Operazione Rif. PA 2022-17295/RER approvata con DGR 1379/2022 del 01/08/2022 finanziata con risorse del Programma Fondo sociale europeo Plus 2021-2027 della Regione Emilia –Romagna.

Progetto n. **1** - Edizione n. **1**

MODULO: N. 6

Titolo: SICUREZZA DEI SISTEMI INFORMATICI

DOCENTE: MARCO PRANDINI

Parte 1 – Introduzione ai temi di cybersecurity

Introduzione

- Inquadramento della materia
  - Perché interessarsi alla sicurezza informatica?
  - Elementi di base: minacce, vulnerabilità, exploit e rischio
  - Tipologie di attacco e loro conseguenze
  - Panoramica delle metodologie di difesa
- Organizzazione del corso
  - Attività
  - Esami
  - Strumenti

La sicurezza informatica ci riguarda?

- Sì, ben prima che come professionisti. Nelle nostre vite
  - Infrastrutture critiche per la "civiltà"
  - Sistemi di comunicazione ed elaborazione delle informazioni
  - Archivi di informazioni personali

  sono tutti elementi *informatizzati* ormai irrinunciabili e in molti casi, se danneggiati, insostituibili (in assoluto o in tempo utile per evitare conseguenze gravi)
- *Sicurezza informatica* è tutto ciò che ha a che fare col contrasto di azioni deliberate che provochino danni
  - Termini diversi hanno sfumature specifiche, ma spesso sono usati "popolarmente" in modo intercambiabile: sicurezza dell'informazione, IT security, cybersecurity, ...
  - Useremo sicurezza nel senso del termine inglese *security* ricordando che in italiano significa anche contrasto di eventi accidentali che provochino danni (in inglese tradotto *safety*)

Impatto sociale della cyber(in)security

Woman dies during a ransomware attack on a German hospital

The Verge, Sep 17, 2020

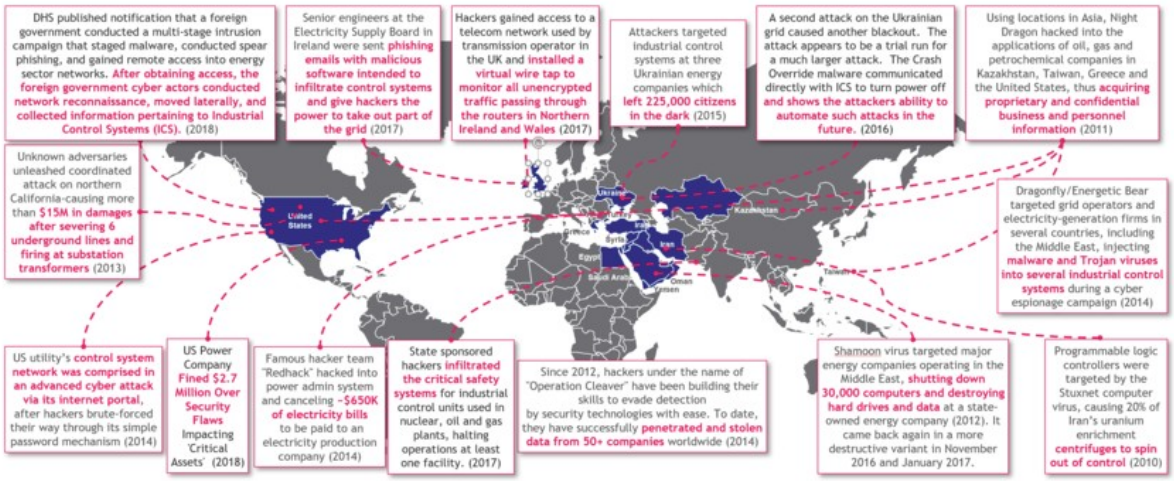
2000: Maroochy waste management

2008: Refahiye pipeline

2018: Saudi Chemical Company

2020: Natanz "stuxnet 2"

Hackers are causing blackouts. It's time to boost our cyber resilience. World Economic Forum, Mar 27, 2019



Impatto economico della cyber(in)security

- Se il cybercrime fosse una nazione, farebbe parte del G3, con un GDP>10T$ previsto per il 2025

- Un business criminale in crescita
  - Più lucrativo del mercato mondiale della droga
  - Più dannoso di tutti i disastri naturali cumulati
- Un modello criminale attrattivo
  - Utilizzabile in innumerevoli settori
  - A basso rischio (0,05%) di individuazione e prosecuzione legale
- Sono richiesti investimenti ingenti per la difesa
  - Dal 2004 al 2017 il mercato è cresciuto di 35 volte
  - Spesa stimata nel quadriennio 2018-2021: 1T$

Il rischio cyber

- Affrontare i problemi di sicurezza informatica è sostanzialmente un esercizio di *gestione del rischio*
  - ”il potenziale danno immateriale, perdita economica, o distruzione di risorse che risulterebbe da un evento (malevolo)”
- Semplificando in modo estremo:

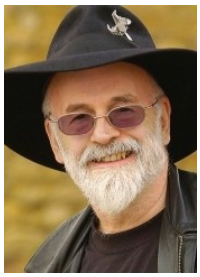
  RISCHIO = PROBABILITÀ x IMPATTO

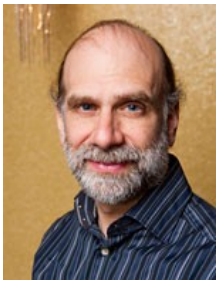
  es. se nell’arco di un anno c’è una probabilità del 4% di subire un danno di 15.000€ dovuto a un’azione malevola, il rischio è pari a 600€/anno
- Per gestire il rischio dobbiamo conoscerlo
  - valutare le probabilità di ogni evento potenzialmente dannoso
  - quantificare l’impatto di ogni possibile azione malevola
- Per mitigare il rischio si progettano e implementano contromisure (che devono essere convenienti!)
  - bisogna saperne valutare l’efficacia, in termini di riduzione della probabilità degli eventi dannosi e/o del loro impatto

Detto così sembra facile...

“Progress just means bad things happen faster.”

– Terry Pratchett (from *Witches Abroad*)



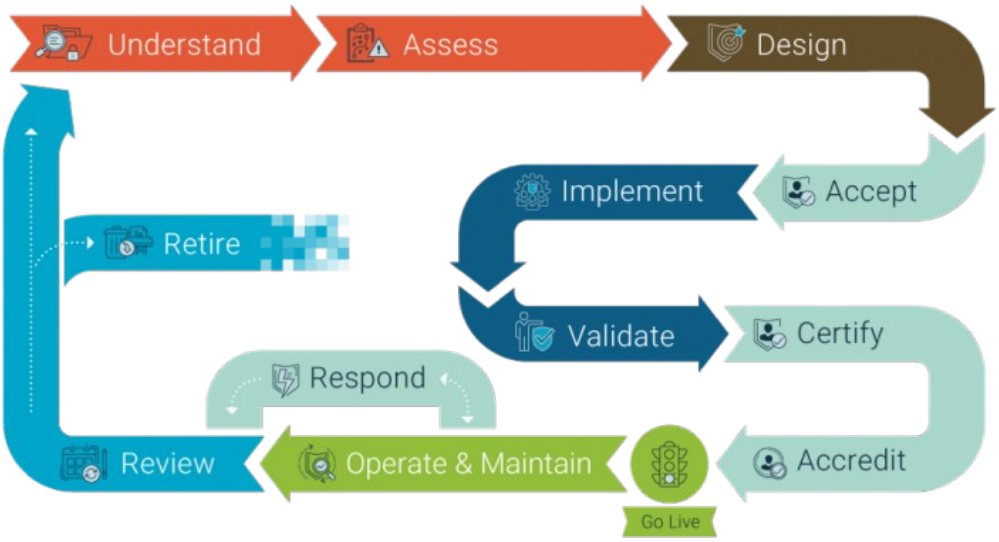


“If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."

– Bruce Schneier

Un processo continuo

Sicurezza non è valutare la situazione presente e comprare un **prodotto**, bensì definire un **processo** per tenere traccia delle continue evoluzioni dei rischi e dell'efficacia delle contromisure



Proprietà di sicurezza

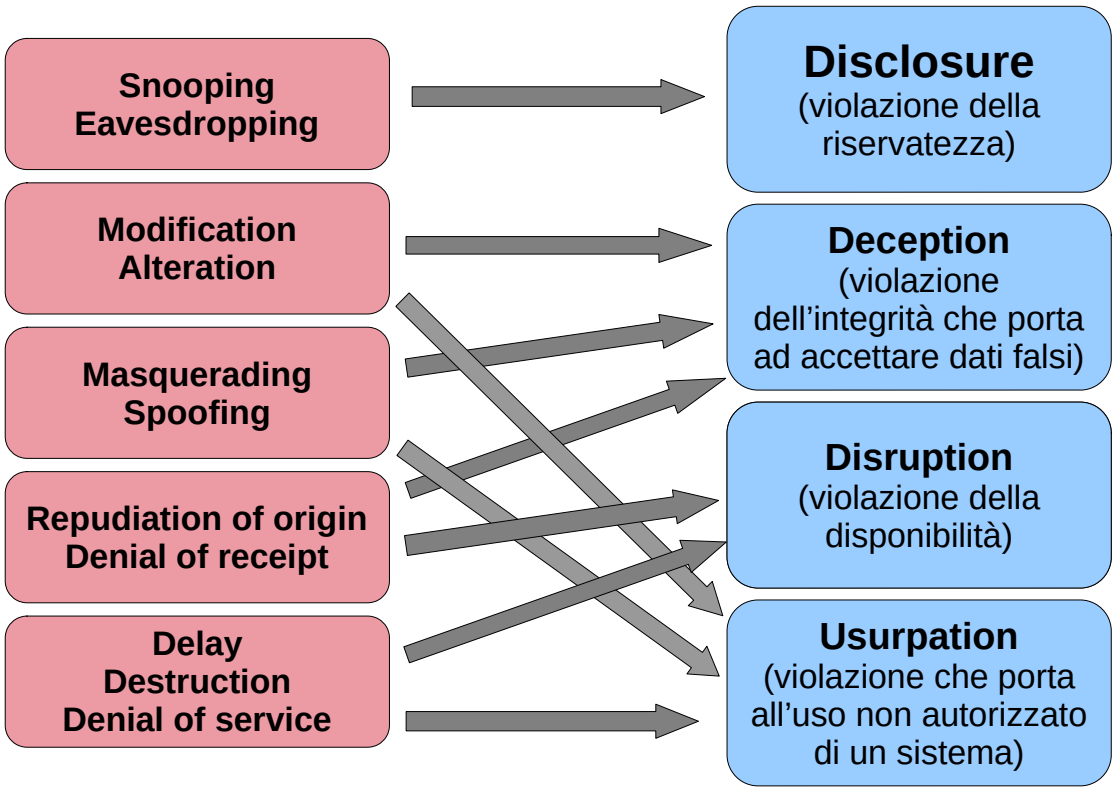
- La sicurezza di un sistema può essere scomposta in tre proprietà chiave, riassunte dalla sigla **CIA**

- Confidentiality (riservatezza)
  - Mantenere inaccessibili dati, o proprietà di un sistema, a chi non sia autorizzato a conoscerli
- Integrity (integrità)
  - Poter garantire che il contenuto e/o l'origine di un dato corrispondano a quanto si ritiene corretto
- Availability (disponibilità)
  - Poter garantire la possibilità effettiva di accedere a dati e servizi quando necessario

Le minacce e gli attacchi

- Minaccia (threat): una condizione che potenzialmente può compromettere una o più delle proprietà di sicurezza
  - Esiste indipendentemente dal fatto che venga concretizzata
  - Attacco (attack): l'azione che porta al concretizzarsi di una minaccia
  - Attaccante (attacker): l'entità che sferra l'attacco
- Le minacce sono indissolubilmente legate alle intenzioni dei potenziali attaccanti
  - Script kiddies
  - Criminali comuni
  - Insider disonesti e impiegati vendicativi
  - Reporter
  - Ricercatori
  - Attivisti
  - Criminali organizzati
  - Spie industriali
  - Governi ed eserciti

Tipologie di attacchi e minacce



Politiche e meccanismi

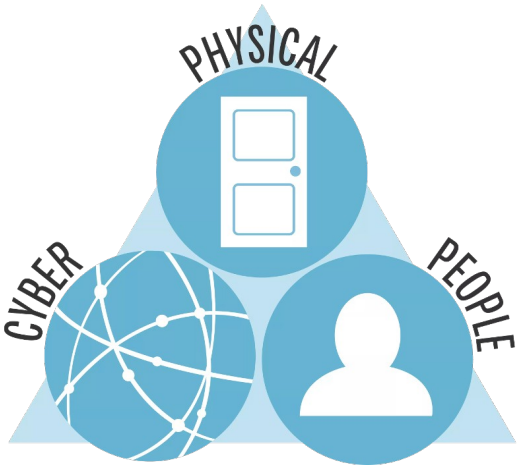
- Una politica di sicurezza (*security policy*) è la dichiarazione di ciò che è consentito o proibito fare
- Un meccanismo di sicurezza (*security mechanism*) è un metodo, uno strumento o una procedura per far rispettare una politica di sicurezza
- Non sono necessariamente tecnici, anzi molto spesso, tra i più importanti, ci sono comportamenti e regole di interazione tra persone

Obiettivi delle politiche e dei meccanismi

- Le politiche dichiarano qual è il fine della sicurezza
- I meccanismi specificano il mezzo per contrastare gli attacchi, e possono combinare diverse strategie:
  - Prevenzione (*prevention*): l'attacco deve fallire
    - Meccanismi invasivi
    - Implementazione inalterabile e non aggirabile
  - Rilevazione (*detection*): l'attacco potrebbe avere successo ma deve essere notato e riportato
    - Inefficace rispetto ad alcune minacce, es. disclosure
  - Reazione (*response*): l'attacco rilevato viene mitigato per ridurre la gravità o l'estensione del danno
  - Ripristino (*recovery*): le conseguenze dell'attacco vengono ridotte o azzerate, ripristinando le proprietà di sicurezza violate

Superficie di attacco

- Politiche e meccanismi si applicano a ogni interazione del sistema col mondo esterno (o tra sottosistemi)
- Ogni modo reso accessibile a un attaccante per stimolare un'interazione è un *vettore di attacco*
- Ogni vettore può essere realizzato combinando uno o più canali di accesso
  - Fisico
  - "Cyber" (accesso remoto via cavo o wireless)
  - Umano
- L'insieme dei vettori costituisce la superficie di attacco



Vulnerabilità ed exploit

- Se le politiche e i meccanismi di protezione di un sistema fossero perfetti, le minacce non potrebbero concretizzarsi
  - Neutralizzano i vettori di attacco
- Gli attacchi hanno successo se esistono errori
  - Nell'individuazione della superficie di attacco (porosità – un vettore esiste là dove non dovrebbe)
  - Nella definizione di una politica o nell'implementazione di un meccanismo (vulnerabilità / vulnerability)
    - Può essere strutturale nell'hardware o software
    - Puo dipendere dalla configurazione
    - Può dipendere da un uso scorretto
- Exploit
  - Uno strumento per trarre vantaggio da una vulnerabilità concretizzando una minaccia
    - Tecnico (cracking)
    - Umano (social engineering)

Qualche esempio di vulnerabilità

- Uno switch propaga pacchetti a destinatari non designati se la tabella di switching è satura (vincolo hardware)
- Un router accetta qualsiasi annuncio gli pervenga riguardante la topologia della rete (caratteristica intrinseca del protocollo)
- Un utente clicca un link di un messaggio non verificando la fonte (errore umano di applicazione di una procedura)
- Un processo non controlla prima di sovrascrivere un'area di memoria che non gli appartiene (errore di implementazione del software)
- Un processo interpreta sequenze di byte come comandi anche se dovrebbero essere considerate puri dati (errore di progetto del software)
- Un computer che gestisce dati riservati può avere le porte USB abilitate (errore di definizione della politica di sicurezza)

I vettori umani, fisici e software che permettono di accedere a un computer sono normalmente usati per installare *malware*

- Worm
- Spyware
- Ransomware
- Trojan horse

Cybersecurity Kill Chain

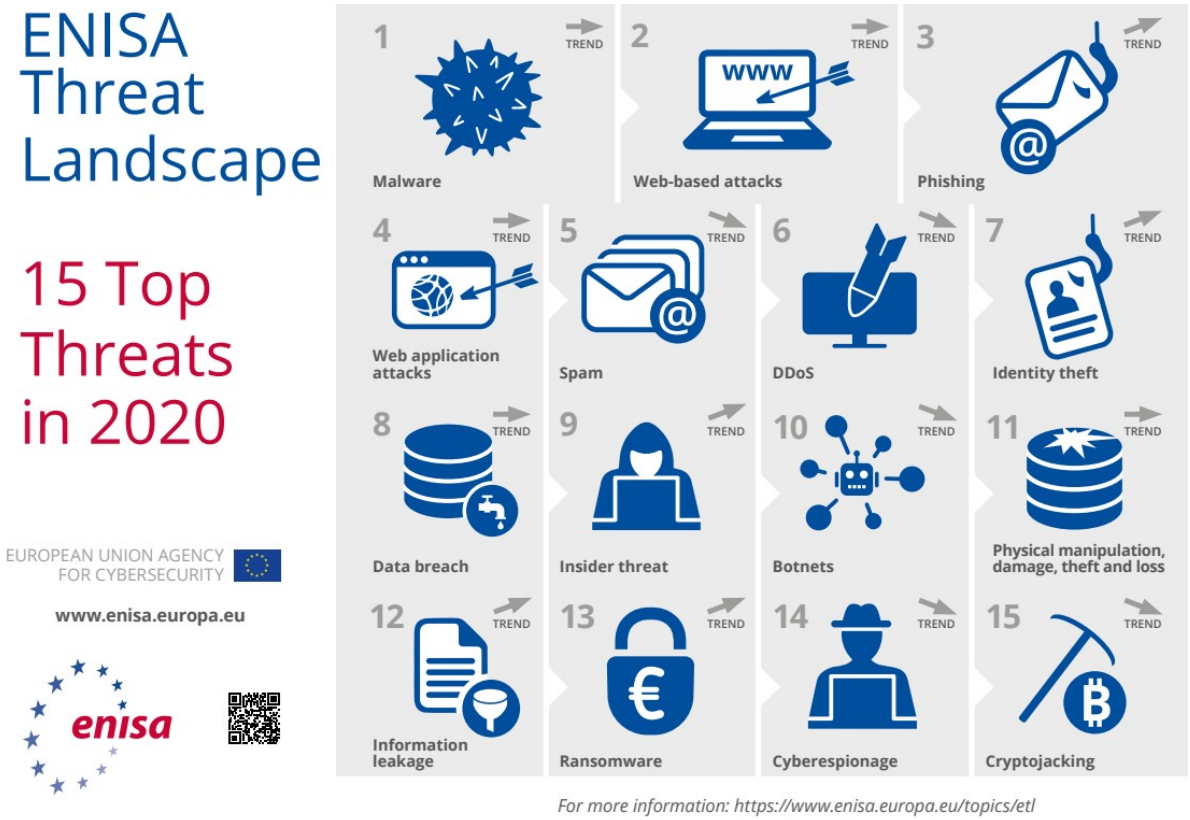
Lockheed-Martin, 2011

Un modello per descrivere le fasi di un attacco

MITRE ATT&CK

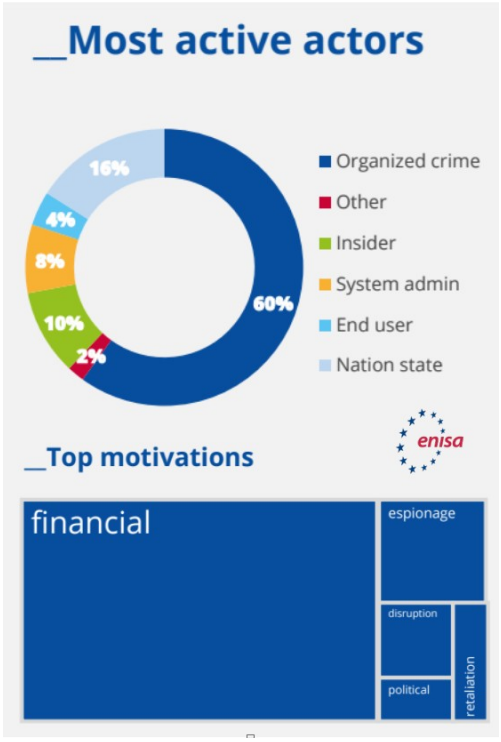
Una base di conoscenza di come queste fasi vengono realmente eseguite https://attack.mitre.org/

Il panorama delle minacce



For more information: https://www.enisa.europa.eu/topics/etl

Chi, perché e come



- **I punti di ingresso sono ancora principalmente legati all'elemento umano**
  - Furto di credenziali
  - Social engineering
  - Errori di configurazione
  - Abuso di privilegi
- **L'azione conseguente più comune è l'installazione di malware**
  - Con 230.000 varianti nuove ogni giorno, la rilevazione è ancora un punto dolente
  - Dopo l'ingresso, il movimento all'interno dell'organizzazione è rapido ed efficace

I bersagli

_Five most desired assets by cybercriminals

01_Industrial property and trade secrets

Industrial property and trade secrets are the most desirable assets because of their high value to their owners, the market and some cases the criminal world.

02_State/military classified information

This asset includes any information that a state deems sensitive. In 2019, the trade and diplomatic tensions between countries made this type of information even more attractive.

03_Server infrastructure

Server infrastructure is the first sensitive asset that is not data. In many attacks, taking over the victim's server infrastructure, is the primary objective.

04_Authentication data

Authentication data is valuable assets for generating profits but also as an objective to support an attack.

05_Financial data

Financial data such as credit card, banking and payment information is always value to cybercriminals.

enisa

__Most targeted sectors

Digital Services_ Services such as e-mail, social and collaborative platforms and cloud providers were under attack during 2019. These were also used as proxies for further attacks.

Government Administration_ The financial returns from ransoms paid makes the public sector one of the most attractive targets for ransomware attacks.

Technology Industry_ The technology industry was under attack in 2019 mainly through supply chain attacks trying to compromise the development of software through zero-day exploits and backdoors attacks.

Financial_ The number of incidents with financial organisations and not necessarily banks, increased substantially during the reporting period.

Healthcare_ The number of attacks against the healthcare sector continues to grow.

L'effetto COVID

- Lockdown =
  - Telelavoro → maggiore utilizzo di dispositivi e reti non gestiti
  - Incremento dell'uso dei servizi online personali → e-commerce, e-banking, social network, più usati da utenti esperti e più nuovi utenti non consapevoli dei rischi
- *Coronavirus is alone blamed for a 238% rise in cyber attacks on banks.*
- *Phishing attacks have seen a dramatic increase of 600% since the end of February.*
- *Ransomware attacks rose 148% in March and the average ransomware payment rose by 33% to $111,605 as compared to Q4 2019.*

(Source: Fintech News)

I maggiori incidenti del 2020

	Data breaches	Ransomware	Sabot/Espion	Cyberwar
J	Mitsubishi (employees, projects) CheckPeople (56M US citizens) Wawa (30M credit cards)	Travelex (6M$) US def. contr. CPI (500k$ - 2 months to recover)		7 events (IR,TK,RU,IL)
F	Clearview AI 3bn photos+customer list (law enforcement) Tetrad (747GB data on households)	UK Redcar Council (10M£)	IR DDoS of interet infrastr.	4 events (RU,CN)
M	Virgin Media (900k users) US Census (200M citizens)	UK Durham fire/police/govt.svcs	SA exploit global telco bug to track citizens CN espionage on 75 org. ww.	3 mass surveillance (KP,KR,UZ) 2 wide industry attaks (CN,US)
A	Nintendo (160k accounts) Zoom (500k accounts)	Energias de Portugal (9.9M€)	AZ SCADA wind turbines	9 events (VN,RU,CN,IR)
M	EasyJet (9M records) CAM4 adult live (10M+ users)	21 incidents reported, including Fresenius hospital operator & NYC law firm representing celebs	JP/IT/DE/UK industrial suppliers RU→DE spl.ch.→energy/water NO state fund empl. tricked 10M$	11 events (RU,CN,IR,IL)
J		UC Covid-19 research data (1.14M$) Most Honda offices shut down (Enel blocked a similar attack)	Backdoor found in mandatory tax-filing software for foreign companies operating in China	8 events (KP,CN,IN)
J		Telecom Argentina (7.5M$) Garmin (3 days down)	IL water infrastructure NZ Stock Exchange DdoS KP worldwide ATM robbery IR→US mf backdoor injection CN→TW code&design theft	5 events (RU,CN,US)
A	235M Instagram, TikTok and YouTube user profiles Carnival customers & employees	NL CWT travel (4.5M$) Konica Minolta (1 week down)		9 events (KP,IR,RU,CN,IN)
S	SK Covid tracing (390k patients)	31 incidents, including (DE) Duesseldorf University H. (AG) Dir. Nac. Migraciones (4M$) (PK) electric company (4M$)	Georgia COVID research espion.	9 events (IR,CN,RU)
O	Marriott fined 18M£ for 2014-2018 leak of 339M customer data	40 incidents, including ERT (disrupted vaccine tests) DE Software AG (20M$)		24 events (IR,CN,RU,GR,KP)

Lo scenario degli attacchi in sintesi

01_ Attack surface in cybersecurity continues to expand as we are entering a new phase of the digital transformation.

02_ There will be a new social and economic norm after the COVID-19 pandemic even more dependent on a secure and reliable cyberspace.

03_ The use of social media platforms in targeted attacks is a serious trend and reaches different domains and types of threats.

04_ Finely targeted and persistent attacks on high-value data (e.g. intellectual property and state secrets) are being meticulously planned and executed by state-sponsored actors.

05_ Massively distributed attacks with a short duration and wide impact are used with multiple objectives such as credential theft.

enisa

06_ The motivation behind the majority of cyberattacks is still financial.

07_ Ransomware remains widespread with costly consequences to many organisations.

08_ Still many cybersecurity incidents go unnoticed or take a long time to be detected.

09_ With more security automation, organisations will be invest more in preparedness using Cyber Threat Intelligence as its main capability.

10_ The number of phishing victims continues to grow since it exploits the human dimension being the weakest link.

With all the changes observed in the cyber threat landscape and the challenges created by the COVID-19 pandemic, there is still a long way before cyberspace becomes a trustworthy and safe environment for everyone.

Difesa

- La messa in sicurezza deve essere un processo metodico
- I *framework* e le *metodologie* possono aiutare nella sistematizzazione
- Le *certificazioni* possono dare evidenza, fornita da una terza parte disinteressata, che misure efficaci siano state adottate da una controparte
  - La sicurezza della supply chain è diventata un elemento cruciale
- Vediamo solo una minuscola panoramica di alcuni elementi importanti

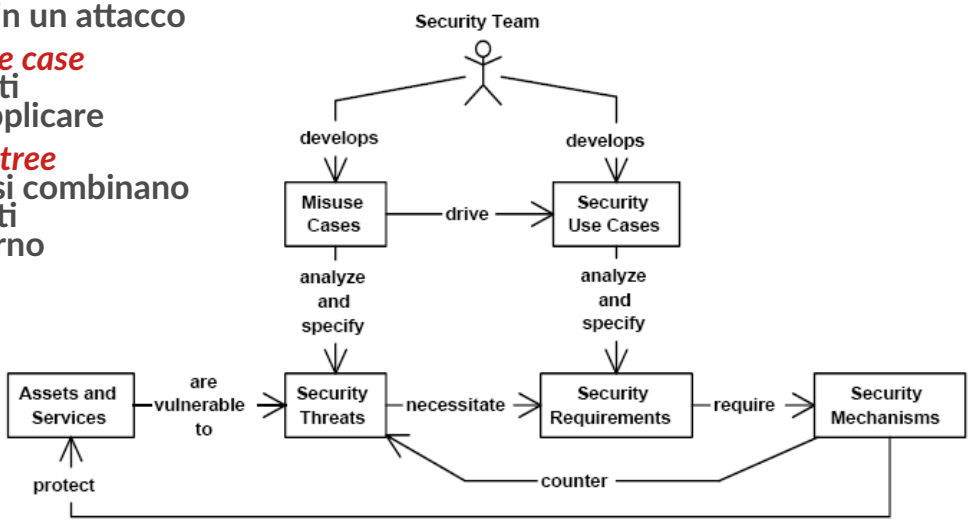
https://www.nist.gov/cyberframework/framework
Credit: N. Hanacek/NIST

Prevenzione

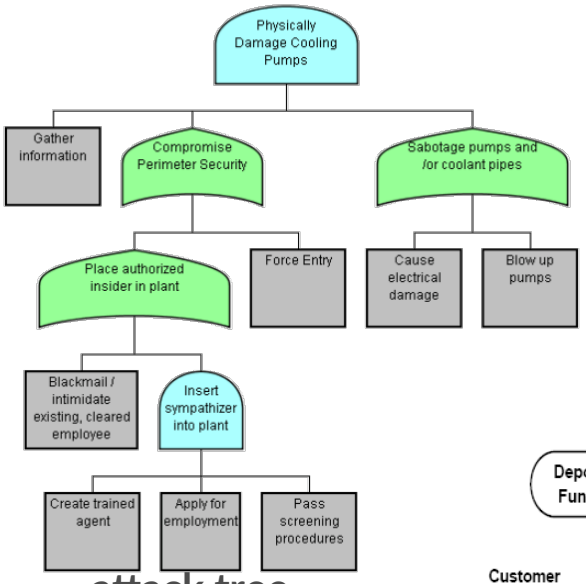
- Come tutti i processi ingegneristici, politiche e meccanismi derivano da
  - Analisi di requisiti
  - Progetto
  - Implementazione
  - Test
- Devono essere applicati a
  - Processi organizzativi
  - Contesto fisico
  - Sistemi
  - Reti
  - Applicazioni

Prevenzione - Security Engineering

- Prima sfida: non trascurare nemmeno un dettaglio
  - Inventario di tutti i componenti fisici
  - Catalogo di tutti i servizi
- Raccolta dei requisiti
  - Molto diversa da quella tradizionale: focalizzata sul “non deve accadere” invece che sul “deve funzionare”
  - Studio dei *misuse case* per verificare se una minaccia si può concretizzare in un attacco
  - Studio dei *security use case* per distillare i requisiti dei meccanismi da applicare
  - Definizione di *attack tree* per modellare come si combinano diversi possibili eventi e condizioni al contorno

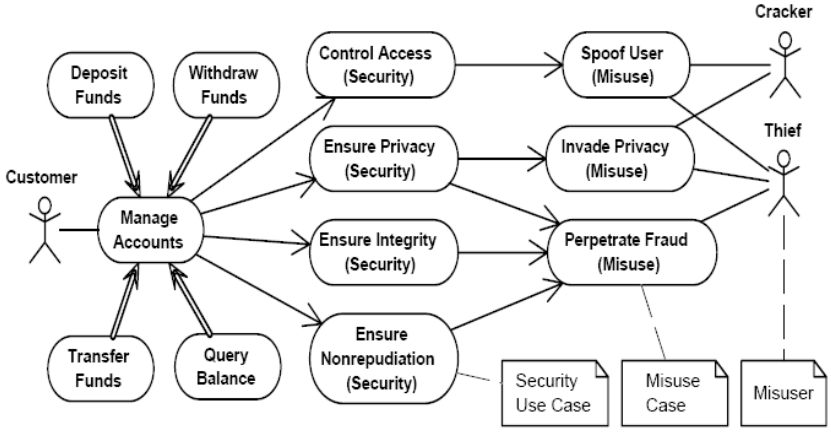


Security Engineering - esempi



attack tree

use/misuse cases



Security Engineering – migliori pratiche

1) Basare le decisioni della sicurezza su una esplicita politica
   a) Identity
   b) Access control
   c) Content-specific
   d) Network and infrastructure
   e) Regulatory
   f) Advisor and information
2) Evitare un singolo punto di fallimento (defense in depth)
3) Fallire in modo certo
4) Bilanciare sicurezza e usabilità
5) Essere consapevoli dell'esistenza dell'ingegneria sociale
6) Usare ridondanza e diversità riduce i rischi
7) Validare tutti gli input
8) Dividere in compartimenti i beni
9) Progettare per il deployment
10) Progettare per il ripristino

Prevenzione - Testing

- Fondamentale per
  - verificare se sono sfuggite vulnerabilità
  - verificare se il sistema è esposto a rischi nuovi rispetto al momento della progettazione
- Problema concettuale: copertura
  - Non su può dimostrare l'assenza di problemi
  - Solo tentare di sollecitare il sistema nel modo più completo possibile per trovare eventuali problemi esistenti
- Tre livelli di approfondimento
  - Vulnerability Assessment
  - Penetration Testing
  - Red Team Operations

Rilevazione

- Osservare il sistema durante tutte le fasi del suo funzionamento
- IDS = Intrusion Detection System
  - qualsiasi sistema in grado di rilevare i tentativi di attacco
    - basato sulla firma → cerca gli attacchi noti
    - rilevamento delle anomalie → cerca le deviazioni dai comportamenti sicuri
- IPS = Sistema di prevenzione delle intrusioni
  - in poche parole: un IDS che può attivare contromisure
- SIEM = Informazioni sulla sicurezza e gestione degli eventi
  - un'etichetta commerciale e completa per strumenti, politiche e processi che gestiscono origini dati e incidenti

Certificazioni

- Di processo per le aziende
  - ISO 27000
  - ITIL (Information Technology Infrastructure Library)
  - COBIT (Control Objectives for Information and Related Technologies)
- Di competenza per i professionisti – una pletora, ad esempio TIBER-EU suggerisce per i Red Team
  - CCITM, CCSAM → CREST - UK
  - CISSP, SSCP, CCSP → ISC2 - origini USA
  - CSX-P, CISM, CRISC, CISA → ISACA - origini USA
  - Security+, CySA+ → CompTIA – USA
  - ECSA, CEH, LPT, CHFI → EC Council - USA
  - GPEN, GWAPT, GXPN, GMOB, GAWN → SANS institute - USA
  - OSCP, OSWP, OSEE, OSWE, OSCE → Offensive Security – USA
  - eCCPT, eWPT, eWPTX, eMAPT, eCXD, eCPTX → eLearnSecurity - USA

Lo scenario europeo e italiano

- Gli attaccanti si organizzano, devono farlo anche i difensori
- È indispensabile un cambiamento di scala

  singola impresa → supply chain → sistema paese → digital single market
- Va tutelato l'interesse nazionale in un quadro di alleanze UE
  - Quadro strategico nazionale per la sicurezza dello spazio cibernetico (Pres. CdM, 2013)
  - **Direttiva "NIS" recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (n. 2016/1148 del Parlamento Europeo del Consiglio)**
  - **Piano nazionale per la protezione cibernetica e la sicurezza informatica** (Pres. CdM, 2017)
  - **Attuazione della Direttiva NIS (DLGS n.65 , 18 maggio 2018)**
- Ci sono due problemi incombenti:
  - Skill shortage
  - Capacity building

Aggredire lo skill shortage

- I numeri
  - Numero stimato di posizioni lavorative disponibili e non coperte in ambito cybersecurity
    - Worldwide: 2.93 milioni (2018) -> 4.07 milioni (2019)
    - Europa: 142.000 (2018) -> 291.000 (2019)
  - Deficit stimato in Europa per il 2022 pari a 350.000 addetti
- Come agire?
  - Nuove forme di innovazione didattica
    - supporto alle comunità di studenti appassionati di cybersecurity
  - Allargare la ricerca anche a personale con formazione non prettamente informatica ed ingegneristica
    - Iniziative nazionali che avviano alla cybersecurity anche i più giovani