

Programmazione Sicura



Cenni storici e
Terminologia



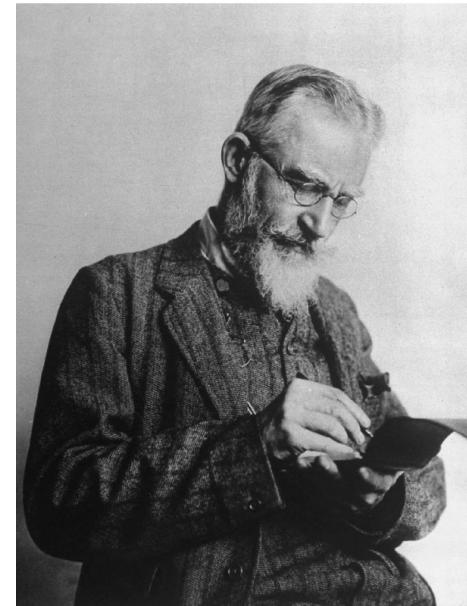
Barbara Masucci
UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA
DIPARTIMENTO DI ECCELLENZA



La storia insegna

"If history repeats itself, and
the unexpected always happens,
how incapable must Man be of
learning from experience"

George Bernard Shaw (1856 - 1950)
Scrittore, drammaturgo, linguista,
critico musicale



- Vediamo alcuni **eempi di incidenti** che si sono ripetuti negli anni
- Ciascun incidente mette in luce una **vulnerabilità** e ha comportato **conseguenze** di tipo diverso



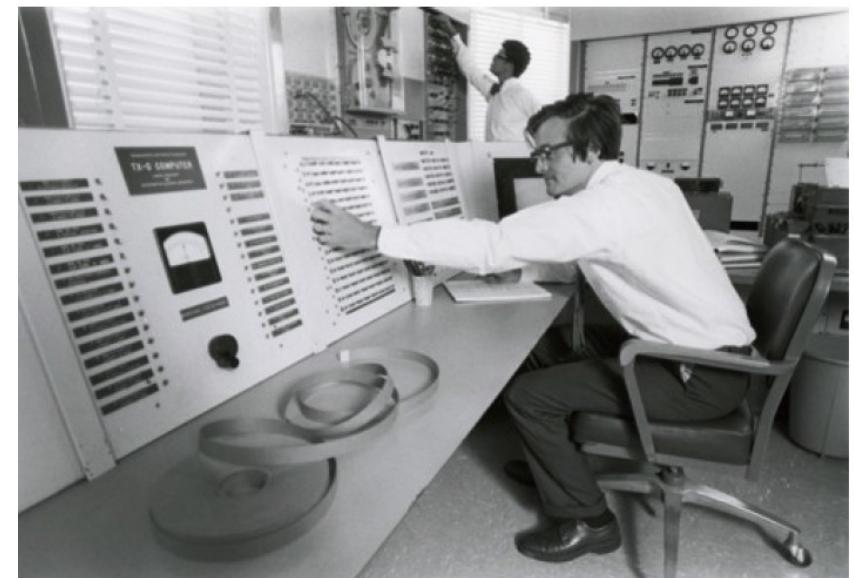
MIT Tech Model Railroad Club

- Nel 1945 nasce il **circolo di modellismo ferroviario** del MIT
 - Membri: professori e studenti del MIT
 - Passione condivisa: **capire a fondo la natura delle cose** e saperla controllare in modo creativo



MIT Tech Model Railroad Club

- Dopo un po' la passione dei membri del club si sposta dal modellismo ai computer
 - Molti dei membri del club rivestono un ruolo importante nella storia della Computer Science
 - Ad esempio, nel 1955 Alan Kotok progetta il **TX-0**, che si evolverà poi nel **PDP-1**, usato al MIT e ad Harward



Hacking

- L'attività dei membri del MIT Tech Railroad Club veniva indicata con il termine "**hacking**"
 - Esplorare i dettagli dei sistemi informatici e i modi con cui estenderne le capacità, contrariamente alla maggioranza degli utenti, che impara solo lo stretto necessario (*Guy L. Steele, et al., The Hacker's Dictionary*)
- Più recentemente, soprattutto dai media, il termine è usato con **accezione negativa**
 - Infrangere sistemi informatici
 - Rendere inutilizzabili risorse
 - Rubare e divulgare dati sensibili



Hacker

Classificazione

Cracker: programmati specializzati nell'infrangere sistemi di sicurezza per sottrarre o distruggere dati

Script Kiddie: cracker che adoperano script scritti da altri, non essendo in grado di produrli da sè

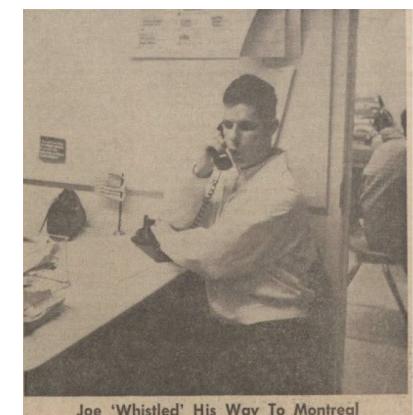
Phracher: rubano programmi che offrono servizi telefonici gratuiti o penetrano computer e database di società telefoniche

Phreaker: utilizzano informazioni telefoniche (numeri telefonici, carte telefoniche,...) per accedere ad altri computer



Phone Phreaking

- Nel 1956 un bambino di 8 anni non vedente e dotato di orecchio assoluto, Josef Carl Engressia, scopre **come attivare gli switch telefonici di AT &T** riproducendo un suono alla frequenza di 2600 Hz
- Diventato poi studente universitario e soprannominato "**whistler**" per questa sua caratteristica, vende ai compagni la possibilità di fare long distance call a \$1 ciascuna...
- Conseguenza: viene incriminato per frode...



War dialing

- Nel 1963 viene descritta nel giornale degli studenti del MIT un **utilizzo illecito** del sistema **PDP-1** di Harward
- Connessione del PDP-1 alla rete telefonica per effettuare **war dialing** allo scopo di fare telefonate gratis
- Conseguenza: bolletta astronomica per Harward



Services curtailed

Telephone hackers active

By Henry Lichstein

Many telephone services have been curtailed because of so-called hackers, according to Professor Carlton Tucker, administrator of the Institute phone system to many areas without a prorata charge. Among the tie-lines discovered have been ones to the Millstone Radar Facility, the Sudbury defense installation, IBM in Kingston, New York, and the MITRE Corporation.

Stating "It means the students who are doing this are depriving the rest of you of privileges you otherwise might have," Prof. Tucker noted that two or three students are expelled each year for abuses on the phone system.

The hackers have accomplished such things as tying up all the tie-lines between Harvard and MIT, or making long-distance calls by charging them to a local radar installation. One method involved connecting the PDP-1 computer to the phone system to search the lines until a dial tone, indicating an outside line, was found.

Tie lines connect MIT's phone

Commenting on these incidents, Prof. Tucker said "If any of these people are caught (by the telephone company) they are liable to be put in jail. I try to warn them and protect them."

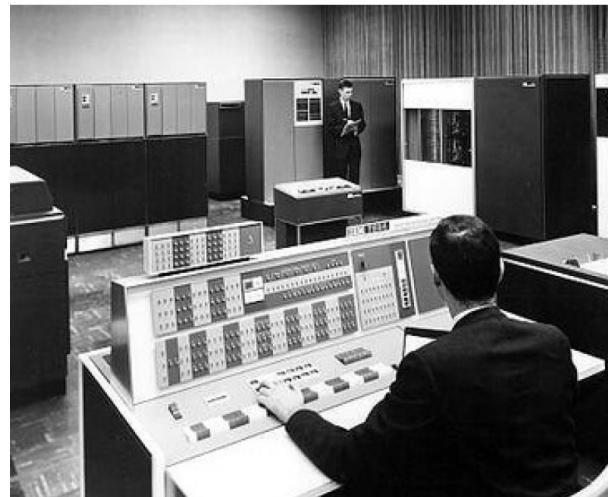
While Tucker felt "we don't have too much trouble with the boys; we appreciate their curiosity," he also said that repeated involvement, for instance, caused the expulsion from the Institute of one member of the Class of '63 one week before his graduation.

Because of the "hacking", the majority of the MIT phones are "trapped". They are set up so tie-line calls may not be made. Originally, these tie-lines were open to general use.

Next The Tech

Divulgazione della prima vulnerabilità

- Nel 1965 David Matthews del MIT scopre un **difetto** nel SO CTSS (Compatible Time Sharing System) su un **IBM 7094**
 - In particolari condizioni (due utenti che editano file nella stessa directory) il messaggio di welcome del sistema viene scambiato con **il file delle password ad ogni login!**
 - La vulnerabilità viene resa nota



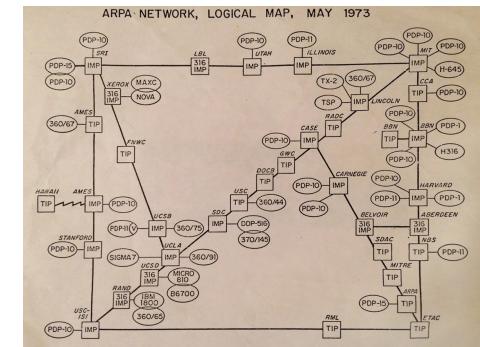
Phone Phreaking

- Nel 1971 John Draper
 - Scopre che un fischietto giocattolo contenuto nelle scatole di cereali **Captain Crunch** riproduce una frequenza che consente di effettuare telefonate gratis
 - Crea una Blue Box per il **phone phreaking** e in seguito viene arrestato



Da Creeper a Reaper

- Nel 1971 Bob Thomas crea il primo programma in grado di muoversi su ARPANET: **Creeper**
 - Scritto in assembly **PDP-10**, Creeper passa da una macchina all'altra lasciando il messaggio **I'm the Creeper: catch me if you can**

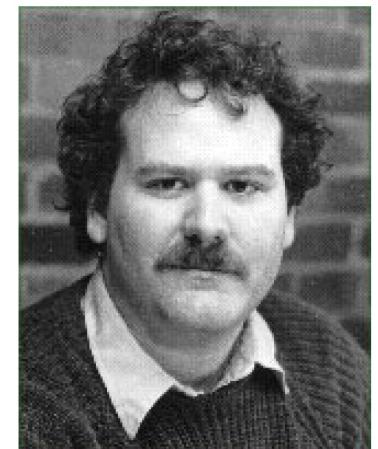
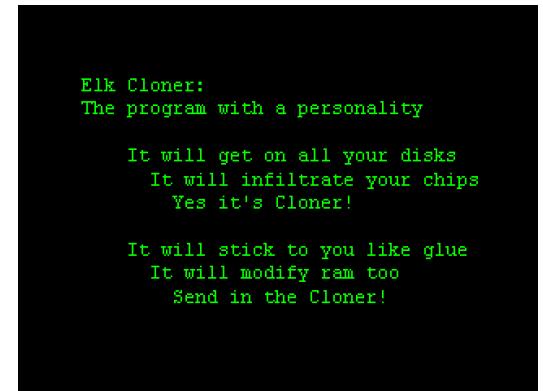


```
BBN-TENEX 1.25, BBN EXEC 1.30
@FULL
@LOGIN RT
JOB 3 ON TTY12 08-APR-72
YOU HAVE A MESSAGE
@SYSTAT
UP 8513319 3 JOBS
LOAD AV 3.87 2.95 2.14
JOB TTY USER SUBSYS
1 DET SYSTEM NETSER
2 DET SYSTEM TIPSER
3 12 RT EXEC
@
I'M THE CREEPER : CATCH ME IF YOU CAN
```



Virus

- Nel 1981 Richard Skrenta crea il primo virus a larga diffusione: **Elk Cloner**
 - Il programma si diffonde tramite floppy disk ed infetta il sistema operativo **Apple II**
 - Attaccato ad un gioco, si attiva alla sua 50-esima esecuzione e mostra un messaggio a video
- Il termine “virus” viene introdotto più tardi
 - Fred Cohen,
Computer Viruses: Theory and Experiments, 1984



Brain

➤ Nel 1986 appare il primo virus per **PC IBM-compatibili**:
Brain

- Creato dai fratelli pakistani Basit e Amjad Farooq Alvi per sperimentare i rischi dell'utilizzo della rete
- Infetta il Boot Sector dei floppy disk
- Provoca rallentamenti al sistema e intasa la memoria
- Soprannominato "**influenza pakistana**"

Displacement	Hex codes	ASCII value
0000(0000)	FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 00 20	-0J04†•M0
0016(0010)	20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F	Welcome to
0032(0020)	20 74 68 65 20 44 75 6E 67 65 6F 6E 20 20 20 20	the Dungeon
0048(0030)	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0064(0040)	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0080(0050)	20 20 63 29 20 31 39 38 36 20 42 61 73 69 74 20	
0096(0060)	26 20 41 6D 6A 61 64 20 28 70 76 74 29 20 4C 74	(c) 1986 Basit
0112(0070)	64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20	& Amjad (put) Lt
0128(0080)	20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20	d
0144(0090)	53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49	BRAIN COMPUTER
0160(00A0)	5A 41 4D 20 42 4C 4F 43 4B 20 41 4C 4C 41 4D 41	SERVICES, 730 NI
0176(00B0)	20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20	ZAM BLOCK ALLAMA
0192(00C0)	20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F 52	.IQBAL TOWN
0208(00D0)	45 2D 50 41 4B 49 53 54 41 4E 2E 2E 50 48 4F 4E	LAHOR
0224(00E0)	45 20 3A 34 33 30 37 39 31 2C 34 34 33 32 34 3B	E-PAKISTAN, PHJN
0240(00F0)	2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20	E :430791,443248
		,280530.

Welcome to the Dungeon
(c) 1986 Basit & Amjad (pvt) Ltd.
BRAIN COMPUTER SERVICES
730 NIZAB BLOCK ALLAMA IQBAL TOWN
LAHORE-PAKISTAN
PHONE : 430791,443248,280530.
Beware of this VIRUS....
Contact us for vaccination..... \$#@%\$@!!



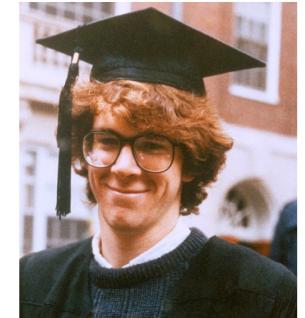
Vienna

- Il primo esempio di virus problematico appare nel 1987: **Vienna**
 - Dopo l'infezione nei sistemi MS-DOS, danneggia dati e distrugge file
- Per eliminarlo, Bernd Fix propone il **primo antivirus dedicato**



Il worm di Morris

- Il 2 Novembre 1988 Internet viene colpita dal **Worm di Morris**, uno studente della Cornell University
 - Il worm sfrutta bug del sistema operativo Unix per penetrare negli host attraverso la rete
 - In una sola ora rende inutilizzabili i computer di molti centri di ricerca, sovraccaricandoli con molteplici copie di sé stesso
 - Per bloccare il worm viene formato un team di esperti



CERT

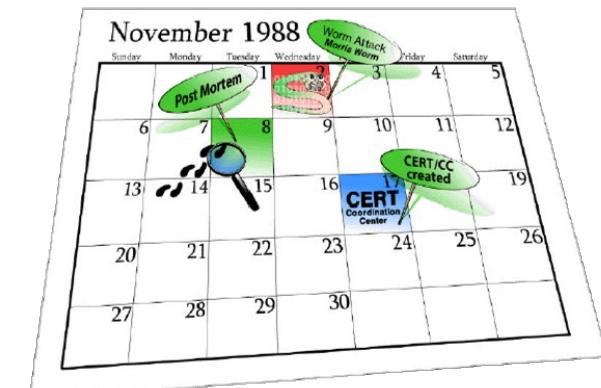
Computer Emergency Response Team

Team di esperti nell'ambito della sicurezza

- Creato dal DARPA (Defense Advanced Research Projects Agency) in seguito all'attacco del worm

Si occupa di

- Identificare il tipo di incidenti
- Quantificare le perdite economiche
- Analizzare le vulnerabilità dei prodotti



Ransomware

- Nel 1989 viene rilasciato AIDS, il primo **ransomware** della storia
 - Una volta installato, AIDS conta quante volte il PC viene riavviato
 - Al 90-mo riavvio, rende inaccessibili tutti i file e chiede un **riscatto** di \$189



Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue



Virus polimorfico

- Nel 1992 viene rilasciato 1260, il primo **virus polimorfico**
 - Il virus si riproduce cifrando il suo codice con una chiave diversa ogni volta
 - La chiave è conservata nel virus e serve per decifrare il codice
 - In tal modo la ricerca di signature note da parte degli antivirus è vana



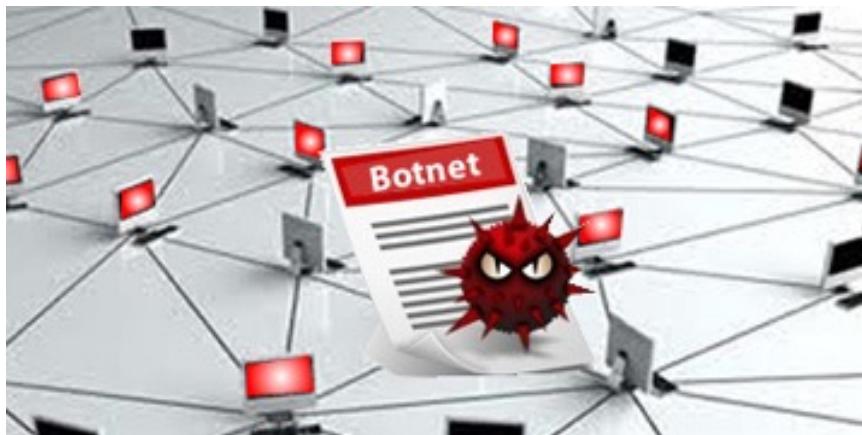
Macro Virus

- Nel 1999 viene rilasciato **Melissa**, il primo **macro virus**
 - Scritto come **macro** di applicazioni utente
 - Utilizza la **posta elettronica** e strumenti di **social engineering** per diffondersi
 - L'autore, David L. Smith, viene condannato a 10 anni di reclusione e a un multa di 5000 dollari
- Nel 2000 **I Love You** attacca 50 milioni di computer
 - Stesse modalità di diffusione di Melissa
 - Provoca danni per 5 miliardi di dollari
 - Due fratelli filippini, Irene e Onel de Guzmàñ sono ritenuti autori del virus ma non incriminati
 - Mancanza di leggi contro la scrittura di malware



Botnet

- Nel 2004 Jeanson James Ancheta costruisce la prima **botnet**
 - Insieme di dispositivi connessi ad Internet (controllati solitamente da un operatore maligno) che svolgono operazioni illegali
- Arrestato dall'FBI nel 2006, viene condannato a 5 anni di carcere



DDOS

- Nel 2007 l'Estonia subisce una serie di attacchi tramite Internet
- Gli attacchi, di tipologia **Distributed Denial Of Service**, colpiscono diversi obiettivi
 - Siti istituzionali
 - Banche
 - Televisioni
 - Giornali



Phishing

- Nel 2007 viene violato un sito interno al Pentagono
- La tecnica utilizzata (**phishing**) consiste nell'indurre le vittime a
 - Rivelare i propri dati confidenziali
 - Installare software malizioso



Password Leakage

- Nel 2012 la rete sociale LinkedIn viene violata da parte di cybercriminali russi
- **Trafugati 2,5 milioni di password** degli utenti
- Gli utenti lanciano una class action e ottengono un risarcimento globale di 1.25 milioni di dollari



Datagate

- Nel 2013 un dipendente della NSA, Edward Snowden, **trafuga e rende pubbliche** migliaia di informazioni confidenziali della NSA
- In particolare, dettagli di diversi **programmi di sorveglianza di massa** del governo statunitense e britannico
- Accusato di spionaggio e furto di proprietà governative, fugge in Russia, dove attualmente si nasconde
- Il caso Snowden ha messo in imbarazzo gli USA davanti al mondo intero



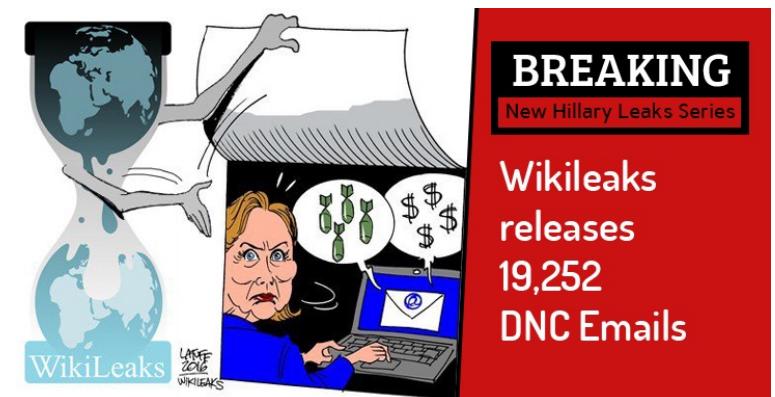
Data Leakage

- Nel 2015 il sito di incontri online **Ashley Madison** viene violato dal gruppo **Impact Team**
 - A urtare gli hacker, la promessa, non mantenuta di cancellazione sicura a 19\$ per utente
- I dati di **32 milioni di account** (credenziali, numeri di carta di credito, posizione GPS) rilasciati nel dark web



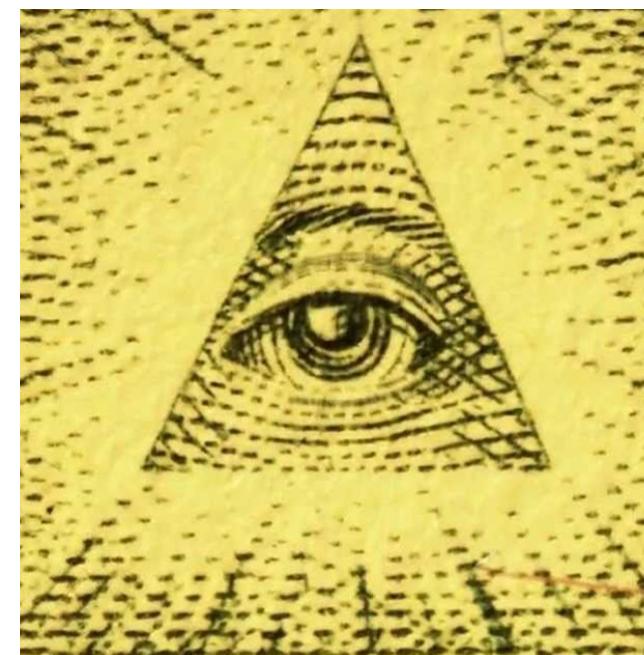
E-mail Leakage

- Nel 2016 **Wikileaks** pubblica **19252 e-mail** di persone affiliate al DNC (partito democratico negli USA)
- Contenuti
 - Interazioni del DNC con i media
 - Campagne di Clinton/Sanders
 - Finanziamenti
 - Informazioni sensibili
- Di conseguenza, 4 dirigenti del DNC si dimettono



Eye Pyramid

- Nel 2017 i due fratelli Giulio e Francesca Maria Occhionero vengono accusati di spionaggio
- Uso del software **Eye Pyramid** per monitorare dispositivi di politici, imprenditori, istituzioni e pubbliche amministrazioni



Incidenti nel 2019

- I danni causati da crimini informatici passano da 11,7 milioni di dollari del 2017 a **oltre 13 milioni di dollari** nel 2019
- Il **55% delle aziende** dichiara di aver subito un attacco relativo a
 - Furto di dati
 - Ransomware
 - Malware verso dispositivi mobili



Incidenti nel 2020

- Il **97% delle aziende** dichiara di aver subito un attacco relativo a furto di dati
 - Aumento di incidenti causato dalla pandemia
 - 630.000 incidenti solo nel primo semestre, di cui 160.000 classificati come 'critici'
 - 15 milioni di record di dati finiscono in vendita nel dark web



Incidenti nel 2021

- Il 2021, a causa della pandemia, è stato **un anno funesto** per la Sicurezza Informatica
 - Negli USA, gli attacchi a Colonial Pipeline, Kaseya, Twitch, lo spyware di Nso
 - In Italia, il data breach del sistema SORESA per i vaccini in Campania, l'attacco alla Regione Lazio, il commercio dei green pass falsi

"il 2021 è stato l'anno in cui ci siamo resi conto che i problemi che abbiamo scelto di non risolvere anni o decenni fa sono tornati uno dopo l'altro a perseguitarci".



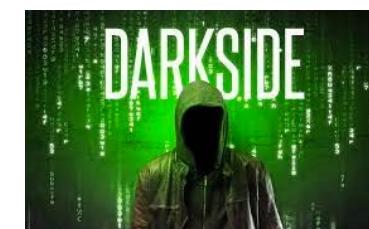
Colonial Pipeline

- Maggio 2021: Una delle più grandi interruzioni di infrastrutture critiche degli USA



- Un ransomware ha colpito la società che gestisce un oledotto che trasporta il carburante nella costa orientale degli USA

- Attacco ad opera della banda russa DarkSide
- L'azienda ha pagato un riscatto di 4 milioni di dollari in bitcoin

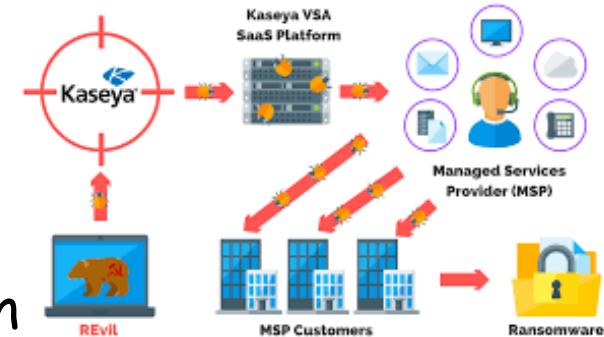


- Annunciata una taglia di 10 milioni di dollari sul gruppo



Kaseya

- Luglio 2021: Compromissione della società di software Kaseya
 - Sfruttata una falla nel sistema VSA
 - Infettati 1500 enti in tutto il mondo con un ransomware
- Attacco ad opera del gruppo REvil con sede in Russia
 - Chiesti riscatti da 45mila a 5 milioni di dollari
 - A Luglio 2021 Kaseya ha distribuito uno strumento per decifrare i file cifrati dal ransomware
 - A Ottobre 2021 uno dei presunti autori è stato arrestato



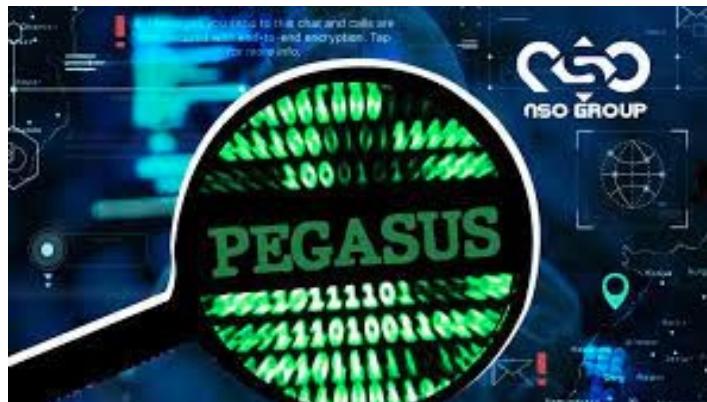
Twitch

- Ottobre 2021: Data leakage del servizio di streaming Twitch, di proprietà di Amazon
 - 128 GB di dati rubati, tra cui il codice sorgente del servizio
 - Incidente causato da un cambiamento di configurazione del server, che ha consentito un accesso non autorizzato



Nso

- Novembre 2021: Apple fa causa a Nso, società israeliana produttrice dello spyware Pegasus
 - Pegasus installato su dispositivi iOS e Android per spiare persone in tutto il mondo
 - Lo spyware oltre a leggere messaggi e immagini era in grado di attivare microfono e fotocamera dei dispositivi colpiti senza che l'utente potesse accorgersene



Log4Shell

- Dicembre 2021: Scoperta una vulnerabilità nella libreria open source Apache Log4j

 - Basata su Java, Log4J è molto utilizzata in ambito aziendale per la gestione dei file di log
 - Migliaia di server in tutto il mondo esposti ad attacchi semplici grazie all'exploit **Log4Shell**
 - Per infettare un server, basta modificare la stringa USER AGENT del proprio browser in modo malizioso
 - La vulnerabilità consente l'esecuzione di codice remoto sul server vittima



In Italia

➤ **Febbraio 2021:** Falla nei sistemi di prenotazione dei vaccini in Campania

➤ Esposti i dati sensibili dei vaccinati



➤ **Aprile 2021:** Attacco ransomware ai registri elettronici delle scuole

➤ Colpito il 40% delle scuole italiane



➤ **Agosto 2021:** Attacco ransomware alla Regione Lazio

➤ Bloccati tutti i servizi sanitari e amministrativi



In Italia

- Novembre 2021: Scoperta di un archivio contenente centinaia di green pass falsi ma validi
 - Adolf Hitler risulta vaccinato l'11 Luglio 2021 con il vaccino Johnson in un centro vaccinale francese...
 - In un forum, l'utente con nickname przedsiebiorca ha affermato di poter generare qualsiasi green pass al costo di 300 dollari l'uno



In Italia

- Dicembre 2021: Data leakage della società Sogin
 - Società di stato incaricata di smantellare le ex centrali nucleari e mettere in sicurezza i rifiuti radioattivi
 - 800 GB di dati rubati: password, documenti di appalti, contenuti privati, file e foto
- La refurtiva è stata messa in vendita su due forum in rete dall'utente con nickname zerox296
 - Chiesti 250000 dollari in criptovaluta Monero



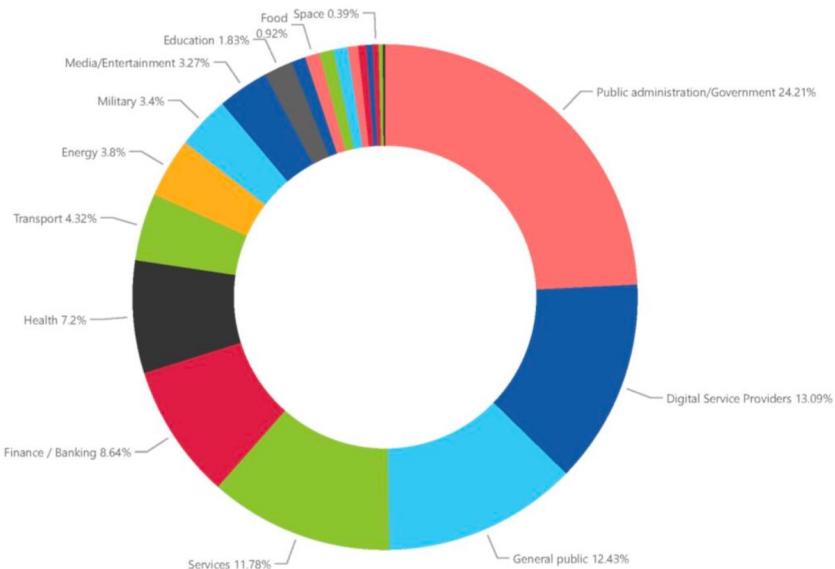
Incidenti nel 2022

- Se il 2021 è stato **un annus horribilis** per la Sicurezza Informatica...
il 2022 è stato addirittura peggiore!
- L'ENISA Threat Landscape ha evidenziato un aumento di
 - Ransomware
 - Malware
 - Attacchi di Social Engineering
 - Furto di dati
 - Denial of Service
 - Fake news



Incidenti nel 2022

- Obiettivi degli attacchi
 - Pubbliche amministrazioni
 - Digital Server Provider
 - Servizi pubblici e finanziari
 - Organizzazioni sanitarie
 - Trasporti
 - Settore militare
 - Istruzione e ricerca



Incidenti nel 2022

- **Febbraio 2022:** Estorsione digitale del gruppo Lapsus\$ contro Nvidia, Samsung e Microsoft
 - Arrestati a Londra 7 ragazzi tra 16 e 21 anni



- **Marzo 2022:** Attacco DDoS al Ministero della Difesa Ucraino



- **Maggio 2022:** Attacco ransomware al Costa Rica da parte del gruppo Conti
 - Emergenza nazionale



Incidenti nel 2022

➤ **Giugno 2022:** Attacco ransomware ai servizi sanitari nel Massachusetts, USA

➤ Colpiti due milioni di utenti



➤ **Luglio 2022:** Attacco a società di telecomunicazioni da parte di cybercriminali cinesi



➤ **Agosto 2022:** Furto di criptovalute da provider di servizi finanziari



Incidenti nel 2022

- Settembre 2022: Attacco a servizi di trasporto, UK
- Ottobre 2022: Attacchi DDoS a siti web di aeroporti USA
- Novembre 2022: Attacchi ad istituti di istruzione e ricerca in tutto il mondo

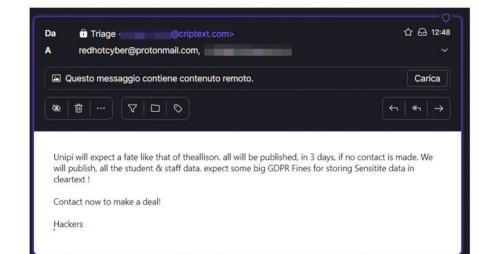


In Italia

- Gennaio 2022: Attacco malware alla Croce Rossa
- Marzo 2022: Attacco ransomware a Trenitalia, riconducibile ad hacker russi
- Giugno 2022: Attacco ransomware a UniPI ad opera del gruppo BlackCat
- Agosto 2022: Attacco ransomware alla ASL di Torino



Croce Rossa Italiana



Incidenti nel 2023

- Il trend del 2022 è proseguito nel 2023
 - Circa **3000** incidenti riportati, con un incremento del **12%** rispetto al 2022

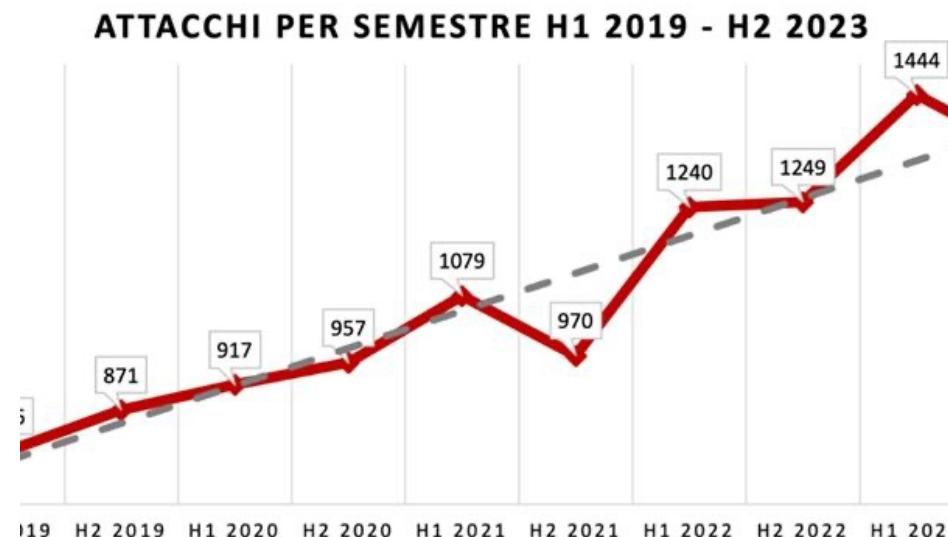
“

L'Italia rimane maglia nera per quanto riguarda la sicurezza informatica. Nel primo semestre del 2023 gli attacchi cyber in Italia sono cresciuti del 40% rispetto allo stesso periodo dell'anno precedente. Tutti i dati del rapporto Clusit 2023.



Incidenti nel 2023

- Secondo un report del CLUSIT
 - In media, 232 attacchi al mese
 - 81% degli attacchi classificati di "gravità elevata"
 - Di questi, l'11% degli attacchi ha preso di mira l'Italia

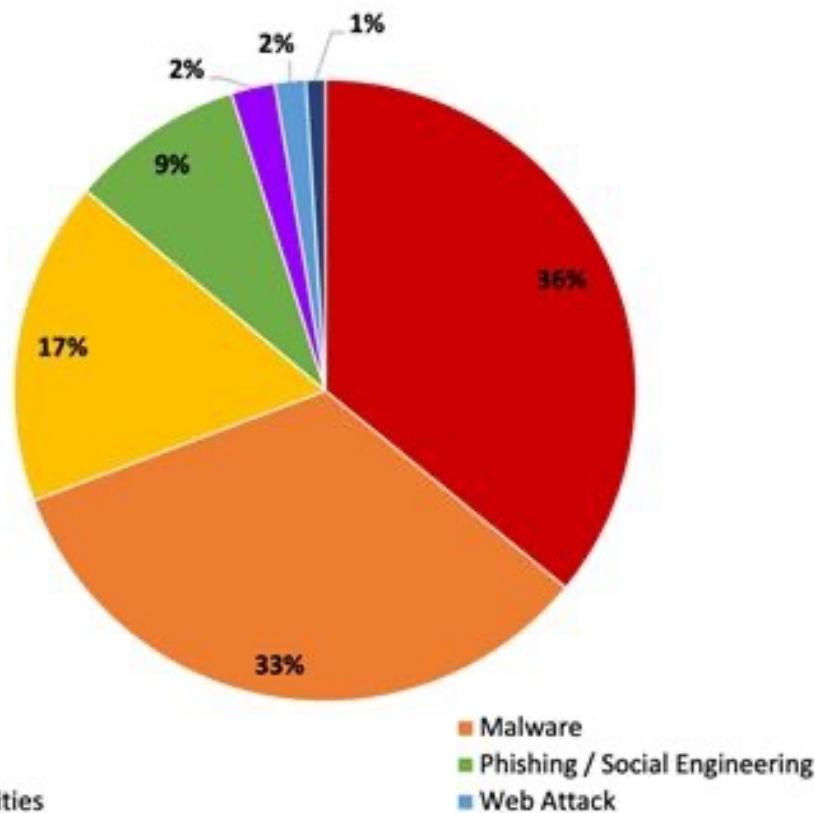


© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia



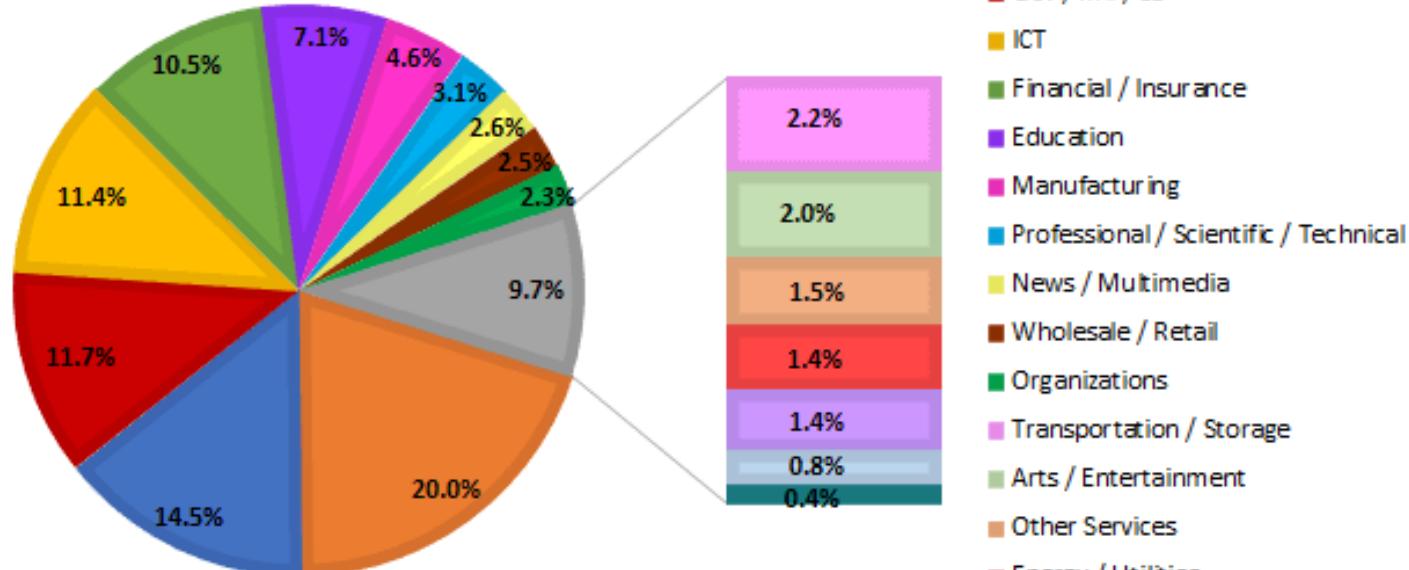
Incidenti nel 2023

Principali tecniche di attacco



Incidenti nel 2023

Obiettivi degli attacchi



E nel 2024?

- Con alta probabilità, il trend del 2023 non darà tregua neanche al 2024...
- I cyber-criminali continueranno a causare interruzioni nella vita delle persone e a seminare il panico





Lezioni apprese

- Il termine "hacking" ha cambiato radicalmente significato nel tempo
 - Da desiderio di manifestare la propria superiorità a complesso insieme di attività per ottenere un vantaggio economico o politico
- L'hacking in stile black hat finisce quasi sempre nello stesso modo
 - Una denuncia, un processo, una condanna penale
- Bisogna imparare a difendersi
 - Per farlo, è necessario capire come avvengono gli attacchi





Lezioni apprese

➤ Difendersi è più complesso rispetto ad attaccare

- All'attaccante può bastare una singola falla, ma il difensore deve individuare tutte le falle e ripararle
- L'attaccante può scegliere metodi e obiettivo dell'attacco, mentre il difensore deve adattarsi all'attaccante
- L'attaccante spesso è visto come un eroe se ha successo, mentre il difensore è visto come un perdente se fallisce
- L'attaccante conosce bene gli strumenti che usa, mentre il difensore può scontrarsi con tecniche mai viste prima



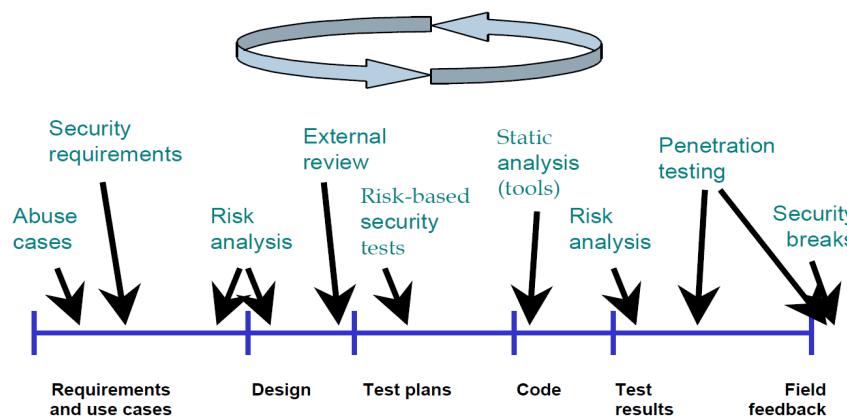
lessons
learned

Lezioni apprese

➤ Gli obiettivi di un attaccante sono molteplici

- Un apparato hardware
- Un software (sistema operativo, libreria, applicazione)
- Una procedura/algoritmo
- Una persona

➤ Il programmatore deve considerare minacce e obiettivi in tutto il ciclo di vita del software





Lezioni apprese

➤ La storia si ripete

- Gli errori commessi sono quasi sempre gli stessi
- Le risposte agli incidenti sono quasi sempre le stesse



- Il programmatore ha a sua disposizione una grande arma:
la storia...

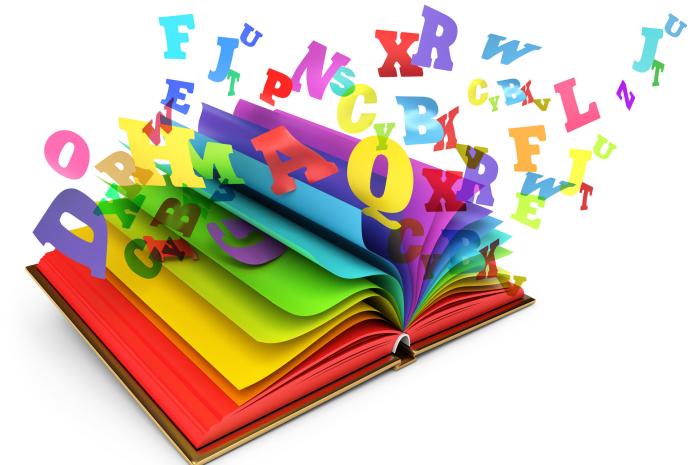
che gli insegna quello che NON deve fare



Terminologia

Introduciamo una serie di termini che saranno usati durante il corso

- Asset
- Minacce
- Attaccanti
- Bug, difetti, debolezze
- Vulnerabilità
- Exploit
- Vettore di attacco
- Politiche di sicurezza
- Analisi dei rischi
- Meccanismi di sicurezza



Asset

- Un **asset** è una entità generica che interagisce con il mondo circostante
- La natura dell'entità dipende dal contesto
 - Un edificio
 - Un dispositivo hardware
 - Un software
 - Un dato sensibile
 - Un algoritmo
 - Una procedura
 - Una persona



Asset

L'obiettivo di questo corso è la
Programmazione Sicura

Pertanto: asset = software



Asset e utenti

- Un utente può **interagire con un asset** in tre modi
 - Correttamente
 - Non correttamente, in modo involontario
 - Non correttamente, in modo malizioso

- Un **uso non corretto** di un asset può comportare rischi gravi, tra cui
 - Furto di dati sensibili, beni preziosi, denaro
 - Modifica o distruzione di informazioni sensibili
 - Compromissione di servizi



Minacce

- Una **minaccia (threat)** è una potenziale causa di incidente, risultante in un danno all'asset
- Le minacce possono tramutarsi in realtà in due modi
 - Accidentale
 - Doloso



Minacce

- Microsoft ha introdotto una classificazione possibile delle minacce: **STRIDE**
 - Spoofing (spacciarsi per un'altra entità)
 - Tampering (modificare le informazioni)
 - Repudiation (negare di aver eseguito un'azione)
 - Information Disclosure (divulgare informazioni)
 - Denial of Service (negare un servizio)
 - Elevation of Privilege (elevare i propri privilegi)



Attaccanti

➤ Un attaccante interagisce con l'asset

- In modo deliberato, malizioso, doloso
- Alla ricerca di un malfunzionamento sfruttabile
- Allo scopo di tramutare una minaccia in realtà
- Motivato dal conseguimento di un vantaggio



Attaccanti

➤ White hat (ethical hacker)

- Viola asset per fini non maliziosi
(stimare il livello di sicurezza)

➤ Black hat

- Viola asset per fini maliziosi o per tornaconto personale

➤ Gray hat

- Viola asset e, in cambio di denaro, si offre di irrobustirli



Attaccanti

➤ Hacktivist

- Viola asset per fini ideologici, politici, religiosi
- Svolge attività di cyber terrorismo e rende accessibili al pubblico documenti confidenziali



➤ Nation state

- Team di attaccanti sponsorizzati da una nazione



➤ Organized criminal gang

- Team di attaccanti che viola asset per profitti illegali



Bug, difetti, debolezze

- Un **bug** è un errore di implementazione dell'asset
- Una **difetto** è una deviazione dell'asset da requisiti e specifiche di progetto
- Una **debolezza** (weakness) è un difetto che potrebbe rendere reale una minaccia
 - Osservazione: un asset debole non è necessariamente compromesso
 - Deve poter essere raggiunto dall'attaccante e deve poter essere violato



FAULTY



Vulnerabilità

- Una **vulnerabilità** è una debolezza che un attaccante è in grado di usare per tramutare una minaccia in realtà
- E' la somma di tre fattori
 - Una debolezza esistente
 - L'accessibilità dell'attaccante alla debolezza
 - La capacità dell'attaccante di sfruttare la debolezza per conseguire un vantaggio



Exploit

- Un **exploit** è una procedura che
 - Sfrutta una vulnerabilità
 - Causa un comportamento inatteso in un asset
 - Permette di trasformare una minaccia in realtà



Vulnerability



Exploit



Payload



Asset e sicurezza

- Le funzionalità esposte da un asset implicano un **rischio di abuso**
- Esempi di abuso includono la violazione della triade **CIA**
 - **Confidentiality**
(impedire l'interazione in lettura tra un asset e un utente non autorizzato)
 - **Integrity**
(impedire l'interazione in scrittura tra un asset e un utente non autorizzato)
 - **Availability**
(rendere disponibili le funzioni di un asset a utenti esplicitamente autorizzati)



Asset e sicurezza

Nella triade **CIA**, qual è la proprietà più importante?

- L'**Integrity** è quasi sempre più importante della **Confidentiality**
 - Esempi: conto bancario, informazioni sanitarie, etc.
- L'**Availability** può essere addirittura di intralcio in alcuni scenari
 - La privacy di un utente può implicare la mancata disponibilità di informazioni e servizi a terzi



Vettore di attacco

- Un **vettore di attacco** è uno strumento qualsiasi attraverso il quale si può veicolare una vulnerabilità
 - Una connessione TCP verso un server
 - Una shell locale
 - Una linea telefonica incustodita
- La **superficie di attacco** di un asset è l'insieme di tutti i suoi vettori di attacco
 - Misura l'esposizione dell'asset agli attacchi



Politica di sicurezza

- Una **politica di sicurezza (security policy)** definisce in modo non ambiguo il livello di sicurezza di un asset
 - Che significa che "l'asset è sicuro"?
 - Da quale interazione ci si vuole difendere?
 - Da quali utenti ci si vuole difendere?
- La politica di sicurezza nasce spesso da **un'analisi dei rischi (risk analysis)** che cerca di identificare
 - Cosa potrà andare storto con l'asset
 - Quanto sarà probabile un incidente
 - Quanto costerà un incidente



Meccanismi di sicurezza

- Un **meccanismo di sicurezza** è uno strumento che consente di attuare una politica di sicurezza
- Ci sono tre diverse categorie
 - Meccanismi di **prevenzione**
(tendono ad impedire le interazioni tra un asset e un utente)
 - Meccanismi di **rilevazione**
(controllano le interazioni tra un asset e un utente)
 - Meccanismi di **reazione**
(per ripristinare il sistema in seguito ad un incidente)



Prevenzione

- Un asset soggetto a **prevenzione** non è in grado di interagire con nessuno
 - Aspetto positivo: non è attaccabile dai malintenzionati!
 - Aspetto negativo: non è utilizzabile neanche dagli utenti normali!
- E' necessario un **aumento dell'esposizione dell'asset** affinchè gli utenti possano fruirne
 - Apertura di porte TCP in un servizio di rete, piuttosto che disconnessione totale
 - Lettura di input in una applicazione locale, piuttosto che nessun input



Rilevazione

➤ Con l'aumento dell'esposizione aumentano anche i rischi



➤ I rischi vanno controllati con **meccanismi di rilevazione**

- Controllo del traffico sulle porte TCP aperte
- Controllo degli input passati a una funzione



Meccanismi di sicurezza

Operazioni tipiche dei meccanismi di sicurezza sono:

- **Autenticazione**

L'utente che si presenta all'asset è effettivamente chi dice di essere?

- **Controllo degli accessi**

L'utente ha i diritti per accedere all'asset?

- **Auditing**

Monitorare e registrare le interazioni di un utente con l'asset

- **Azione**

Svolgere azioni correttive per far rispettare la politica di sicurezza



Come opera un attaccante

Dalla minaccia all'esecuzione

