La sicurezza Informatica

Indice del Corso

Modulo 1: La sicurezza

Indice del Modulo

Definizione di sicurezza

La Sicurezza è la capacità di applicare la Security Policy scelta, ovvero le regole che determinano chi può accedere alle risorse e alle informazioni, e in che modo.

< NOTA BENE >

Con il termine accesso si intende la visualizzazione, la stampa e la consapevolezza dell'esistenza di una risorsa, non solo la lettura.

La sicurezza informatica coinvolge tre aspetti molto importanti di un sistema:

1. **Confidenzialità/ Riservatezza**
   Le informazioni non di dominio pubblico devono essere disponibili solo a chi è autorizzato. I sistemi di sicurezza devono garantire l'identità dei soggetti che vogliono informazioni confidenziali e sulla base di questa e delle autorizzazioni definite consentire o meno l'accesso.

2. **Integrità**
   Le informazioni devono essere modificabili sono da chi è autorizzato: anche per quelle di dominio pubblico, come il contenuto del sito, è fondamentale garantire l'integrità. I cosiddetti "defacement", alterazioni di siti da parte di hacker, costituiscono una porzione rilevante degli incidenti e possono causare notevoli danni di immagine. L'integrità è tanto più critica quando l'informazione è una fonte "ufficiale", la cui alterazione ha un impatto su dinamiche sociali ed economiche. In generale chi accede ad un'informazione critica deve avere a disposizione un sistema in grado di verificarne la fonte e l'integrità.

3. **Disponibilità**
   Le informazioni devono essere disponibili, ovvero accessibili ai soggetti autorizzati, deve esserci cioè la disponibilità di servizi preposti alle gestione dell'informazione. È evidente che una indisponibilità può ugualmente avere un impatto significativo su un'attività centrata sull'erogazione di servizi e informazioni. La disponibilità delle risorse ICT (rete, elaboratori, potenza di calcolo) fa parte di questa categoria: la loro indisponibilità ha un impatto diretto sulla capacità operativa dei soggetti.

Analisi del Rischio

< RISCHIO >

È evidente che la sicurezza totale non esiste. Per indirizzare in modo corretto gli investimenti bisogna capire quali sono gli incidenti che possono causare i danni maggiori.

L'Analisi del Rischio è la valutazione sistematica del danno che deriva da una violazione delle politiche di sicurezza e dalla probabilità concreta che possa accadere.

Consente di definire in dettaglio le policy come norme di comportamento e linee guida per futuri sviluppi: sulla base dell'Analisi si mettono a punto le contromisure tecnologiche da adottare e da mantenere per la sicurezza dei processi, come ad esempio le comunicazioni cifrate, i sistemi di difesa perimetrale o le valutazioni periodiche del livello di sicurezza del Sistema Informativo.

L'Analisi del Rischio è riconosciuta fondamentale in tutti gli "standard" e linee guida per la costruzione di un sistema di sicurezza, a partire dalla BS779 e dalle "Linee Guida AIPA per il Piano della Sicurezza". La normativa sulla "Privacy" prevede che venga redatto un documento programmatico sulla sicurezza, con i criteri e le procedure per assicurare integrità dei dati e sicurezza nelle trasmissioni, stabiliti sulla base dell'Analisi.

Minaccia, vulnerabilità e impatto

Il rischio è calcolato in funzione di tre fattori: Minaccia, Vulnerabilità e Impatto. Clicca sulle singole voci per conoscerne il significato.

RISCHIO = MINACCIA + VULNERABILITA' + IMPATTO

Il Rischio aumenta all'aumentare di ciascuna delle tre variabili.

Minaccia

Una **minaccia** è una potenziale causa di incidente (deliberato o accidentale) che può danneggiare uno o tutti i beni del patrimonio informativo.

L'Analisi del Rischio prende in considerazione le minacce "a largo raggio":

- eventi **naturali**
- eventi di **natura umana** (deliberati o accidentali, tra questi gli "attacchi" degli hacker)
- eventi di **natura tecnologica** (avarie, guasti).

Sono da considerare minacce l'incendio, l'alluvione, il *black-out elettrico*, i guasti agli elaboratori, le minacce intenzionali. In questo senso il concetto di sicurezza si estende ben oltre l'immagine comune che la identifica come il problema degli hacker o dei virus.

Una minaccia sono i soggetti avversi, che trarrebbero un beneficio diretto da un incidente e le condizioni ambientali particolari, come la prossimità a fiumi o corsi d'acqua non adeguatamente protetti.

Vulnerabilità

Una **vulnerabilità** è un punto debole nei sistemi di gestione che può trasformare una minaccia in danno. Ad esempio un elaboratore mal configurato, la mancanza di un sistema antincendio o di controllo accessi.

Se viene sfruttata si verifica un **incidente**, con conseguente perdita di confidenzialità, integrità o disponibilità delle informazioni (oltre ad eventuali danni alle infrastrutture).

Una minaccia è bloccata dal controllo di una vulnerabilità.

Impatto

L'**impatto** è il danno effettivo di un incidente, la parte più critica da valutare, la più difficile ma la più importante.

Il Rischio di sicurezza

Il Rischio di Sicurezza è la probabilità che una minaccia si avvantaggi delle vulnerabilità per provocare un incidente.
La valutazione del rischio dipende dal contesto, questo significa che se il danno ha un impatto minimo non è così necessario ridurre la vulnerabilità del sistema.

Una volta approfondito il concetto di rischio, possiamo affermare che l'obiettivo della sua analisi è valutare quelli cui è soggetto il sistema e stabilire quali devono essere assolutamente ridotti. Poi è necessario definire una priorità di intervento per ogni rischio evidenziato.

Le fasi dell'Analisi del Rischio.

< RISCHIO >

Le principali fasi dell'analisi di Rischio sono le seguenti:
(clicca sulle voci per visualizzarne il contenuto)
1 > identificare i beni da proteggere (data asset)
2 > individuare con precisione il ciclo di vita dei "data asset"
3 > identificare gli impatti causati da perdita di riservatezza, integrità e disponibilità
4 > identificare le minacce
5 > identificare le vulnerabilità

1. **Identificare i beni da proteggere (data asset)**
   Tutto ciò che viene considerato un patrimonio da tutelare (informazioni, hardware, software, personale, beni immobiliari, ecc.).

2. **Individuare con precisione il ciclo di vita dei "data asset"**
   È necessario per comprendere le criticità e i punti deboli (vulnerabilità) dei beni da proteggere. Si tratta di identificate i componenti hardware e software impiegati per il trattamento delle informazioni, il personale coinvolto e le procedure gestionali e operative utilizzate. Questo tramite un'analisi del processo informativo da parte di personale specializzato, in collaborazione con elementi chiave del livello organizzativo dei processi in analisi.

3. **Identificare gli impatti causati da perdita di riservatezza, integrità e disponibilità**
   È necessario prendere in considerazione: Sicurezza Personale, Riservatezza (legge sulla privacy), rispetto di leggi e contratti, rallentamento o interruzione della continuità operativa, perdita d'immagine. Per ciascuno di questi aspetti è indispensabile dare una valutazione almeno qualitativa del potenziale danno.

4. **Identificare le minacce**
   Può avvenire sulla base di dati storici, quante volte nel passato si è verificata la stessa minaccia. È necessario considerare anche con quali probabilità le minacce si possono manifestare.

5. **Identificare le vulnerabilità**
   È necessario valutare in che misura le vulnerabilità possono essere sfruttate dalle minacce e prendere in considerazione tutte le contromisure esistenti.

Trattamento del Rischio

Una volta determinati i rischi a cui è soggetto il sistema occorre predisporre un **Piano di Trattamento del Rischio**.

Con Trattamento del Rischio si intende:

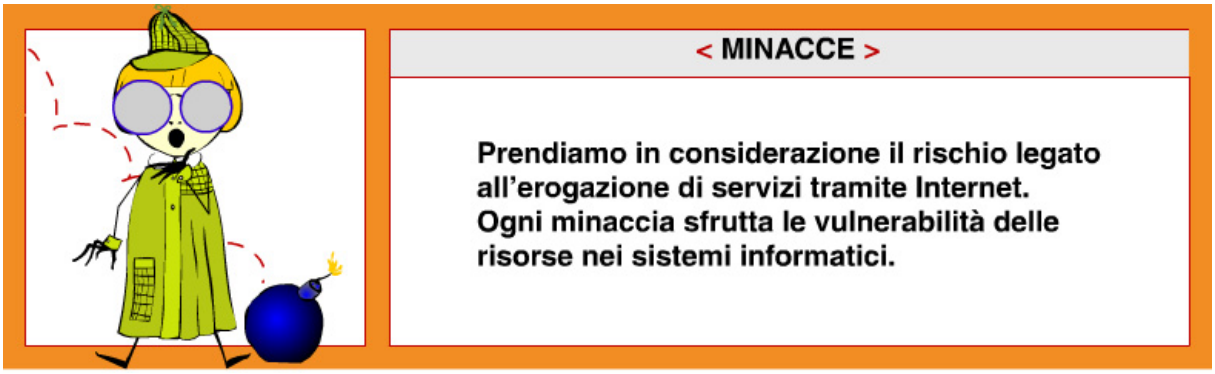
- decidere se un rischio è accettabile o deve essere ridotto con adeguate contromisure
- la predisposizione delle contromisure.

Si è già detto che il Rischio può essere accettato se giudicato sufficientemente basso. Questo perché, di solito, non è possibile azzerarlo. Il Rischio non accettabile va ridotto e riportato sotto la soglia di accettabilità.

Modulo 2: La sicurezza informatica

Indice del Modulo

Il Rischio Comunicativo: le minacce



- **un'intercettazione**
  Indica che qualcuno/qualcosa non autorizzato (persona, programma, sistema informatico) ha ottenuto l'accesso a una risorsa.
- **un'interruzione**
  Una risorsa del sistema risulta smarrita, non disponibile o inutilizzabile.
- **una modifica**
  Un'entità non autorizzata, oltre ad accedere a una risorsa interferisce con essa.
- **una falsificazione**
  Un'entità non autorizzata crea oggetti contraffatti su un sistema.

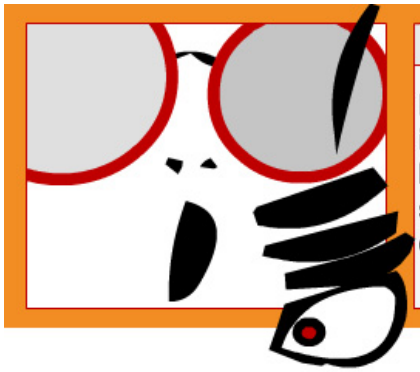
Per sferrare un attacco bisogna avere metodo (capacità, conoscenze, strumenti), opportunità, movente. Costituiscono una minaccia per un sistema informativo:

- **soggetti determinati a danneggiare l'organizzazione o ad ottenere un profitto**
  Può trattarsi di concorrenti, dipendenti o ex-dipendenti insoddisfatti o interessati per fini personali al patrimonio aziendale.

- **soggetti determinati a utilizzare le risorse dell'organizzazione**
  L'interesse principale di chi attacca non è il patrimonio informativo, ma le risorse ICT: disponibilità di banda, risorse di calcolo, ecc… che possono essere estremamente utili per: preparare ulteriori attacchi, confondere le tracce, condurre attacchi distribuiti.

- **script kiddies**, ovvero soggetti che per diletto o per dimostrare le proprie capacità tentano di violare la sicurezza dei sistem. L'obiettivo è scelto a caso. Possono esser attratti dall'importanza o visibilità di un'organizzazione che può dare "lustro all'impresa". Spesso l'unico danno che producono è quello di lasciare e pubblicizzare traccia del loro passaggio, ad esempio attraverso *defacement* del sito.

- **robot automatici**, come virus e worm, che utilizzano vulnerabilità per diffondersi tra i sistemi .L'obiettivo è scelto in modo casuale, ad esempio con liste di contatti di posta elettronica. Possono causare danni considerevoli: interruzione del servizio, costi diretti per il ripristino dei sistemi, perdita di informazioni, ecc. Inoltre, spesso aprono "back door" che annullano i sistemi di difesa e lasciano il sistema in balia di soggetti più determinati.



< NOTA BENE >

E' in crescita l'attenzione ai problemi della Sicurezza in ambito ICT.
Infatti è difficile ipotizzare che un sistema in grado di scambiare informazioni con ambienti potenzialmente ostili non sia soggetto ad alcuna minaccia.

Le Vulnerabilità dei Sistemi

Alla base di ogni sistema di sicurezza troviamo due elementi:

- **autenticazione**
- **autorizzazione**

Come previsto dalla politica di sicurezza dell'organizzazione, ogni sistema informativo deve preventivamente riconoscere (autenticare) il richiedente e assegnargli i diritti di accesso (autorizzazione).

< VULNERABILITA' >

Le vulnerabilità cui sono soggetti i sistemi derivano da:

> errori nel progetto
> errori nell'implementazione
> errori nella configurazione di programmi o servizi

Tipologie di vulnerabilità

Le Vulnerabilità sono punti deboli nei meccanismi di autenticazione e in quelli di autorizzazione.

Attacco ai meccanismi di autenticazione

Chi attacca può cercare di farsi passare per un utente legittimo, ad esempio catturandone o indovinandone la password, oppure di indurre il sistema a comportarsi in modo anomalo, ottenendo diritti di accesso ai dati superiori a quelli previsti, per consentirgli ad esempio di modificare il contenuto di un sito il cui accesso è, ovviamente, "in sola lettura".

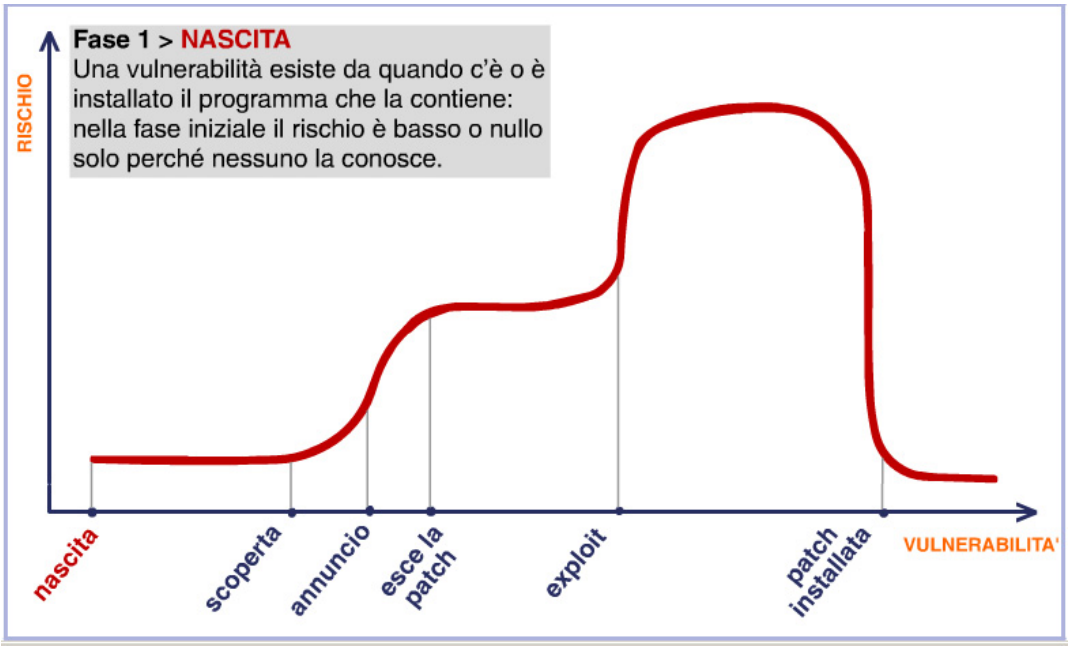
Attacco ai meccanismi di autorizzazione

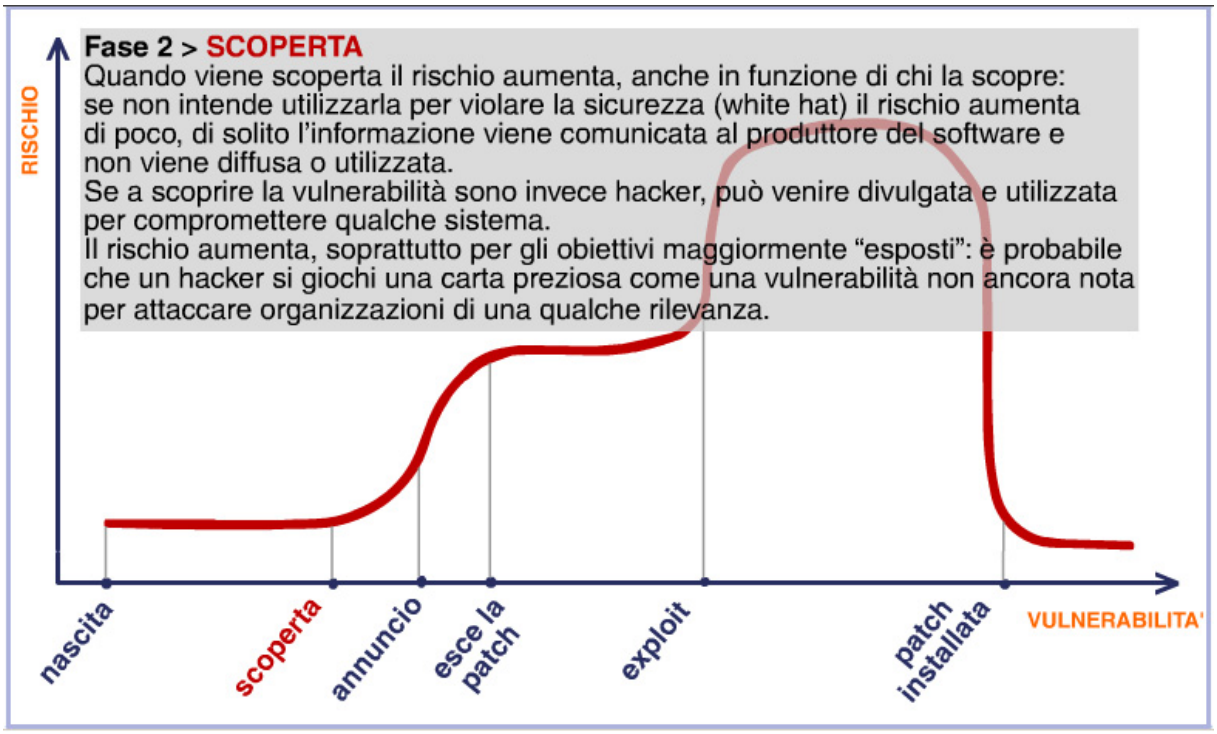
Ci sono poi attacchi cosiddetti "Denial of Service", mirati a rendere indisponibili i servizi, ad esempio sommergendoli di richieste legittime fino ad esaurirne le capacità e infine quelli che sfruttano "l'ingenuità" delle persone, inducendole ad abbassare la guardia.

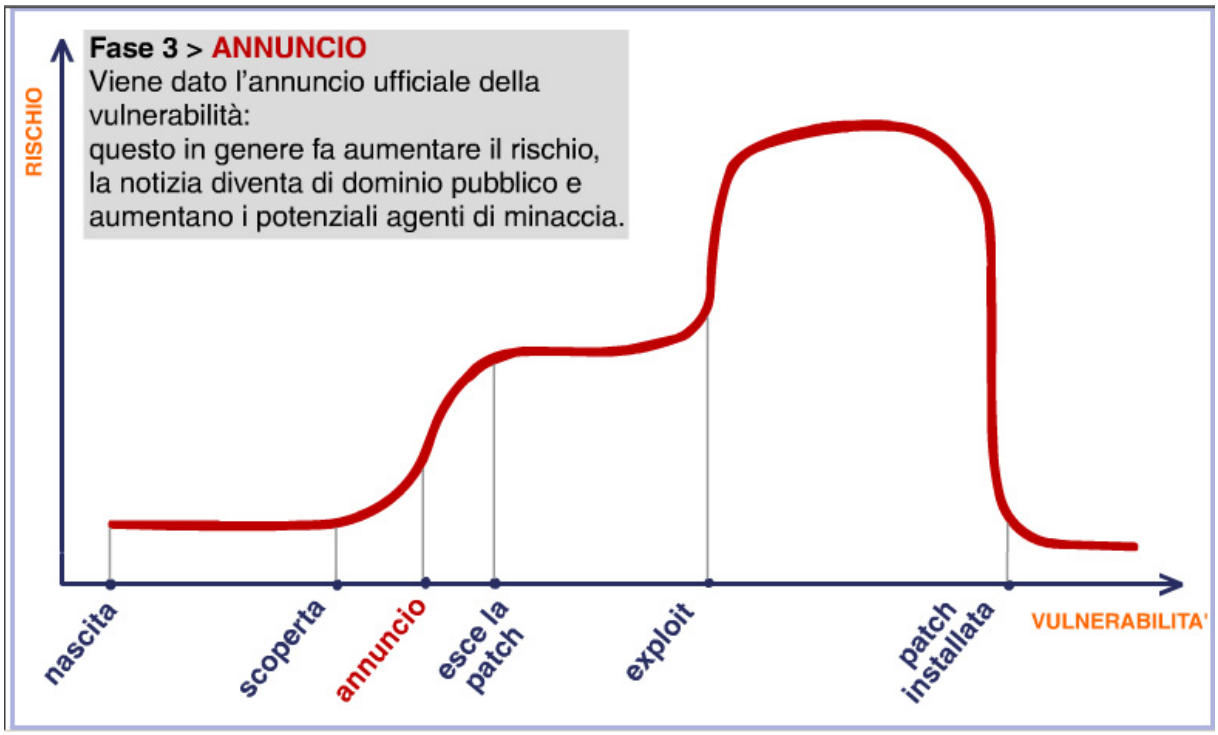
Ciclo di vita di una Vulnerabilità e Rischio

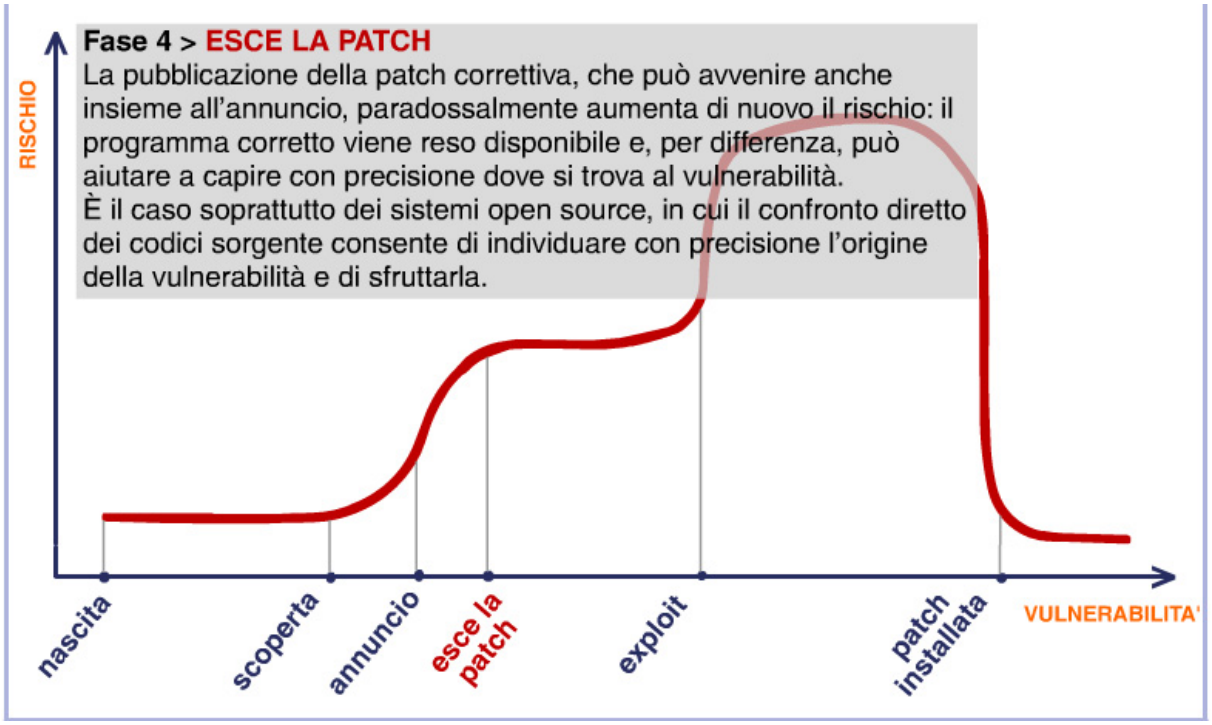
È già stato detto che le vulnerabilità derivano da errori di progetto o di implementazione di un programma, che consentono violazioni delle politiche di sicurezza.

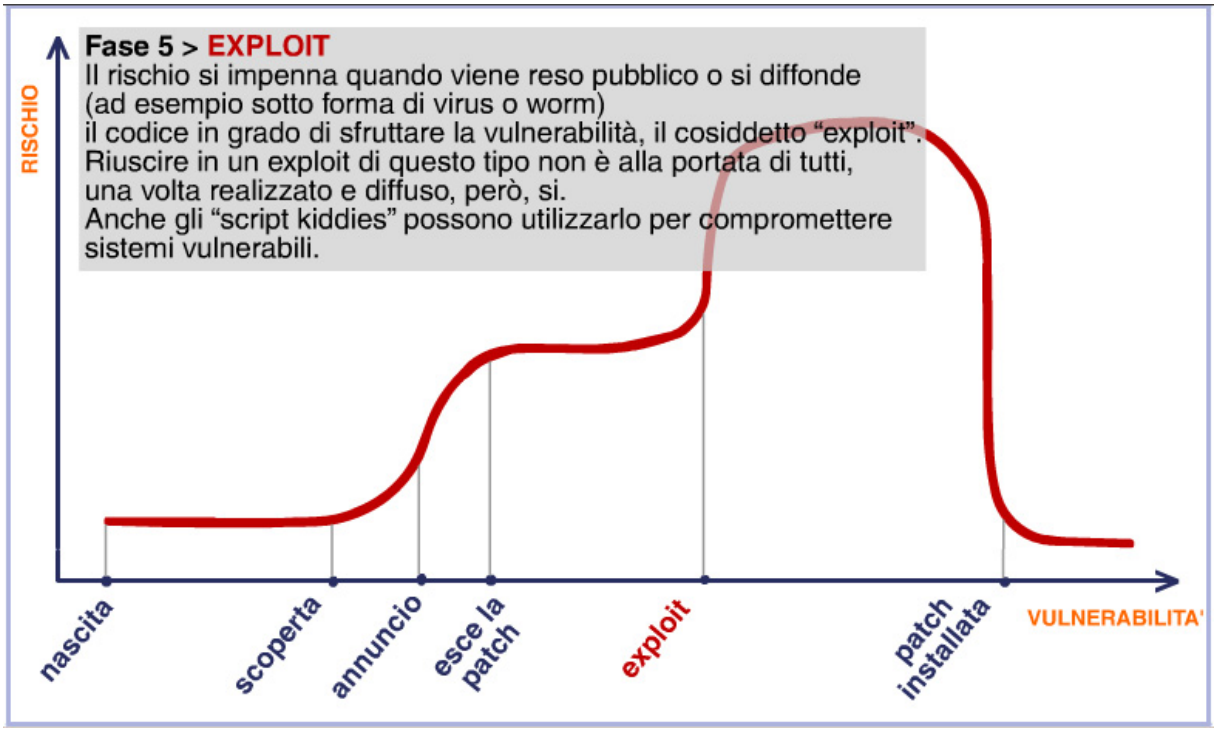
Analizziamo ora il ciclo di vita di una vulnerabilità tramite lo schema del livello del rischio e di come varia in funzione del tempo e dei diversi "momenti" della "vita" di una vulnerabilità.

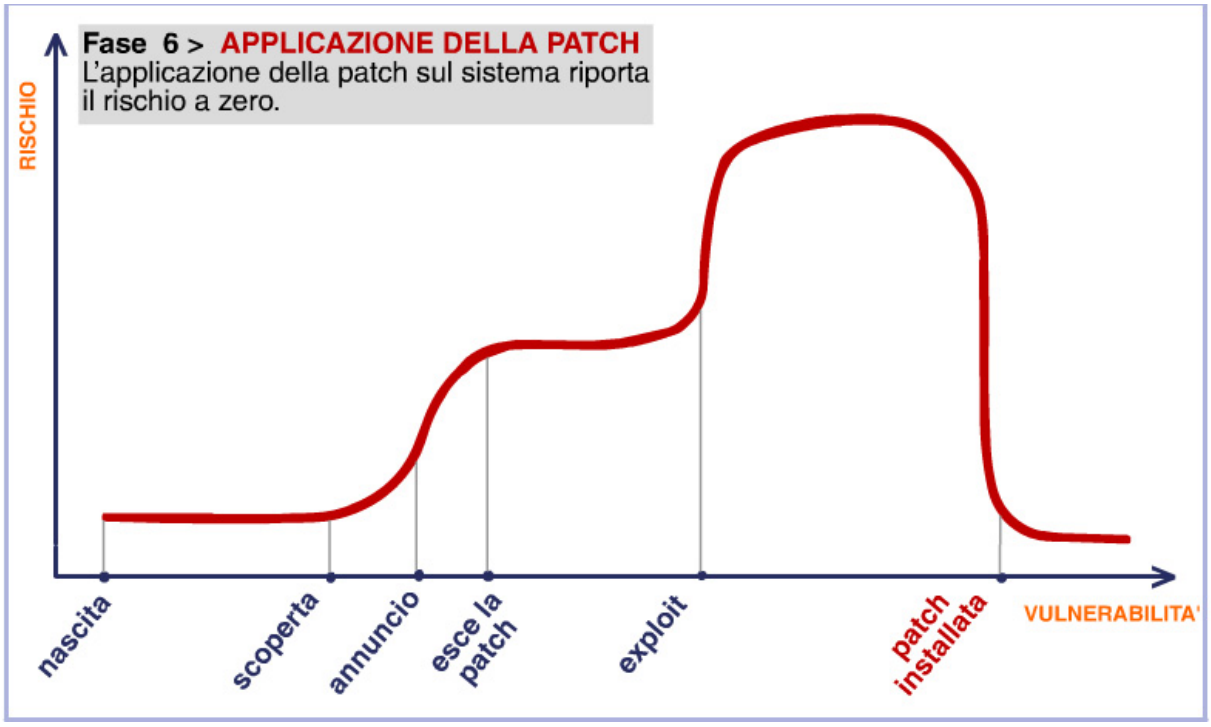



Fase 2 > SCOPERTA
Quando viene scoperta il rischio aumenta, anche in funzione di chi la scopre:
se non intende utilizzarla per violare la sicurezza (white hat) il rischio aumenta di poco, di solito l'informazione viene comunicata al produttore del software e non viene diffusa o utilizzata.
Se a scoprire la vulnerabilità sono invece hacker, può venire divulgata e utilizzata per compromettere qualche sistema.
Il rischio aumenta, soprattutto per gli obiettivi maggiormente "esposti": è probabile che un hacker si giochi una carta preziosa come una vulnerabilità non ancora nota per attaccare organizzazioni di una qualche rilevanza.
RISCHIO
nascita
scoperta
annuncio
esce la patch
exploit
patch installata
VULNERABILITA'


Fase 3 > ANNUNCIO
Viene dato l'annuncio ufficiale della vulnerabilità:
questo in genere fa aumentare il rischio, la notizia diventa di dominio pubblico e aumentano i potenziali agenti di minaccia.
RISCHIO
nascita
scoperta
annuncio
esce la patch
exploit
patch installata
VULNERABILITA'


RISCHIO
Fase 4 > ESCE LA PATCH
La pubblicazione della patch correttiva, che può avvenire anche insieme all'annuncio, paradossalmente aumenta di nuovo il rischio: il programma corretto viene reso disponibile e, per differenza, può aiutare a capire con precisione dove si trova al vulnerabilità.
È il caso soprattutto dei sistemi open source, in cui il confronto diretto dei codici sorgente consente di individuare con precisione l'origine della vulnerabilità e di sfruttarla.
nascita
scoperta
annuncio
esce la patch
exploit
patch installata
VULNERABILITA'


RISCHIO
Fase 5 > EXPLOIT
Il rischio si impenna quando viene reso pubblico o si diffonde (ad esempio sotto forma di virus o worm) il codice in grado di sfruttare la vulnerabilità, il cosiddetto "exploit".
Riuscire in un exploit di questo tipo non è alla portata di tutti, una volta realizzato e diffuso, però, si.
Anche gli "script kiddies" possono utilizzarlo per compromettere sistemi vulnerabili.
nascita
scoperta
annuncio
esce la patch
exploit
patch installata
VULNERABILITA'

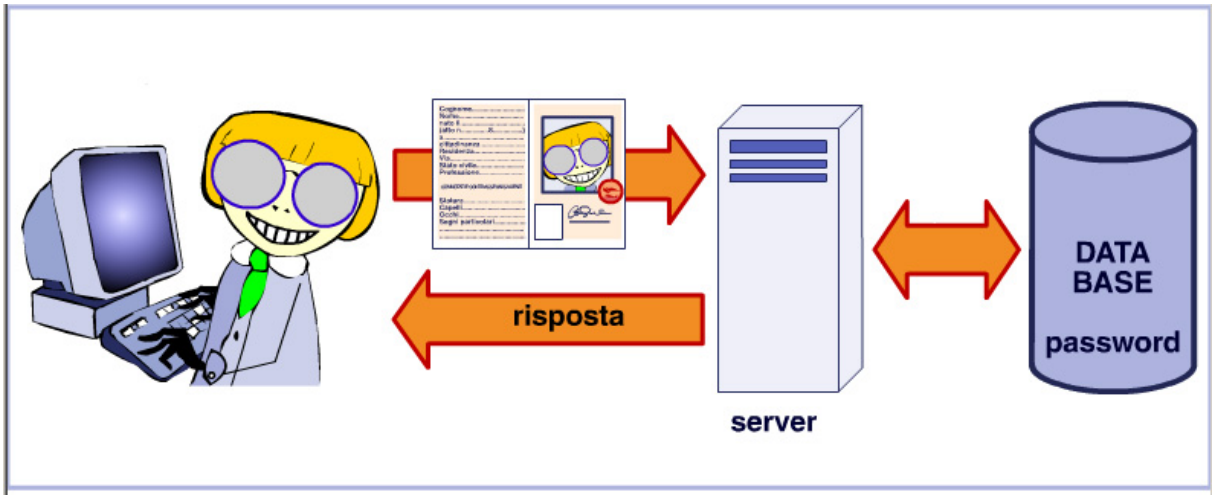

Fase 6 > APPLICAZIONE DELLA PATCH
L'applicazione della patch sul sistema riporta il rischio a zero.
RISCHIO
nascita
scoperta
annuncio
esce la patch
exploit
patch installata
VULNERABILITA'

Modulo 3: L’autenticazione

Indice del Modulo

Caratteristiche dell'autenticazione

L'autenticazione è il processo con cui il sistema che regola l'accesso alle informazioni (il server) si accerta dell'identità di chi chiede di entrare (il client).



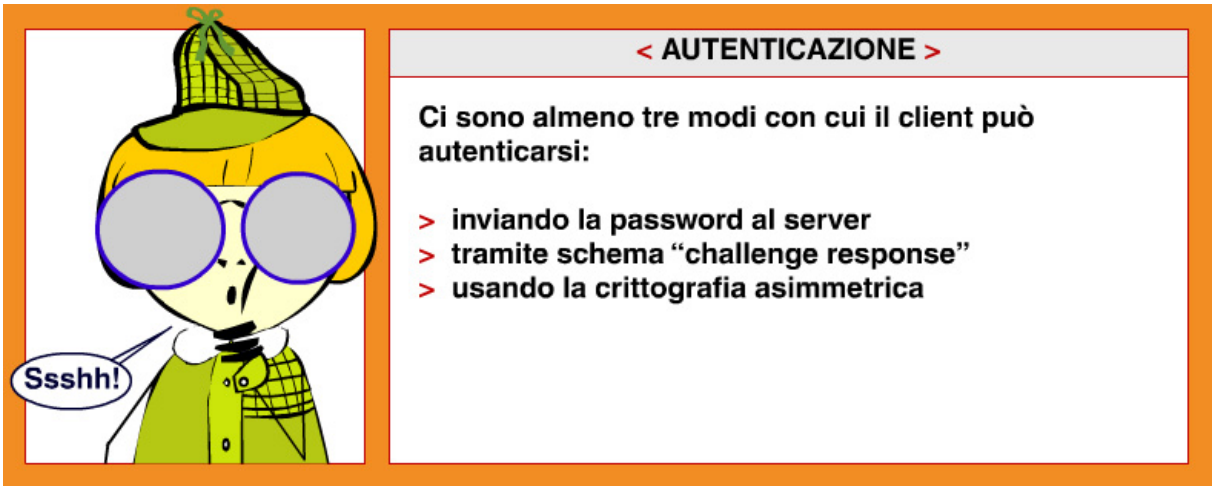
Solitamente l'autenticazione è basata su:

- **Qualcosa che il soggetto conosce**
  Il segreto che solo il soggetto autorizzato deve conoscere. È lo schema di autenticazione classico basato su "username/password", in cui la password deve essere conservata per non essere smarrita né resa pubblica. Impararla "a memoria" è la soluzione più comune, non esente da limiti.

- **Qualcosa che il soggetto possiede**
  Di solito è un dispositivo elettronico (hardware token o chiave USB) con dentro il segreto con cui si dimostra la propria identità. Ciò significa chiavi segrete con tanti bits, più robuste ma impossibili da memorizzare e dotate di un PIN (Personal Identification Number) senza il quale non funzionano, per impedirne l'utilizzo in caso di furto o smarrimento.

- **Caratteristiche biometriche del soggetto**
  Impronte digitali, riconoscimento del volto, scansione dell'iride.

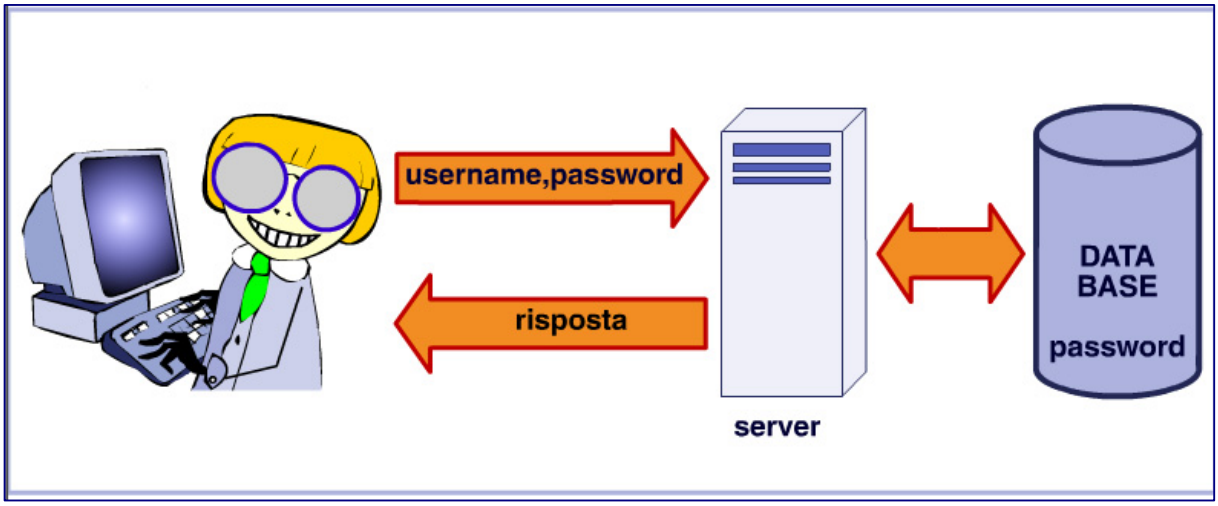
Autenticazione mediante password



Analizziamoli nelle prossime lezioni.

Autenticazione mediante password trasmessa al server

La password è trasmessa lungo il canale di comunicazione. Il server ottiene username e password in chiaro (non cifrata) e verifica se è corretta confrontandola con quella memorizzata sul DataBase di autenticazione, accessibile dal server.



Per ragioni di sicurezza, sul DataBase non vengono conservate le password in chiaro ma cifrate mediante una funzione hash a cui si può aggiungere un'altra stringa di caratteri (salt):

PasswordCifrata = Hash (PasswordInChiaro)
PasswordCifrata = Hash (PasswordInChiaro + Salt)

In questo modo la compromissione del DataBase di Autenticazione non comporta la perdita di riservatezza delle password in chiaro.

Quando riceve la password il server ne calcola la funzione Hash e la confronta con quanto presente nel DataBase di Autenticazione.

Approfondimento: Cos'è una Hash Function?

Una "hash function" H è una funzione che trasforma una sequenza di caratteri di lunghezza variabile in una stringa di lunghezza fissa, chiamato "valore hash" h = H (x).

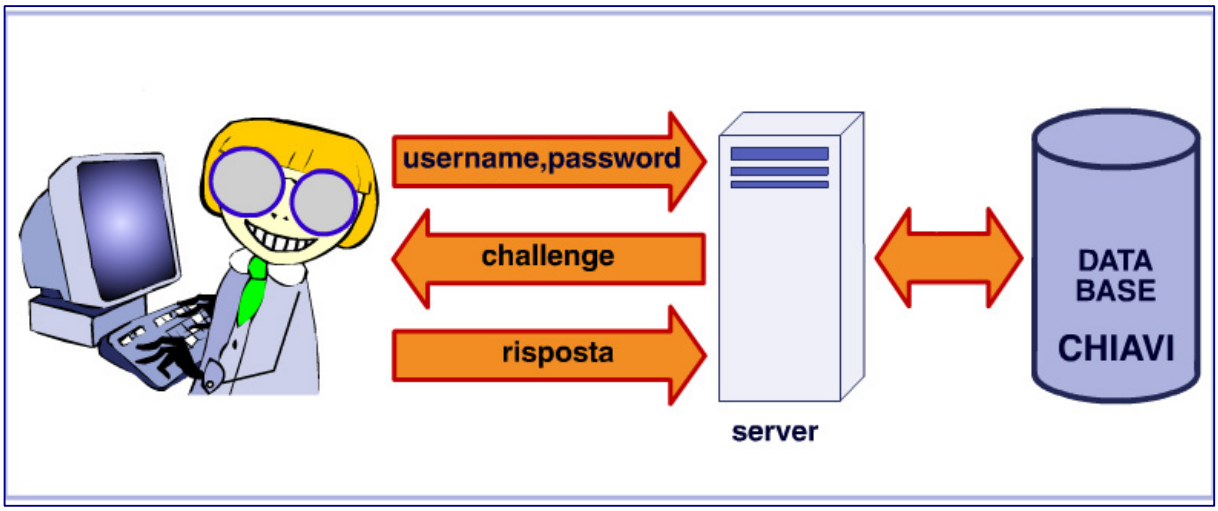
In crittografia sono utili Hash function con le seguenti caratteristiche:

- H(x) è semplice da calcolare
- H(x) è "one-way", ovvero difficile da invertire: dato un valore h è computazionalmente impossibile trovare una stringa x che produce lo stesso valore h
- H(x) è "collision-free" ovvero data una stringa arbitraria x è computazionalmente impossibile trovarne un'altra y con il medesimo valore di hash, tale che H(x) = H(y).

Il valore della funzione hash rappresenta in modo conciso la stringa di testo che l'ha prodotta e può essere considerata una "impronta digitale" del testo stesso. Esempi di Hash function largamente utilizzate in ambito ICT sono MD2 e MD5 e SHA.

Riferimenti:
MD5 http://www.ietf.org/rfc/rfc1321.txt
MD2 http://www.ietf.org/rfc/rfc1319.txt
SHA http://www.ietf.org/rfc/rfc3174.txt

Autenticazione con schema challenge response



In questo schema il client invia il proprio username al server, che genera una sequenza di caratteri casuale, detta challenge e gliela invia.

Il client deve cifrare il challenge con la password segreta ed inviare la risposta al server:
Risposta=Crypt(Challenge,Password)

Per verificare la correttezza, il server deve fare lo stesso calcolo, ovvero disporre di:

- **password in chiaro**
- oppure **dell'Hash (PasswordInChiaro)**
- oppure **dell'Hash (PasswordInChiaro + Salt).**

Tutto ciò fa sì che se qualcuno riesce ad impossessarsi del DataBase di Autenticazione non ottiene comunque le password in chiaro per tutti gli username.

Autenticazione mediante Crittografia Asimmetrica

La tecnica crittografica più comune è quella cosiddetta asimmetrica, in quanto all'algoritmo di cifratura sono applicate due chiavi di cifratura e decifratura diverse tra loro.

Le caratteristiche di questa autenticazione possono essere riassunte così:

- **Testo cifrato** = C (E, testo in chiaro)
- **Testo in chiaro** = C (D, testo cifrato)

In cui E = chiave di encription, D = chiave di decription, C algoritmo di cifratura.

È quindi troppo difficile ricavare D da E.

Con questo schema non è necessario tenere segrete entrambe le chiavi, anzi una delle due è resa pubblica (Chiave Pubblica), l'altra invece no (Chiave Privata).

Utilizzo della Crittografia Asimmetrica

Gli utilizzi di questo tipo di cifratura sono molteplici:

- per **dimostrare l'identità** di un soggetto si utilizza la chiave privata con un'autenticazione challenge response, combinata con il server (autenticazione)
- per **inviare un messaggio confidenziale** è sufficiente cifrare il messaggio con la chiave pubblica del ricevente (confidenzialità)
- per **dimostrare l'autenticità di un testo e la sua integrità** (non alterazione) è sufficiente cifrare il testo con la chiave privata del mittente. Il destinatario può verificarlo con quella pubblica rispettiva (firma digitale).

I limiti della Crittografia Asimmetrica

Alcuni limiti di questa tecnica sono:

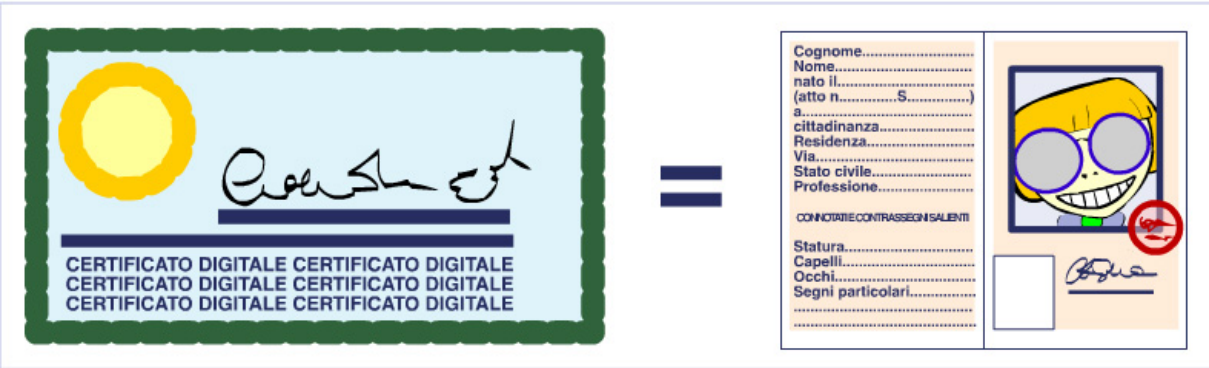
- le chiavi sono **molto lunghe** (128-256 caratteri), non possono essere scelte a memoria, devono essere conservate su un medium ed eventualmente cifrate con chiavi tradizionali. La sicurezza quindi risente di come si conserva la chiave privata, che non può essere memorizzata
- resta il problema della **distribuzione delle chiavi pubbliche** e della loro **associazione con l'identità della persona**: bisogna provarla a soggetti con cui prima non ci sono state relazioni. Tipica è l'autenticazione di siti web: affinché l'informazione venga considerata attendibile, chi naviga deve poter autenticare il sito cui si collega. Questo può avvenire tramite crittografia simmetrica, ma per l'utente generico non è pratico procurarsi le chiavi pubbliche di ogni server a cui si collega.

Per questo sono state sviluppate soluzioni che utilizzano Certificati Digitali.

Certificati Digitali

Il Certificato Digitale è un documento (digitale) che serve a certificare l'associazione tra una chiave pubblica e l'identità a cui è riferita. Contiene la chiave pubblica e le informazioni sull'identità dell'intestatario ed è firmato in modo digitale da una Certification Authority (CA).

Il Certificato Digitale è l'equivalente elettronico di una Carta di Identità: la fototessera e gli altri segni distintivi hanno il ruolo della chiave pubblica, mentre quella privata è la capacità di presentarsi di persona, rendendo possibile il confronto con la foto.



La Carta di Identità contiene anche i dati anagrafici (Nome Cognome, data e luogo di nascita) che costituiscono l'identità ed è rilasciata e firmata dall'Anagrafe del Comune di Residenza, che funziona da Certification Authority.

A seconda del contesto ci si può fidare di Certification Authority diverse: a livello aziendale basta il tesserino rilasciato dall'azienda, a livello internazionale la Carta di Identità non è sufficiente ed è necessario il Passaporto, analogo ma rilasciato da un altro ente.

Approfondimento: Cos'è la Certification Authority?

La **Certification Authority** è un ente che può emettere certificati: verifica l'effettiva titolarità del richiedente e rilascia i certificati, tramite la seguente procedura:

- il **soggetto** genera una coppia di chiavi, pubblica e privata, e presenta alla CA quella pubblica assieme alle proprie generalità
- la **CA** verifica, con meccanismi esterni, che l'identità corrisponda e "firma" il certificato con la propria chiave privata.

Il Certificato Digitale non contiene dati riservati e può quindi essere reso pubblico.

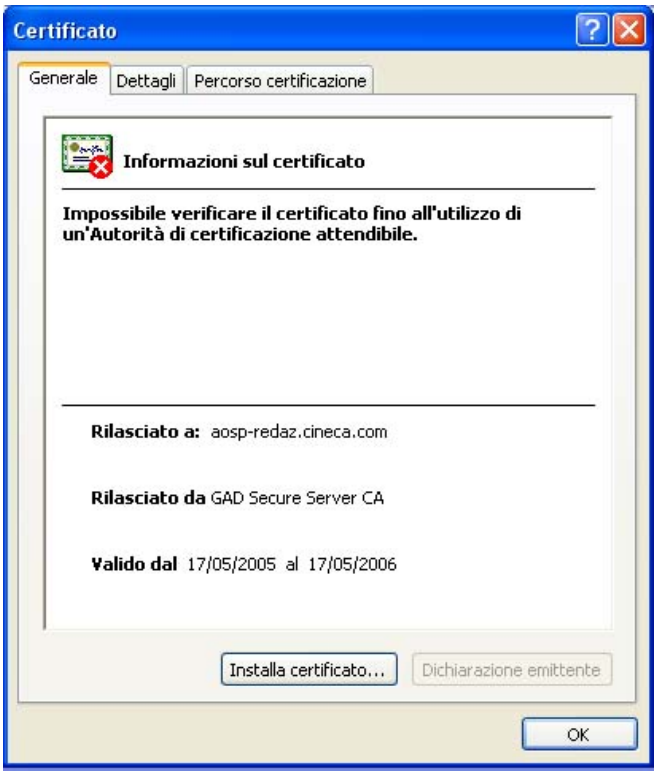
La verifica dell'identità mediante certificato avviene come segue:

- chi deve autenticarsi (il **client**) presenta il certificato digitale all'autenticatore (il server)
- il **server** controlla l'integrità del certificato verificando la firma della CA
- se il certificato è valido, il server estrae la chiave pubblica e con questa verifica l'identità mediante uno scambio challenge response.

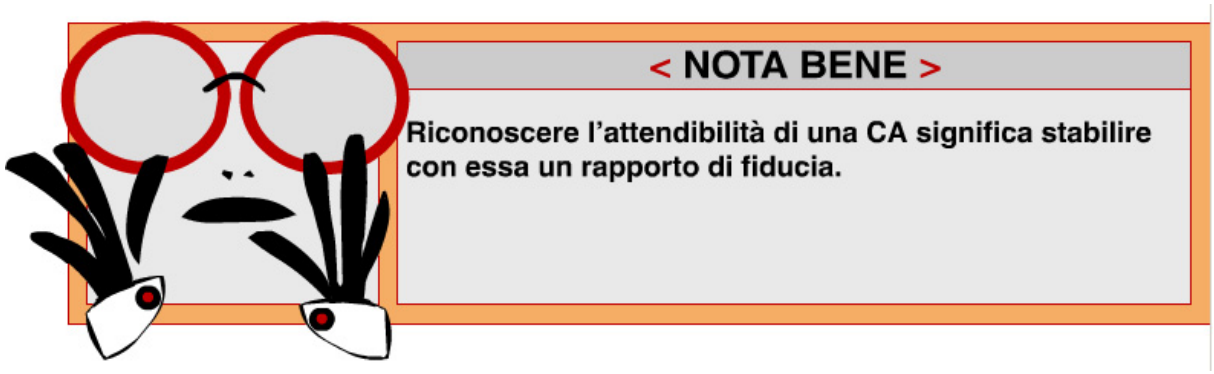
Come si comporta il browser se il certificato è stato emesso da una CA non riconosciuta?

Quando, navigando in Internet, si accede a una pagina del tipo https può aprirsi una finestra di allarme come questa:

Se si desidera procedere appare questa finestra:



Analizzato il certificato e accettata l'attendibilità della CA, quindi del certificato emesso, si può installarlo sul computer. Da questo momento quando si accede al sito non si aprono più finestre di allarme.

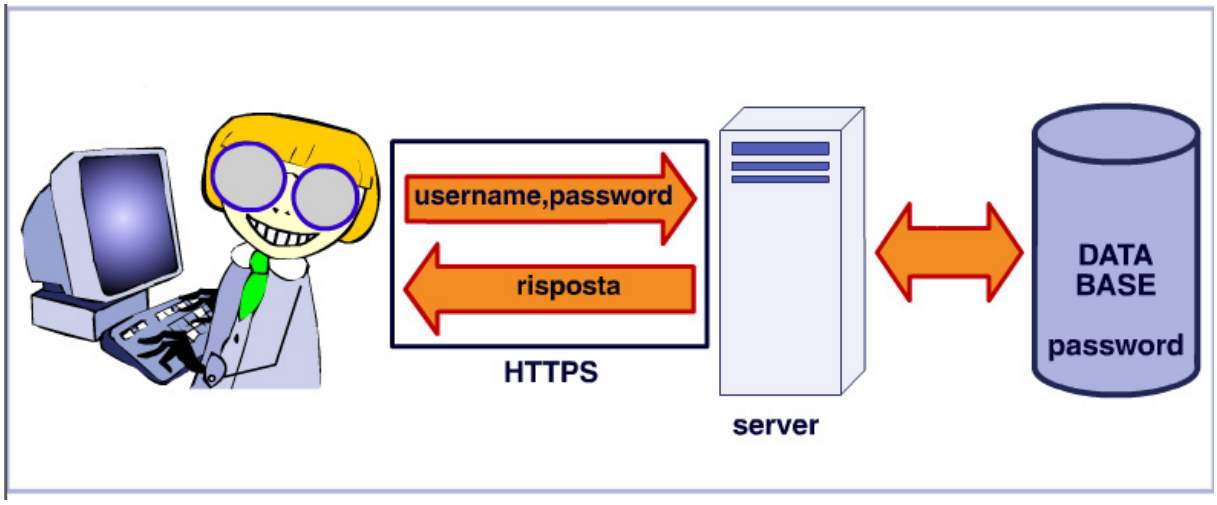


Soluzioni Tunnelled

L'impiego della crittografia asimmetrica per l'autenticazione, pur vantaggioso rispetto agli altri metodi, è più scomodo da utilizzare della semplice "username/password". Con molti utenti e una non eccessiva criticità delle applicazioni lo sforzo di far generare la coppia di chiavi pubblica e privata ed il certificato digitale personale non è giustificato.

Una via di mezzo molto usata è l'utilizzo della crittografia asimmetrica per creare un **canale di comunicazione cifrato** tra client e server, in cui il primo autentica il secondo tramite chiave pubblica. Per autenticare il client invece ci sono meccanismi più semplici ma sicuri, ad esempio basati sulla trasmissione della password al server in un canale cifrato, non intercettabile.

Il server di solito è dotato di un certificato firmato da una Certification Authority, che il client riconosce come fidata. Una implementazione diffusa è quella dei protocolli SSL o TLS, utilizzati per aumentare la sicurezza di altri protocolli: ad esempio la navigazione è più sicura con HTTPS, il protocollo standard HTTP impiegato su un canale sicuro SSL (da cui la "S" finale nel nome). Con HTTPS il client può autenticare in sicurezza il server. Inoltre se l'applicazione richiede anche l'autenticazione del client, questa può avvenire con una semplice username/password trasmessi sul canale cifrato.



Un canale sicuro con cifratura e autenticazione delle due parti si può creare anche a livello di "trasporto IP" con reti private virtuali (VPN), per cui il protocollo più utilizzato è IPSEC.

Modulo 4: Gli Attacchi

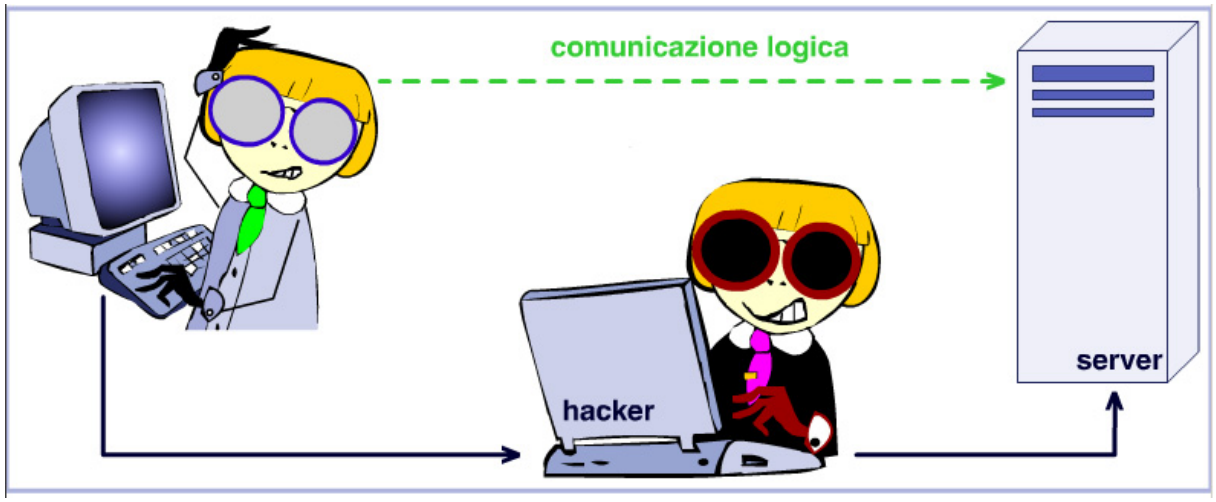
Indice del Modulo

Gli attacchi

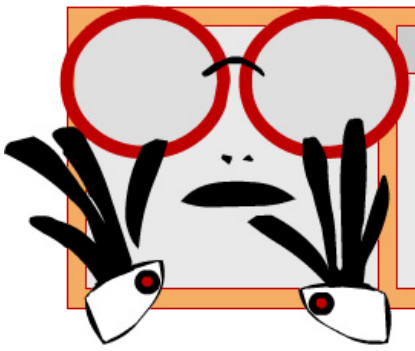
La sicurezza informatica cerca di assicurare la riservatezza, l'integrità e la disponibilità dei componenti di un sistema di elaborazione. Gli attacchi vengono compiuti verso l'hardware, il software e i dati. L'interazione tra questi è la base delle vulnerabilità della sicurezza. Persone e sistemi possono architettare attacchi che sfruttano queste vulnerabilità.

Attacchi Man in the Middle

Alcune delle tecniche si basano sulla cosiddetta posizione Man in The Middle (MitM): l'attaccante si trova sul canale di comunicazione tra client e server.



Può trattarsi di una posizione passiva, in cui il MitM può solo leggere il traffico in transito (ad esempio perché ne riceve una copia), oppure attiva, in cui l'attaccante può intercettare i pacchetti in transito e modificarne il contenuto.



< NOTA BENE >

Quando la comunicazione avviene in Internet è impossibile essere certi della sicurezza di ogni elemento della rete: il Man-in-The-Middle è una minaccia costante.

Da una posizione MitM sono possibili diverse attività utili ad un hacker:

- **Sniffing**: tutto il traffico in transito può essere catturato ed analizzato. In particolare l'attaccante può leggere tutti i dati sensibili trasmessi in chiaro.
- **Injecting**: possibilità di alterare il flusso informativo. Ad esempio, su una connessione in chiaro autenticata con username/password, se un MitM invia comandi al server vengono iniettati sul canale autenticato, risultando legittimi e spediti dal client.
- **Interruzione di servizio**: un MitM attivo può semplicemente interrompere la comunicazione tra client e server creando un Denial of Service.

Come possono essere condotti i MitM

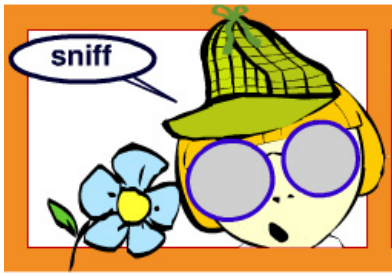
Per approfondire l'argomento bisogna sapere che, per ottenere una posizione Man-in-the-Middle, si possono attaccare i diversi protocolli utilizzati in modo trasparente, durante il processo di connessione ad un computer remoto. Le situazioni più comuni sono:

1. **DNS poisoning**
Collegandosi ad un host remoto il più delle volte si fornisce il suo nome, che viene tradotto in indirizzo IP dal protocollo DNS. Il client chiede al server DNS (name server) l'indirizzo associato ad un nome e attende la risposta. Un attaccante può fornire al client una risposta sbagliata, prima che arrivi quella ufficiale, oppure compromettere il Name server per alterare il suo DataBase.

2. **DHCP spoofing**
Su rete locale viene spesso utilizzato il protocollo DHCP per configurare in automatico la rete di un host mobile, utilizzato per le postazioni di lavoro. Il PC manda in broadcast sulla rete un messaggio per "scoprire" i server DHCP disponibili, che a priori non conosce, e attende la risposta. Anche in questo caso l'attaccante può fornire una risposta sbagliata, prima che arrivi quella attesa. Poiché tra i parametri configurabili via DHCP c'è anche il default-gateway (il router a cui vengono inviati i pacchetti non destinati alla rete locale), l'attaccante può fare in modo che si imposti come default gateway un IP a piacimento, che riceve tutto il traffico inviato fuori della rete locale.

3. **ARP poisoning**
Su rete locale gli indirizzi IP sono tradotti in "MAC address" tramite il protocollo ARP, in cui ogni host delle rete locale può informare gli altri dell'associazione tra il proprio IP address e il MAC address. In questo scenario l'attaccante (B) che vuole intromettersi tra A e C manda ad A un pacchetto ARP informandolo che l'indirizzo IP di C corrisponde al proprio MAC address (MAC B:B) allo stesso modo manda a C un pacchetto ARP con l'IP di A coincidente col MAC address B:B. Poiché la comunicazione LAN avviene con i MAC address, B può ricevere e controllare tutto il traffico tra A e C.

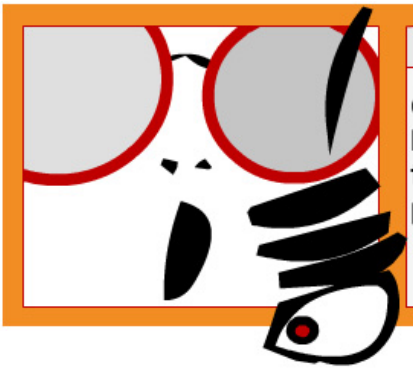
Attacchi ai meccanismi di autenticazione



< SNIFFING >

L'autenticazione basata sull'invio della password al server rischia attacchi di tipo sniffing: cattura della password.

Un man-in-the-middle può sempre farlo quando si utilizza un protocollo che prevede la trasmissione della password in chiaro. Anche se il canale è cifrato, la password è resa disponibile al server in chiaro: un hacker che l'ha compromesso è in grado di ottenerla e di riutilizzarla su altri sistemi (per questo è meglio utilizzare password diverse in ambienti con diversi livelli di sicurezza).
Se si usano schemi di tipo challenge-response, la password non è trasmessa ma deve esser nota al server e conservata nel DataBase di Autenticazione: stesso rischio di prima.



< NOTA BENE >

Curate la sicurezza dei server ma anche dei client. Infatti un hacker capace di violare il client può catturare tutte le informazioni sensibili digitate sulla sua tastiera, password comprese.

< AUTENTICAZIONE >

I modi per indovinare la password (password cracking) sono:

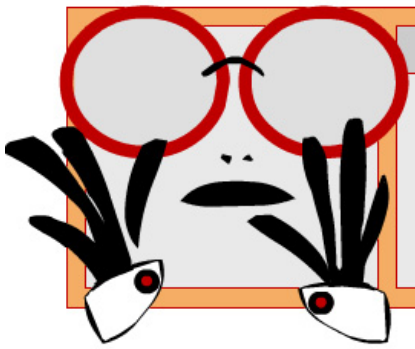
- **provare tutte le possibili combinazioni**
- **tentare le combinazioni più comuni (ad esempio derivanti dallo username)**
- **raccogliere informazioni derivanti dalle password (ad esempio gli scambi challenge response riusciti) e analizzarle off-line senza insospettire l'autenticatore.**

Ingegneria sociale

Per Ingegneria Sociale si intendono le tecniche di attacco alla componente umana del sistema di difesa, che portano ad abbassare la guardia e a commettere errori o leggerezze utilizzabili dall'hacker.

I casi più classici sono le password scritte su bigliettini, incustoditi o smarriti, o i falsi messaggi di posta elettronica in cui si invita ad installare programmi che si rivelano "cavalli di Troia". Un esempio recente è il cosiddetto phishing, di cui tratteremo tra breve.

Una contromisura è la formazione, non solo per gli specialisti ma anche per gli utilizzatori dei sistemi, che devono diventare consapevoli rispetto alla sicurezza e alla separazione dei privilegi.

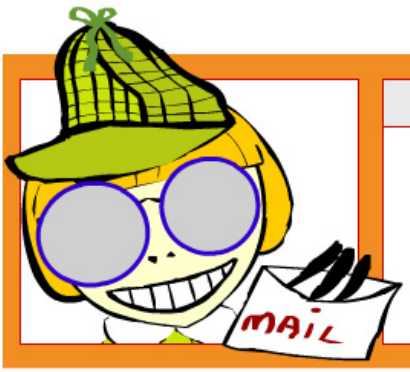


< NOTA BENE >

Per evitare che comportamenti deliberati o accidentali causino danni al sistema fornite a ogni utente i privilegi minimi.

Il Phishing

Il Phishing è un metodo per indurre un utente a fornire informazioni riservate: credenziali di accesso, numero di carta di credito...



< PHISHING >

Di solito arriva una mail di cui apparentemente si conosce la provenienza (ad esempio una banca). La mail invita a visitare il proprio sito e soprattutto ad autenticarsi o fornire altri dati riservati.

La mail ha un aspetto assai simile a quello dell'organizzazione presa di mira e, ovviamente il mittente falsificato: sembra vera. Di solito ha un link che rimanda a un sito diverso da quello ufficiale ma anch'esso simile. L'inganno sta nella URL nascosta nel link: è diversa da quello originale.

L'hacker cerca di mascherare la cosa in vari modi:

- utilizzando una **URL molto simile** all'originale
- utilizzando come **testo del link l'URL corretta** che **nasconde quella fasulla**
- utilizzando **features** o **bugs** dei browser che consentono di controllare cosa appare "in basso a sinistra" quando il cursore passa sul link (facendo comparire l'URL originale) o addirittura cosa appare sulla barra dell'indirizzo quando si visita il sito dell'hacker (facendo comparire l' URL originale).

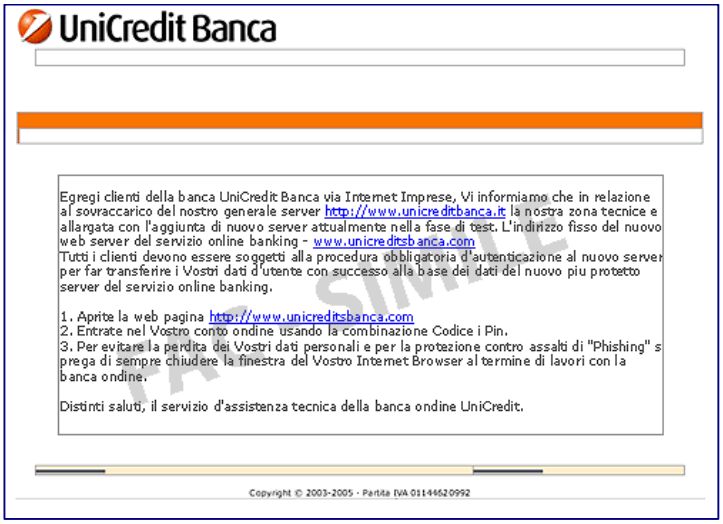
L'autenticazione tramite SSL e il controllo del certificato non aiuta: l'hacker può avere ottenuto un certificato valido e assolutamente originale per il proprio sito .. non c'è nulla di male… solo che non è quello che l'utente cercava!

Difendiamoci dal Phishing

Le difese consistono nell'aggiornare il software, per dare agli hacker meno strumenti per nascondere le proprie intenzioni, e nel tenere gli occhi ben aperti:

- se vi collegate ad un sito con cui scambiate informazioni riservate, siate certi di utilizzare l'URL corretta
- digitate l'URL personalmente sulla "barra indirizzo" del browser
- utilizzate i vostri bookmark o seguite link di siti fidati
- non fidatevi di link in pagine HTML che arrivano ad esempio con messaggi di posta

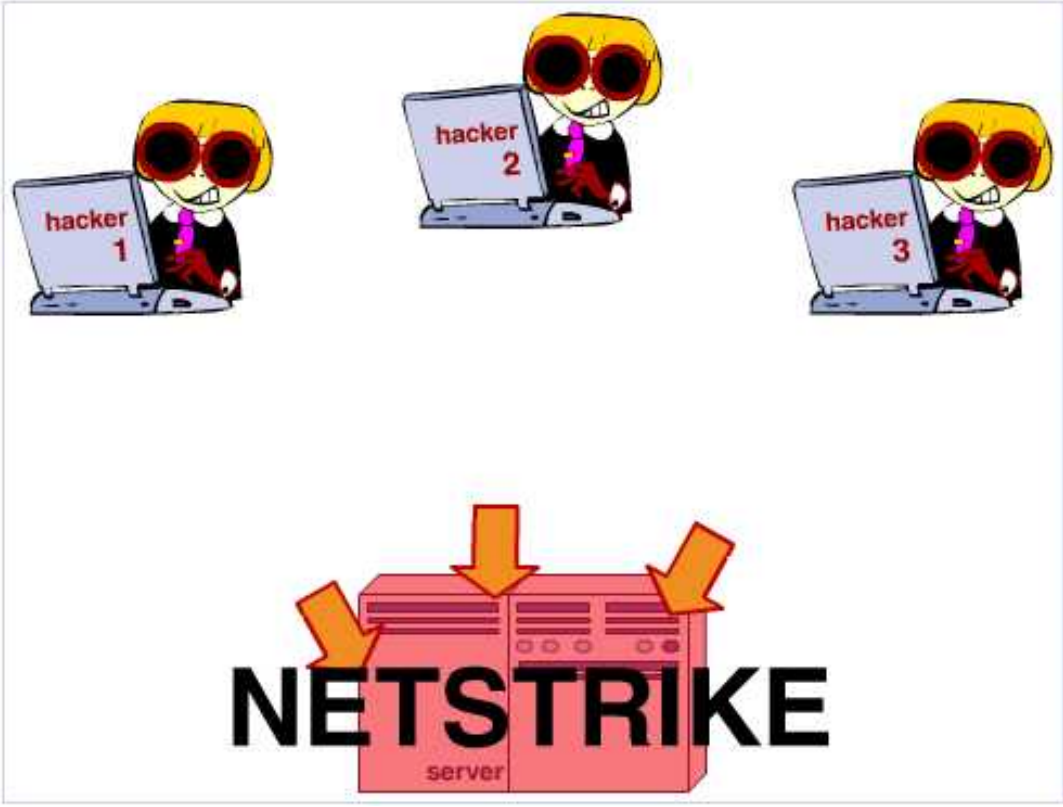
Ecco un caso reale di phishing: il messaggio fatto circolare per posta elettronica invita a collegarsi al sito www.unicreditsbanca.com, nome simile ma diverso dall'originale www.unicreditbanca.it.



Attacchi DOS

Gli attacchi di tipo Denial of Service (Dos) servono a interrompere un servizio informativo e a causare una perdita di disponibilità dell'informazione.

L'attaccante non accede a informazioni riservate, ma può comunque procurare danni economici o di immagine o guadagnarci in visibilità e prestigio. Un esempio è il cosiddetto **netstrike** o sciopero in rete: un grande numero di "manifestanti" si accorda per scaricare contemporaneamente contenuti dallo stesso sito esaurendone le risorse e oscurandolo. E dimostrando l'alta partecipazione alla manifestazione in rete.



Un altro scopo di un Dos può essere mettere fuori uso sistemi di vigilanza (ad esempio sistemi di Intrusion Detection) per nascondere e rendere possibili altri attacchi più diretti.

Ci sono due diverse categorie di DOS:

- quelli che mirano a esaurire le risorse del sistema (disponibilità di banda, tempo di CPU, disco, ecc.) con una grande quantità di richieste legittime
- quelli che mirano a causare un malfunzionamento, sfruttando errori nei programmi (vulnerabilità) o interrompendo le comunicazioni da posizioni Man-in-the-Middle.

Attacchi DDos

Per esaurire le risorse di un server, ad esempio la banda, bisogna averne di più.

Questo si può ottenere disponendo di molti sistemi che attaccano contemporaneamente la stessa vittima: il cosiddetto Distributed Denial of Service (DDos).

In un DDos un hacker può compromettere una grande quantità di host e, all'insaputa dei legittimi proprietari, installare su di essi agenti software per scatenare simultaneamente un attacco contro la stessa vittima. La "potenza di fuoco" complessiva può essere elevata e trovare e bloccare l'attacco è assai difficile: arriva da molti punti in apparenza scollegati.

Considerazioni sugli attacchi DOS e DDos

I DOS sono relativamente facili da condurre e difficili da trattare.

- Un errore di implementazione in un programma che fornisce un servizio di rete può facilmente portare ad un Dos. È più facile sfruttare il baco per ottenere il DOS che per penetrare il sistema, come per i Buffer Overflow, trattati più avanti. Se il servizio è erogato da un solo processo (single threaded), il suo crash significa interruzione totale.

- È più facile causare un DOS quando una richiesta leggera (poche decine di byte inviati) implica una risposta pesante che richiede al server una elaborazione complessa, come ad esempio nei motori di ricerca.

- In caso di grosse quantità di richieste, non è facile distinguere quelle dagli utenti legittimi da quelle generate dall'attaccante. Di solito come unico indizio, il server ha l'indirizzo IP di provenienza, per cui si può porre un limite alle richieste di ognuno in per un periodo di tempo. Spesso gli IP coinvolti nell'attacco sono molti, o perché è distribuito o perché la sua tipologia consente di falsificare l'indirizzo di provenienza.

- Spesso si possono fare Dos con molti indirizzi falsificati: tracciarne l'origine è molto complesso e bloccarli richiede un difficile intervento di filtro tempestivo e coordinato fra i vari soggetti che gestiscono la rete.

Attacchi ai meccanismi di autorizzazione

> **L'autorizzazione è il processo con cui il server stabilisce ed implementa le restrizioni di accesso ai dati per gli utilizzatori legittimi del sistema.**

Ad esempio un server web pubblico non limita i soggetti che possono visitare il sito (non c'è necessità di autenticazione), ma deve consentire l'accesso **in sola lettura** alla sola parte di dati relative alle pagine. Un attaccante che riesce ad aggirare l'autorizzazione può accedere a informazioni sul server diverse da quelle del sito, oppure alterarne il contenuto (*web defacement*).

Molti attacchi di questo tipo coinvolgono la validazione dei dati in ingresso: l'hacker fornisce dati malevoli a un programma che è quindi costretto a comportarsi in modo diverso da come dovrebbe. Tutto ciò non stupisce: i dati in ingresso sono l'unico modo con cui interagire con un sistema che si intende compromettere.

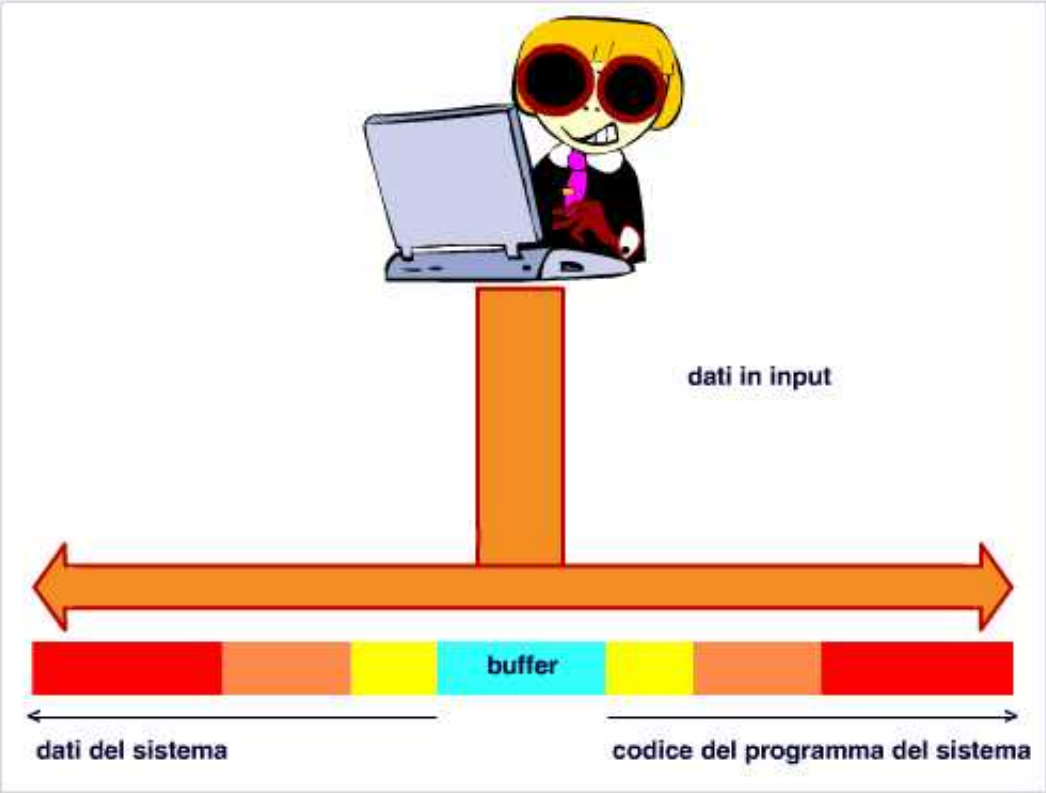
Buffer Overflow

Un buffer (o array o stringa) è uno spazio in cui vengono conservati i dati, risiede in memoria e, poiché essa è finita, lo sono anche sue la capacità. In alcuni linguaggi di programmazione non bisogna chiarire la dimensione massima del buffer, pertanto un errore di superamento del limite non è rilevabile.

Il Buffer Overflow è l'equivalente informatico del versare due litri d'acqua in una brocca che ne tiene uno: parte del liquido trabocca e provoca un disastro. Nell'elaborazione informatica questi errori provocano un danno di gran lunga peggiore!

> **Il Buffer Overflow (BOF) avviene quando l'attaccante invia una stringa più grande del buffer in cui viene immagazzinata, causando la sovrascrittura di parti di memoria circostanti.**

Il programma del sistema sotto attacco copia i dati in input nella memoria, andando oltre lo spazio allocato. Poiché la memoria contiene anche il programma in esecuzione, l'attaccante può inserire codice malevole e prendere il controllo del sistema operativo.



Code injection

Un'altra vulnerabilità legata ad una mancata validazione dell'input accade tutte le volte che in un programma (ad es un cgi-bin) viene eseguita una sub-shell per interpretare un comando con una stringa passata dall'utente. Se non si controlla bene il dato in input, un attaccante può immettere una sequenza di caratteri "speciali" per la shell che mandano in esecuzione un comando arbitrario.

Uno scenario simile è la costruzione di una query SQL per interrogare un DataBase con un input dell'utente. La query può essere manipolata per estrarre e fornire all'attaccante dati diversi da quelli a cui avrebbe accesso, o per alterare il contenuto del DataBase

Quali sono i programmi a rischio?

I programmi per attaccare i meccanismi di autorizzazione sono quelli che elaborano i dati provenienti da soggetti che hanno diritti inferiori a quelli del programma.

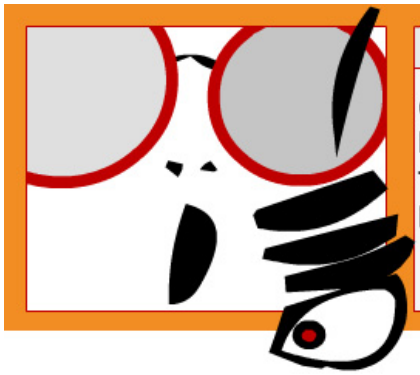
Inducendo il programma a comportarsi in modo anomalo, l'attaccante può ottenere i suoi stessi privilegi.

Questo avviene in modo assai frequente:

- **Lato server**
  - Network daemon (spesso in ascolto con privilegi elevati)
  - Web based application, critiche perché spesso scritte da programmatori non esperti e poco attenti alla sicurezza.
  - Processi locali che utilizzano privilegi elevati (ad es: suid bit programs in Unix, System services in Windows).

- **Lato client**

Qualunque cosa tratti dati esterni, ad esempio Web browser, mail reader.



< NOTA BENE >

Curate la sicurezza dei server ma anche dei client. Infatti un hacker capace di violare il client può catturare tutte le informazioni sensibili digitate sulla sua tastiera, password comprese.

Quali sono le macchine a rischio?

Sono da considerare a rischio i server, ovvero tutte le macchine che forniscono servizi e informazioni.

Cause del rischio

I server

- conservano le informazioni sensibili
- implementano meccanismi di autenticazione e autorizzazione e sono perciò esposti ai relativi attacchi
- hanno un vasto insieme di utenti e quindi di potenziali attaccanti.

Strumenti di difesa

I server

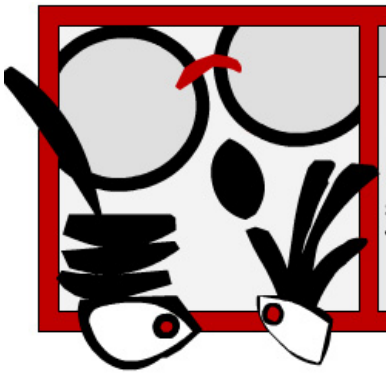
- sono amministrati da sistemisti professionisti che conoscono (o dovrebbero conoscere) bene le problematiche di sicurezza
- sono utilizzati prevalentemente o esclusivamente per i servizi aziendali, il software installato dovrebbe essere ben selezionato e controllato
- implementano diversi livelli di autorizzazione, ciò consente di dare agli utenti i privilegi minimi indispensabili (diversi a utenti diversi).
- sono macchine "fisse" che possono quindi beneficiare di difese perimetrali, come Firewall, sistemi di Intrusion Detection e Intrusion Prevention
- sono generalmente pochi, quindi meglio difendibili.

Sono da considerare a rischio le stazioni di lavoro individuale.

< RISCHIO >

Le stazioni di lavoro individuale presentano aspetti critici in quanto:

1 > sono gestite da utilizzatori che non sono sistemisti professionisti
2 > danno l'accesso ai sistemi informativi interni e entrano in possesso delle credenziali dell'utente
3 > possono essere utilizzate in vario modo: per accedere alla rete interna, navigare in Internet, installare software non sicuri
4 > nell'organizzazione ci sono tanti utenti, è più difficile controllarli tutti
5 > spesso i livelli di autorizzazione sono male usati
6 > i sistemi portatili non usufruiscono di difese perimetrali, si collegano a reti potenzialmente ostili e devono difendersi da soli



< ATTENZIONE >

**E' indispensabile adeguare la vostra stazione di lavoro alle policy di sicurezza della vostra organizzazione.
Infatti ogni volta che digitate un'informazione sensibile sulla tastiera o la leggete sullo schermo riponete completa fiducia nel sistema che state utilizzando.**

Modulo 5: Sistemi e comportamenti di difesa

Indice del Modulo

- I sistemi Firewall
- I sistemi IDS e IPS
- Il ruolo dei diversi sistemi di difesa
- Le regole principali

I sistemi Firewall

Per Firewall di solito si intende l'insieme di hardware o software che difendono uno o più sistemi e che implementano politiche di sicurezza, filtrando il traffico di rete destinato o proveniente dai sistemi da proteggere.

Le funzioni di firewall sono implementate su vari livelli:

- a livello di rete da un apparato dell'infrastruttura di rete
- i server moderni possono essere configurati per fungere da firewall. In questo caso si parla di "host firewall"
- le postazioni di lavoro (portatili) possono implementare funzioni di firewall (Personal Firewall).

I firewall si distinguono per l'analisi che effettuano sul traffico di rete e per il meccanismo con cui stabiliscono il traffico frequente.

Approfondimento: Tipologie di firewall

- **Stateless packet filter**
  Nelle implementazioni più semplici ogni singolo pacchetto viene esaminato e sono presi in considerazione solo gli indirizzi IP e le porte sorgente e destinazione. Si parla in questi casi di stateless packet filter.

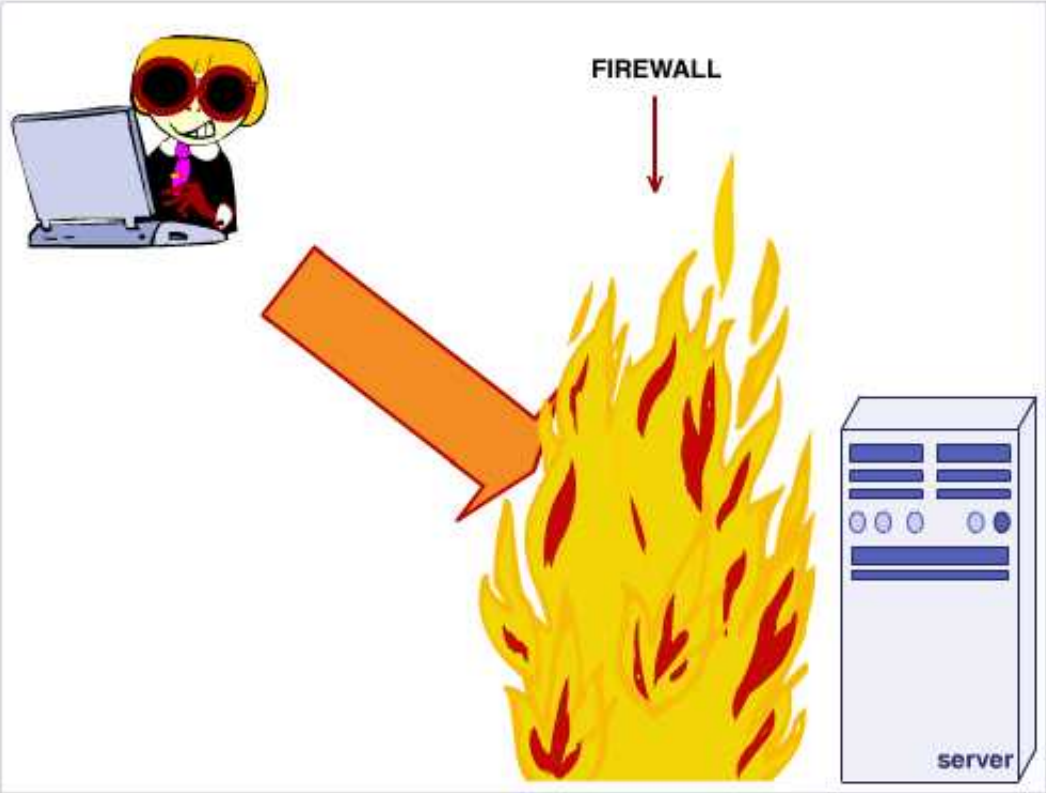
- **Firewall statefeull**
  In determinate condizioni non è semplice distinguere se un pacchetto fa parte di un flusso autorizzato o meno, ad esempio se è una risposta di un server esterno ad una richiesta legittima o un tentativo non consentito di utilizzare servizi interni. Questo problema viene risolto dai firewall statefeull, che tengono traccia delle comunicazioni ed esaminano (almeno in parte) il contenuto dei pacchetti, riconoscendo la risposta dall'aver visto o meno passare prima la domanda.

- **Application gateway**
  I firewall più sofisticati impongono restrizioni a livello applicativo. Vengono chiamati "application gateway" perché devono conoscere il protocollo applicativo per poterlo comprendere e interpretare correttamente.

I firewall sono configurati sulla base delle necessità di comunicazione dell'infrastruttura da proteggere. È buona norma, comunque, negare qualunque comunicazione non esplicitamente permessa, permettendo solo quelle necessarie alla funzionalità dei servizi.

Ad esempio le stazioni di lavoro devono navigare e accedere ad altri servizi in Internet, ma non essere direttamente visibili all'esterno dell'organizzazione.

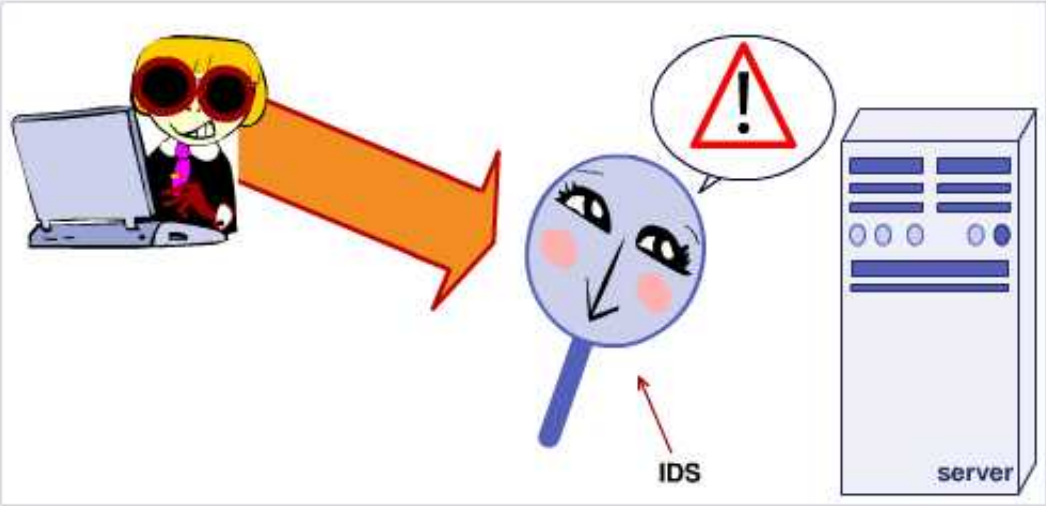
In generale i server devono esser visibili all'esterno solo per i servizi fruiti all'esterno: ad esempio un web server deve essere verosimilmente raggiungibile solo sulle porte 80 (http) e 443 (https), le altre è meglio non renderle accessibili.



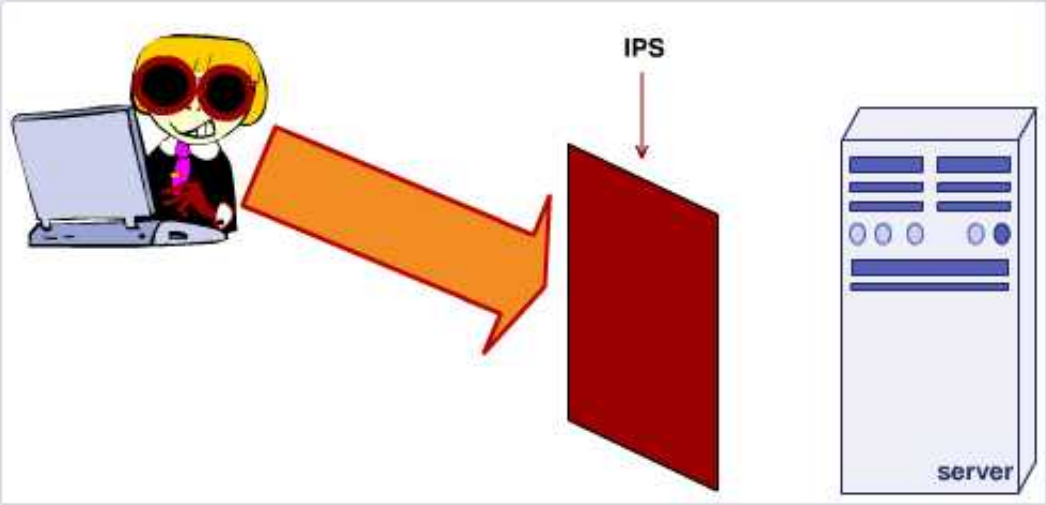
I sistemi IDS e IPS

> **I sistemi di Intrusion Detection (IDS) o Intrusion Prevention (IPS) servono per analizzare il traffico di rete e cercare possibili tentativi di compromissione o attacco.**

Individuato un traffico sospetto, può essere segnalato ad un operatore per un'ulteriore analisi dal sistema di Intrusion Detection



Il traffico sospetto può, invece, essere bloccato automaticamente dal sistema di Intrusion Protection



È chiaro che per agire in tal senso sistemi IDS e IPS devono:

- poter analizzare il traffico
- per i sistemi IPS, essere inseriti sui collegamenti di rete per bloccare il traffico, quando serve.

I sistemi IDS o IPS possono essere installati sui singoli host (Host Based). In questo caso possono utilizzare altre informazioni per riconoscere un attacco, come i file di log o le attività.

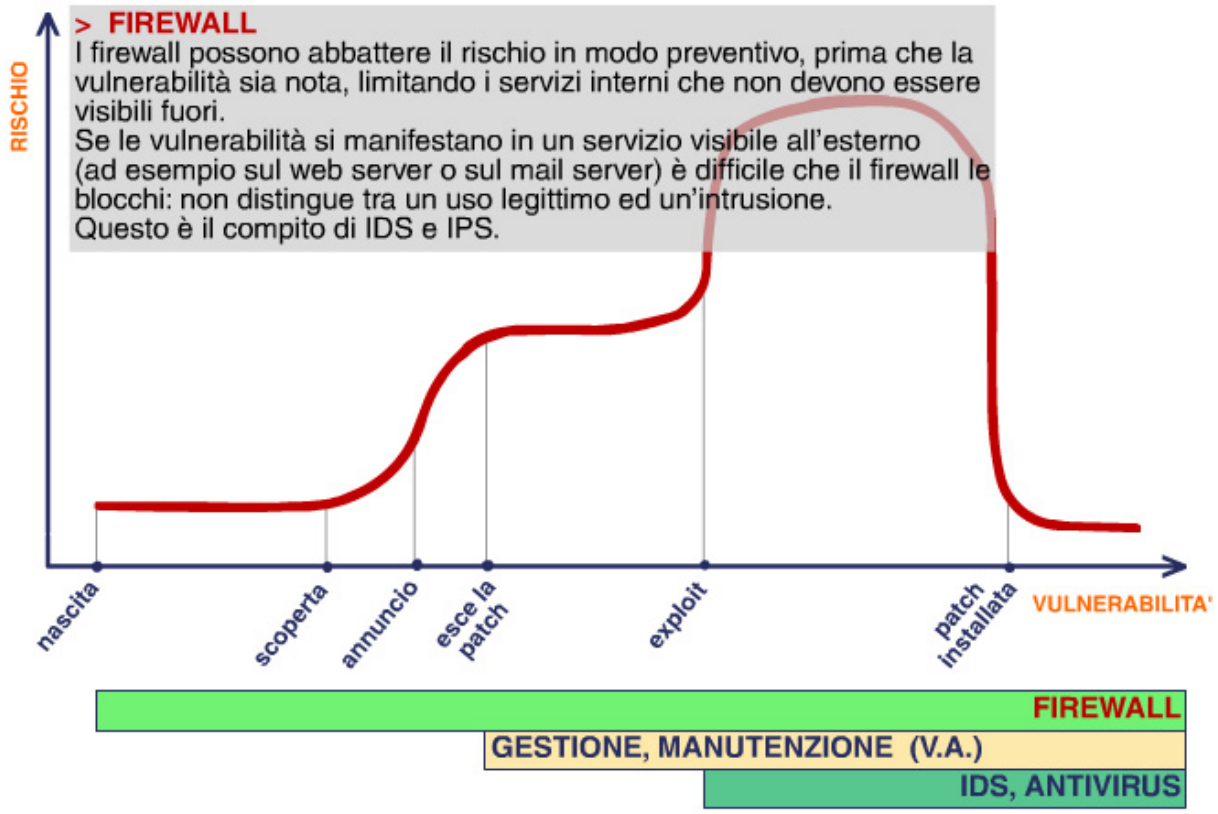
Le strategie di Analisi delle attività possono essere di due tipi:

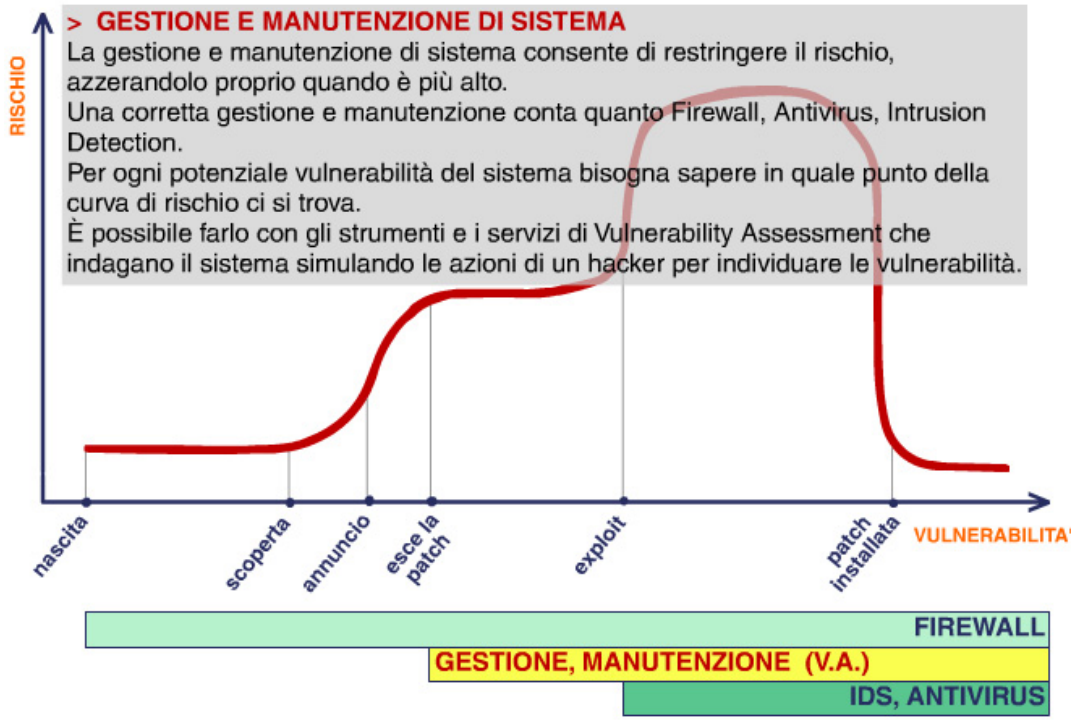
- **Ricerca di "pattern" di attività riconducibili ad attacchi noti (signatures) o sospetti**
  È il modo utilizzato dagli antivirus, di fatto sistemi IPS "host based", che proteggono o individuano solo attacchi "noti".

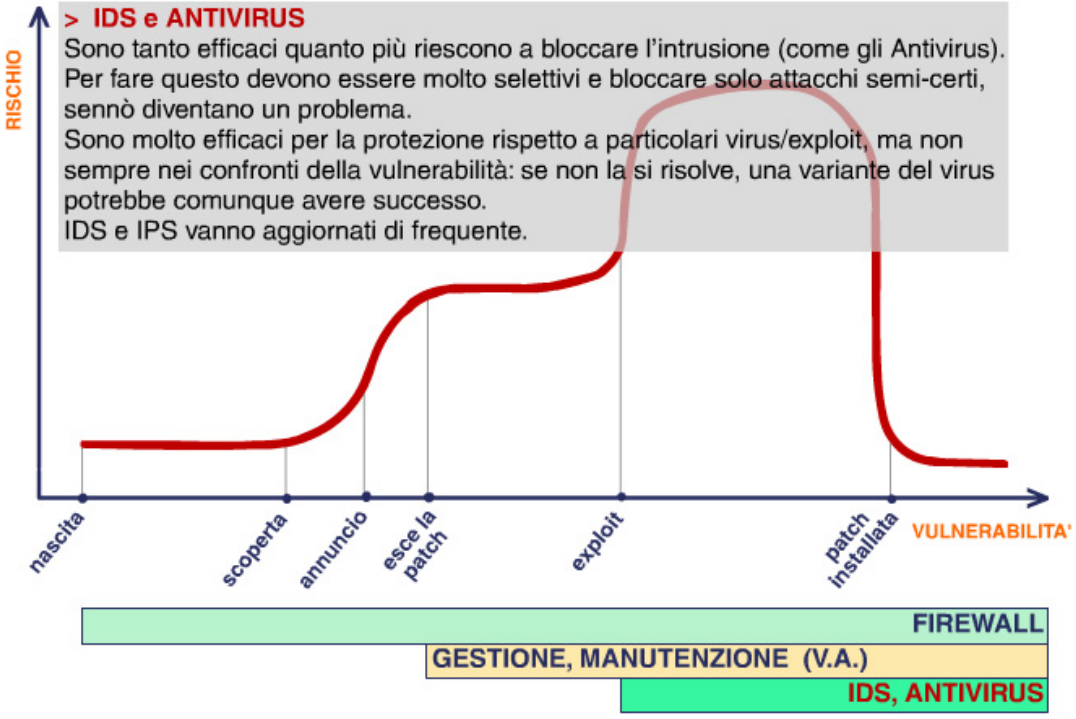
- **Ricerca di "comportamenti anomali"**
  Il sistema scopre e impara il comportamento "medio" (ad esempio analisi statistiche del traffico e delle attività dei processi) e segnala eventuali scostamenti. È in grado così di rilevare anomalie legate ad attacchi non "noti", ma è maggiormente suscettibile di falsi positivi.

Il ruolo dei diversi sistemi di difesa

Dal grafico sul ciclo di vita di una vulnerabilità si può valutare in che modo i sistemi di difesa più comuni contribuiscono ad abbattere il rischio. Clicca, nell'immagine, sui tre sistemi di difesa per conoscerne le caratteristiche.




> GESTIONE E MANUTENZIONE DI SISTEMA
La gestione e manutenzione di sistema consente di restringere il rischio, azzerandolo proprio quando è più alto.
Una corretta gestione e manutenzione conta quanto Firewall, Antivirus, Intrusion Detection.
Per ogni potenziale vulnerabilità del sistema bisogna sapere in quale punto della curva di rischio ci si trova.
È possibile farlo con gli strumenti e i servizi di Vulnerability Assessment che indagano il sistema simulando le azioni di un hacker per individuare le vulnerabilità.
RISCHIO
nascita
scoperta
annuncio
esce la patch
exploit
patch installata
VULNERABILITA'
FIREWALL
GESTIONE, MANUTENZIONE (V.A.)
IDS, ANTIVIRUS


> IDS e ANTIVIRUS
Sono tanto efficaci quanto più riescono a bloccare l'intrusione (come gli Antivirus).
Per fare questo devono essere molto selettivi e bloccare solo attacchi semi-certi, sennò diventano un problema.
Sono molto efficaci per la protezione rispetto a particolari virus/exploit, ma non sempre nei confronti della vulnerabilità: se non la si risolve, una variante del virus potrebbe comunque avere successo.
IDS e IPS vanno aggiornati di frequente.
RISCHIO
nascita
scoperta
annuncio
esce la patch
exploit
patch installata
VULNERABILITA'
FIREWALL
GESTIONE, MANUTENZIONE (V.A.)
IDS, ANTIVIRUS

Le regole principali

Riassumendo, le regole principali per mantenere in sicurezza un sistema sono:

1. Individuare ambiti di sicurezza distinti e tenerli il più possibile separati (firewall).

   A livello di progetto della rete e della infrastruttura IT:
   - utilizzare (V)LAN separate e connesse tra loro tramite Firewall, con configurazioni che permettono solo comunicazioni indispensabili

   A livello utente:
   - utilizzare password diverse per diversi domini
   - se una macchina fa parte di un dominio ad elevato livello di sicurezza, limitarne il più possibile l'utilizzo in contesti differenti (ad esempio non utilizzare il portatile dell'organizzazione, con cui si accede ad informazioni e sistemi riservati, per installare giochi o altri programmi di dubbia provenienza).

2. Usare comunicazioni cifrate, con mutua autenticazione, per evitare attacchi del tipo Man-in-the-Middle.

3. Mantenere aggiornato il software (Patch management):
   - I vendor hanno strumenti che "analizzano" il software e propongono aggiornamenti (Windows Update, Office Update, Microsoft Baseline Security Analyzer, Linux RH "up2date", ecc.).
   - Seguire regolarmente gli avvisi dei fornitori sulle vulnerabilità dei software.

     Questo compito è tanto più impegnativo quanto più la macchina è critica, complessa, con molto sw installato proveniente da differenti fonti.

4. Applicare il principio dei privilegi minimi e delle configurazioni minime:
   - utilizzare account non privilegiati se non è indispensabile
   - limitare allo stretto necessario il software installato e i servizi che la macchina fornisce all'esterno.

5. Utilizzare buone password e cambiarle con regolarità.

6. Eseguire verifiche periodiche con test di vulnerabilità.

7. Utilizzare antivirus e sistemi di backup per evitare di perdere dati preziosi.

8. Infine è indispensabile rendere consapevoli delle tematiche della sicurezza tutte le parti dell'organizzazione, anche il personale non tecnico/specialistico. Per questo bisogna fare formazione, con approfondimenti adeguati ai diversi ruoli e mansioni.