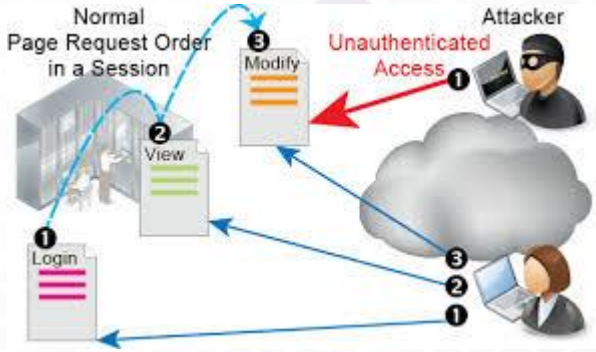
- ***Packet Sniffing:*** (dall'inglese **odorare**), rappresenta l'attività di intercettazione passiva dei dati che transitano in una rete telematica. Può essere svolta sia per scopi legittimi (ad esempio l'analisi e l'individuazione di problemi di comunicazione o di tentativi di intrusione) sia per **scopi illeciti** contro la sicurezza informatica (intercettazione fraudolenta di password o altre informazioni sensibili). I prodotti software utilizzati per eseguire queste attività vengono detti **sniffer** ed oltre a intercettare e memorizzare il traffico, offrono funzionalità di analisi del traffico stesso.

CYBER SECURITY - TIPI DI ATTACCHI

- ***Cookie Poisoning:*** l'avvelenamento da cookie è la modifica di un cookie (informazioni personali nel computer di un utente Web) da parte di un malintenzionato al fine di ottenere informazioni non autorizzate sull'utente, per scopi quali il furto di identità.

- L'utente malintenzionato può utilizzare le informazioni per aprire nuovi account o per accedere agli account esistenti della vittima.

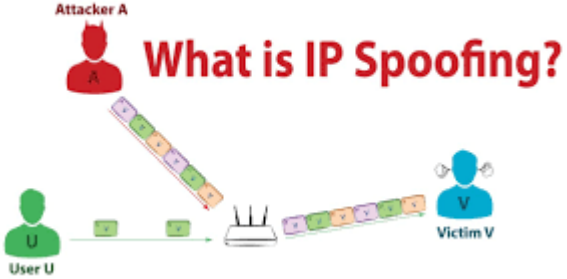
- I cookie memorizzati sul disco rigido contengono bit di informazioni che consentono ai siti Web visitati di autenticare l'identità dell'utente, velocizzare le transazioni, monitorarne il comportamento e personalizzarne le presentazioni.



- I cookie possono essere accessibili anche da persone non autorizzate a farlo. Salvo laddove non siano in atto misure di sicurezza, un utente malintenzionato può esaminare un cookie per determinarne lo scopo e modificarlo in modo che possa agevolarlo all'ottenimento di informazioni della vittima dal sito Web che ha inviato il cookie.

CYBER SECURITY - TIPI DI ATTACCHI

- ***Spoofing:*** è un tipo di attacco informatico che impiega in varie maniere la falsificazione dell'identità (spoof). Lo spoofing può avvenire a qualunque livello della pila ISO/OSI e può riguardare anche la falsificazione delle informazioni applicative.



- ***Malware:*** abbreviazione di **malicious software**, che significa letteralmente software malintenzionato. Indica un qualsiasi programma informatico 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.

CYBER SECURITY - TIPI DI ATTACCHI

- ***Phishing:*** rappresenta un tipo di **truffa** effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire **informazioni personali**, **dati finanziari** o **codici di accesso**, fingendosi un ente affidabile in una comunicazione digitale.

- Si tratta di una attività illegale che sfrutta una tecnica di ingegneria sociale: il malintenzionato effettua un invio massivo di messaggi di **posta elettronica** che imitano, nell'**aspetto** e nel **contenuto**, messaggi legittimi di fornitori di servizi;
- Tali messaggi fraudolenti richiedono di fornire informazioni riservate come, ad esempio, il numero della **carta di credito** o la **password** per accedere ad un determinato servizio.

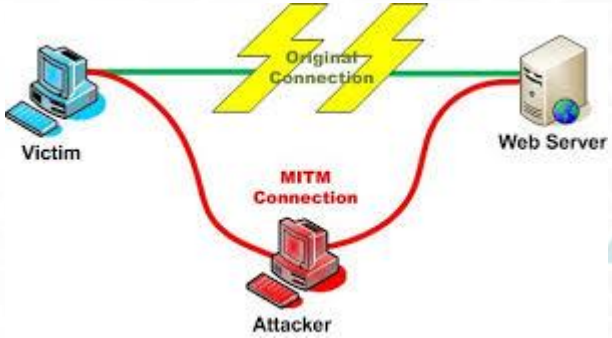
CYBER SECURITY - TIPI DI ATTACCHI

- ***Key Logger:*** è uno strumento hardware o software in grado di effettuare lo sniffing della tastiera di un computer;
- E' in grado di intercettare e catturare segretamente tutto ciò che viene digitato sulla tastiera senza che l'utente si accorga di essere monitorato;
- In alcuni casi vengono usati legalmente dai datori di lavoro per controllare l'uso dei loro computer da parte dei propri lavoratori;

- Essi sono purtoppo usati soprattutto per scopi fraudolenti, perché permettono agli hacker di registrare ogni lettera, carattere e simbolo introdotto dall'utente sulla tastiera;
- Come la maggior parte dei malware, questi virus inviano le informazioni raccolte ad un server.

CYBER SECURITY - TIPI DI ATTACCHI

- **Man in the middle:** in italiano "uomo nel mezzo", è un attacco informatico in cui qualcuno segretamente ritrasmette o altera la comunicazione tra due parti che credono di comunicare direttamente tra di loro.

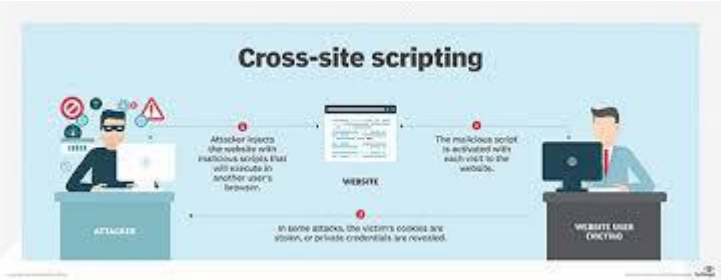


- In questi casi l'attaccante crea connessioni indipendenti con le vittime e ritrasmette i messaggi per far credere loro che stiano comunicando direttamente tramite una connessione privata, mentre in realtà l'intera conversazione è controllata dall'attaccante.

- Il malintenzionato deve essere in grado di intercettare tutti i messaggi importanti che passano tra le due vittime e iniettarne di nuovi.

- In molte circostanze questo è semplice, per esempio, un attaccante all'interno di un WI-FI access point non criptato, può inserire se stesso come "uomo nel mezzo"

CYBER SECURITY - TIPI DI ATTACCHI



- ***Cross Site Scripting (XSS):*** *E'* una vulnerabilità che affligge siti web dinamici che impiegano un insufficiente controllo dell'input nei form;

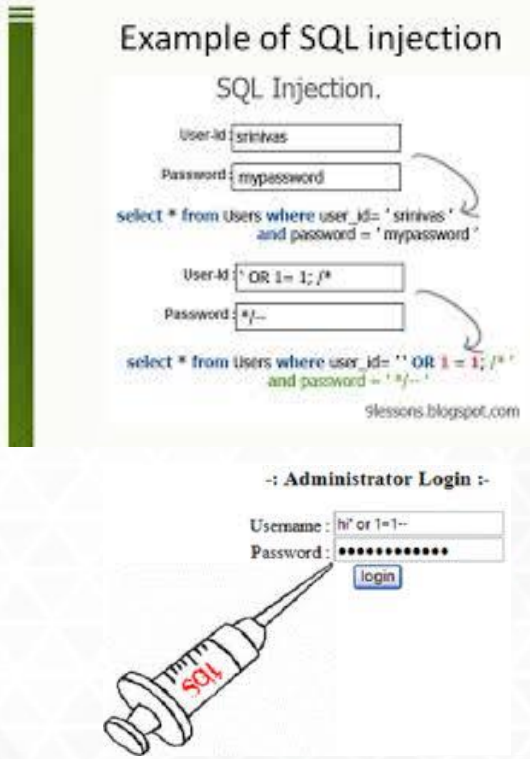
- Un XSS permette di inserire o eseguire codice lato client al fine di attuare un insieme variegato di attacchi informatici;

- Consente la raccolta, la manipolazione e il reindirizzamento di informazioni riservate, la visualizzazione e la modifica di dati presenti sui server, nonchè l'alterazione del comportamento dinamico delle pagine web.

CYBER SECURITY - TIPI DI ATTACCHI

- ***SQL Injection:*** E' una tecnica di code injection, usata per attaccare applicazioni di gestione dati, con la quale vengono inserite delle stringhe di codice SQL malevole all'interno di campi di input all'interno di pagine web, in modo che queste ultime vengano poi eseguite (ad esempio per fare inviare il contenuto del database all'attaccante)

- L'SQL injection sfrutta le vulnerabilità di sicurezza del codice di un'applicazione, quando l'input dell'utente non è correttamente filtrato da 'caratteri di escape' contenuti nelle stringhe SQL oppure non è fortemente tipizzato e di conseguenza viene eseguito inaspettatamente.

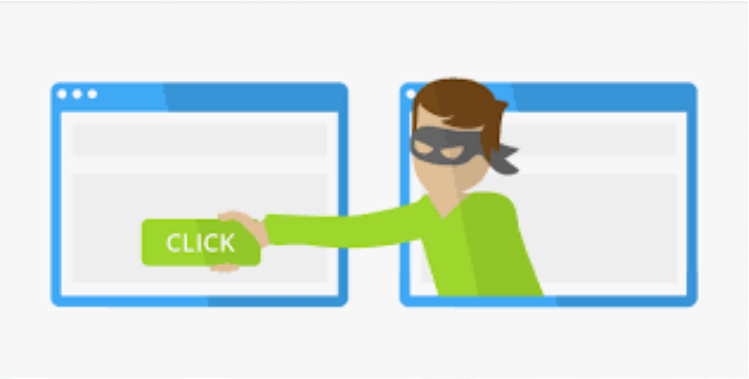


CYBER SECURITY - TIPI DI ATTACCHI

- ***Spam:*** è l'invio anche verso indirizzi generici, non verificati o sconosciuti, di messaggi di posta ripetuti ad alta frequenza o a carattere di monotematicità tale da renderli indesiderati, generalmente commerciali o offensivi ed è noto anche come posta spazzatura (in inglese junk mail).

- Può essere attuato attraverso qualunque sistema di comunicazione, ma il più usato è Internet, attraverso messaggi di posta elettronica, chat, tag board, forum, Facebook e altri servizi di rete sociale.

CYBER SECURITY - TIPI DI ATTACCHI



- ***Clickjacking*: (Rapimento del clic):** E' una tecnica informatica fraudolenta. Durante una normale navigazione web, l'utente clicca con il puntatore del mouse su di un oggetto (ad esempio un link), ma in realtà il suo clic viene reindirizzato, a sua insaputa, su di un altro oggetto, che può portare alle più svariate conseguenze: dal semplice invio di spam, al download di un file, fino all'ordinare prodotti da siti di e-commerce.

CYBER SECURITY – FASI D'ATTACCO

CYBER SECURITY - FASI DELL' ATTACCO

- ***Footprinting:*** rappresenta l'attività di monitoraggio delle informazioni disponibili su un server, in particolare in ambito web, allo scopo di mettere in evidenza eventuali debolezze del sistema per poi sfruttarle.

- E' possibile estrapolare informazioni spesso adoperando semplici tool gratuiti, a volte addirittura **Google**, per capire con che tipo di entità si sta avendo a che fare e, soprattutto, cosa sia possibile fare per comprometterne il funzionamento:

  - *nome di dominio;*
  - *sottodomini;*
  - *blocchi di rete;*
  - *indirizzi IP;*
  - *servizi TCP/UDP attivi;*
  - *architettura del server;*
  - *sistemi di protezione;*
  - *protocolli di rete sfruttabili (email, WEB e così via);*
  - *eventuali VPN;*
  - *meccanismi di controllo degli accessi.*

CYBER SECURITY - FASI DELL' ATTACCO

- ***Enumeration***: Rappresenta il processo di estrazione del nome degli utenti, delle macchine e dei servizi, prelevandoli da un sistema o applicazione attiva.

- Nella fase di enumerazione l'attaccante cerca di creare connessioni attive al sistema utilizzando le informazioni rilevate durante la fase di scanning.

- Le informazioni che possono essere ricavate da questo attacco sono:

- *risorse di rete;*
- *utenti e gruppi attivi online;*
- *nomi delle macchine online;*
- *applicazioni attive;*
- *dettagli dei servizi SNMP;*

CYBER SECURITY - FASI DELL' ATTACCO

- ***Scanning:*** *R*appresenta la fase che permette di individuare quali servizi espone un sistema remoto al fine di identificare gli host connessi, le porte aperte e i servizi attivi su di essi.

- Gli obbiettivi di questa operazione permettono di identificare:

- *Gli host attivi e i loro ip;*
- *I sistemi operativi utilizzati;*
- *I servizi attivi sulle macchine identificate (detto anche fingerprint);*
- *Possibili vulnerabilità presenti.*

CYBER SECURITY - FASI DELL' ATTACCO

- ***Attacco:*** Dopo aver preso nota dei servizi (con relativa versione), delle condivisioni e del sistema operativo, l'hacker, deciso l'obiettivo (singola applicazione o server intero), tenta l'intrusione mediante:

- Attacchi di tipo forza bruta alle password dei servizi di accesso remoto, se presenti (ssh, telnet, VNC, eccetera) o dei programmi Web;
- Attacchi ai servizi e programmi Web rincorrendo exploit provocati in genere da input non validato e buffer overflow. I programmi Web sono generalmente il punto più debole della catena;
- Attacchi a dispositivi di rete o modem fisicamente connessi al server;
- Ingegneria sociale (social engineering).

CYBER SECURITY - FASI DELL' ATTACCO

- ***Pulire le traccie:*** Dopo essere entrato in un sistema, l'hacker tenterà di effettuare una serie di operazioni in modo che la vittima non si accorga della presenza di qualcosa di estraneo, come ad esempio la cancellazione dei file di log.

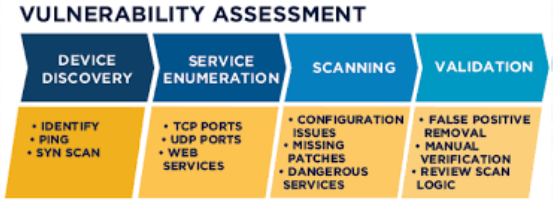
- Nella maggior parte dei casi di attacchi informatici, la strategia è silenziosa e non si ci accorge dell'attacco finché non è avvenuto e ha compromesso il sistema.

- Questione differente è il caso degli attacchi che hanno come obiettivo il danno di immagine: l'attacco sarà visibile con la comparsa di schermate di errore o di denuncia, con il blocco delle pagine, e con altri metodi con i quali gli hacker rendono evidente l'attacco.

VERIFICHE DI SICUREZZA

CYBER SECURITY - VULNERABILITY ASSESSMENT

- Si tratta di **un'analisi di sicurezza** che ha l'obiettivo di identificare tutte le vulnerabilità potenziali dei sistemi e delle applicazioni, valutando il danno potenziale che l'eventuale "attaccante" può infliggere all'unità produttiva;
- Personale altamente qualificato, in un secondo momento, integra e verifica i risultati attraverso una meticolosa attività manuale;
- Queste attività hanno lo scopo di rifinire la ricerca evidenziando eventuali errori commessi durante il processo;
- Uno degli aspetti chiave di questa tipologia di analisi è **l'isolamento tempestivo delle vulnerabilità reali**.



CYBER SECURITY - VULNERABILITY ASSESSMENT

- Un valido strumento di Vulnerability Assessment permette all'utente di avere un'overview aggiornata del livello di sicurezza degli asset IT.

- Un buon tool che possa rispondere a tutti i requisiti di sicurezza, in un modo esaustivo e completo, deve presentare una serie di caratteristiche:

- Riconoscere ed identificare un ampio numero di differenti vulnerabilità;
- *Compliance*. Questo è un fattore chiave (infografica GDPR) per evitare sanzioni salate e perdita di reputazione;
- Grande usabilità. E' necessaria un'esposizione chiara ed accessibile delle informazioni, combinata ad una buona profondità dello scan.

CYBER SECURITY - PENETRATION TEST

- Il ***Penetration Testing o PenTest*** è il processo che permette di analizzare in profondità la sicurezza di uno o più sistemi.
- L'attività deve essere una parte importante dei processi aziendali in modo da assicurare la piena consapevolezza dei punti deboli dell'infrastruttura IT e non.
- Per ogni PenTest può essere applicata una diversa metodologia; si intende un insieme di regole da poter seguire per condurre un PenTest in maniera corretta.

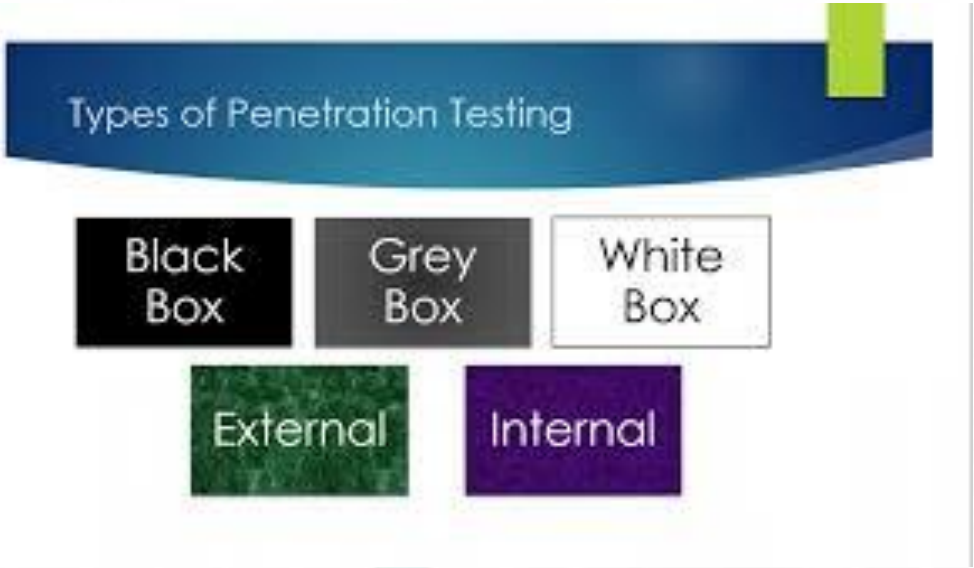
CYBER SECURITY - PENETRATION TEST

- Tale pratica può essere condotta indipendentemente o come attività schedulata nel proprio ufficio di IT Security.

- Uno scheduling comporta l'implementazione di adeguate misure di sicurezza, redigere un documento di analisi dei rischi, revisione del Codice, creazione di modelli di minacce ed altro…

CYBER SECURITY - PENETRATION TEST

- **Esistono sostanzialmente tre approcci metodologici al Penetration Testing:**



CYBER SECURITY - PENETRATION TEST

Penetration Testing profile

- Black Box
- White Box
- Grey Box

- External
- Internal

- Destructive
- None-destructive

- Announced
- Unannounced

CYBER SECURITY - PENETRATION TEST

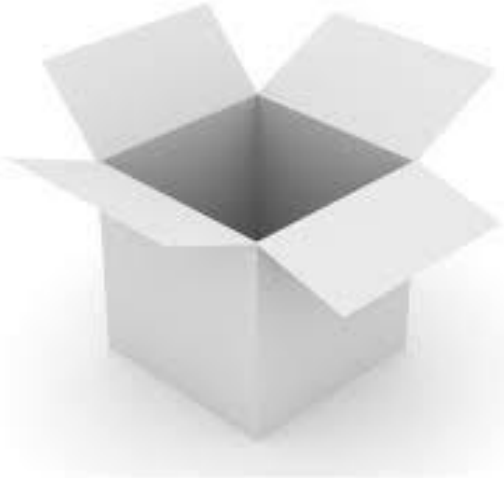
- Si parla di “Scatola Oscura” o **Black Box** quando coloro che compiono l’attività non hanno cognizione delle tecnologie implementate nell’organizzazione target.
- Devono essere adottate tutte le tecniche di hacking conosciute ed è importante saper classificare le vulnerabilità in base al loro livello di rischio.
- Tale metodologia può essere più costosa in termini di tempo e risorse rispetto ad un approccio di tipo White Box ed è soggetto alle reali abilità dell’attaccante.

CYBER SECURITY - PENETRATION TEST

- La metodologia **White Box**, al contrario, è una tipologia di PenTest dove l'attaccante è a conoscenza di tutto l'ambiente che andrà a testare.

- È il miglior modo per valutare e concentrarsi su tutte quelle tecnologie che possono risultare critiche. In questo caso si vanno a valutare i rischi esterni che l'azienda/organizzazione incorre, non considerando le vulnerabilità interne (es. Social Enginering / Dipendente Scontento).

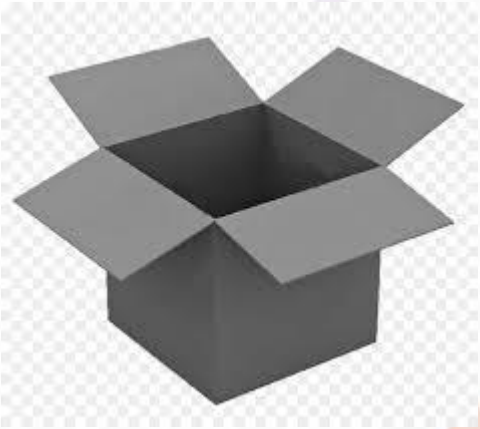
- Gli step sono simili alle fasi di Black Box, ma in qualche modo l'approccio White Box può essere integrato nei cicli di vita di implementazioni Hardware/Software per eliminare le possibili problematiche a monte di un possibile attacco.



CYBER SECURITY - PENETRATION TEST

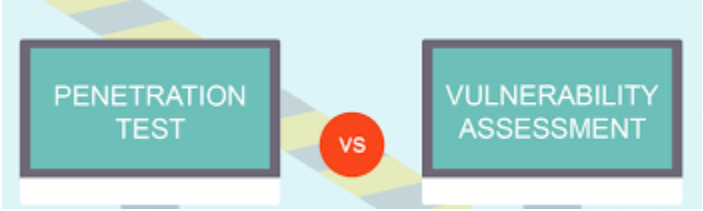
- Si parla di **Gray Box**, quando il team che effettua il penetration test, possiede solo poche informazioni riguardo il target da attaccare;

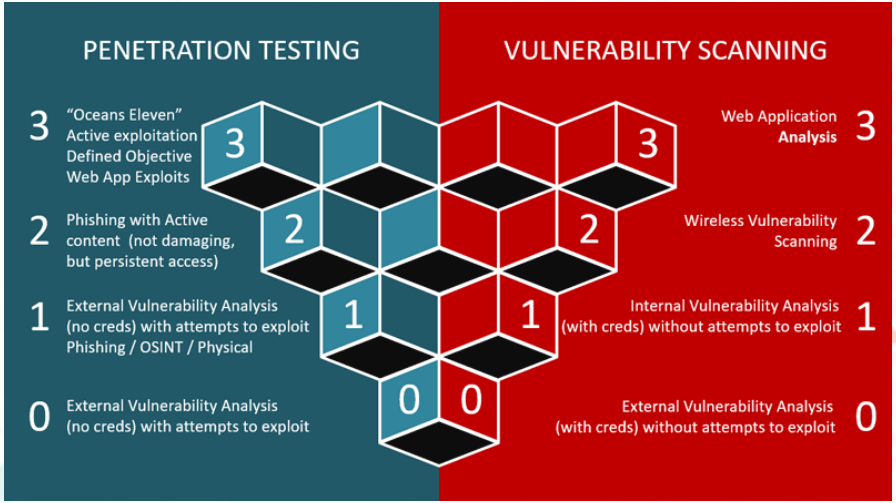
- Il cliente può decidere di rendere disponibile esclusivamente alcune informazioni riguardo la propria infrastruttura o talvolta il solo accesso alla rete interna.



CYBER SECURITY - VA vs PT

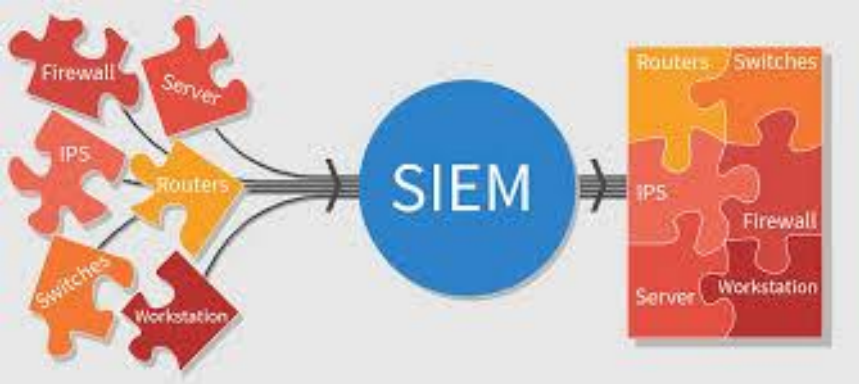
- La differenza basilare è che:
- Nel Vulnerability Assessment si vanno ad evidenziare tutte le possibili vulnerabilità, procedendo alla valutazione del possibile impatto;
- Nel PenTest si procede invece ad identificare tutte le vulnerabilità ed sfruttare possibili exploit pubblici o custom (0-day) con l'aggiunta di privilege escalation e mantenimento dell'accesso ai sistemi target.





CYBER SECURITY - LINEE GUIDA

- Esistono varie **linee guida** che possono essere d'aiuto per chi voglia incominciare ad implementare controlli periodici:
- SP-800-115 del NIST (National Institute of Standards and Technology, del Governo americano [**https://www.nist.gov**]
- Open Source Security Testing Methodology Manual (**http://www.isecom.org/research**/)
- Information Systems Security Assessment Framework (**https://ht.transparencytoolkit.org/FileServer/FileServer/whitepapers/issaf/issaf0.2.1A.pdf**)
- Open Web Application Security Project Testing Guide (**https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents**)
- Web Application Security Consortium Threat Classification (**http://www.webappsec.org/**)
- Penetration Testing Execution Standard (**http://www.pentest-standard.org/index.php/Main_Page**)



TOOL DI MONITORING

CYBER SECURITY - FREE TOOL

CYBER SECURITY - COMMERCIAL TOOL

IL NOSTRO APPROCCIO

GDPR - Overview

"Le aree"

PROCEDURE
- Gestione di un Data Breach (Incident & Investigation)
- Gestione dei Diritti: accesso, cancellazione, modifica, portabilità
- "Privacy by Design" e "Privacy by Default"

CONSULENZE
- Data Protection Design
- Privacy Assessment
- Privacy: governance & policies
- Privacy by Design – Privacy by Default
- Training e "awareness"

ATTIVITA'
- Assessment
- Prevention
- Detection

Impatto sulle aree di un organizzazione

Legal & Compliance
"Adeguamento Privacy GDPR"

Consulenze

- *Adeguamento all'Organizzazione in materia di Privacy*
- *Consulenza riguardo alla manutenzione nel tempo del Sistema di gestione degli adempimenti Privacy*
- *Formazione e sensibilizzazione in materia di Privacy*

Attività di supporto agli adempimenti Privacy

- *Servizi per l'adeguamento delle piattaforme web alla direttiva e-privacy*
- *Consulenza progettuale in materia di Privacy*
- *Consulenza in merito alle attività di video-sorveglianza e localizzazione satellitare in ambito aziendale*
- *Verifica di conformità sui processi di trattamento dei dati e gap analisys*
- *Valutazione di impatto (Privacy Impact Assessment – P.I.A.) in merito ai processi di trattamento di dati personali*

Process & Organization

“Attività di verifica sulla conformità di processi e organizzazione aziendale”

Consulenze

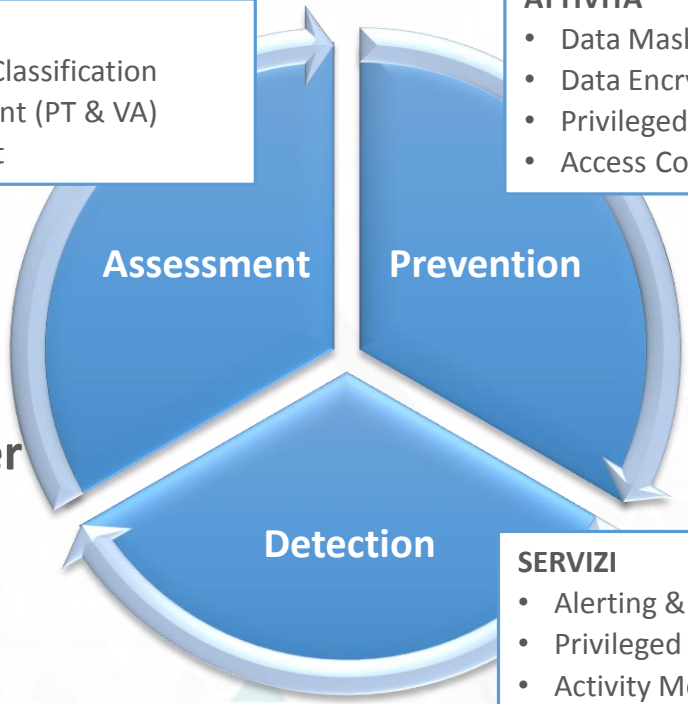
- *Definizione delle procedure di controllo*
- *Definizione delle procedure per «Data Breach Management»*
- *Definizione delle procedure per «Investigation Management»*
- *Definizione delle procedure per «Incident Response»*
- *Definizione dei processi di «Governance»*
- *Check-up per la compliance: Privacy, 27001*

Technical

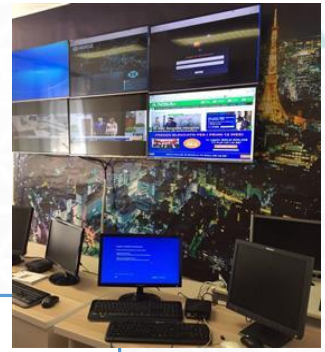
"Le macro aree di attività"

ATTIVITA'
- Data discovery & Classification
- Security Assessment (PT & VA)
- Technology impact

ATTIVITA'
- Data Masking
- Data Encryption
- Privileged User Management
- Access Control



SERVIZI
- Alerting & Reporting (SOC H24)
- Privileged user monitoring
- Activity Monitoring (SOC H24)
- Incident Response (SOC H24)



Attività e Servizi offerti per ogni macro area

Piano d'azione
"Ipotesi"

Assessment
- *Analisi dei flussi e dei processi di trattamento dati*
- *Risk assessment*
- *Privacy impact assessment*
- *Training e awareness*

OUTPUT
Gap Analisys in merito all'applicazione delle tematiche inerenti al GDPR

Organizational
- *Definizione delle procedure di controllo*
- *Definizione delle procedure per "Data Breach Management"*
- *Definizione delle procedure per "Investigation Management"*
- *Definizione delle procedure per "Incident Response"*

OUTPUT
Gap Analisys + Processi + Procedure definite e applicate / applicabili

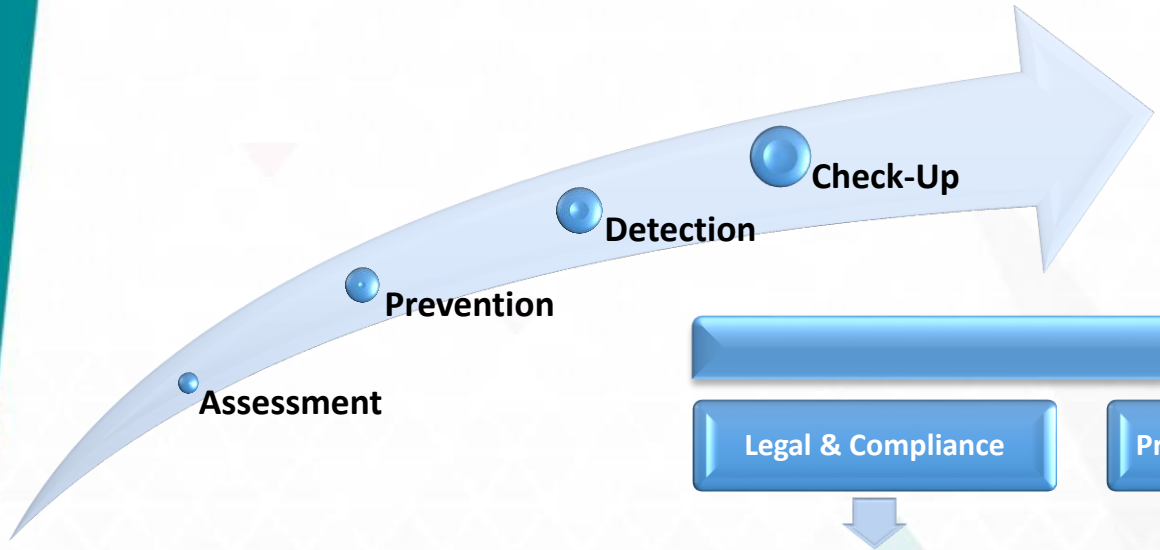
Technology
- *Security Assessment*
- *Personal data discovery & classification*
- *Encryption dati sensibili*
- *Masking su sistemi di non produzione*
- *Applicazione di regole e policies per il controllo delle utenze e accessi Privilegiati (SoD)*
- *Configurazione e avvio di soluzioni software e/o appliance per Audit & Reporting*
- *Configurazione e avvio di soluzioni software e/o appliance per Activity Monitoring*
- *Configurazione e avvio di soluzioni software e/o appliance per Incident Response*

OUTPUT
Misure di sicurezza definite e applicate sui sistemi

GDPR: Check-Up Periodico

"Monitoraggio e mantenimento degli standard"

Per ogni area, pianifichiamo un check-up degli standard raggiunti, ***adeguando***, ***mantenendo***, ***integrando*** laddove necessario e realizzando un piano di ***miglioramento continuo nel tempo***



DOMANDE?

Guerrino Pescali

Data Protector Manager

guerrino.pescali@vantea.com