Operazione Rif. PA 2023-19410/RER approvata con DGR 1317/2023 del 31/07/2023 finanziata con risorse del Programma Fondo sociale europeo Plus 2021-2027 della Regione Emilia –Romagna.

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

TECNICO PER LA PROGETTAZIONE E LO SVILUPPO DI APPLICAZIONI INFORMATICHE

MODULO: N. 5 Titolo: SICUREZZA DEI SISTEMI INFORMATICI E DISPIEGO DELLE APPLICAZIONI
DURATA: 21 ORE DOCENTE: MARCO PRANDINI

CYBERSECURITY: I FONDAMENTI

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

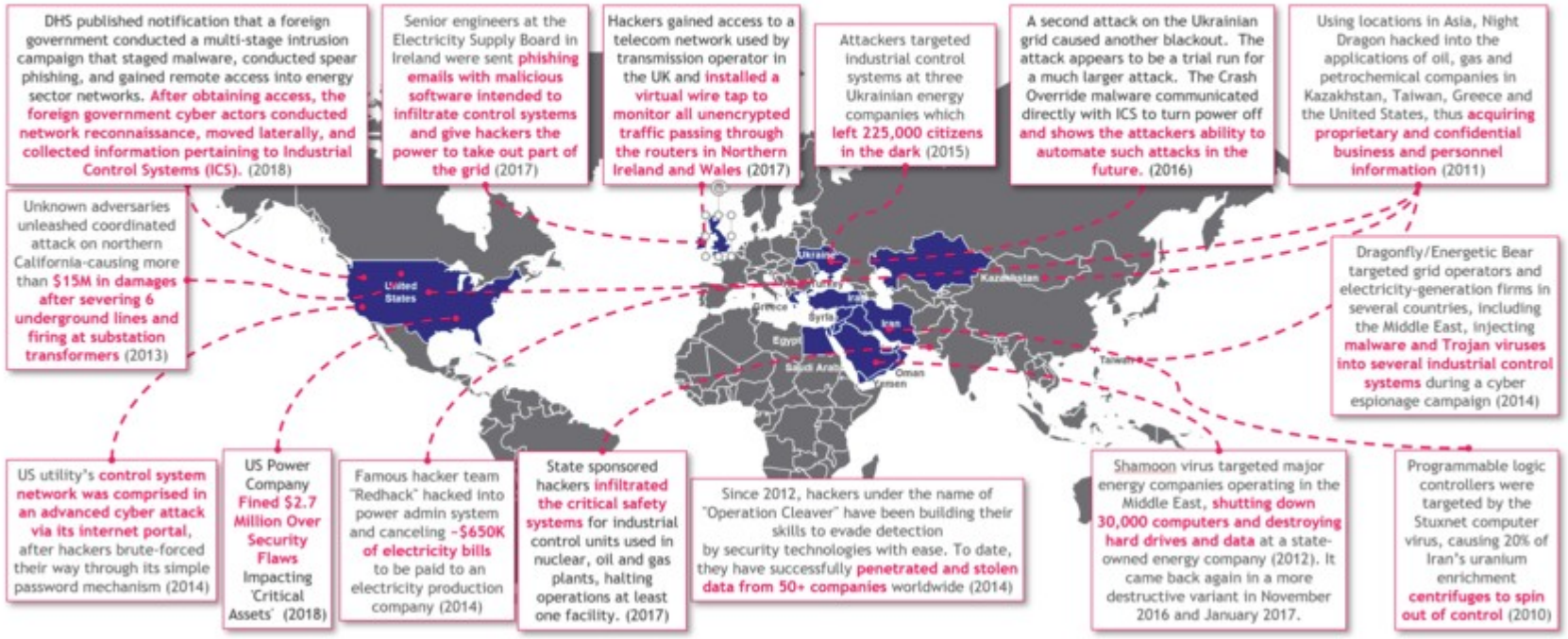
2000: Maroochy waste management

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:

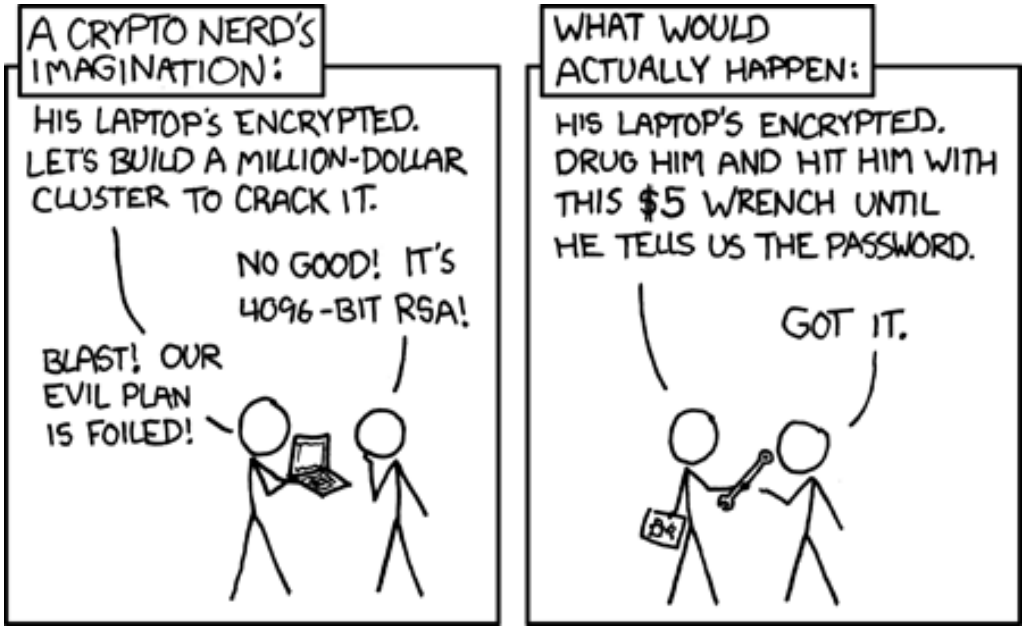
  RISCHIO = PROBABILITÀ x IMPATTO

  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

Il rischio cyber

- 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

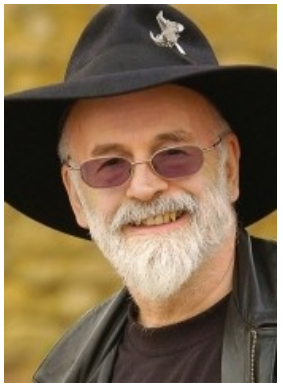


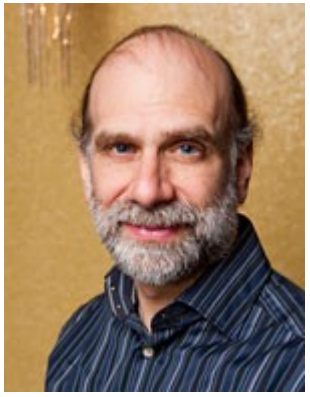
https://xkcd.com/538/

Detto così sembra facile...

"Progress just means bad things happen faster."

– Terry Pratchett (from *Witches Abroad*)



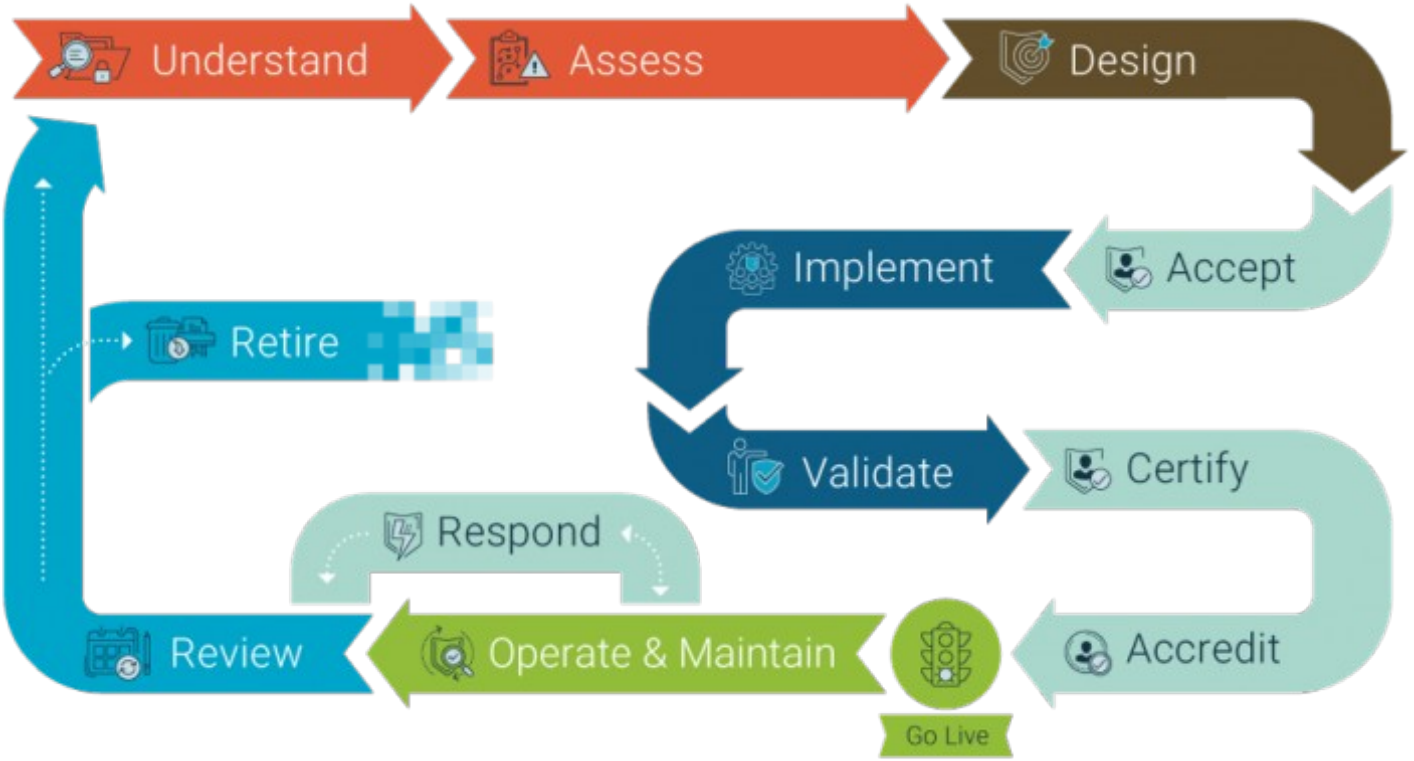


"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."

– Bruce Schneier

Un processo continuo

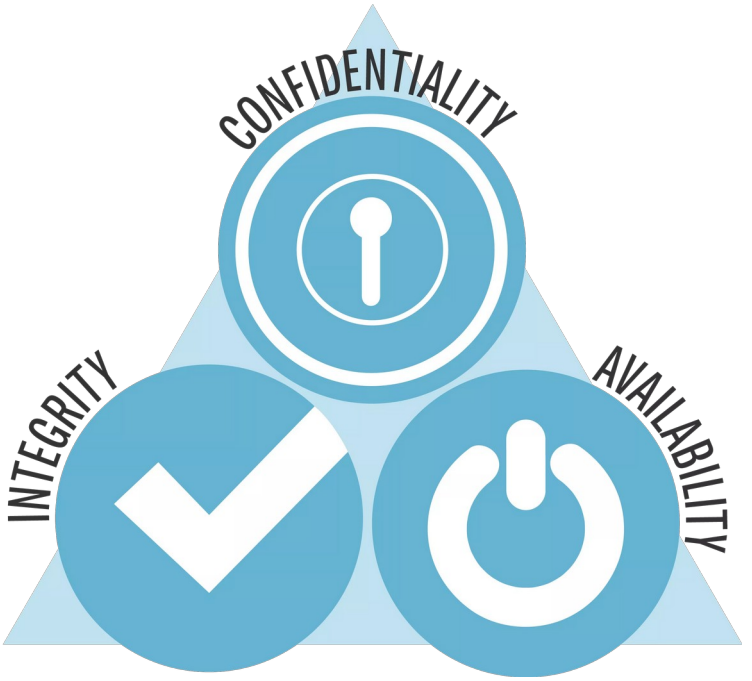
Sicurezza non è valutare la situazione presente e comprare un prodotto, bensì definire un processo per tenere traccia delle continue evoluzioni dei rischi e dell'efficacia delle contromisure



Proprietà di sicurezza

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

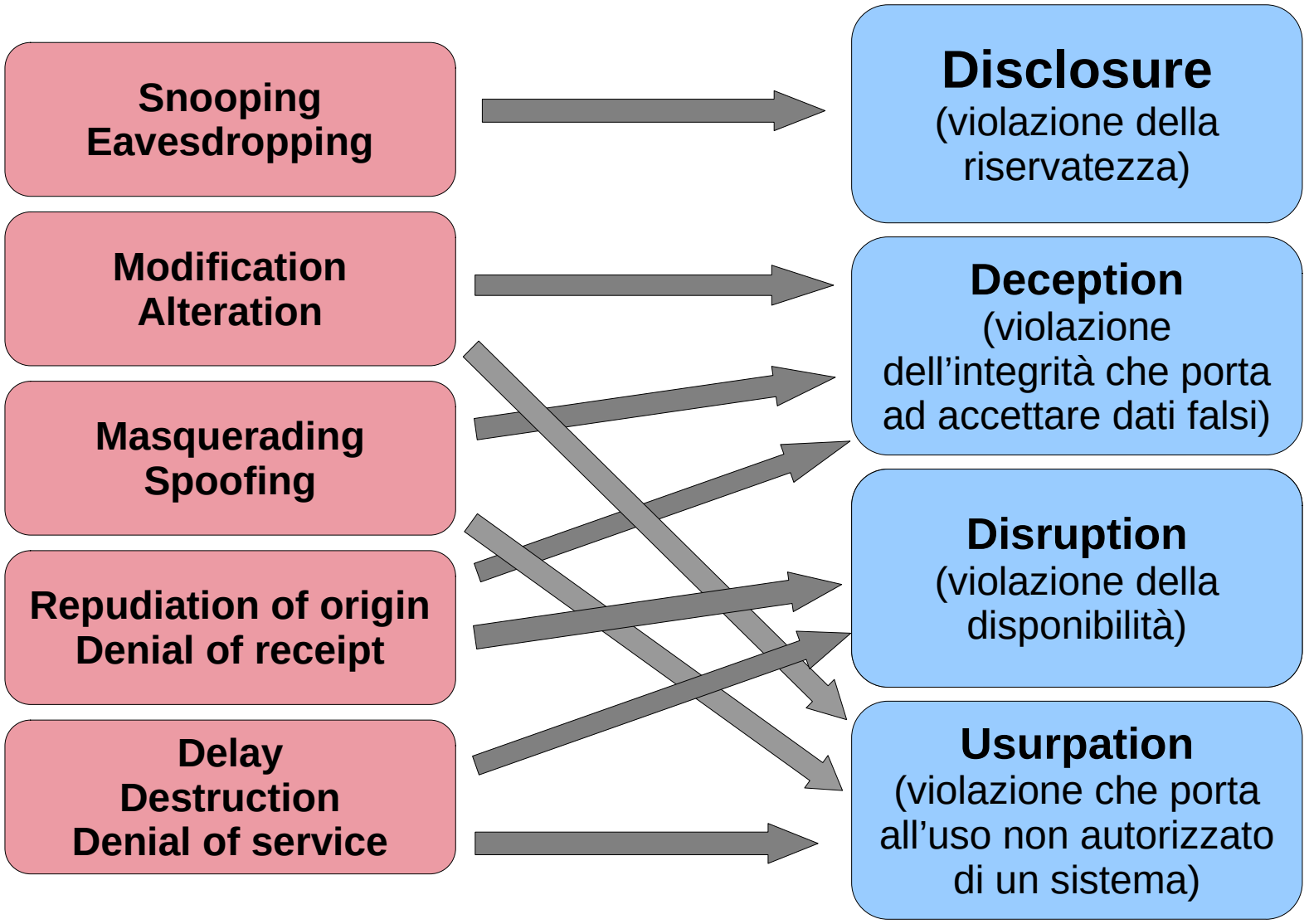
- Confidentiality (riservatezza)
  - Mantenere inaccessibili dati, o proprietà di un sistema, a chi non sia autorizzato a conoscerli
- Integrity (integrità)
  - Poter garantire che il contenuto e/o l'origine di un dato corrispondano a quanto si ritiene corretto
- Availability (disponibilità)
  - Poter 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
  - Impiegati vendicativi
  - Reporter
  - Ricercatori
  - Attivisti
  - Criminali organizzati
  - Spie industriali
  - Governi ed eserciti

Tipologie di attacchi e minacce



Il panorama delle minacce

ENISA Threat Landscape

15 Top Threats in 2020

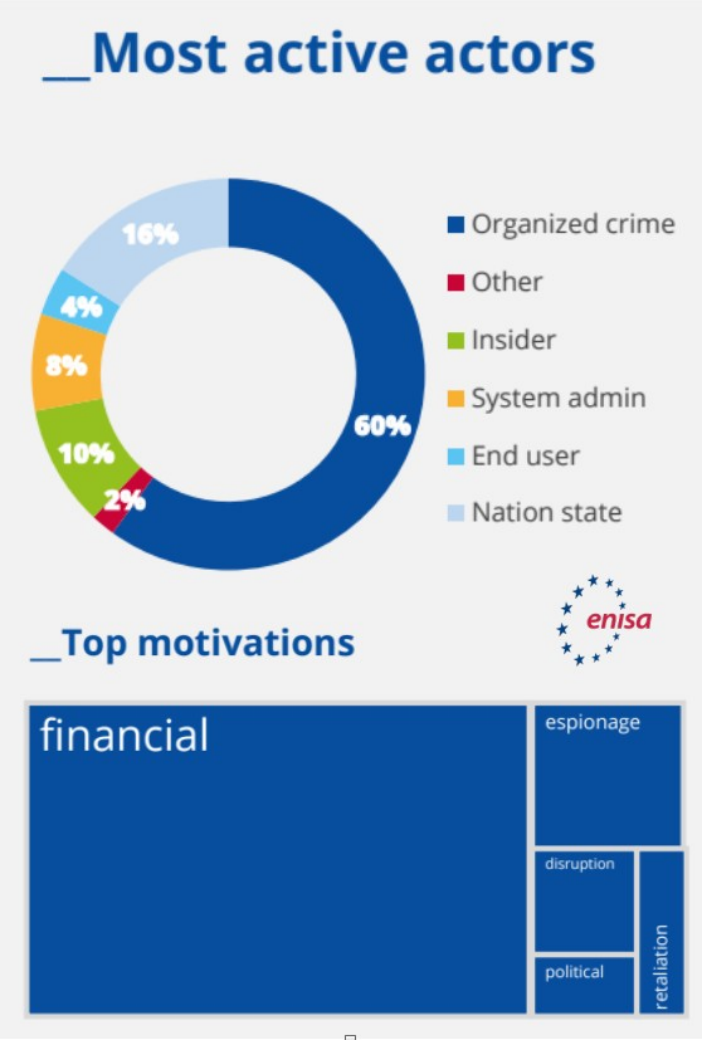
EUROPEAN UNION AGENCY FOR CYBERSECURITY

www.enisa.europa.eu

enisa

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.

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.

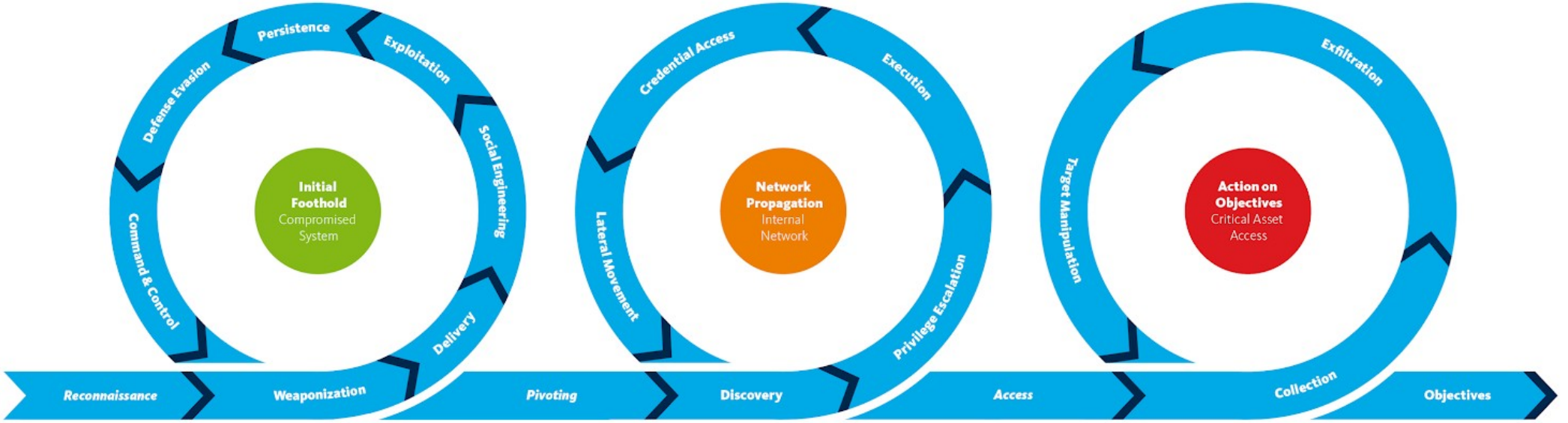
10_ The number of phishing victims continues to grow since it exploits the human dimension being the weakest link.

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.

Come avviene un attacco

- I modi di entrare in un sistema sono vari e spesso usano come anello debole della catena l'essere umano
- Spesso l'obiettivo è installare qualche tipo di malware (software malevolo)
  - che può consentire accesso al sistema – RAT Remote Access Trojan
  - che può rendere il sistema inutilizzabile – Cryptolocker, Ransomware
  - che esporta verso l'attaccante i dati della vittima - Spyware
  - che utilizza la vittima per effettuare altri attacchi – Botnet agent

ma non solo...



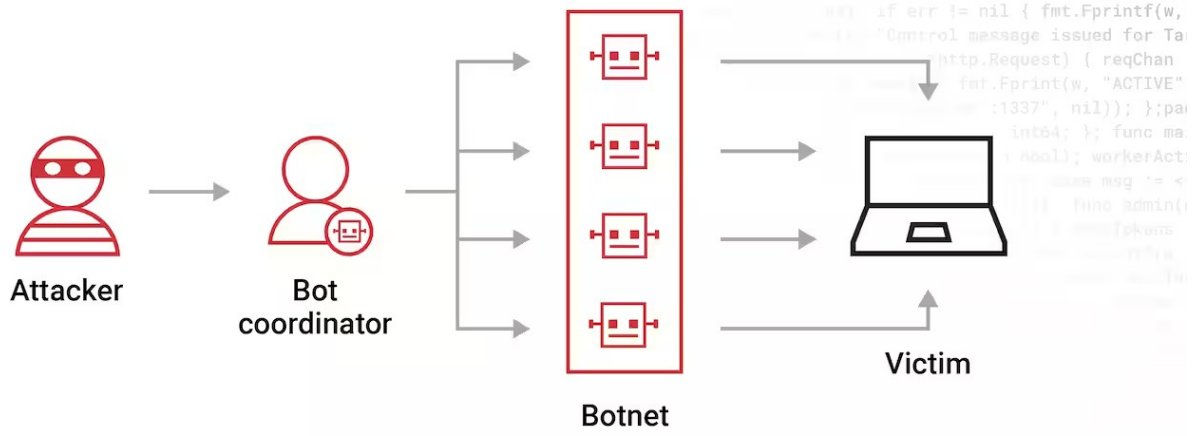
Pols, Paul (2017). "The Unified Kill Chain". Cyber Security Academy.

Esempi di attacchi: Interruzione del Servizio

- Lo scopo è violare la “A” della triade
- Non servono strumenti sofisticati per rubare dati o alterare programmi, spesso solo forza bruta per causare un volume di traffico o di carico di calcolo insostenibile per la vittima

  --> Denial of Service (DoS)
- Spesso per farlo ci si avvale di un’armata di computer in sè di poco valore, ma facili da compromettere, e in numero tale da creare una grande forza d’urto

  --> Distributed DoS



How a botnet works

Esempi di attacchi: furti di identità

- Qualcuno ruba le tue informazioni personali (ad esempio il codice fiscale) e lo utilizza senza la tua autorizzazione per creare nuovi account, fare acquisti o commettere altre frodi

US hacker charged with stealing 130m credit card IDs

The New York Times | http://ny6.ms/12RDzOm

TECHNOLOGY | NYT NOW

Russian Hackers Amass Over a Billion Internet Passwords

By NICOLE PERLROTH and DAVID GELLES AUG. 5, 2014

A Russian crime ring has amassed the largest known collection of stolen Internet credentials, including 1.2 billion user name and password combinations and more than 500 million email addresses, security researchers say.

The records, discovered by Hold Security, a firm in Milwaukee, include confidential material gathered from 420,000 websites, including household names, and small Internet sites. Hold Security has a history of uncovering significant hacks, including the theft last year of tens of millions of records from Adobe Systems.

BUSINESS

Yahoo says 1 billion user accounts were hacked

Breaking In

The breach disclosed by Equifax ranks among the largest ever publicly disclosed by a company.

Selected data breaches by number of: Accounts/cards Customers

COMPANY	SIZE OF BREACH	YEAR
Yahoo*	1 billion	2016
Yahoo*	500 million	2016
Equifax	**143**	**2017**
Heartland Payment Sys.	130	2009
LinkedIn	117	2016
Sony	100	2011
TJX	90	2007
Anthem	80	2015
J.P. Morgan	76†	2014
Target	70‡	2013
Home Depot	56	2014

*Believed to be separate incidents †Millions of households ‡Initial disclosure

Source: the companies

THE WALL STREET JOURNAL.

Esempi di attacchi: phishing

- E-mail, messaggi di testo, telefonate o siti Web fraudolenti progettati per indurre gli utenti a scaricare **malware**, condividere informazioni sensibili o dati personali o intraprendere altre azioni che espongono se stessi o le proprie organizzazioni alla criminalità informatica
- Il phishing è la seconda causa più comune di violazione dei dati, e costa alle vittime in media 4,91 milioni di dollari
- Google trova 300.000 nuovi siti di phishing al mese, e molti di essi sono online solo per meno di un'ora

Esempi di attacchi: phishing

Esempi di attacchi: phishing

Esempi di attacchi: ransomware

- Crittografare i dati critici di un utente o di un'organizzazione, impedendo l'accesso ai file, database, o applicazioni. L'aggressore richiede il pagamento di un riscatto per decifrarli

What is WannaCry ransomware and why is it attacking global computers?

Malicious software has attacked Britain's health service and companies in Spain, Russia, the Ukraine and Taiwan. What is it and how is it holding data to ransom?

Another Hacked Florida City Pays a Ransom, This Time for $460,000

The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks

Even when public agencies and companies hit by ransomware could recover their files on their own, insurers prefer to pay the ransom. Why? The attacks are good for business.

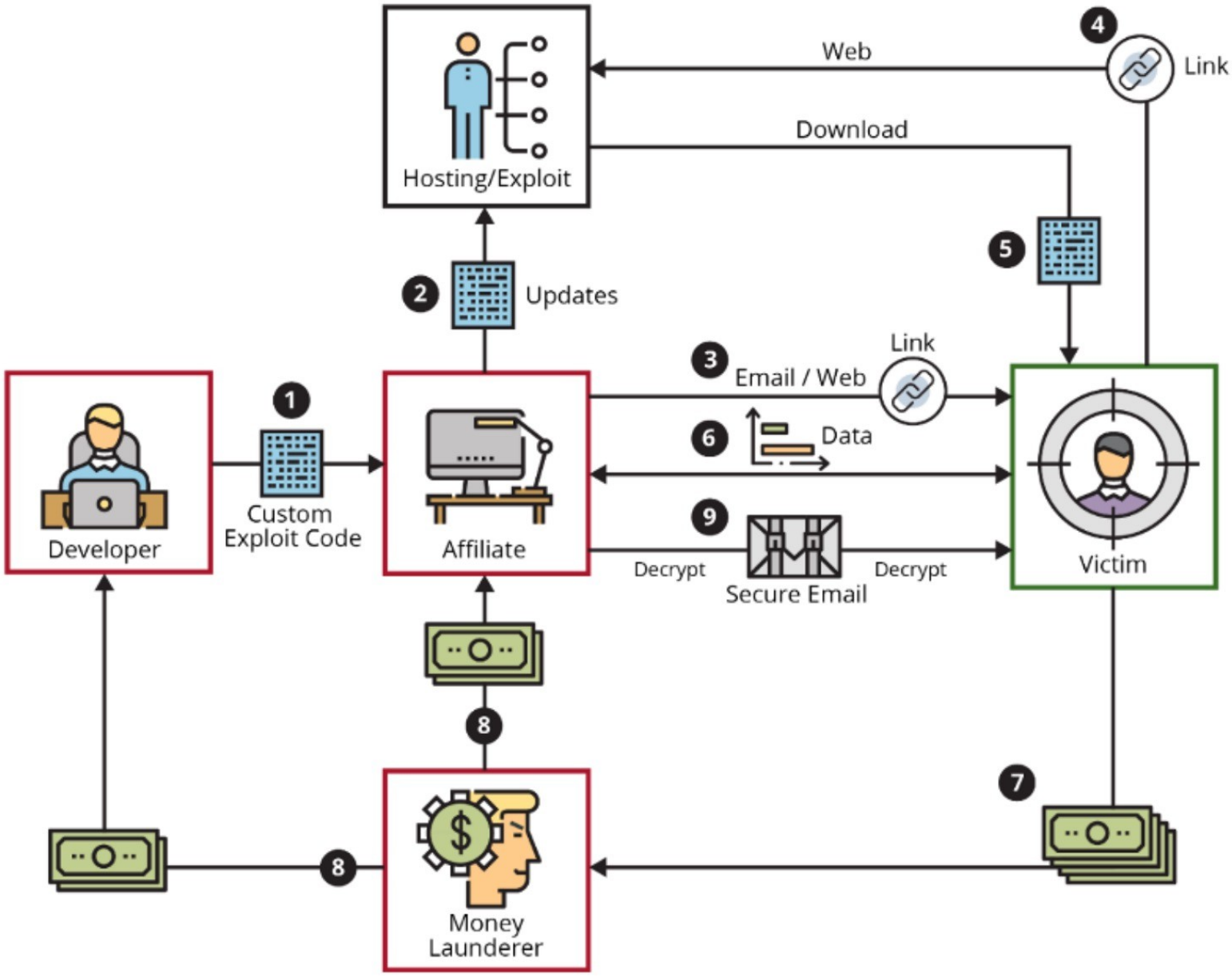
Esempi di attacchi: Ransomware as a Service

- Nel ransomware come servizio, come DarkSide, uno sviluppatore di malware addebita una tariffa utente agli affiliati, che potrebbero non avere le competenze tecniche per creare un ransomware ma sono in grado di penetrare in un sistema informatico della vittima

- Questi servizi includono il supporto tecnico per i cracker, inclusa la negoziazione con le vittime e la conduzione di campagne di pressione su misura

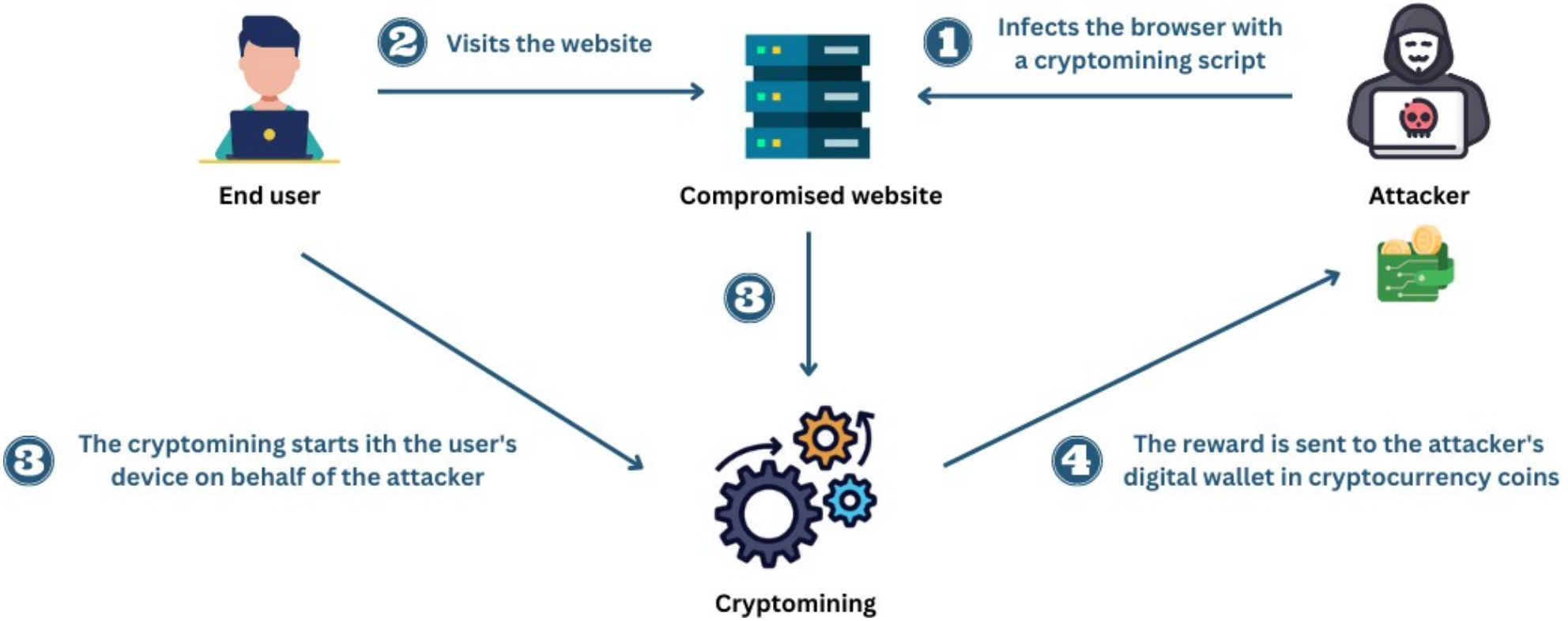
- Le tariffe per gli utenti di DarkSide variavano a seconda dell'impatto: 25% per riscatti inferiori a 500.000 dollari, con sconti progressivi, fino al 10% per riscatti superiori a 5 milioni di dollari

Esempi di attacchi: Ransomware as a Service



Esempi di attacchi: crypto-jacking

- Uso non autorizzato dei dispositivi delle persone per estrarre criptovaluta. Funziona incorporando un JavaScript, ogni visitatore esegue solo una piccola parte di mining, ma il totale del tempo di calcolo raccolto può generare vero valore



Esempi di attacchi: supply chain

- Sfrutta l'estrema interdipendenza del mondo moderno
- Aggredisce un bersaglio intermedio di per sé non interessante, ma che fornisce componenti hardware o software alle vere vittime
- Esempi:
  - Target

    https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

  - Solarwinds

    https://www.cybersecurity360.it/nuove-minacce/attacco-agli-usa-nuovi-dettagli-del-breach-solarwinds-e-come-mitigare-i-rischi/

    https://www.avantgrade.com/digital-marketing/attacco-hacker-solarwinds

Esempi di attacchi: alla vecchia maniera

- Il furto di un dispositivo fisico resta uno strumento valido anche nel mondo digitale e iperconnesso
  - salta le difese predisposte a controllare il traffico di rete
  - salta le protezioni offerte dal sistema operativo dei calcolatori
  - può causare immediata perdita di Confidenzialità e Disponibilità
- Anche la brutale distruzione...
  - di nuovo minaccia la Disponibilità
- Al giorno d'oggi un elemento è particolarmente a rischio: ovviamente lo smartphone
  - contiene dati di immediato valore
  - rappresenta il punto privilegiato per regolare l'accesso a tutti i dati e i servizi esterni utilizzati dal proprietario (si pensi alle app di autenticazione, ai servizi che mandano SMS di conferma, ecc.)

Quanti incidenti: qualche mese 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)

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 2021 riassunti https://securityinsight.nl/report/check-point-2022-cyber-security-report

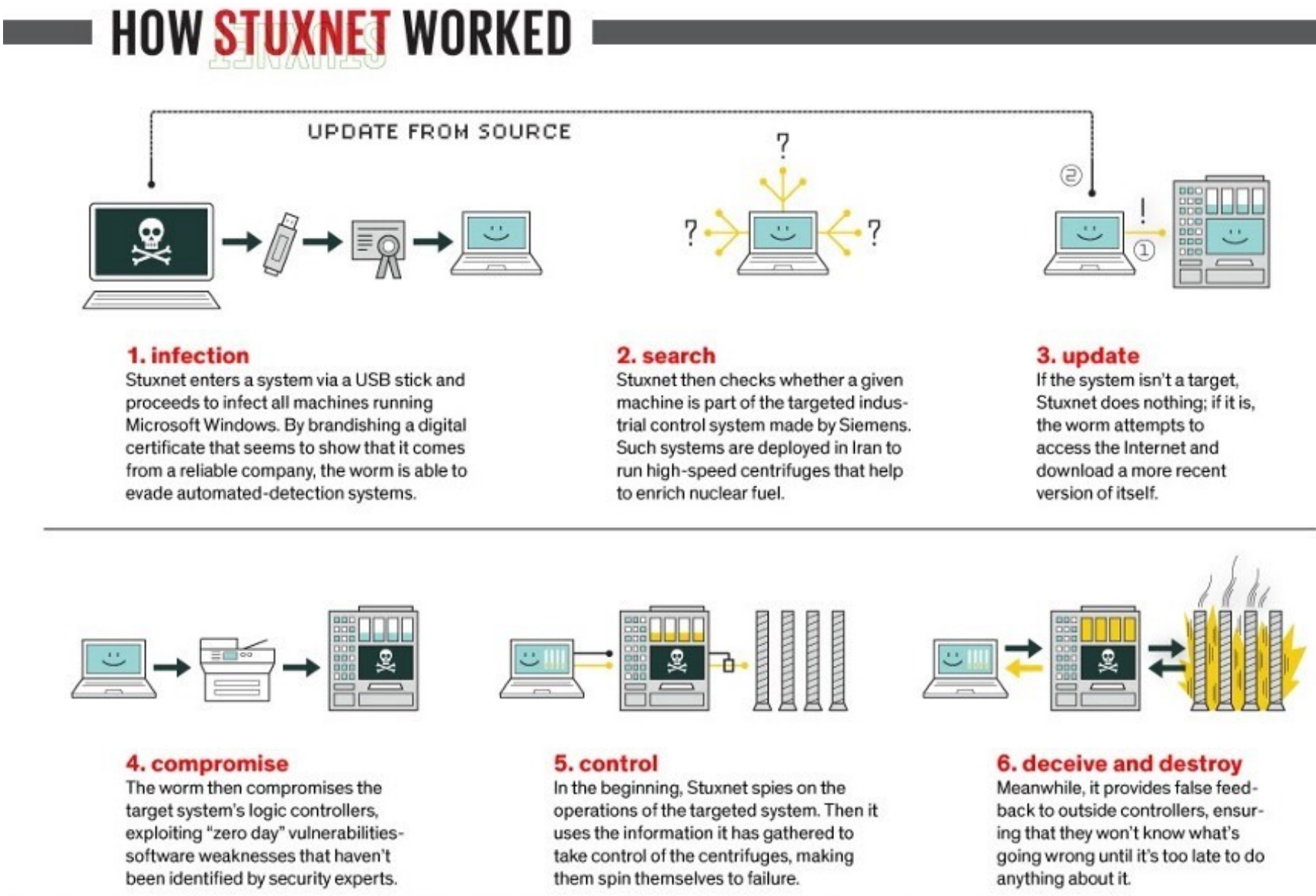
Quanti incidenti: 2022 in sintesi

- **January**
  - Ukraine has been hit by a large scale cyber-attack that took down several of its government and ministries websites
  - In Iran, television channels and radio stations were hacked by an exiled opposition group
- **February**
  - A ransomware disrupted operations of oil port terminals in Belgium, Germany, and Netherlands
  - Ukraine has been at the centre of a series of DDoS attacks on its armed forces, defence ministry, public radio, and national banks
  - Hackers leveraged an announce of OpenSea to scam NFT users and steal millions of dollars
- **March**
  - Ukraine has claimed attacks taking down multiple Russian and Belarusian key websites, including that of the Kremlin
  - A ransomware gang stole 2 code signing certificates used by NVIDIA to sign their drivers and executables
  - One of the largest Russian meat producers had their IT systems encrypted, resulting in distribution disruptions for several days
- **April**
  - A set of vulnerabilities in the ALAC audio format that could have been used for remote code execution on two-thirds of the world's mobile devices
  - Vulnerability in Everscale blockchain wallet, giving an attacker full control of victim's funds
- **May**
  - Costa Rica has been victim of a ransomware attack, resulting in the loss of $200 million
  - A ransomware occurred in December 2021 lead to the closing of the Lincoln College, a 157-year-old institution of Illinois
  - A Russian banking services organization experienced the largest DDoS attack ever recorded (450 GB/sec)
- **June**
  - The largest ever-recorded HTTPS DDoS attack targeting Cloudfare customers has been mitigated
  - Russia has increased attacks against governments and NGOs supporting Ukraine
- **July**
  - Norway and Lithuania were victims of a large-scale DDoS
  - Twitter has suffered a data breach affecting 5.4 million accounts
- **August**
  - Cisco has been breached by a ransomware group
  - DDoS attack targeting Lockheed Martin
  - The largest water company supply of the UK has been victim of a ransomware, causing the disruption of the company's IT system and allowing them to access more than 5TB of data
  - A cryptocurrency mining campaign imitating Google Translate Desktop
- **September**
  - A traffic jam attack to hack the Russian taxi service Yandex
  - Iran has performed multiple cyberattacks to disrupt Albania's government systems
  - Uber has suffered a data breach
- **October**
  - Hacktivist groups have been leaking information on Iranian government officials and offering support in sharing information
  - Personal information of 10 million Australians has been stolen
  - Russian attacks tacking down different US and Bulgarian state government websites
  - The largest copper manufacturer has been victim of a cyberattack that shut down many of its IT systems
- **November**
  - Ukraine IT Army leaked 27K files from the Russia's Central Bank
  - The Azov ransomware has being distributed worldwide
  - Meta employees granted access to user's Facebook and Instagram profiles in return of thousands of dollars in bribes
  - The European Parliament website has been hacked following a vote declaring Russia a state sponsor of terrorism
  - A ransomware group has been running a campaign targeting USA, Canada, United Kingdom, Australia, and New Zeland
- **December**
  - Release of a batch of data from Australian Medibank's system
  - 300,00 users across 71 countries were affected by an Android campaign to steal Facebook credentials

Esempi di incidenti: guerra cyber

- Nel 2009, il segretario alla Difesa americano Robert Gates ha dichiarato che il cyberspazio è "quinto dominio" delle operazioni militari, accanto a terra, mare, aria e spazio
- Gli Stati Uniti attualmente schierano 6.200 cyber-soldati
- Il cyber è diventato l'arma preferita da molti paesi come North Corea, Russia, Cina e Iran per rubare, interrompere servizi, e minacciare
- New York Times, 26 July 2016
  - *"Spy agency consensus grows that Russia hacked D.N.C."* American intelligence agencies have told the White House they now have "high confidence" that the Russian government was behind the theft of emails and documents from the Democratic National Committee
- The Washington Post, 22 September 2017
  - *"DHS tells states about Russian hacking during 2016 election"* The Department of Homeland Security contacted election officials in 21 states Friday to notify them that they had been targeted by Russian government hackers during the 2016 election campaign

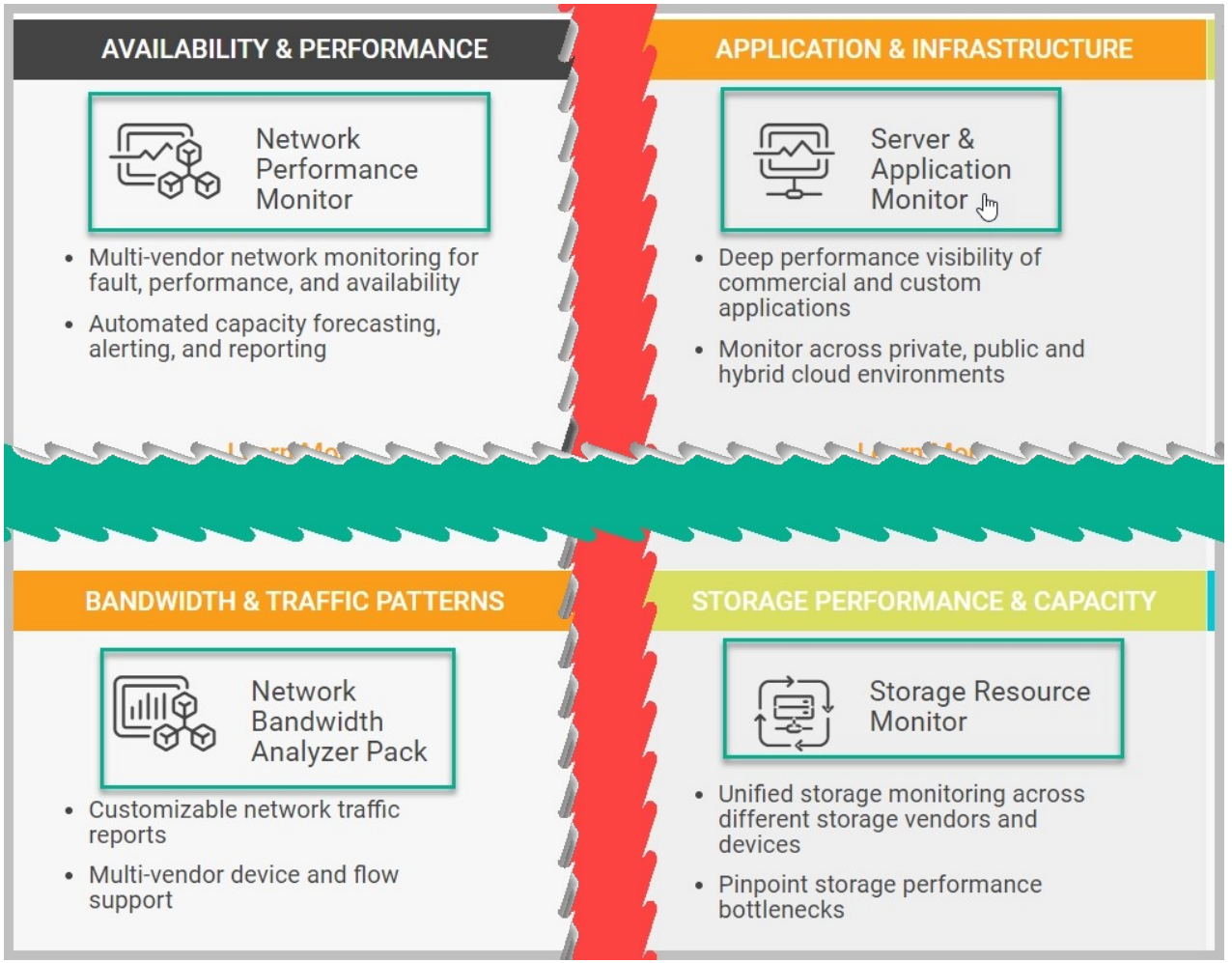
Esempi di incidenti: guerra cyber



Esempi di incidenti: Solarwinds

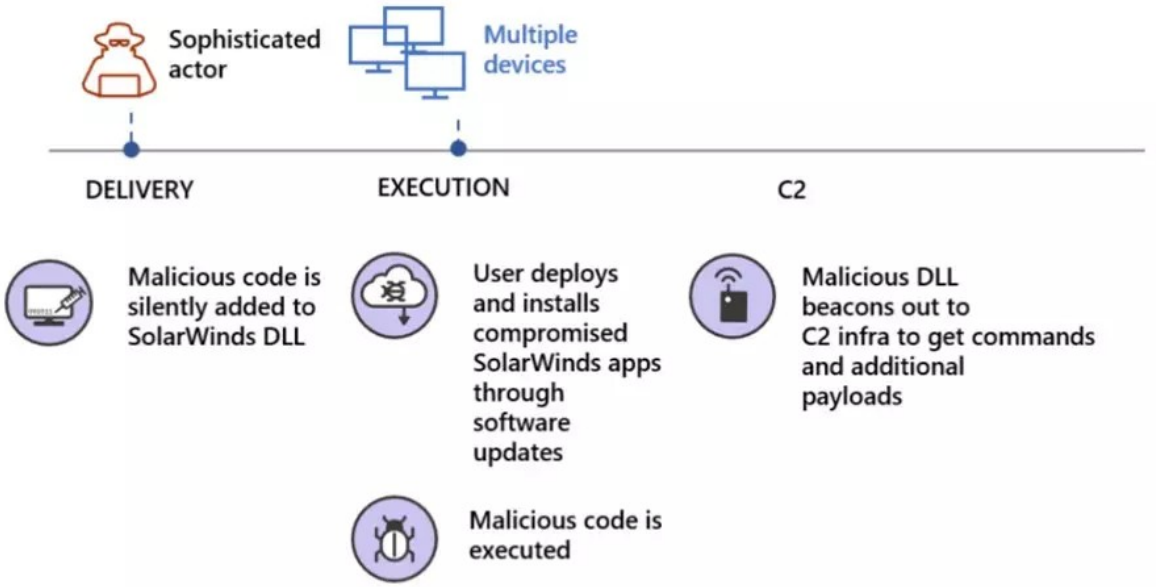
- Solarwinds fornisce servizi a terzi, tra cui
  - l'esercito USA;
  - il Pentagono;
  - il Dipartimento di Stato;
  - la NASA (National Aeronautics and Space Administration);
  - l'NSA (National Security Agency);
  - le poste USPS (United States Postal Service);
  - il Ministero di Giustizia;
  - l'Ufficio del Presidente USA;
  - le principali 5 aziende di accounting.

    ...
  - *Telecom Italia*



Esempi di incidenti supply chain: Solarwinds

- Falla nella piattaforma Orion
  - accesso senza autenticazione
  - visibilità di tutti i dati dei clienti
- Elemento di grande interesse: persistenza
  - invece che cercare un modo di restare dentro tutti i sistemi vittima, gli attaccanti hanno trovato un modo di violare il processo di aggiornamento delle librerie, apparentemente innocue, usate da loro



Esempi di incidenti supply chain: repository

- **ARS Tecnica, 16 February 2021 "New type of supply-chain attack hit Apple, Microsoft and 33 other companies"**

  The so-called dependency confusion or namespace confusion attack starts by placing malicious code in an official public repository such as NPM (JavaScript) or PyPI (Python). By giving the submissions the same package name as dependencies used by companies such as Apple, Microsoft, Tesla, and 33 other companies, a researcher was able to get these companies to automatically download and install the counterfeit code

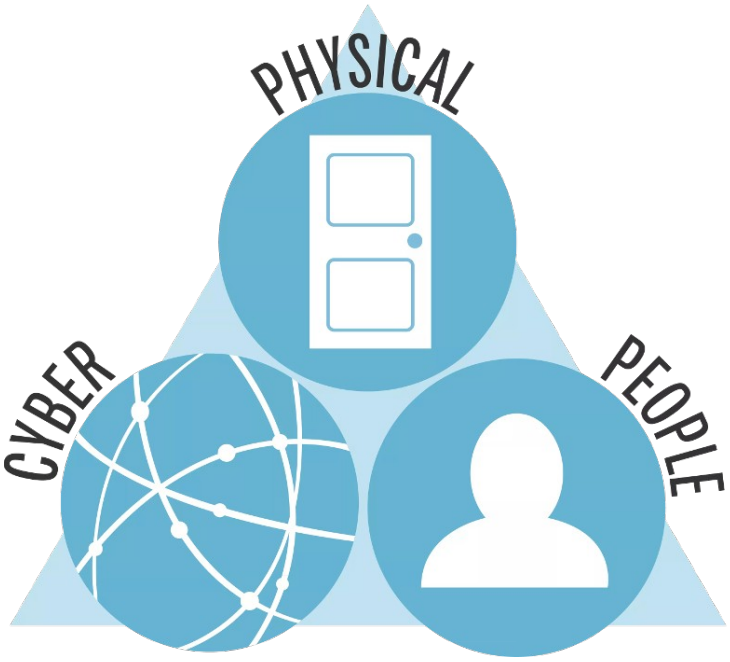
- **Succede anche sugli app store, colpendo normali utenti di smartphone!**

Vulnerabilità

- Vettori di attacco
- Vulnerabilità
  - origini
  - ciclo di vita
- Elementi vulnerabili
  - persone
  - ambiente
  - dispositivi
  - reti
  - sistemi
  - applicazioni

Superficie di attacco

- Ogni modo possibile di interagire con il sistema (attenzione: che sia previsto come metodo lecito da progetto, o puramente incidentale) è accessibile anche 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 i sistemi fossero perfetti, le minacce non potrebbero concretizzarsi
  - perfetto = fa solo quello per cui è stato progettato, ed è stato progettato per fare solo ciò che serve all'utente legittimo – approfondiremo poi
- 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)

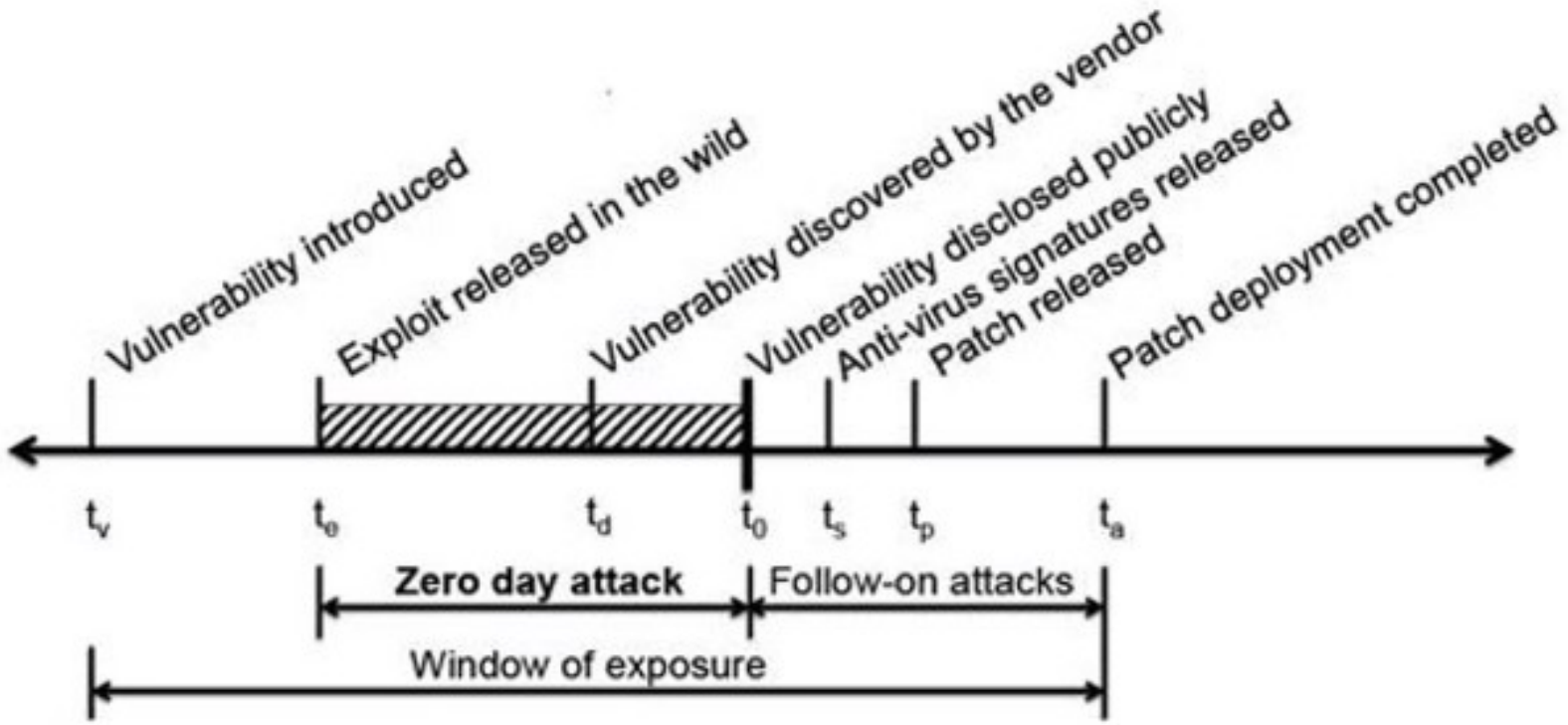
Qualche esempio di vulnerabilità

- 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

Il ciclo di vita della vulnerabilità



Leyla Bilge, Tudor Dumitras, Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World, ACM CCS 2012.

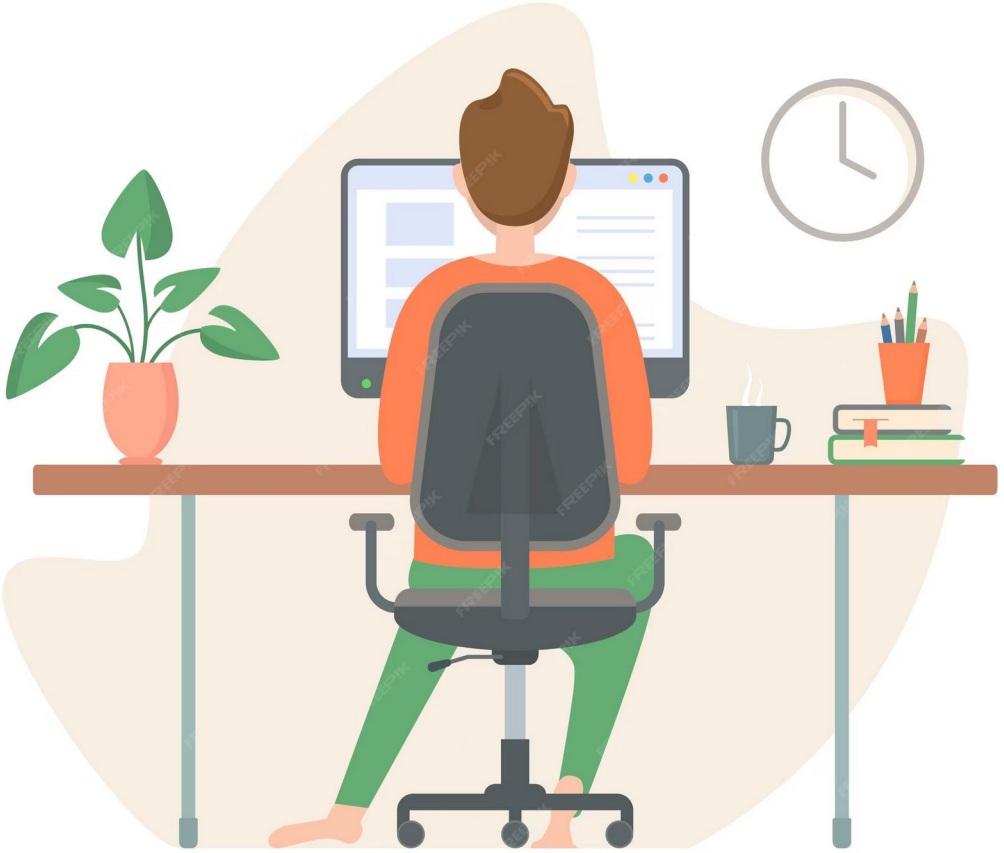
Modi e tempi

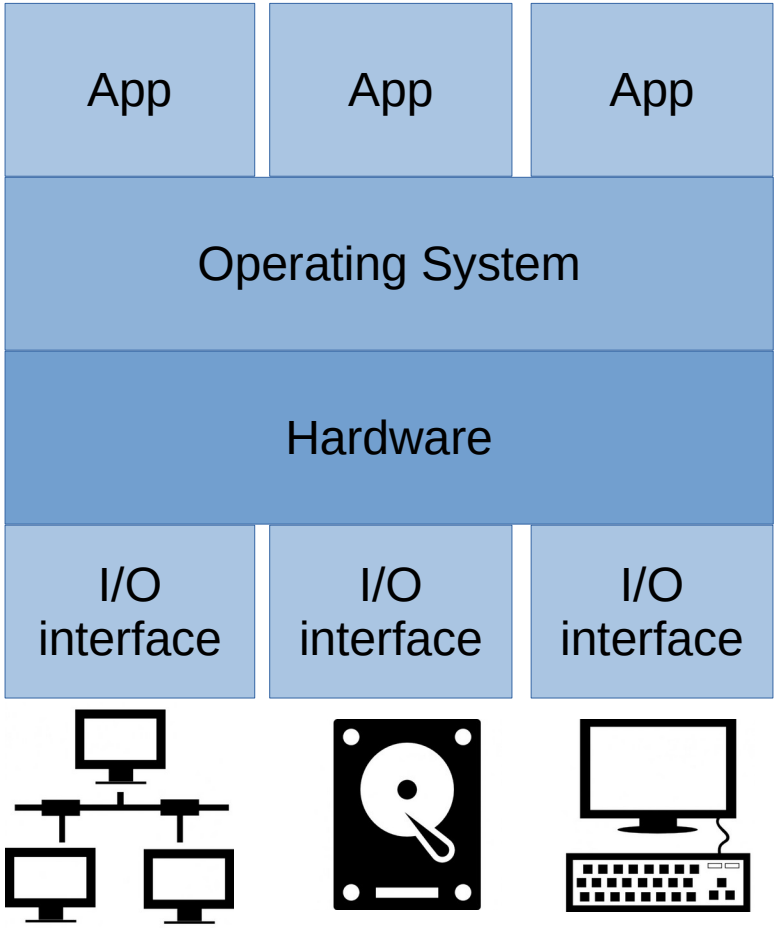
- **Vulnerabilità zero-day**: una vulnerabilità sconosciuta a coloro che dovrebbero essere interessati a mitigarla
- **Finestra di opportunità**: tempo trascorso da quando il primo exploit del software diventa attivo al momento in cui il fornitore interessato rilascia una patch e viene applicata
- **Attacco zero-day**: un attacco che si verifica durante la finestra di opportunità
  - Nel 2005 la durata media di una finestra era di 54 giorni, nel 2014 è cresciuta a quasi 12 mesi
- Gli attacchi si intensificano dopo la finestra, perché tutti vengono a conoscenza della vulnerabilità
  - tipicamente scansioni massicce iniziano dopo 15 minuti dalla pubblicazione della CVE

Pubblicare le vulnerabilità

- La comunità pubblica le vulnerabilità scoperte, secondo un principio di *responsible disclosure*
  - Common Vulnerabilities and Exposures http://cve.mitre.org/
  - National Vulnerability Database http://nvd.nist.gov/
  - Open Sourced Vulnerability Database http://osvdb.org/
  - SecurityFocus http://www.securityfocus.com/vulnerabilities
  - US-CERT http://www.kb.cert.org/vuls/
- Ci sono iniziative per cercarle attivamente
  - Google project zero
  - Programmi di *bug bounty* che le pagano profumatamente (es. Zerodium)
- Esistono database di exploit pronti per sfruttarle
  - https://www.cvedetails.com/
  - https://www.exploit-db.com/
  - https://packetstormsecurity.com/

Dove si annidano le vulnerabilità?





Fattori non tecnologici

- Un intero mondo; queste liste sono incomplete e soprattutto ogni punto meriterebbe ore di approfondimento... ma giusto per dare qualche idea:
- Vulnerabilità dovute alla definizione dei processi:
  - elencare ogni singolo elemento senza dimenticare nulla
  - elencare in che modo ogni elemento potrebbe interagire con altri
  - definire quali interazioni sono ammesse e sotto quali condizioni
  - mettere in condizione tutti gli attori di implementare le regole e verificare se vengono violate
    - in questo punto si nascondono “dettagli” come vincoli di costo, spazio, tempo, normative, costrutti sociali... il mondo reale insomma
- Vulnerabilità dovute a comportamenti delle persone
  - involontaria mancanza di rispetto delle regole per ignoranza, incapacità, pigrizia
  - volontaria mancanza di rispetto delle regole per ostilità, corruzione, minacce, idealismo

Disponibilità

- Per erogare con continuità un servizio, il sistema deve essere acceso e connesso!
  - Le infrastrutture che garantiscono un ambiente affidabile sono complesse e molto costose → indispensabile condividerle

https://datacenter.com/news_and_insight/data-center-redundancy-2plus1-2n-distributed-redundancy/

- *Data center* o *server farm* sono i luoghi in cui vengono ospitati in grande quantità i sistemi di calcolo
  - Housing o Co-location: fornitura di spazio e connettività per sistemi acquistati e gestiti dal cliente
  - Managed housing: fornitura dei sistemi in housing (su hardware comunque dedicato al cliente) e loro gestione sistemistica
  - Hosting: fornitura di uno o più servizi specifici (storage, web, posta, …) su hardware condiviso tra più clienti
    - Il modello cloud è un caso speciale dell'hosting tradizionale

Problematiche principali di un data center

- Resistenza della struttura
  - cause naturali: terremoti, inondazioni, ...
  - cause artificiali: incidenti aerei e ferroviari, terrorismo, ...

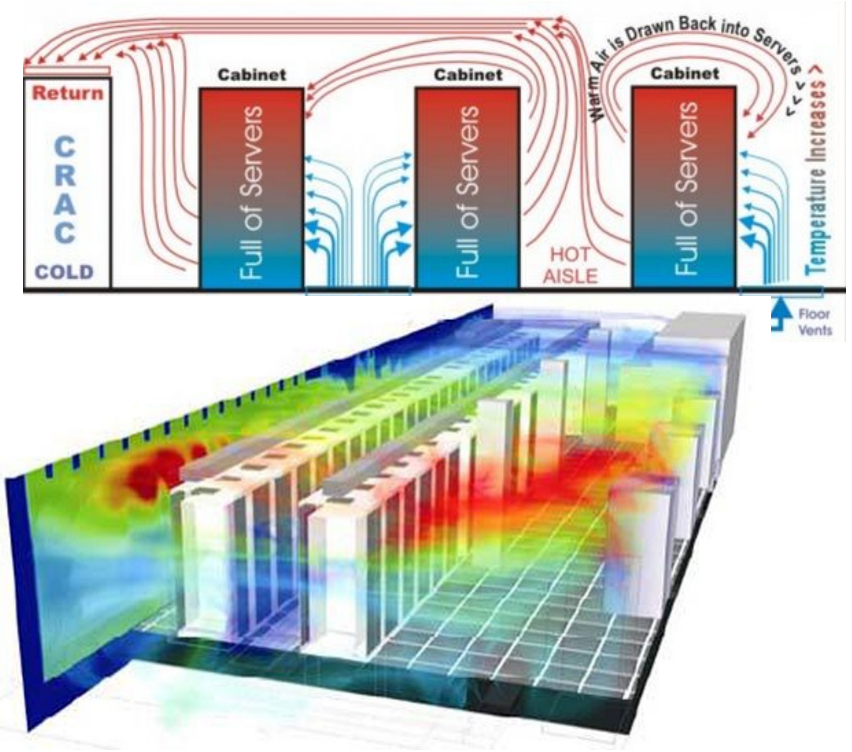
    https://goo.gl/maps/zUwqeZJrJrQU7eG97
  - cause interne: incendi, da controllare con sistemi che consentano l'intervento anche quando l'incendio stesso li danneggia parzialmente
    - ogni sistema complesso, anche se introdotto per limitare danni, può causarne altri di imprevisti

      https://journal.uptimeinstitute.com/fire-suppression-systems-bring-risk/
- Sicurezza e controllo degli accessi
  - perimetro esterno blindato
  - staff (armato) 24/7
  - segmentazione settori con liste di controllo accessi separate e concordate in anticipo sull'ingresso
  - apertura varchi a più fattori
  - videosorveglianza con registrazione off-site

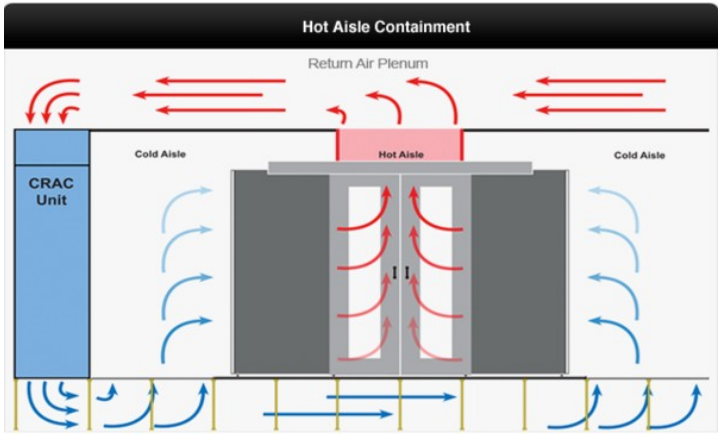
Problematiche principali di un data center

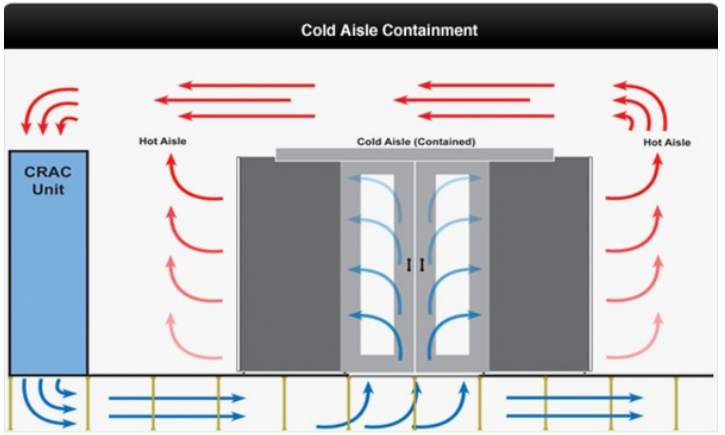
- Condizionamento dell'aria
  - gestione di temperatura e umidità con sistemi tolleranti ai guasti e alle interruzioni di erogazione dell'energia elettrica

https://www.colocationamerica.com/blog/cooling-innovations-for-data-centers



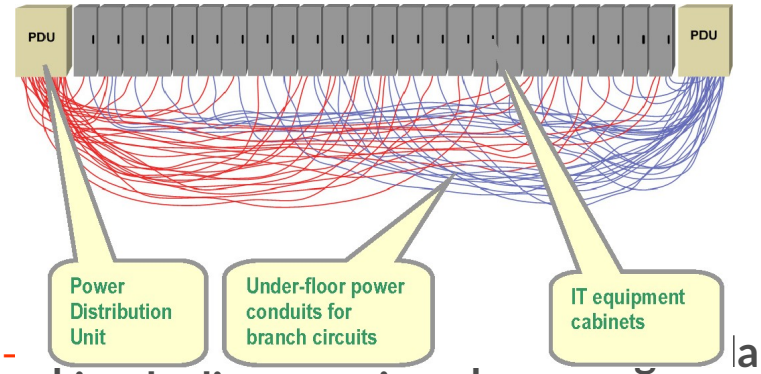
https://datacenterresources.com/articles/identifying-data-center-cooling-issues/





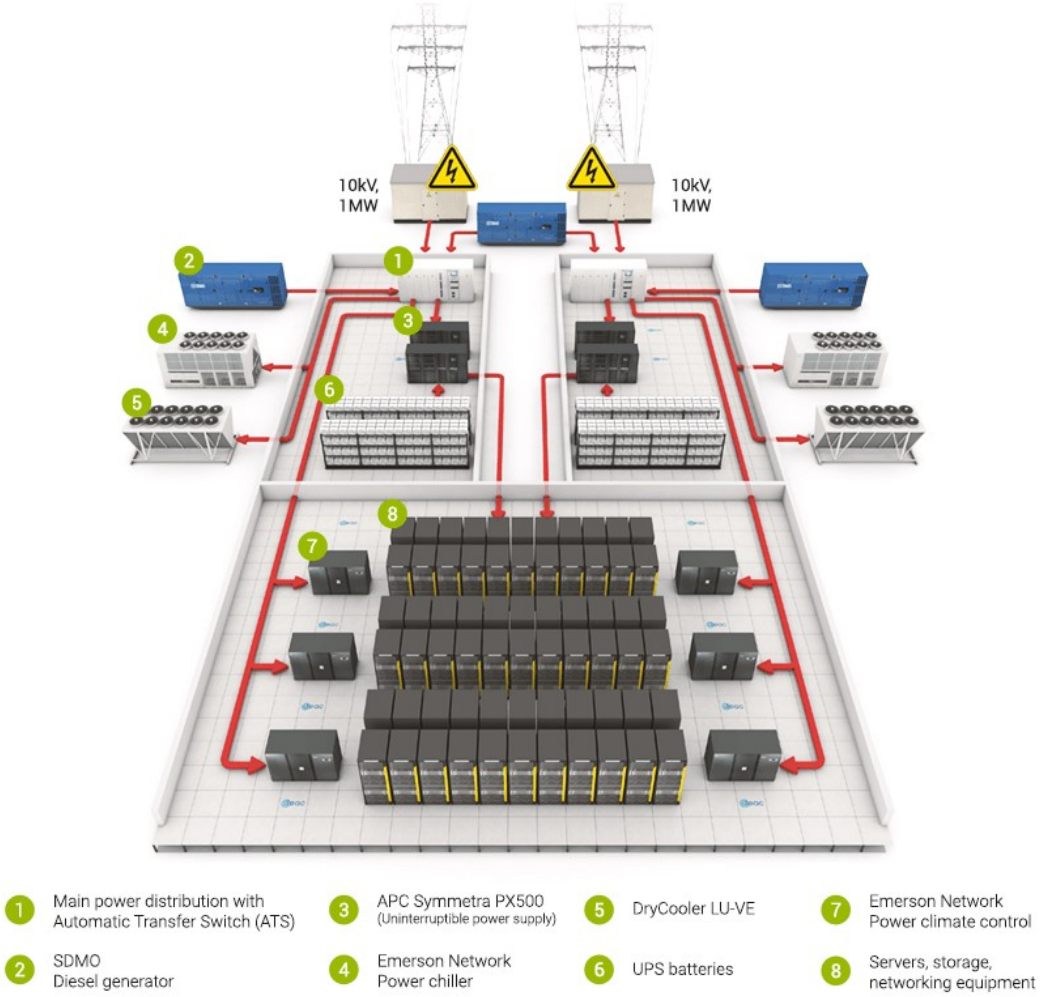
Problematiche principali di un data center

- Condizionamento dell'alimentazione elettrica
  - erogazione su almeno due linee indipendenti per ogni apparato



  - [illegible] la vita degli apparati
  - sistemi di continuità ad intervento istantaneo e di durata prolungata
    - motogeneratori → lunga durata, avviamento lento
    - batterie → intervento istantaneo, bassa capacità
- Consumi

https://www.thegreengrid.org/en/resources/library-and-tools/20-PUE:-A-Comprehensive-Examination-of-the-Metric



© deac.eu

Problematiche principali di un data center

- Connettività di rete
  - connessione tramite provider indipendenti
    - è comune per i datacenter principali avvalersi di oltre 10 carrier
    - spesso fungono da internet exchange

https://www.datacentermap.com/singapore/singapore/equinix-singapore_connectivity.html

https://www.datacentermap.com/usa/california/los-angeles/one-wilshire_connectivity.html

https://www.datacentermap.com/united-kingdom/london/telehouse-london-north_connectivity.html

  - collocazione fisica dei cavi su percorsi indipendenti

https://www.datacenterdynamics.com/en/news/google-cloud-us-east1-data-centers-disrupted-due-physical-damage-multiple-fiber-bundles/

- Alta disponibilità
  - fatto tutto quanto detto sopra, il sistema di calcolo deve essere ridondante e resistente a guasti – ne parlerete più avanti

On premises - messa in sicurezza fisica

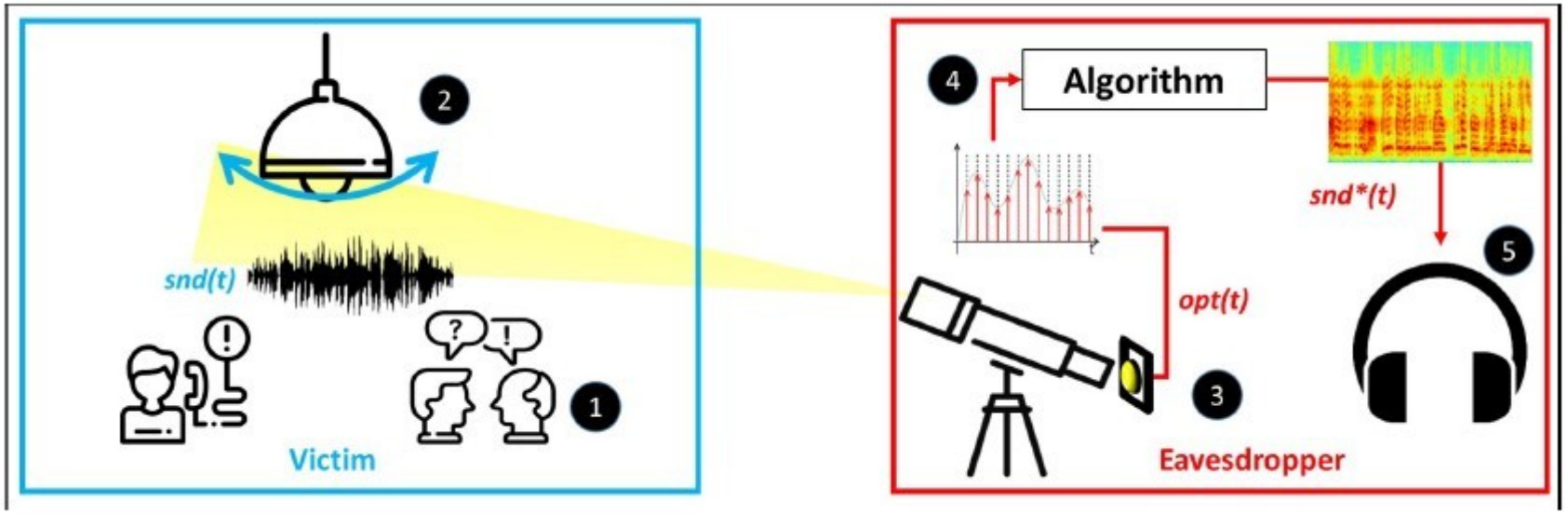
- Un server è prima di tutto un sistema di calcolo, collocato in un ambiente e connesso a una varietà di dispositivi
  - Normalmente si concentrano le difese sul fronte degli attacchi via rete, a componenti software come applicazioni e sistema operativo
  - Le corrispondenti contromisure possono facilmente essere scavalcate da un attaccante con accesso fisico al sistema!
  - Le minacce principali sono:
    - Furto dello storage o dell'intero calcolatore
    - Connessione di sistemi di raccolta dati alle interfacce
    - Avvio del sistema con un sistema operativo arbitrario
  - La gravità di queste minacce dipende fortemante dallo specifico ambiente
- Molti di questi problemi sono cambiati nello scenario sempre più comune di virtualizzazione sul Cloud, ma altri concettualmente simili sono apparsi, e la logica delle stesse contromisure si può adattare

Alcune vulnerabilità sfruttabili in presenza

- BadUSB e simili
  https://threatpost.com/badusb-attack-code-publicly-disclosed/108663/
- Thunderspy
  https://thunderspy.io/
- Keylogging e videoghosting
  https://www.keelog.com/
- Key injection
  https://www.blackhillsinfosec.com/executing-keyboard-injection-attacks/
- Disk un/plugging
  https://www.blackhat.com/docs/eu-15/materials/eu-15-Boteanu-Bypassing-Self-Encrypting-Drives-SED-In-Enterprise-Environments-wp.pdf
- Power glitching
  https://www.darkreading.com/edge/theedge/glitching-the-hardware-attack-that-can-disrupt-secure-software-/b/d-id/1336119
- Gruppo di ricerca su Air Gap Jumping (key points)
- Insicuro a casa: sicurezza vs comodità

Furto di dati con canali fisici

- Non solo dati digitali, ma non per questo meno importanti
  - Rilevazione ottica di onde sonore: Lamphone
    https://www.nassiben.com/lamphone



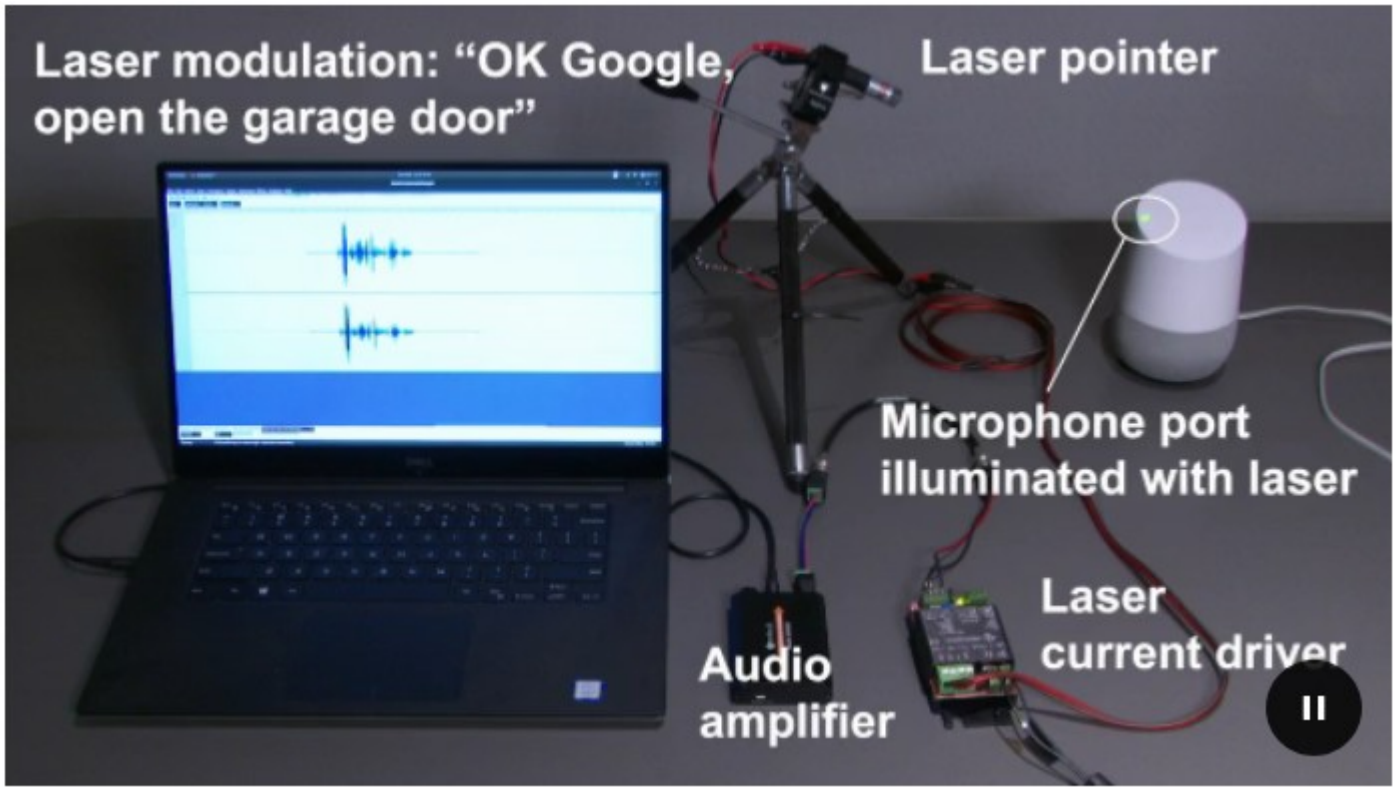
  - Giroscopio /accelerometro in uno smartphone usato per identificare parlato o digitazione su tastiera nelle vicinanze

    https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/michalevsky

    https://www.innovations-report.com//html/reports/information-technology/georgia-tech-turns-iphone-spiphone-184116.html

Iniezione di comandi vocali con un raggio laser

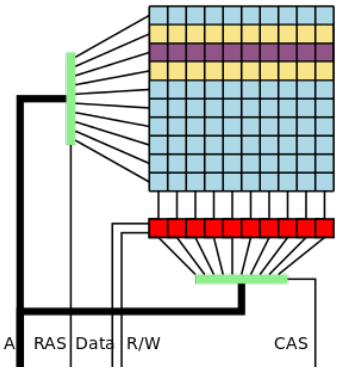
https://www.wired.com/story/lasers-hack-amazon-echo-google-home/



Esfiltrazione di dati con canali fisici

- (estremamente semplificato)
- Power analysis
  - se il dispositivo non è opportunamente isolato, osservando il consumo si possono dedurre dati sensibili
- Timing analysis
  - se si codificano i programmi in modo “banale”, osservando il tempo impiegato da certe operazioni si possono dedurre dati sensibili
- Emissioni elettromagnetiche
  - tastiere, monitor, ecc... si comportano come antenne
  - https://en.wikipedia.org/wiki/Tempest_(codename)

Dispositivi vulnerabili



- Meltdown
  - praticamente tutti le CPU Intel, forse AMD e ARM
  - accesso alla memoria protetta del sistema operativo
  - https://meltdownattack.com/#faq-systems-meltdown
- Spectre
  - praticamente tutte le CPU da computer e da smartphone
  - accesso alla memoria di altri processi del sistema
  - https://meltdownattack.com/#faq-systems-spectre
- Power glitching
  - si può indurre un comportamento illecito in un componente “giocando” con la tensione di alimentazione
- Rowhammer
  - si può cambiare il contenuto della memoria di un altro processo se il processo dell’attaccante occupa zone fisicamente adiacenti

Il computer e le applicazioni

- Una volta curata la sicurezza fisica garantendo
  - che i componenti non possano essere rubati, distrutti, sostituiti con equivalenti malevoli
  - che non possano essere installati componenti aggiuntivi malevoli
  - che non esistano canali fisici o di rete per intervenire sulle comunicazioni
- Dobbiamo garantire che il software che gira sul computer
  - sia esattamente quello che vogliamo
  - funzioni correttamente
- Vediamo qualche esempio di come fare, e qualche controesempio di vulnerabilità

Attacchi fisici alle risorse logiche

- Per andare a regime il sistema attraversa un processo di boot, che può essere diviso in queste fasi:
  (1) BIOS – Individua i dispositivi di possibile caricamento del boot loader e l'ordine per esaminarli
    - Molti BIOS prevedono la possibilità di proteggere con password l'avvio o la modifica della configurazione
  (2) Boot Loader – Sceglie il sistema operativo e gli passa eventuali parametri
    - Gestione della "maintenance mode"
    - Stesso tipo di protezione con password come descritto per BIOS
  (3) Sistema opeativo – carica i device driver (da non sottostimare) e avvia il processo *init*
  (4) *init* – gestisce i *runlevel* o i *target* per coordinare l'inizializzazione del sistema, cioè avviare i servizi nell'ordine corretto
- Ognuna di queste fasi potrebbe essere dirottata da un attaccante con accesso fisico, per far caricare software malevolo

Sicurezza del processo di boot

- Problema: come assicurarsi che ogni componente software eseguito da un computer sia autentico, integro e benevolo?
  - Anti-malware verificano le applicazioni
  - Chi verifica gli anti-malware?? Il S.O. (idealmente rendendo AM inutile)
  - Chi verifica il S.O.? Il boot loader potrebbe
  - Chi verifica il boot loader? Il BIOS potrebbe, specialmente se assistito da HW speciale, che non possa essere modificato dal S.O., e quindi sia immune da infezioni

    → *hardware root of (a chain of) trust*

    https://medium.com/@martin_24447/trusted-boot-b1ae7e6d2890

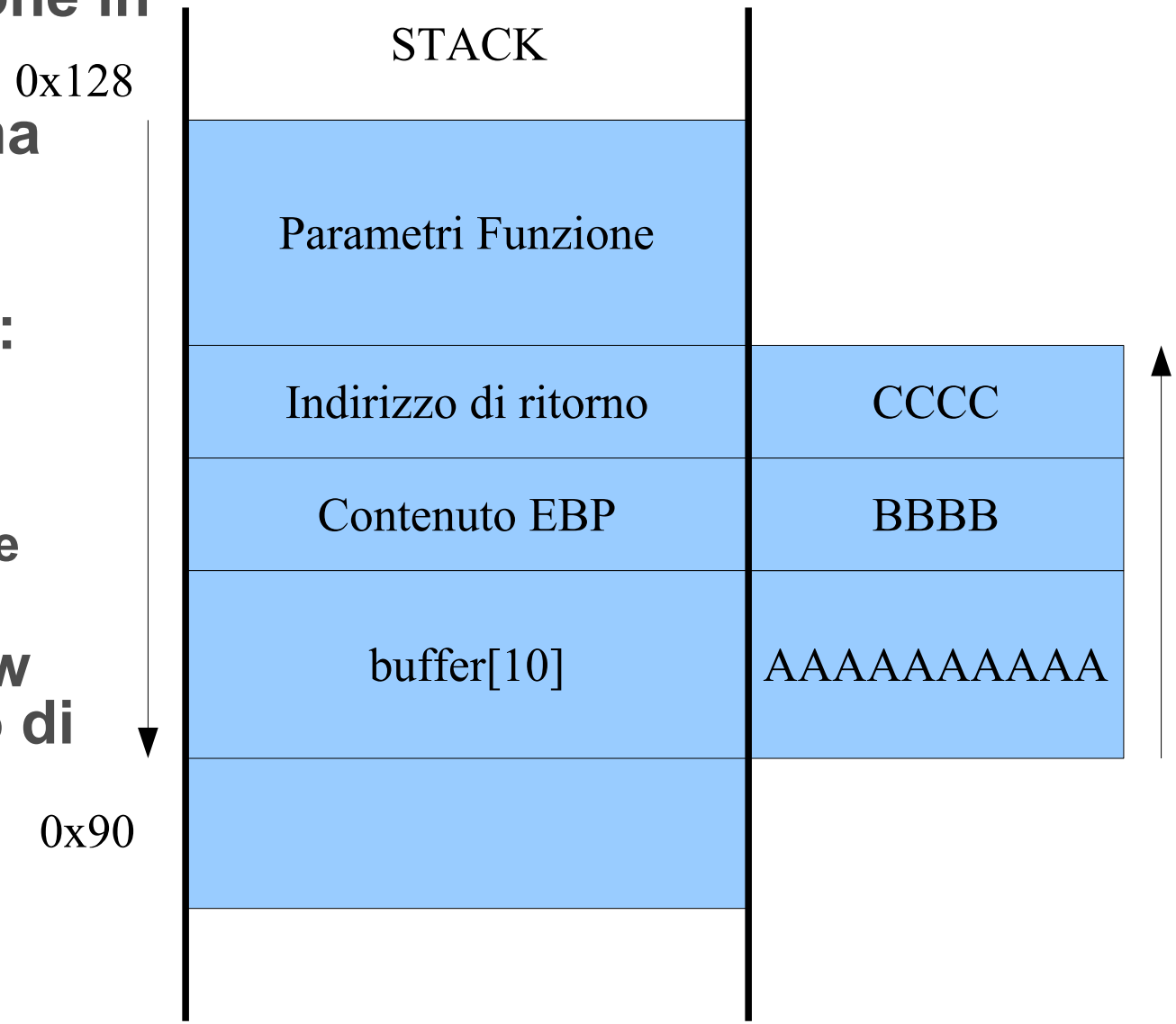
    https://dl.acm.org/doi/pdf/10.1145/3380774.3382016

Measured / Trusted / Secure Boot

- *Measured Boot* si riferisce a un processo generale, che tipicamente usa un TPM come hardware root of trust
  - TPM = Trusted Platform Module: chip con funzionalità crittografiche
    - fa parte delle specifiche del *Trusted Computing Group* https://trustedcomputinggroup.org/
  - M.B. non definisce come prevenire un avvio malevolo
- *Trusted Boot* è un processo che usa gli strumenti del M. B. e riesce a bloccare il boot non appena individua un componente non fidato
- *Secure Boot* è il nome specifico dato all'implementazione di trusted boot basata su UEFI
  - UEFI = Unified Extensible Firmware Interface http://www.uefi.org/
  - Implementazione Software + chiavi in firmware
  - Serve un BIOS standard per la fase di POST
  - Può avvalersi del TPM per velocizzare e migliorare i controlli di integrità

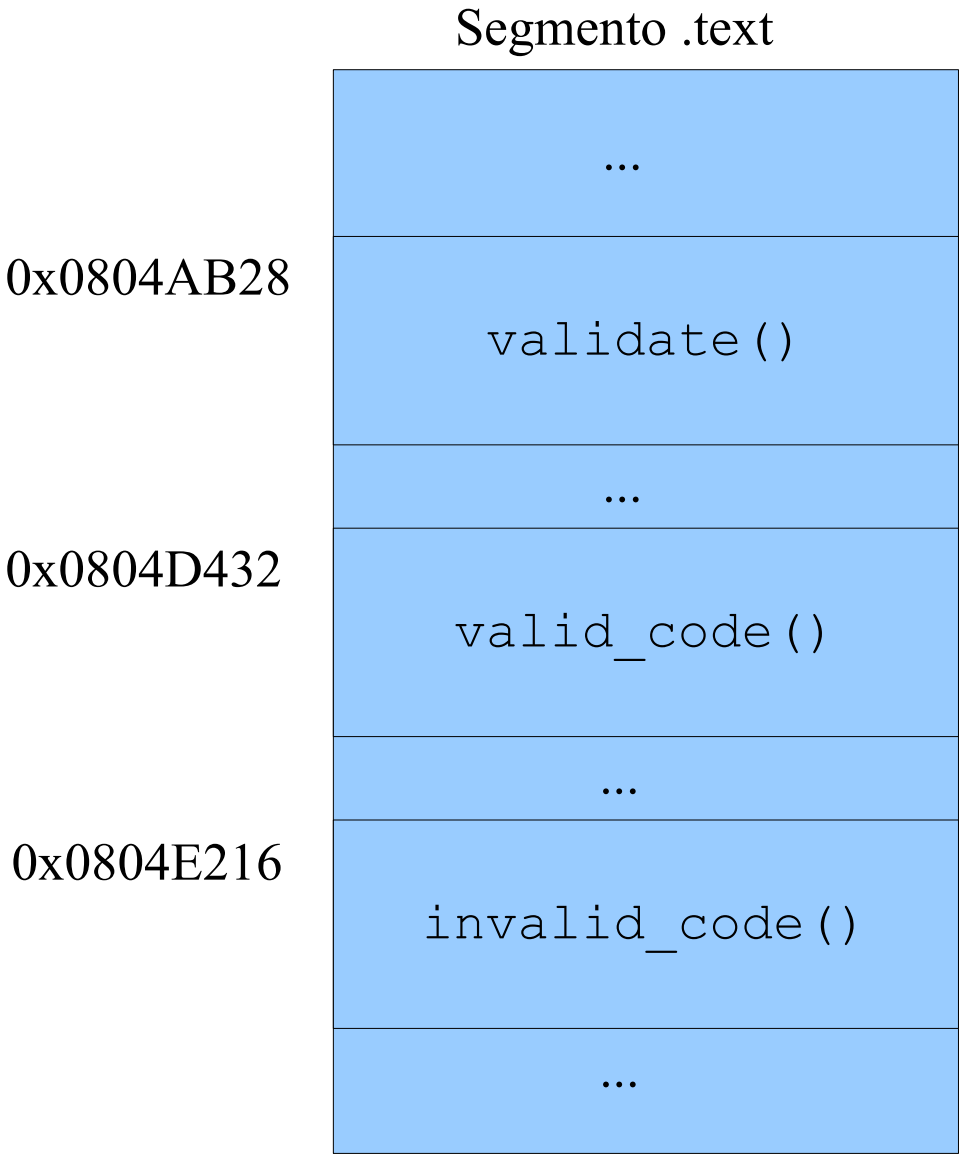
Vulnerabilità del codice nativo: stack overflow

- Esempio di disposizione in memoria.
- L'attaccante scrive una stringa lunga più del dovuto
- Nell'esempio di prima:
  - 10 Byte di padding
  - 4 byte per coprire EBP
  - 4 byte per sovrascrivere l'indirizzo di ritorno
- Si noti come l'overflow sovrascriva l'indirizzo di ritorno.



Stringa: "AAAAAAAAAABBBBCCCC"

Vulnerabilità del codice nativo: stack overflow



- L'obiettivo di un attaccante, che non ha le credenziali adatte a fare in modo che `validate` ritorni 1, è di forzare l'esecuzione del codice di `valid_code`
- `validate` utilizza la funzione `gets` per ottenere la password
- La `gets` è non sicura
- In tali condizioni un attacco di stack overflow è molto semplice

Vulnerabilità del codice nativo: stack overflow

- Nel momento in cui `validate` richiede l'input all'utente l'attaccante prepara una stringa così composta
  - 10 byte di padding
  - 4 byte per "scavalcare" l'EBP
  - 4 byte per scrivere l'indirizzo di `valid_code`: 0x0804D432
- Quando `validate` eseguirà la `RET`, invece che tornare al chiamante, salterà a `valid_code`

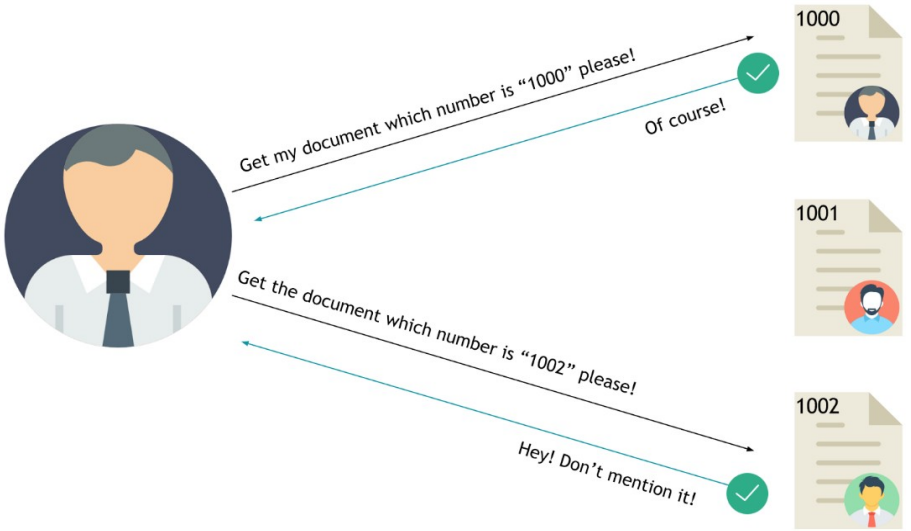
E' necessario tradurre l'indirizzo di `valid_code` nella sua rappresentazione ASCII.
Il risultato comprende anche caratteri non stampabili.
Esistono varie tecniche per passare al processo tali caratteri (ad es. printf di bash).

Stringa d'attacco: "AAAAAAAAAAABBBB\x32\xD4\x04\x08"

L'indirizzo è fornito con i byte in ordine inverso:
l'architettura IA32 è infatti **little endian**

Vulnerabilità di applicazioni web: IDOR

- Insecure Direct Object Reference
  - oggetto erogato semplicemente perché si sa come si chiama
- Mitigazioni
  - non esporre mai dati direttamente dal server web
  - eventualmente, per alleggerire, creare mappature effimere e con id non prevedibili (hash)
  - usare funzioni che implementino AAA ad ogni richiesta



`https://www.example.com/login.php`
- login come user, redirect a

`https://www.example.com/userapp.php`
- riscrittura a mano

`https://www.example.com/adminapp.php`
- funzionalità di amministrazione!

```
https://www.example.com/fileop.php?
f=a.txt&action=backup

https://www.example.com/fileop.php?
f=a.txt&action=delete
```

Vulnerabilità di applicazioni web: file disclosure

- File Disclosure
  - a metà strada tra Injection e Broken access control
  - un caso particolare di IDOR in cui l'oggetto è un elemento del filesystem; caso classico: path traversal

- Variante sull'esempio di injection

```
Show the document: <input type=text name="doc">
```

  - lato server sanifico l'input, bloccando i caratteri di combinazione dei comandi shell (`;` `&` `&&` `||` ...)

```
<?php shell_exec("cat ".$VerifiedHome."/".$_GET["doc"]) ?>
```

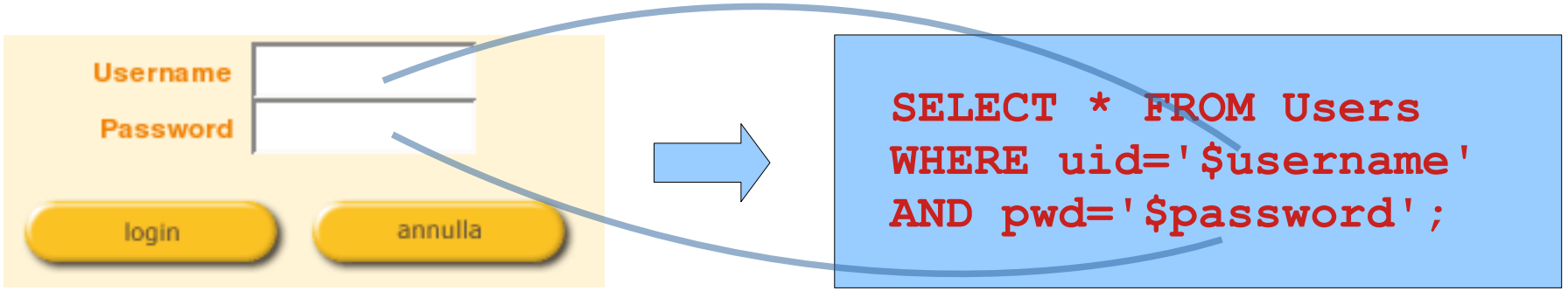
  - ma se lascio liberi i caratteri validi per i path

```
doc =  ../../../../etc/passwd
```

⇓

```
cat /home/maybe/deep/username/../../../../etc/passwd
```

Vulnerabilità di applicazioni web: SQL injection



user: `admin` password: `' OR 'a'='a`

⇒ query:
```
SELECT * FROM Users
WHERE uid='admin' AND pwd='' OR 'a'='a';
```

user: ` ` password: `'; DROP DATABASE WebApp; --`

⇒ query:
```
SELECT * FROM Users WHERE uid='' AND pwd='';
DROP DATABASE WebApp; --';
```

Innumerevoli esempi: SQL injection cheat sheet
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/

Vulnerabilità di applicazioni web: XSS (cross-site scripting)

- Una URL con uso apparentemente lecito di un parametro per personalizzare una pagina di benvenuto

```
http://www.yourdomain.com/welcomedir/welcomepage.php?name=John
```

- Il codice vulnerabile lato server (non sanifica il parametro)

```
<?php
    echo 'Welcome to our site ' . stripslashes($_GET['name']);
?>
```

- L'URL preparata dall'attaccante, su cui l'utente viene portato a cliccare

```
http://www.yourdomain.com/welcomedir/welcomepage.php?name=
<script language=javascript>alert('Hijacked!');</script>
```

- Il codice HTML ricevuto dal browser

```
Welcome to our site
<script language=javascript>alert('Hijacked!');</script>
```

- Do try this at home

```
http://php.testsparker.com/products.php?pro=url"></script><script>alert("xss")</script><!--"
```

Componenti di libreria vulnerabili

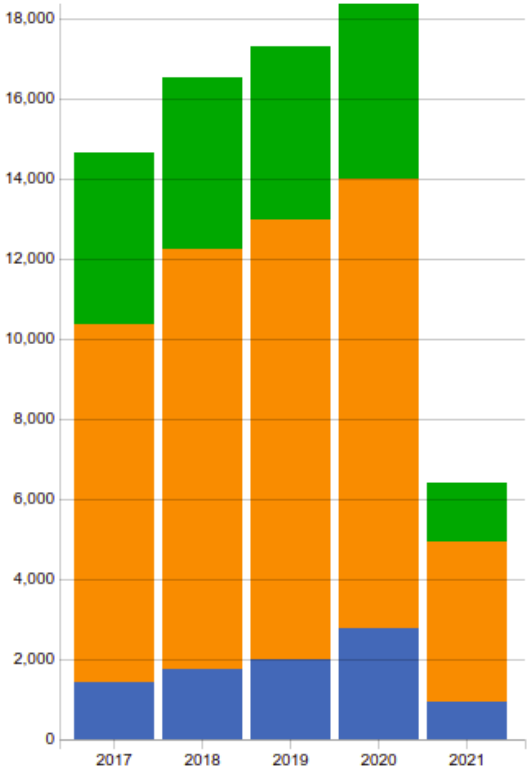
- Si spiega da sé
- Esempi famosi:

Heartbleed
CVE-2014-0160
(OpenSSL)

ShellShock
CVE-2014-6271
(Bash)

GHOST
CVE-2015-0235
(Linux)

DROWN
CVE-2016-0800
(OpenSSL)



- Impatto potenziale: qualsiasi
  - RCE, violazioni AAA, ...
- Stare aggiornati è difficile
  - Sempre più componenti
  - Sempre più complessi

  ... ma necessario
  - https://vulnerability-watch.connettiva.eu/

Vulnerabilità derivanti da configurazione errata

- Anche il sistema progettato e realizzato alla perfezione va configurato
- Errori tipici
  - permessi troppo generosi
    - dati leggibili o addirittura modificabili da utenti che non sarebbero autorizzati
    - possibilità per utenti con privilegi limitati di acquisire poteri superiori
  - esposizione eccessiva
    - programmi installati o addirittura in esecuzione anche se non servono: l'utente legittimo non se ne cura, l'attaccante può sfruttarne le vulnerabilità
    - processi che espongono più dati dello stretto necessario, facilitando la vita a chi raccoglie informazioni utili per attaccarli
  - scelte deboli
    - sistemi che possono usare molti tipi di algoritmo e possono essere convinti a scegliere le varianti più facili da attaccare, che potrebbero essere disattivate in quanto obsolete
    - password semplici da indovinare