introduzione alla cybersecurity e terminologia

cybersecurity

- la cybersecurity è la pratica di **proteggere risorse informatiche** da **eventi avversi**
- esempi
  - dati
    - modifiche o accessi malevoli, perdita dei dati
  - sistemi hardware/software, anche personali
    - infezioni da malware
  - reti
    - intrusioni, uso delle reti per scopi malevoli

principio fondamentale

la sicurezza di un sistema informatico dipende

- **molto** dal processo con cui un sistema viene gestito
  - pianificazione, analisi dei rischi, gestione dei sistemi, formazione del personale, ecc.
- **meno** dagli specifici prodotti adottati
  - specifici firewall, antivirus, ecc.

l'importanza degli aspetti metodologici

- la tecnologia evolve ma certi punti fermi *metodologici* rimangono
- ci aiutano a…
  - … comprendere vulnerabilità e rischi
  - …adottare contromisure che siano efficaci, economiche, scalabili, gestibili, usabili, ecc.
  - …pianificare azioni organiche
  - …studiare nuove problematiche

perché occuparsi di cybersecurity?

- evitare di incorrere in **danni economici**
- **conformità** alle leggi (*compliance*)
  - es. normativa sulla privacy

    GDPR in vigore dal 25 maggio 2018

- il motore principale che muove il mercato della sicurezza è la «**paura**»

chi dovrebbe badare alla cybersecurity?

- imprese
- pubblica amministrazione ed enti pubblici
- chiunque utilizzi sistemi informatici per scopi economicamente o socialmente rilevanti (anche se non a scopo di lucro)
  - l'università (quanto vale il sistema di paghe e stipendi dell'ateneo?)
  - lo studente che scrive la tesi (quanto vale il documento "tesi.doc" il giorno prima della consegna?)

importanti concetti di base e terminologia

obiettivi della sicurezza

- **confidenzialità** o riservatezza o segretezza
  - dati letti solo da chi è “autorizzato”
- **integrità**
  - dei dati (integrità in senso stretto)
    - i dati non sono stati modificati in maniera incontrollata
  - dell’origine (autenticazione)
    - l’origine dei dati è certa
  - dei sistemi (non compromissione)
- **disponibilità**
  - dati o servizi sono disponibili per accesso/uso

obiettivi della sicurezza

- non ripudio
  - della ricezione
  - della trasmissione
  - alcuni la considerano una forma di integrità

- privacy
  - riguarda la cybersecurity del trattamento dei **dati personali**, comprende **confidenzialità, integrità, disponibilità**
  - imposta per legge
    Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR)

hacker

- hacker
  - esperto di vulnerabilità e attacchi
  - non necessariamente malevolo
  - in italiano l'accezione è spesso negativa
  - termini correlati: cracker, hacktivist, white hat, black hat, gray hat, blue hat, script kiddies, lamer, ecc.
    - vedi wikipedia "Hacker (computer security)"

minacce e affini

- vulnerabilità o vulnerabity exposure
  - un problema hw, sw, di configurazione o di procedura che rende possibile un uso improprio di dati o risorse hw e sw
- minaccia (threat)
  - un insieme di circostanze potenzialmente pericolose
    es. un bug del browser assieme alla possibilità di navigare liberamente su Internet costituiscono una minaccia per i dati degli utenti

minacce e affini

- exploit, exploitation
  - la procedura per sfruttare una vulnerabilità
- attacco
  - tentativo di violazione di riservatezza, integrità o disponibilità tramite lo sfruttamento (exploitation) di una vulnerabilità
- intrusione, incidente
  - un attacco riuscito

minacce e affini

- privilege excalation
  - l’azione di un attaccante di guadagnare accesso a risorse che normalmente gli sono precluse
  - è un attacco andato a buon fine
- root compromise
  - situazione in cui l’hacker ha ottenuto il pieno controllo di una macchina

threat model

- un *threat model* specifica “formalmente”
  - che significa “**attacco** eseguito con successo”
  - cosa può fare l’**attaccante**

- usi
  - analisi del rischio
  - prove “formali” di sicurezza
    - negli ambiti di ricerca e certificazione

contromisure o misure preventive

- contromisura
  - procedura, installazione hw o sw, configurazione o altro atto a diminuire la probabilità che una minaccia possa dar luogo ad un attacco o a limitarne le conseguenze

esempi

- installare un firewall è una contromisura che protegge una intranet da semplici tipi di attacchi
- scollegare la intranet da Internet è una contromisura più efficace ma potrebbe essere non “gradita” dall’utenza

soggetti e oggetti

- *soggetto*
  - chi (o cosa) accede ad una risorsa… in modo lecito o illecito, anche inconsapevolmente
- *oggetto*
  - una risorsa da “proteggere”
- *diritti* (di un soggetto su un oggetto)
  - operazioni che il soggetto può compiere sull’oggetto in maniera lecita
  - detti anche *privilegi*
  - dal punto di vista dell’oggetto sono detti *permessi*

soggetti, oggetti, diritti, e programmazione object-oriented

- questa terminologia ricorda quella della OOP
  - dove i soggetti sono comunque degli oggetti
- nella chiamata a metodo…
  - il chiamante è il soggetto
  - il chiamato è l'oggetto
  - il metodo è l'operazione

- nella OOP standard non ci sono diritti
- varianti di chiamate con diritti: web services, remote procedure calls, smart contracts, system calls

soggetti e oggetti

- esempio
  in unix è vero che i processi di root possono cancellare qualsiasi file
  - soggetto: un qualsiasi processo dell'utente root
  - oggetto: un qualsiasi file
  - diritto: cancellazione

policy

- policy
  - un insieme di regole che stabiliscono quali soggetti hanno quali diritti su quali oggetti
  - in certi contesti (es. nella pianificazione) si dà a questa parola un significato più ampio
  - definisce il concetto di sicurezza in un certo contesto (un sistema, una organizzazione, ecc.)
  - una policy può essere espressa…
    - in linguaggio naturale
    - tramite modello matematico
    - tramite linguaggio ad hoc, ecc

meccanismi

- meccanismo
  - ciò che per progetto ha lo scopo di far rispettare la policy

esempio

- autenticazione + controllo di accesso sui file permettono di realizzare politiche di “protezione” dei file tra i vari utenti in windows o unix

azioni di sicurezza

- prevenzione (prevention)
  - ciò che si fa prima che un certo evento avverso (es. attacco) si manifesti in modo da ridurne impatto o probabilità
  - es. installazione di un antivirus
- rilevazione (detection)
  - l'azione di accertare se un evento avverso (es. violazione della policy) è in atto in un certo momento

azioni di sicurezza

- contrasto (contrast)
  - l'azione di fronteggiare un evento avverso (es. attacco) mentre avviene

  es. cambio la configurazione del firewall per bloccare un certo traffico malevolo
- recupero (recovery)
  - il ripristino della normale operatività del sistema dopo un evento avverso
  - aspetti importanti: **tempo, costo**
  - certe azioni preventive riducono (o annullano) il tempo e il costo di recovery

caratteristiche di sistemi

- resilienza
  - la capacità di un sistema di continuare a funzionare in presenza di problemi
  - è un modo per assicurare disponibilità dei servizi
- fail-over
  - un azione automatica per recuperare ad un problema (es. un guasto)
  - per estensione anche i meccanismi che permettono il fail-over

azioni di sicurezza

- spesso la **prevenzione** è meglio degli altri approcci ma…
  - …può non essere percorribile
  - …può essere troppo costosa
  - …può essere non sostenibile dal punto di vista della utilizzabilità del sistema

pianificazione

- insieme di procedure che prevedono
  - una valutazione dei rischi e dei costi
  - la scelta di eventuali contromisure
  - un piano di attuazione delle contromisure scelte
  - ecc.

fiducia (trust)

- qualsiasi azione di sicurezza è basata sulla **fiducia**
- esempi
  - fiducia che certi sistemi si comportino correttamente
  - fiducia che certe pratiche siano adeguate o eseguite correttamente
  - fiducia che certe persone si comportino come previsto
  - fiducia che non vada via la corrente
  - ecc.

fiducia (trust)

- es. nell'applicare una policy assumiamo che essa…
  - dica chiaramente quando il sistema è in uno "stato sicuro" o meno
  - modelli correttamente i requisiti di sicurezza
- es. nell'adottare un meccanismo assumiamo che esso
  - applichi correttamente la policy
  - che funzioni correttamente

fiducia (trust)

- es. se l'amministratore di sistema applica una patch di sicurezza, come contromisura per una certa vulnerabilità, sta assumendo che…
  - la patch risolva la vulnerabilità
  - nessuno abbia modificato la patch nella comunicazione tra produttore e amministratore
  - la patch sia stata testata approfonditamente dal produttore
  - l'ambiente di test del produttore corrisponda a quello di utilizzo
  - l'installazione vada a buon fine
  - il compilatore usato dal produttore per produrre la patch non abbia bugs
  - ecc. ecc. ecc. ecc……

(un)trusted zone

- *zone*: a perimeter that identifies a set of subjects
  - usually, the identification is informal and somewhat implicit
  - e.g., “the intranet of a company” may mean computers and people working in that intranet
- *trusted zone*: a zone where we assume there is no attacker

fiducia e threat model

- nelle zone fidate non è presente un attaccante
- altrove si

quanto fidarsi? l'*assurance*

- quantificare la fiducia che possiamo riporre in un sistema è difficile
- un sistema/processo può essere creato/gestito secondo modalità che facilitano la valutazione di quanto ci si possa fidare di esso
- tali pratiche vanno sotto il nome di **assurance** e prevedono adeguate procedure di…
  - specifica dei requisiti
  - progetto
  - implementazione
  - **valutazione (certificazione)**
- un sistema che adotta criteri di assurance tipicamente deve passare una fase di **certificazione** che colleziona evidenze del fatto che ci si possa fidare di esso

Common Criteria (CC)

- Common Criteria for Information Technology Security Evaluation
- the most known standard for computer security certification
- very general
- typical documentation:
  - *Target of Evaluation (ToE)*
    - it describes what is evaluated
  - *Security Target (ST)*
    - it describes the security features to be evaluated, ToE-dependent
  - *Protection Profile (PP)*
    - it describes security features specified generically for a class of ToE (e.g. firewalls)
    - referred and integrated by document describing a security target
- *Evaluation Assurance Level (EAL)*
  - how confident we can be that a ToE fulfill a ST
  - It is a “number” (e.g., EAL4+)

security in organizations

- SOC: Security Operation Center

  It includes people processes and tools to monitor and improve the information security of an organization and to comply with regulation.

- CSIRT: Computer Security Incident Response Team
  CERT: Computer Emergency Response Team

  It is a team of experts that handles incidents.

  Traditionally, it also collects information about vulnerabilities.

  It may be part of a SOC.

safety vs. security
(secondo il significato in inglese)

- **security**: relativa a incidenti causati volontariamente
  - es. misure antiterrorismo per una centrale nucleare
- **safety**: relativa a incidenti causati da eventi accidentali – tipicamente usata per infrastrutture, veicoli e attrezzature “materiali”
  - es. misure antisismiche per una centrale nucleare
- in italiano purtroppo entrambi i termini si traducono con sicurezza
- questa terminologia è usata anche per la sicurezza di persone/luoghi
  - security (sorveglianza)
  - safety (Legge 626/94 sicurezza sul lavoro)

safety e security: aspetti comuni

- incidenti
- rischi, analisi dei rischi
- contromisure
- policy
- pianificazione
- prevenzione
- resilienza
- normative
- standard
- certifcazioni

e quindi propri anche della cybersecurity

cyberphysical system

- sono sistemi che integrano caratteristiche informatiche e fisiche
- esempi
  - termostati
  - semafori
  - sistemi di controllo industriali
- argomenti correlati:
  IoT, Industry 4.0, critical infrastructure protection

cyberphysical security

- cybersecurity: sicurezza in ambito prettamente informatico
- cyberphysical security: sercurity e safety fisica per mezzo della cybersecurity
  - es. un malware nel sistema di controllo di un semaforo può mettere in pericolo vite umane

- 2010: stuxnet, inizio dell'uso di malware come armi per attaccare infrastrutture, sistemi industriali o militari FISICI
  - minacce e contromisure cyberfisiche (es., pen drive, airgap)
  - Advanced Persistent Threats