Polo Tecnico Professionale Galileo
I.T.I.S. Galileo Galilei
Il mondo della tecnologia

AESIR
ASSOCIAZIONE EX-STUDENTI
ITIS GALILEO GALILEI ROMA

CYBER SECURITY

consapevolezza e negligenza

"la cultura della sicurezza"

Roma, 28-30 gennaio 2020

ing. Giuseppe G. Zorzino
DPO, UNI11697, ERMCP, CISA, CISM, CGEIT, CRISC, LA27001, IA20001, S+, ...

Bio

Giuseppe Giovanni Zorzino

Consulente e docente di sicurezza delle informazioni, attualmente mi occupo di cyberstrategies, sistemi di gestione della sicurezza, governance e sicurezza delle informazioni nelle organizzazioni, privacy, compliance e awareness.

38+ anni di esperienza nell'IT e nell'analisi e sviluppo di basi di dati complesse.

20+ nell'IT security.

Accademia di Pozzuoli, Ufficiale del Corpo del Genio dell'A.M. (ret),
Coordinatore Cybersecurity del CESMA (Centro Studi Militari Aeronautici) "Giulio Douhet".

Membro della Comm. Sicurezza Informatica dell'Ordine degli Ingegneri di Roma, nonché
di ISACA, ERMAcademy, ISACA Rome Chapter, UNIDPO, ISC2 Italian Chapter, HERMES University

Vasta attività di divulgazione e formazione c/o enti pubblici e PMI.

2 brevetti.

Varie certificazioni attive: DPO UNI11697, ERMCP, CISA, CISM, CGEIT, CRISC, Security+, Lead Auditor ISO 27001, Lead Auditor ISO 20000-1, CMMI appr, MCSASec 2003, Certificatore etico, IBM Cert Solution Architect, IBM_Cert_Specialist, …

Obiettivi della conferenza

Al termine della conferenza i partecipanti saranno in grado di comprendere:

- cosa è la cyber security
- chi attacca e come
- Hackers – chi e quali conoscenze
- cosa fare per ridurre l'esposizione ai rischi + comuni

PREREQUISITI
Non sono richiesti prerequisiti specifici.

Sicurezza informatica (da Wikipedia)

La **sicurezza informatica** (in inglese *information security*) è l'insieme dei mezzi e delle tecnologie tesi alla protezione dei sistemi informatici in termini di *confidenzialità, integrità* e *disponibilità* dei beni o asset informatici.

Un sinonimo spesso usato è *cybersecurity*, termine che ne rappresenta una sottoclasse essendo quell'ambito della sicurezza informatica che dipende solo dalla tecnologia. Con esso si enfatizzano spesso qualità di *resilienza, robustezza* e *reattività* che una tecnologia deve possedere per fronteggiare attacchi mirati a comprometterne il suo corretto funzionamento e le sue performance (attacchi cyber).

https://it.wikipedia.org/wiki/Sicurezza_informatica

Cyber security???

- No security is perfect. Nessuno può prevedere ogni nuova tecnica di intrusione.
- Gli aggressori hanno continuato a evolversi, i loro obiettivi hanno continuato ad espandersi e le loro tecniche hanno continuato a cambiare.
- Mentre la sicurezza informatica diventa dominante, le organizzazioni dovrebbero considerare le violazioni dei dati sotto una nuova luce, non una fonte di paura e vergogna, ma una realtà aziendale. Dovrebbero anticipare e affrontare gli incidenti di sicurezza con fiducia.
- Tuttavia, con il giusto mix di tecnologia, intelligenza e competenza, le organizzazioni possono iniziare a colmare il divario di sicurezza. Possono adattarsi per stare al passo con nuove minacce, nuovi strumenti e nuovi modi intelligenti di compromettere le reti.

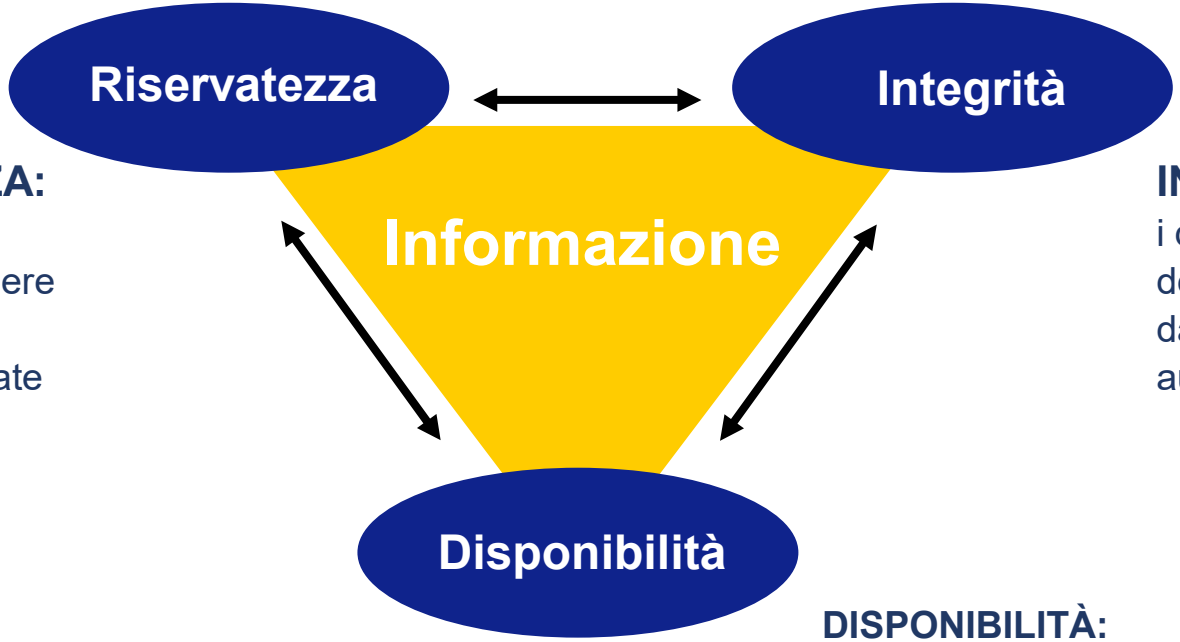
Not a question of "if" but "when"

When will your data breach happen? Not a question of "if" but "when".

http://www.securityinfowatch.com/article/12052877/preparing-for-your-companys-inevitable-data-breach

Che cos'è la Sicurezza delle Informazioni?

Attività volta a definire, conseguire e mantenere:



RISERVATEZZA:
le informazioni devono poter essere accedute solo da persone autorizzate

INTEGRITÀ:
i dati e le informazioni devono essere protette da modifiche non autorizzate

DISPONIBILITÀ:
i sistemi e le applicazioni devono essere disponibili quando necessario

paradigma R.I.D.

Sicurezza delle informazioni è anche garantire …

Autenticità

La proprietà in virtù della quale viene garantito che l'identità di un soggetto o di una risorsa sia quella dichiarata (dal soggetto o dalla risorsa). L'autenticità si applica a entità quali utenti, processi, sistemi e informazioni

Non ripudio

La capacità di provare che un'azione o un evento ha avuto luogo, in modo tale che non si possa successivamente affermare che tale azione non sia avvenuta

Accountability

La proprietà che assicura che le azioni effettuate da un'entità possano essere tracciate e fatte risalire all'entità

Non solo informazioni, ma anche valore

2.4

asset

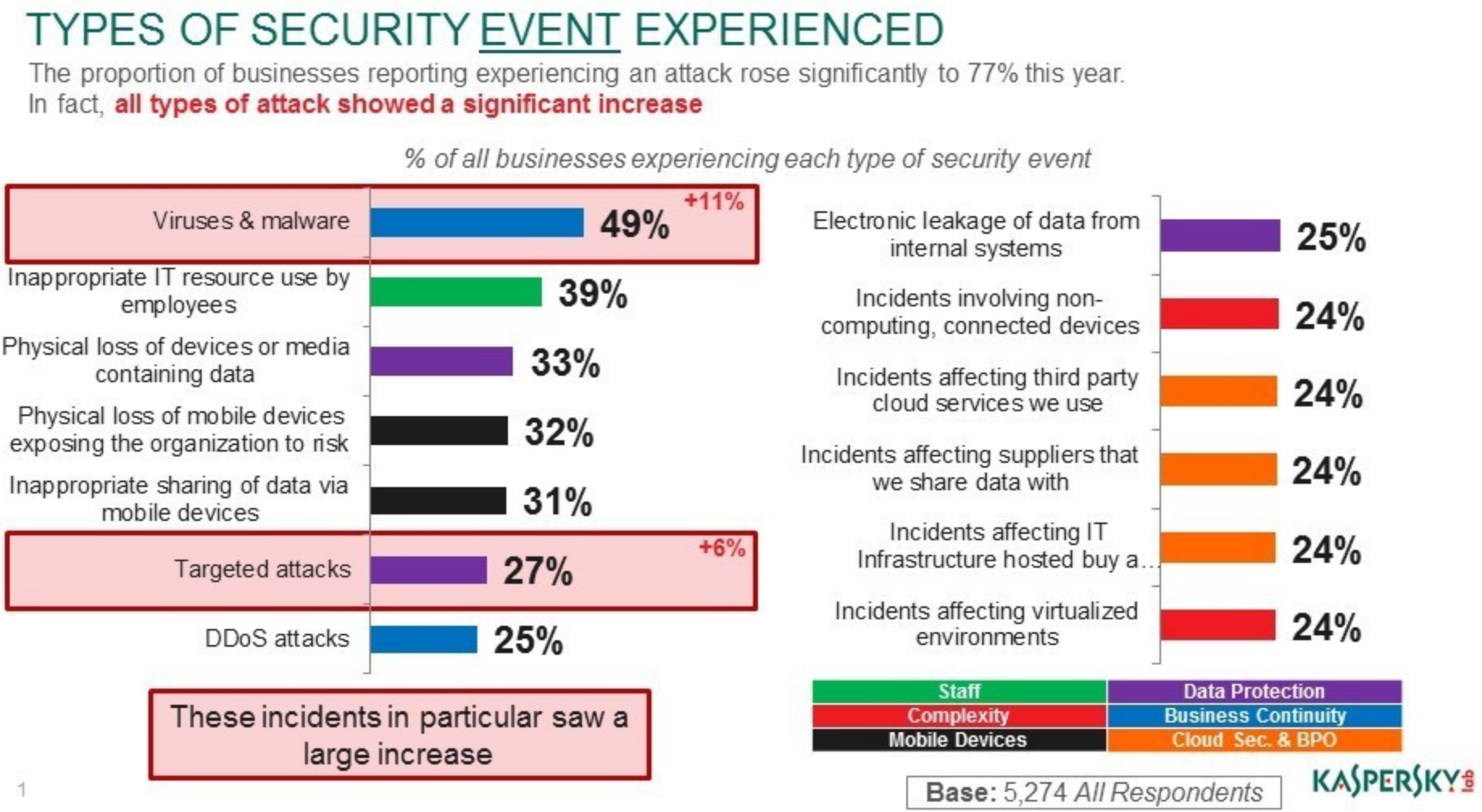
anything that has value to the organisation

NOTE There are many types of assets, including:

- *information;*
- *software, such as a computer program;*
- *physical, such as computer;*
- *services;*
- *people, and their qualifications, skills, and experience; and*
- *intangibles, such as reputation and image.*

ISO/IEC 27000:2012 https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-2:v1:en

Le azioni delle persone causano incidenti di sicurezza

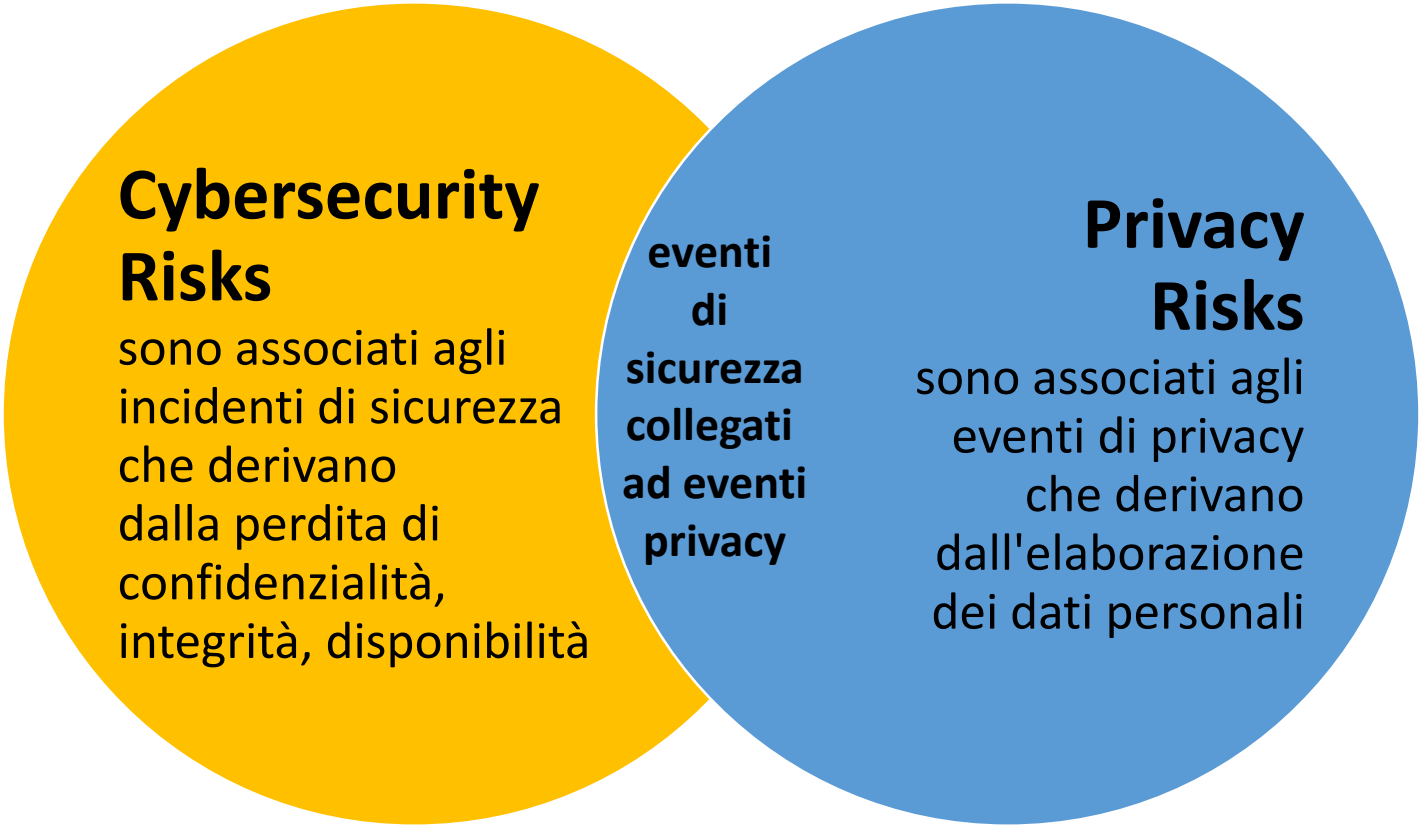


Source: IT Security Risks Survey 2017, global data

Top 10 Crime Types Reported to IC3 in 2017 (by Victim Loss)

IC3 = Internet Crime Complaint Center ➔(FBI), National White Collar Crime Center (NW3C), Bureau of Justice Assistance (BJA). https://www.fbi.gov/news/stories/2017-internet-crime-report-released-050718

Cybersecurity e Privacy Risk



Concetti generali di sicurezza

- Controllo degli accessi (fisici, tecnici, amministrativi)
- Principio del need-to-know (least privilege)
- Separazione e rotazione dei compiti
- Autenticazione
- Auditing
- Attacchi (attivi, passivi, social, password, malware, …)

Cosa si può fare?

- **Prevent**
  - Comprendere quale può essere la minaccia e come si può essere attaccati
- **Protect**
  - Ci sono molti modi per proteggere le informazioni e la presenza online, ma nessuna è quella risolutiva
- **Deter & Detect**
  - Prevenire e proteggere richiedono una mentalità orientata alla sicurezza. Il modo migliore è adottare un approccio diretto

Pensa due volte, clicca una volta!

Think twice, click once!

  - L'elemento fondamentale è mantenere la vita privata fuori da Internet
  - Rilevare la compromissione, recuperare le informazioni e gestire l'impatto, la violazione.
- **Have I been pwned?**
  - www.haveibeenpwned.com (https://haveibeenpwned.com/)

Cosa si può fare?

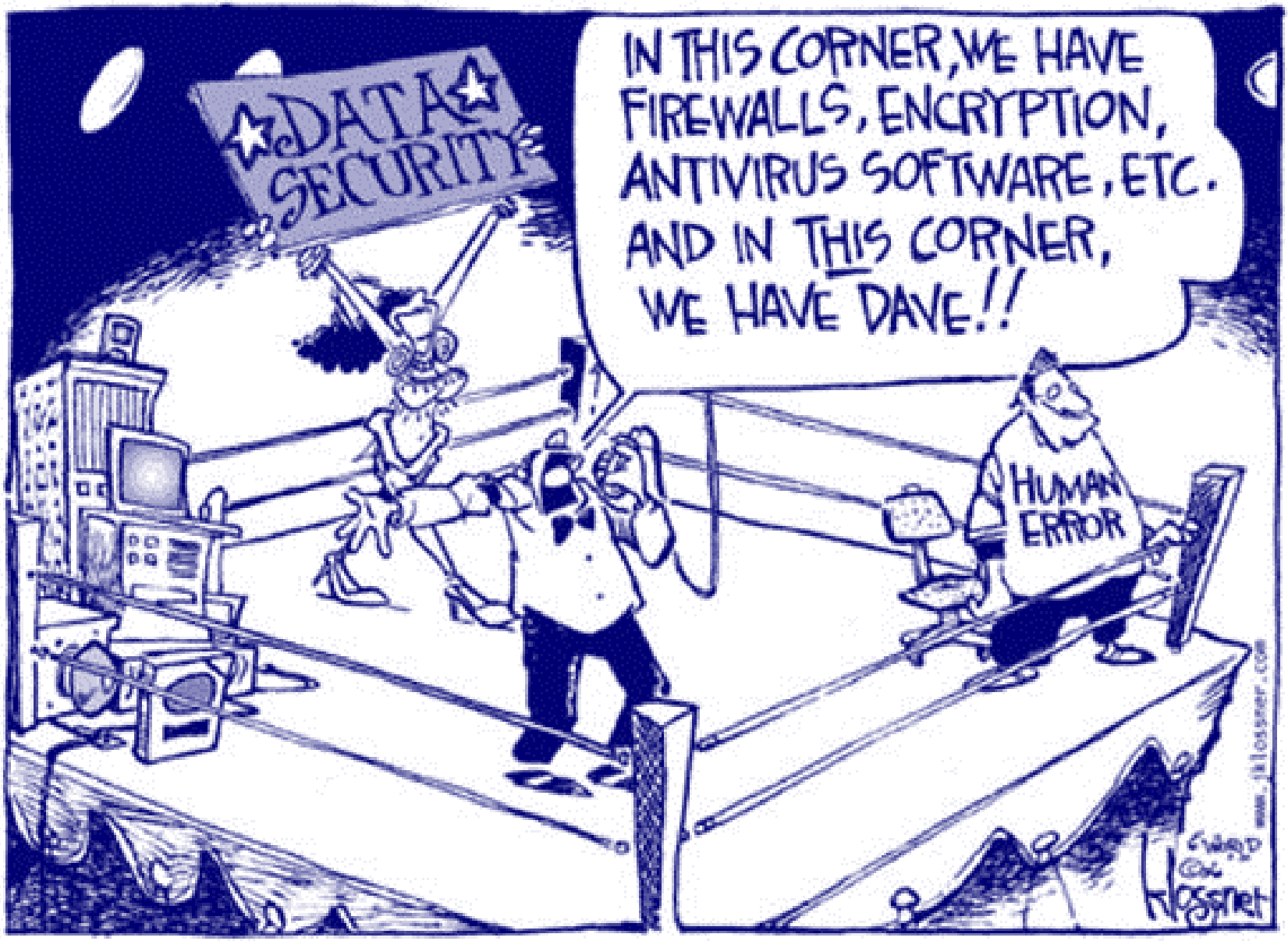
- **Prevent**
  - Comprendere quale può essere la minaccia e com… …taccati
- **Protect**
  - Ci sono molti modi per proteggere le i… …esenza online, ma nessuna è quella risolutiva
- **Deter & Detect**
  - Prevenire e proteggere… …entalità orientata alla sicurezza. Il modo migliore è adottare… …tto

    … volte, clicca una volta!

    Think twice, click once!
  - L'… …entale è mantenere la vita privata fuori da Internet

    …promissione, recuperare le informazioni e gestire l'impatto, la …
- **Have I been pwned?**
  - www.haveibeenpwned.com (https://haveibeenpwned.com/)

HUMAN FIREWALL


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jillosser.com
Jillosser

La sicurezza informatica è una responsabilità di tutti

La sicurezza informatica è una responsabilità di tutti

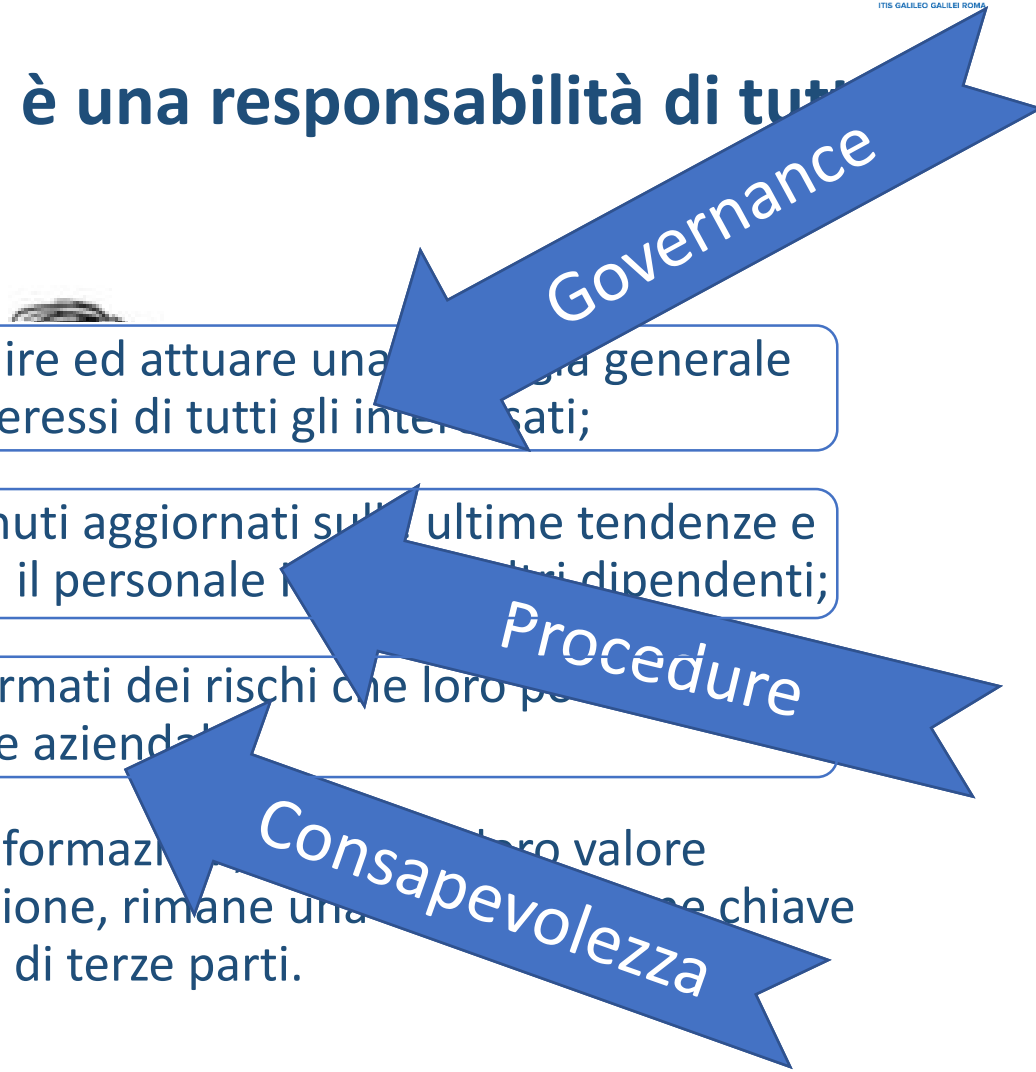
- Gli amministratori devono definire ed attuare una strategia generale informata per proteggere gli interessi di tutti gli interessati;
- I responsabili devono essere tenuti aggiornati sulle ultime tendenze e sviluppi per tenere informati sia il personale IT che gli altri dipendenti;
- i dipendenti devono essere informati dei rischi che loro potrebbero comportare verso la propria rete aziendale.

La priorità sull'importanza delle informazioni, in base al loro valore finanziario e/o attributi di reputazione, rimane una considerazione chiave nella gestione di dati proprietari o di terze parti.

La sicurezza informatica è una responsabilità di tut

- Gli amministratori devono definire ed attuare una ia generale informata per proteggere gli interessi di tutti gli inte sati;
- I responsabili devono essere tenuti aggiornati su ultime tendenze e sviluppi per tenere informati sia il personale i dipendenti;
- i dipendenti devono essere informati dei rischi che loro p comportare verso la propria rete aziend

La priorità sull'importanza delle informazi oro valore finanziario e/o attributi di reputazione, rimane una e chiave nella gestione di dati proprietari o di terze parti.



Definizioni

- **Minaccia** → una potenziale causa di un incidente indesiderato, che può provocare danni a un sistema o un'organizzazione
- **Vulnerabilità** → una debolezza di un bene che può essere sfruttata da una **minaccia**
- **Attacco** → un tentativo di distruggere, esporre, alterare, disabilitare, rubare o ottenere accesso non autorizzato o fare un uso non autorizzato di un **bene**
- **Contromisura** → una protezione che affronta una **minaccia** e mitiga il **rischio**
- **Rischio** → l'indeterminatezza nel raggiungimento degli obiettivi (scostamento dai risultati attesi)

Attacchi informatici

Principi generali:

- Qualunque strato OSI può essere attaccato.
- La sicurezza dell'infrastruttura/sistema coincide con la sicurezza del suo punto più debole.
- Entrare in una rete o in un sistema è solo questione di pazienza e metodo. Si può solo rendere più difficile il processo.
- Se pensate di non poter essere attaccati, probabilmente lo siete già stati o lo siete tuttora.
- L'appetibilità di un bersaglio non dipende soltanto dal tornaconto economico, ma anche da quello sociale (danno d'immagine o escalation di notorietà).

Attacchi

Possono essere generalmente raggruppati in più categorie:

- target (application, network, or mixed)
- attivo o passivo
- modalità (pwd cracking, exploiting code, cryptographic algorithm, ecc.)

Tipologie d'attacco

- **Attacchi fisici**
  - Tailgating, irruzione, line tap
- **Attacchi alla rete**
  - Route poisoning, wardriving, fake AP, DoS, wardialing
- **Attacchi ai servizi/sistemi**
  - Buffer/heap overflow, malware, DoS, bruteforcing
- **Attacchi ai dati**
  - Sniffing, MITM, SQL injection
- **Attacchi alle applicazioni**
  - Buffer/heap overflow, XSS, Authentication bypass

Superfici d'attacco

- **Attacchi fisici**
  - Ingressi secondari, cabine elettriche, patch panel
- **Attacchi alla rete**
  - Router, switch, firewall, protocolli di routing
- **Attacchi ai servizi/sistemi**
  - Mail server, file server, web server e sistemi ospitanti
- **Attacchi ai dati**
  - Database, web application, LAN, WiFi
- **Attacchi alle applicazioni**
  - Office automation, strumenti di controllo, web application

Punti di accesso

- **Servizio o libreria di sistema vulnerabile**
  - Mancanza di security fix
- **Installazioni di default**
  - Funzioni amministrative
  - Utenze privilegiate di default
  - Servizi attivi ma non necessari
- **Errori di configurazione**
  - Introduzione involontaria di backdoor
  - Salvataggio di dati riservati in aree pubbliche
- **Sviluppo non sicuro delle applicazioni**

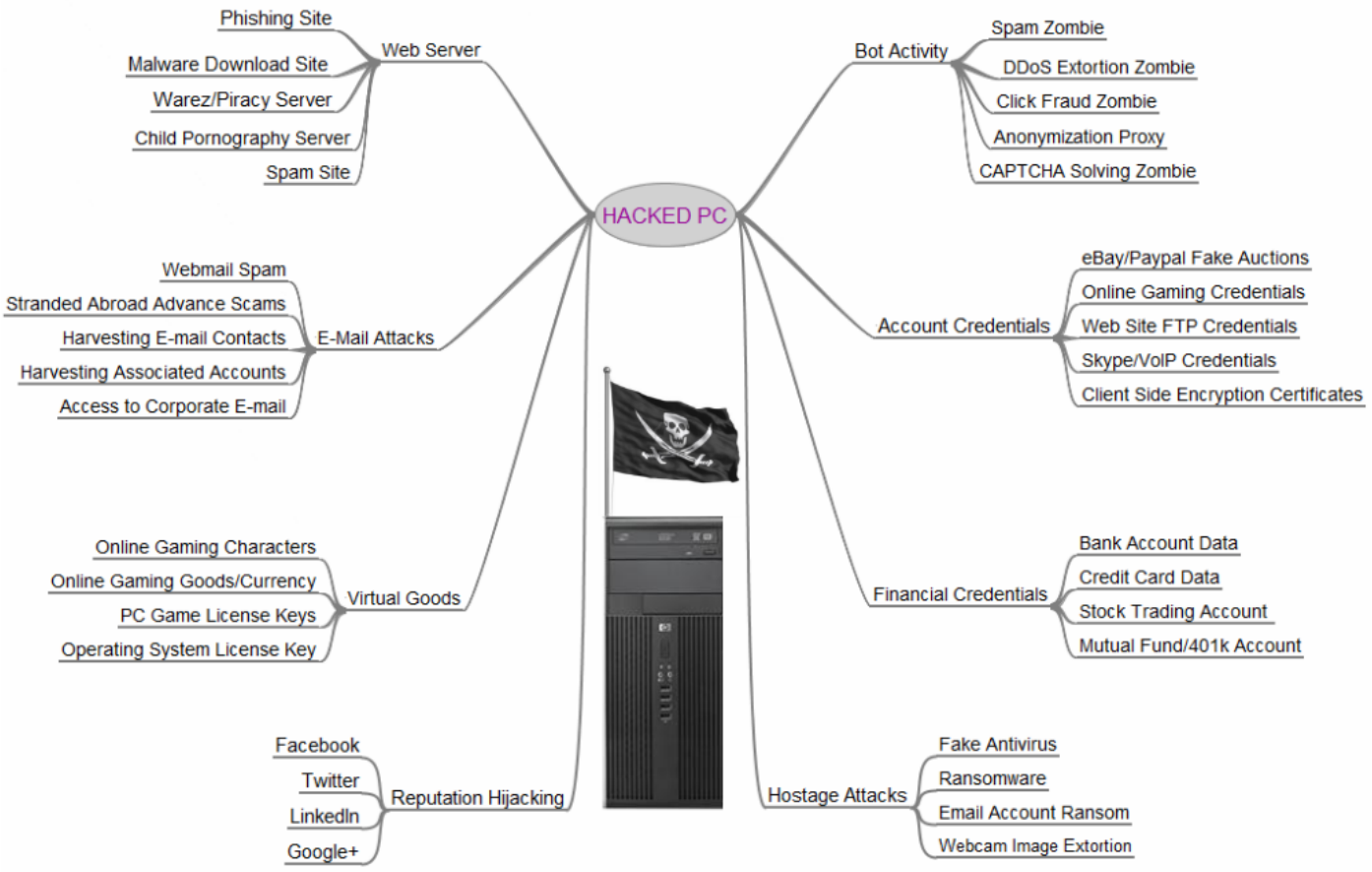
Attacchi

- **Active Attacks**
  - DoS and DDoS
  - Software exploitation and buffer overflow
  - Man-in-the-Middle (MITM) attacks
  - TCP/IP hijacking
  - Replay attacks
  - Spoofing attacks (Phishing)
  - Wardialing
  - Dumpster diving
- **Social Engineering**
- **Vulnerability Scanning**

Attacchi

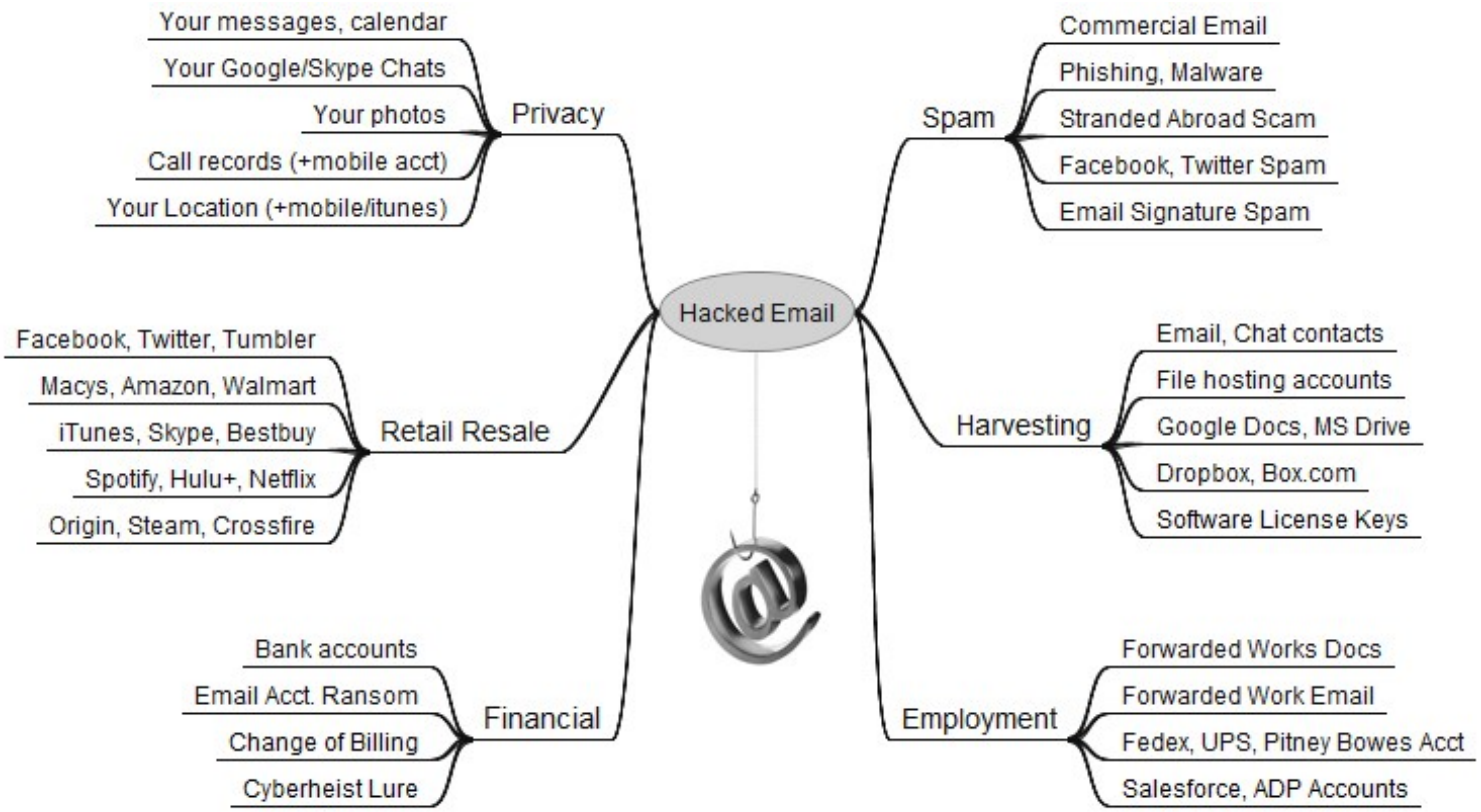
- **Passive Attacks**
  - Sniffing and Eavesdropping attacks
- **Password Attacks**
  - Brute-force attacks
  - Dictionary-based attacks
- **Malicious Code Attacks**
  - Viruses
    - Worms
    - Trojans Horses
    - Rootkits
    - Backdoors
    - Logic Bombs
    - Spyware and Adware

The Scrap Value of a Hacked PC



https://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

The Value of a Hacked Email Account



https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/

Fasi di un attacco informatico

- **Ricognizione**
  - Fase preparatoria in cui l'attaccante raccoglie quante più informazioni possibili sul bersaglio.
  - Rischio di business: **trascurabile**.
- **Scansione**
  - L'attaccante interroga il bersaglio in cerca di informazioni specifiche, sulla base dei dati raccolti nella fase precedente.
  - Rischio di business: **medio** (basta un solo punto debole).
- **Accesso**
  - Sfruttamento delle vulnerabilità rilevate nella fase precedente.
  - Rischio di business: **alto**.

Ricognizione

- **Passiva**

  Acquisizione di informazioni **senza** interrogare il bersaglio.

  – Strumenti tecnologici (motori di ricerca web e dns, sniffer)

  – Annunci di lavoro

  – *Dumpster diving*

- **Attiva**

  Acquisizione di informazioni interrogando direttamente il bersaglio.

  – Strumenti tecnologici (strati 3-7 OSI)

  – Social engineering (via telefono o di persona)

Scansione

- **Network scanner**

  Scandagliano la rete alla ricerca di apparati e porte attive, e rilevano i protocolli e i servizi esposti.

- **Vulnerability scanner**

  Interrogano il bersaglio e, in base alle risposte, capiscono se è presente una vulnerabilità.

- **Web scanner**

  Interrogano siti internet alla ricerca della presenza di alcune pagine.

Fasi opzionali

- **Mantenere aperto l'accesso**
  - Backdoor/Trojan horse/Rootkit
  - Creazione di un'utenza privilegiata
- **Cancellare le tracce**
  - Steganografia
  - Tunnellizzazione
  - Cancellazione di log

Categorie di hackers

- **Blackhat (*crackers*)**
  - Individui le cui capacità tecniche sono indirizzate ad attività malevole, distruttive o semplicemente non autorizzate.
- **Whitehat (*security analyst / ethical hacker*)**
  - Individui con le capacità dei Blackhat, ma usate per anticipare le azioni malevole così da poter individuare le corrette mitigazioni prima del verificarsi di un attacco (presidio preventivo).
- **Greyhat**
  - Individui che operano su entrambi i fronti, a seconda della committente.
- **Hacktivism**
  - Organizzazioni che mirano a lanciare messaggi sociali attraverso la loro attività di hacking.

Un hacker (etico) deve essere …

- Curioso
- Paziente
- Discreto
- “Trasversale”
- Creativo
- Ragionevolmente paranoico

Un hacker deve conoscere …

- Il framework TCP/IP e i protocolli correlati
- Il funzionamento dei principali servizi di rete (http, ftp, ssh, ecc.)
- Gli apparati di rete e le loro interazioni
- I principi di programmazione e la sintassi dei linguaggi più usati
- I database e le relazioni
- Tutti i sistemi operativi a livello “amministratore”
- I principali algoritmi crittografici

Un hacker deve saper …

- Configurare server, workstation, servizi e apparati di rete
- Forgiare richieste arbitrarie (IP, HTTP, ecc.)
- Interpretare log
- Realizzare script in diversi linguaggi
- Debug e reverse engineering di codice
- Crittoanalisi
- ….

I reati informatici

Per “reato informatico” si intende qualsiasi comportamento illecito, sanzionato dall’ordinamento penale, rivolto contro i beni informatici o che si compie utilizzando le tecnologie informatiche.

La Legge n. 547/1993 “Modificazioni ed integrazioni … in tema di criminalità informatica” ha introdotto nuove forme di aggressione criminosa ed è intervenuta in quattro diverse direzioni:

- aggressioni alla **riservatezza** dei dati e delle comunicazioni informatiche;
- aggressioni all’**integrità** dei dati e dei sistemi informatici;
- condotte in tema di **falso**, estese ai documenti informatici;
- **frodi** informatiche.

CP 615-ter
Accesso abusivo ad un sistema informatico o telematico

"*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito …*"

È un reato comune, lo può commettere chiunque.

È sufficiente che il soggetto attivo abbia conoscenze tecniche anche minime, ma sufficienti a superare le misure di sicurezza (tecniche, informatiche, organizzative e procedurali) volte ad escludere o impedire la cognizione delle informazioni a soggetti non autorizzati.

Due ipotesi di reato entrambe di natura dolosa:

- **accesso abusivo** ad un sistema informatico o telematico protetto da misure di sicurezza
- **permanere** in un sistema informatico o telematico contro l'espressa volontà di chi ha diritto ad escluderlo, pur essendo penetrato legittimamente nel sistema

L'art. 615-ter è collocato tra i delitti contro l'inviolabilità del domicilio.

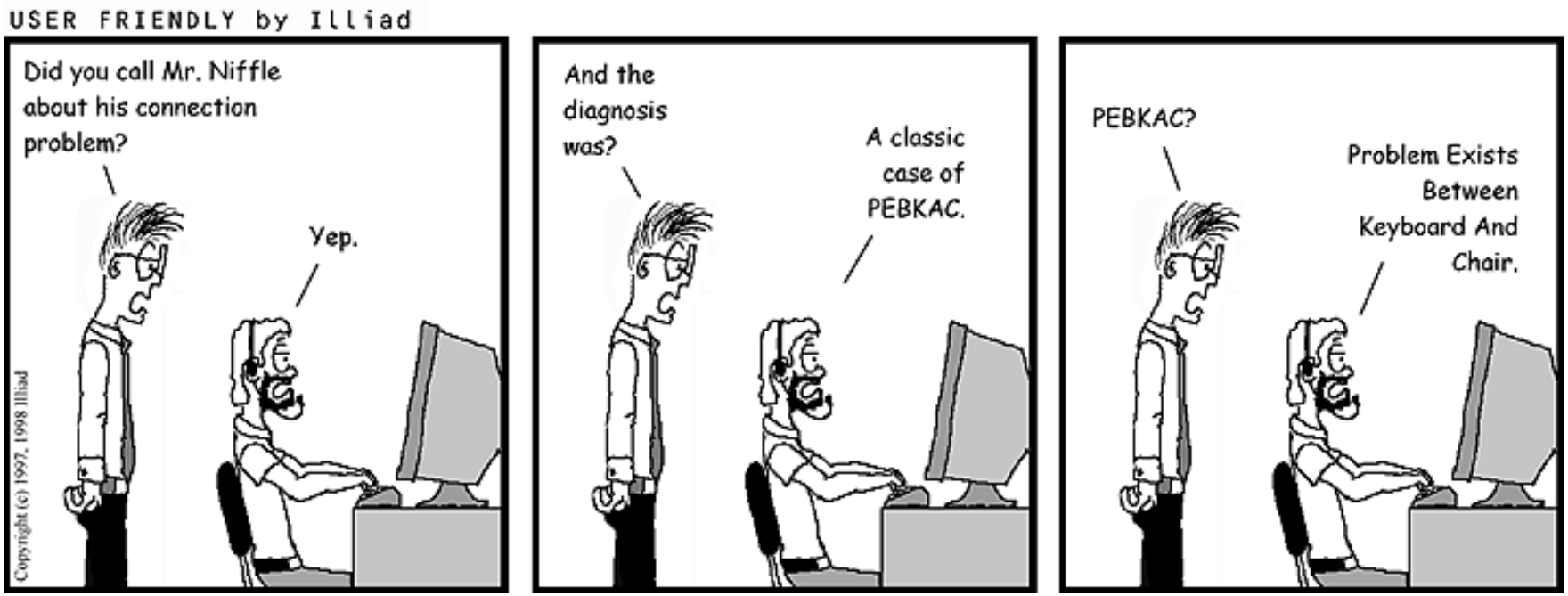
Social Networking Security - 10 punti fondamentali

1. Una volta che un'informazione/immagine/scritto è su Internet, rimane in Internet
2. Ogni cosa che dici/scrivi rimane associata alla tua identità digitale
3. Quello che scrivi ora avrà un impatto sul tuo futuro
4. Chiunque può pubblicare su Internet, quindi controllare prima
5. Chiunque può essere chi vuole su Internet, bisogna essere cauti dei profili
6. Controlla i profili degli amici, poi controlla in altra parte, quindi controlla nuovamente
7. Attenzione ad esprimere giudizi non adeguati, vale il punto 1.
8. Pensa due volte, clicca una volta
9. Leggi e rileggi il tuo post prima di inviare
10. Cerca informazioni su di te saltuariamente, è incredibile quello che si scopre

"Stupendo spot belga sull'ingenuità …"

https://www.youtube.com/watch?v=eASGFYqX7sg

PEBKAC
problem-exists-between-keyboard-and-chair



Domande?


MATICMIND
makes IT easy
Giuseppe G. Zorzino
DPO & Security Advisor
T: +39 06 51065417
M: +39 335 6281204
Mail: giuseppe.zorzino@maticmind.it
Via M. Carucci, 131
00143 ROMA
Tel. +39 06 510651
info@maticmind.it
www.maticmind.it