Sicurezza nei sistemi informatici

Classe 5ASI
ITCG Fermi

Definizioni

- **Riservatezza** (o **confidenzialità**, o **segretezza**) **dei dati**: dati leggibili e comprensibili solo dalle persone autorizzate
- **Integrità dei dati**: dati letti e/o modificati solo da persone autorizzate
- **Disponibilità dei dati**: dati devono essere disponibili in qualunque momento per le persone autorizzate per cui occorre garantire la continuità del servizio
- **Paternità** (o **non ripudiabilità**) **dei dati**: ogni dato deve essere associato ad un utente che non può ripudiare i dati da lui spediti e/o firmati.
- **Autenticazione** ("o" **autenticità**): processo di riconoscimento delle credenziali dell'utente per assicurarsi dell'identità di chi invia e/o esegue operazioni.
  Metodi di verifica dell'identità di un utente: (1) informazioni riservate (es. password), (2) oggetti elettronici (es. smart card), (3) strumenti di riconoscimento biometrici (es. impronta digitale, fondo retina ecc.)
- **Autorizzazione**: per l'utente autenticato occorre stabilire l'insieme delle autorizzazioni (azioni permesse, risorse accessibili, dati consultabili e/o modificabili)

Sicurezza Informatica (o Cybersicurezza)

ENISA (Agenzia dell'Unione europea per la cibersicurezza):

> Is there a need for a definition? Cybersecurity is an enveloping term and it is not possible to make a definition to cover the extent of the things Cybersecurity covers. Therefore, a contextual definition, based

Nonostante non esista una definizione comunemente accettata, tutte le definizioni di cybersicurezza condividono più o meno gli stessi aspetti.

Cybersicurezza (o **sicurezza informatica**): insieme delle misure atte a garantire la disponibilità, l'integrità, e la riservatezza, la paternità delle informazioni gestite dai sistemi informatici, e atte a garantire l'autenticazione delle credenziali dell'utente, e le autorizzazioni per l'utente autenticato.

Definizioni

Minaccia informatica: qualsiasi circostanza, azione, evento intenzionale (attacchi informatici) o accidentale (errori e/o malfunzionamenti) che può causare la perdita di almeno una proprietà di sicurezza (riservatezza, integrità, disponibilità, paternità, autenticazione, autorizzazione).

Esempi di eventi intenzionali ed accidentali

1. **Eventi intenzionali** (o attacchi informatici) (IP spoofing; packet sniffing; connection hijacking; DoS; DDoS)
2. **Eventi accidentali** (o errori e/o malfunzionamenti): (i) inadeguatezza delle strumentazioni, delle politiche, e delle tecnologie di backup; (ii) locale server sensibile alle inondazioni; (iii) armadi contenenti i supporti magnetici/ottici non ignifughi; (iv) errata gestione delle password; (v) mancanza di gruppi di continuità.

Tipi di Minacce Informatiche

1. **Minacce informatiche naturali**: eventi impossibili da impedire e prevenire quali calamità naturali (tempeste, inondazioni, fulmini, incendi, terremoti), atti vandalici, guerre, sommosse popolari, attacchi terroristici.
2. **Minacce informatiche umane**: attacchi informatici messi in atto da soggetti (i) che hanno interessi personali ad acquisire le informazioni di un'azienda/soggetto, o (ii) che vogliono limitare l'operatività delle organizzazioni danneggiando i normali processi aziendali (slide seguente).
   Attacco informatico: tentativo di accesso non autorizzato ad un sistema informativo.

Nel seguito ci concentreremo sulle minacce informatiche umane.

Definizioni

Processo aziendale: insieme di attività tra loro correlate (nello spazio e nel tempo), svolte secondo una determinata sequenzialità e/o simultaneità. Tale insieme di attività ha un punto di partenza ed un punto di arrivo rappresentato da un risultato misurabile (prodotto o servizio) che contribuisce al raggiungimento della missione dell'organizzazione.

Procedura aziendale: insieme delle regole che consentono di eseguire e portare a termine un processo aziendale.

Definizioni

Vulnerabilità informatica: debolezza in un sistema informativo. Le vulnerabilità informatiche possono essere sia organizzative e di processo che tecniche, spesso in combinazione tra loro (tali vulnerabilità possono essere sfruttati da attaccanti per effettuare azioni malevole).

1. **Vulnerabilità organizzative e di processo**: sono riconducibili alla mancata o non corretta definizione o implementazione di misure di sicurezza volte alla tutela della riservatezza, integrità e disponibilità delle informazioni.
2. **Vulnerabilità tecniche**: sono dovute a falle di sicurezza del software applicativo, del firmware, dell'hardware ovvero dei protocolli di comunicazione, dovuti principalmente a bug o non corrette configurazioni.

Prof. Montemurro

Definizioni e Prima Classificazione degli Attacchi

2. **Minacce informatiche umane**

   Hacker: persona che studia ed analizza il sistema informatico allo scopo "benefico" di conoscerne e sfruttarne tutte le potenzialità.

   Cracker: soggetto che penetra nei sistemi in modo non autorizzato violando i sistemi di protezione.

   Prima classificazione degli attacchi informatici

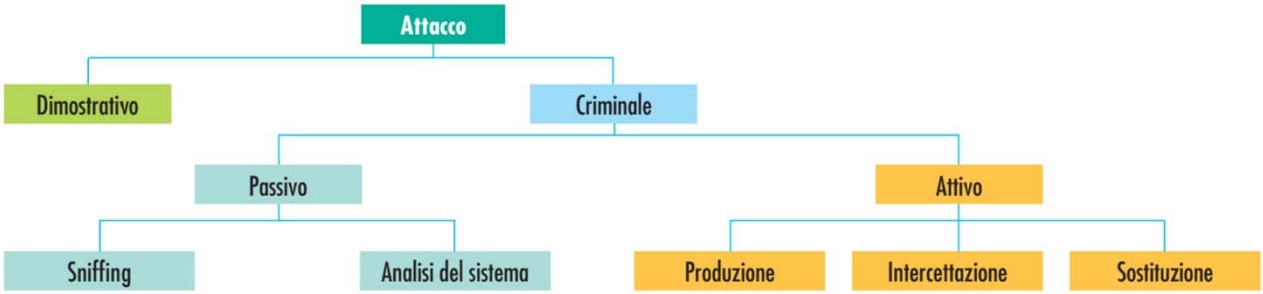
   i. **Attacchi informatici interni**: causati da personale interno (o ex interno) all'organizzazione (es. dipendenti o ex). Questi sono i più insidiosi perché i dipendenti conoscono il sistema informativo, i sistemi di sicurezza, ed hanno le autorizzazioni per accedere al fine di sottrarre direttamente informazioni, e di inserire eventualmente software malevolo in grado di provocare danni, e trasmettere le informazioni all'esterno del sistema informativo.

   ii. **Attacchi informatici esterni**: causati da soggetti esterni all'organizzazione

Prof. Montemurro

Seconda Classificazione degli Attacchi

2. Minacce informatiche umane
Seconda classificazione degli attacchi informatici



Seconda Classificazione degli Attacchi

2. Minacce informatiche umane
Seconda classificazione degli attacchi informatici

i. **Attacchi informatici dimostrativi**: non pericolosi, volti a dimostrare l'abilità del cracker
ii. **Attacchi informatici criminali**: volti a intercettare e/o modifica di dati non propri, e/o ad impedire l'utilizzo di determinati servizi agli utenti
    a. **Attacchi informatici criminali passivi**: non altera sistemi o dati, si limita a spiare i dati (es. **packet sniffing**), o ad eseguire l'analisi del sistema e l'analisi del traffico di rete senza analizzare i contenuti (difficili da rilevare: non producono effetti immediatamente visibili)
    b. **Attacchi informatici criminali attivi**: attacco a un protocollo di comunicazione sicuro in cui l'aggressore trasmette dati al richiedente, o al fornitore di servizi di credenziali (CSP), o al verificatore, o alla parte affidabile (RP).

Seconda Classificazione degli Attacchi

2. **Minacce informatiche umane**

   Principali tipi di attacchi informatici criminali attivi

   i. Intercettazione attiva
   ii. Sostituzione di un host
   iii. Produzione
   iv. Email bombing e spamming infetto
   v. Altri (phishing, ransomware ecc.)

Principali tipi di attacchi informatici criminali attivi

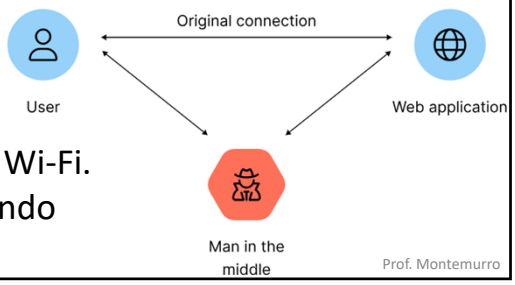
Intercettazione attiva: attacco per intercettare le password al fine di accedere al sistema con l'intento di modificare i dati.

Esempio

Man-in-the-Middle (**MitM**): sono una famiglia di attacchi tutti accomunati dal fatto che all'inizio c'è una connessione legittima tra due dispositivi, poi un terzo soggetto si mette illegittimamente nel mezzo per cui è in grado di intercettare e modificare i dati in transito.

Attacco MitM basato su falso Access Point

Tale attacco funziona quasi sempre: l'attaccante crea un falso Access Point, spesso dal nome simile ma non uguale a quello legittimo, per creare un ponte tra l'utente e il router della rete Wi-Fi. La gente si connette all'Access Point fasullo aprendo così le porte del suo dispositivo all'hacker.



Principali tipi di attacchi informatici criminali attivi

Sostituzione di un host: sostituzione di un dispositivo legittimo con uno malevolo per impersonarlo nella rete.

Esempio

Premessa: a ogni scheda di rete viene assegnato un **indirizzo IP** (o **indirizzo logico**) il quale identifica univocamente la scheda di rete.
IP spoofing: tecnica per eseguire vari tipi di attacchi tra cui anche la sostituzione di un host (anche per il MitM). Tale tecnica consiste nel falsificare l'indirizzo IP del mittente per far sembrare che il traffico provenga da un host legittimo. Fatto ciò, l'attaccante può intercettare e modificare i dati a cui ha accesso l'host del mittente (es. il DB dell'azienda).

Prof. Montemurro

Principali tipi di attacchi informatici criminali attivi

Produzione: malintenzionati producono nuovi componenti software e li inseriscono nel sistema informatico con lo scopo di causare un danno, non per prelevare le informazioni (atti di sabotaggio). L'obiettivo è ridurre l'integrità e la disponibilità dei dati.

Esempi

1. Attacchi con **malware** (**mal**icious soft**ware**)
   i. Attacchi con virus **virus**: programmi che infettano programmi esistenti (**programma ospite**); i virus provocano danni e si replicano infettando altri host durante il trasferimento del file infetto da un host ad un altro
   ii. Attacchi con **worm**: a differenza dei virus, sono programmi autonomi che non si attaccano ad altri programmi, ma si propagano mediante diffusione dentro reti di computer o tramite email; i worm, come i virus, provocano danni e si replicano infettando altri host

Prof. Montemurro

Principali tipi di attacchi informatici criminali attivi

Esempi

1. Attacchi con **malware** (**mal**icious soft**ware**)
   iii. Attacchi **Denial of Service DoS**: far eseguire all'host operazioni inutili per tenerlo occupato così da impedirgli di offrire i propri servizi
   iv. **Trojan horse** (slide successiva)
   v. **Ransomware** (**ransom** soft**ware**): malware che blocca in modo permanente l'accesso ai dati o ai dispositivi finché il proprietario dei dati non paga un riscatto. La maggior parte delle volte i ransomware sono trojan horse.

Principali tipi di attacchi informatici criminali attivi

Email bombing: invio di enormi quantità di messaggi email per mandare in crash il server di posta (è un esempio di DoS).

Spamming infetto: invio di messaggi email contenenti link dannosi per infettare il dispositivo della vittima o rubare dati sensibili.

Esempio

Trojan horse (o **cavallo di troia**): è un malware nascosto all'interno di un altro software apparentemente utile (es. videogiochi). L'obiettivo è assumere il controllo del computer; non si installa automaticamente come i virus. I trojan possono installare backdoor, o keylogger, oppure inviare messaggi di spam.
Keylogger: hardware o software che intercetta tutto quello che viene digitato sulla tastiera del computer.

Principali tipi di attacchi informatici criminali attivi

Phishing: attività illegale che ha come scopo il furto di identità e di dati sensibili tramite le comunicazioni elettroniche (es. email; SMS ecc.), sfruttando tecniche di **ingegneria sociale** per ingannare le vittime.

Schema standard di attacco

1. L'attaccante invia alla vittima un messaggio e-mail che simula quello di un'istituzione nota al destinatario (in genere ci sono errori ortografici).
2. Il messaggio ha toni allarmistici e richiede un intervento urgente.
3. La vittima è invitata a seguire un link presente nella mail.
4. Tale link non punta al vero sito ma ad una copia fittizia identica, in cui viene chiesto di compilare un form con dati riservati.

Principali tipi di attacchi informatici criminali attivi

Ingegneria sociale: nell'ambito della sicurezza informatica, complesso di strategie e metodi di manipolazione psicologica e di persuasione volti a indurre un utente a rivelare informazioni riservate (dati personali, credenziali di accesso, numeri di carte di credito, di conti bancari, di previdenza sociale, ecc.).

Sicurezza nei Sistemi Informativi

Problema: la rete aziendale, essendo connessa ad internet, è soggetta ad attacchi informatici.

Obiettivo: proteggere le informazioni importanti e riservate in quanto esse rappresentano la risorsa più importante di ogni organizzazione. Per farlo si applica il **principio minimo di sicurezza** in base al quale bisogna:

1. proteggersi dagli attacchi informatici passivi;
2. riconoscere gli attacchi informatici attivi.

In pratica, bisogna analizzare tutte le componenti del sistema, e individuare per ciascuna di esse tutte le tecniche di attacco passive e attive.

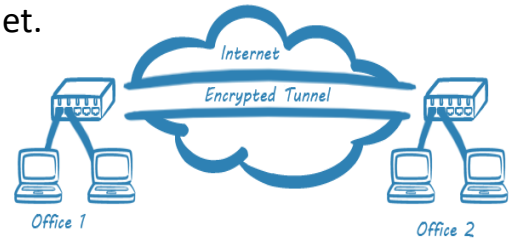
Sicurezza nei Sistemi Informativi

Pilastri della sicurezza

1. **Prevenzione**: mediante protezione dei sistemi e delle comunicazioni con crittografia, firewall, VPN ecc.
2. **Rilevazione**: mediante il monitoraggio ed il controllo degli accessi tramite autenticazione con password, e certificati
3. **Investigazione**: mediante l'analisi dei dati, il controllo interno grazie al confronto ed alla collaborazione degli utenti ecc. (es. si pongono domande agli utenti per portare avanti un'indagine)

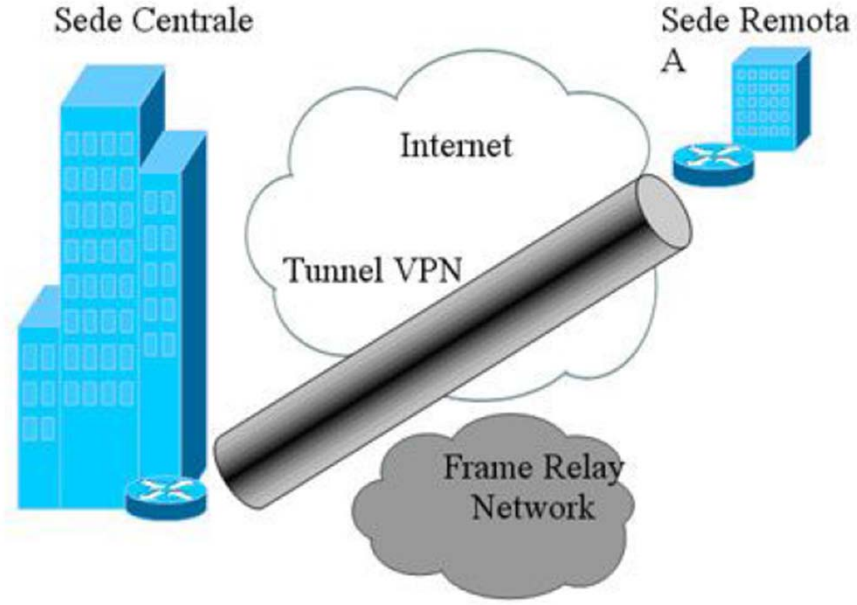
Sicurezza nei Sistemi Informativi: Misure di Prevenzione

1. **Crittografia**: garantisce riservatezza e integrità dei dati, previene attacchi informatici passivi di tipo packet sniffing
2. **Autenticazione degli utenti**: processo di riconoscimento delle credenziali dell'utente per assicurarsi dell'identità di chi invia e/o esegue operazioni
3. **Firewall**: vedi slide su fondamenti di networking
4. **Linee dedicate** (o **reti private**): vedi slide su fondamenti di networking
5. **Reti private virtuali** (o **Virtual Private Network**) **VPN**: è una rete informatica cifrata, privata che si appoggia su una rete di telecomunicazioni **pubblica** (ecco perché virtuale) come internet.
   E' come se all'interno della rete **pubblica** ci fosse un **tunnel** sicuro tra le due reti informatiche che vogliamo collegare.



Prof. Montemurro

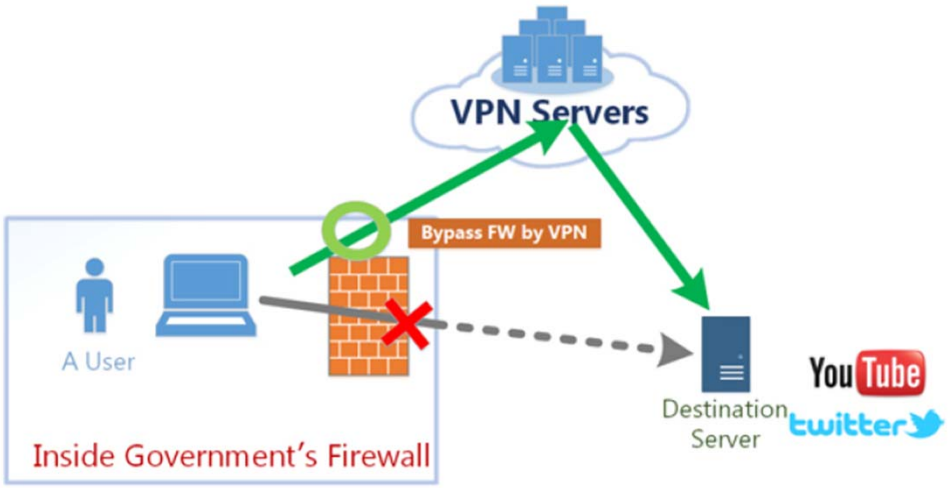
Sicurezza nei Sistemi Informativi: Misure di Prevenzione



Prof. Montemurro

Sicurezza nei Sistemi Informativi: Misure di Prevenzione

Curiosità: VPN per bypassare le georestrizioni.



Prof. Montemurro

Sicurezza nei Sistemi Informativi: Misure di Prevenzione

6. **Posizionamento dei server in locali protetti** (armadi, locali accessibili solo dai tecnici autorizzati, luoghi lontani dalla sede aziendale come i data center il cui accesso è spesso protetto sia in modo fisico che virtuale).
   Data center: insieme di server posti in un unico luogo al fine di favorire una centralizzazione (i) della gestione, (ii) della sicurezza, (iii) della manutenzione dei server stessi.
7. **Sistemi di alimentazione autonoma tramite gruppi di continuità**
8. **Backup periodico**, ossia salvataggio periodico dei dati

Prof. Montemurro


thank you
danke
謝謝
ngiyabonga
teşekkür ederim
gracias
спасибо
dank je
tapadh leat
bedankt
dziękuję
obrigado
sukriya
kop khun krap
go raibh maith agat
arigatô
takk
dakujem
grazie
terima kasih
merci
감사합니다
ευχαριστώ
мерси
mochchakkeram
hvala
mauruuru
sagolun
tack
merci