Cyberconsapevolezza per il bene (del) Comune

20 ottobre 2025
Valentina Lo Voi
Bernardo Palazzi

ACN: COLLOCAMENTO ISTITUZIONALE

PRESIDENTE DEL CONSIGLIO DEI MINISTRI

COMITATO INTERMINISTERIALE PER LA CYBERSICUREZZA

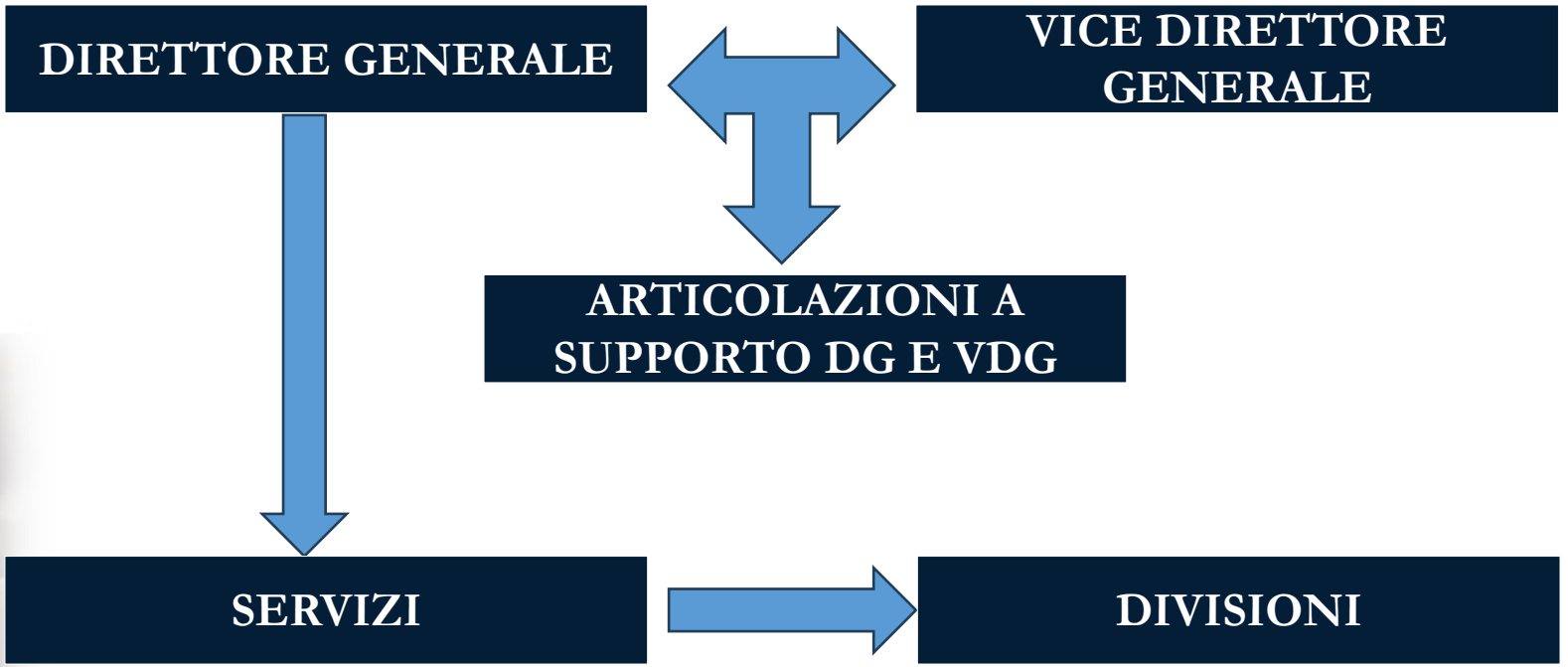
AUTORITÀ DELEGATA PER LA SICUREZZA DELLA REPUBBLICA

Autorità governativa che risponde al Presidente del Consiglio dei ministri e all'Autorità Delegata e gode, sotto alcuni profili, di una normativa «in deroga»

CONTROLLO DEL COPASIR

AGENZIA PER LA CYBERSICUREZZA NAZIONALE

ORGANIGRAMMA



AGENZIA PER LA CYBERSICUREZZA NAZIONALE

Funzioni e Servizi

SERVIZI

- BILANCIO E PROCUREMENT
- CERTIFICAZIONE E VIGILANZA
- GABINETTO
- OPERAZIONI
- PROGRAMMI INDUSTRIALI TECNOLOGICI E DI RICERCA
- REGOLAZIONE
- RISORSE UMANE STRUMENTALI E AMMINISTRAZIONE GENERALE
- CRITTOGRAFIA
- STRATEGIE E COOPERAZIONE

L'ART. 7 DEL D.L. 82/2021

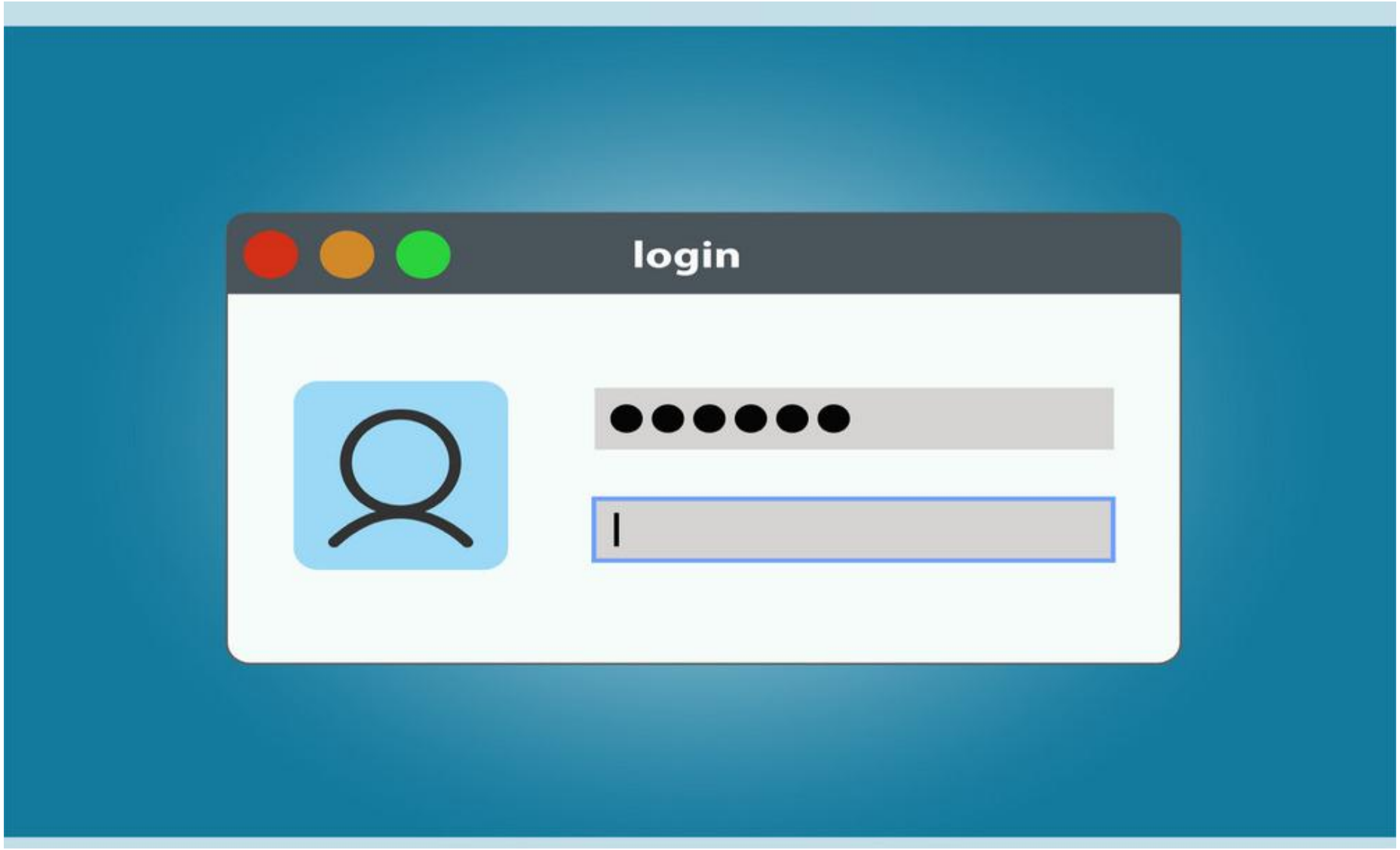
"[l'Agenzia in quanto Autorità nazionale… promuove…] la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore"

FOCUS FUNZIONI ISTITUZIONALI (ART. 7 D.L. 82/2021)

SICUREZZA NAZIONALE | **RESILIENZA** | **AUTONOMIA STRATEGICA**

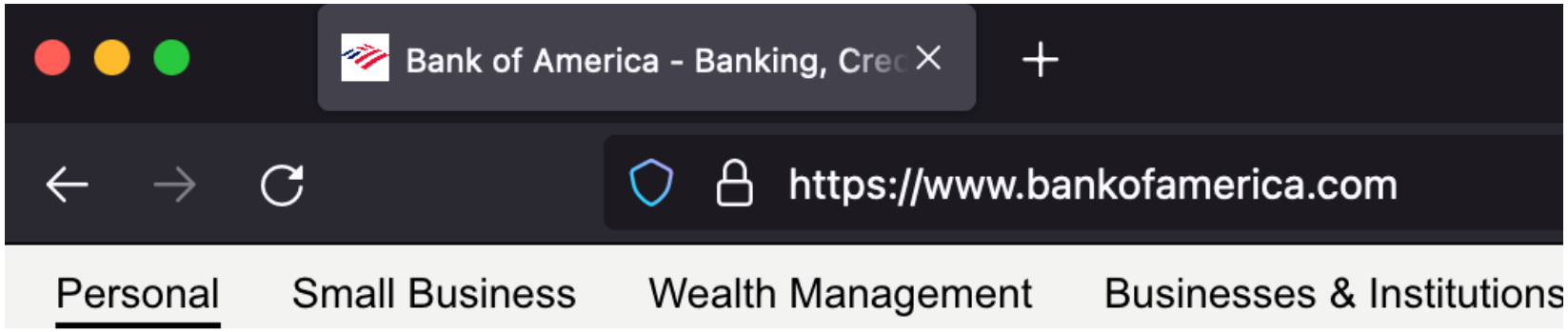
Che cos’è la cybersicurezza?

Perché ne abbiamo bisogno?



Rendere sicure le azioni e proteggere le risorse, perché?

- Che cosa dobbiamo rendere sicuro?
- Quali meccanismi di sicurezza ci servono?
- Come funzionano?



Non possiamo considerare tutto come "scatola nera," non possiamo comprendere tutto, ma i principi servono

LA CYBERSICUREZZA: definizione nella Legge italiana

«*L'insieme delle attività […] necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico*» (art. 1, comma 1, lett. a), d.l. 82/2021)

Sicurezza cibernetica + Resilienza = Cybersicurezza

Sicurezza nazionale nello spazio cibernetico

Resilienza cibernetica

La capacità di anticipare, resistere, recuperare e adattarsi a condizioni avverse, stress, attacchi, o compromissioni su sistemi che utilizzano o si basano su risorse cyber

NIST SP 800-172

Triade CIA

Riservatezza

Confidentiality

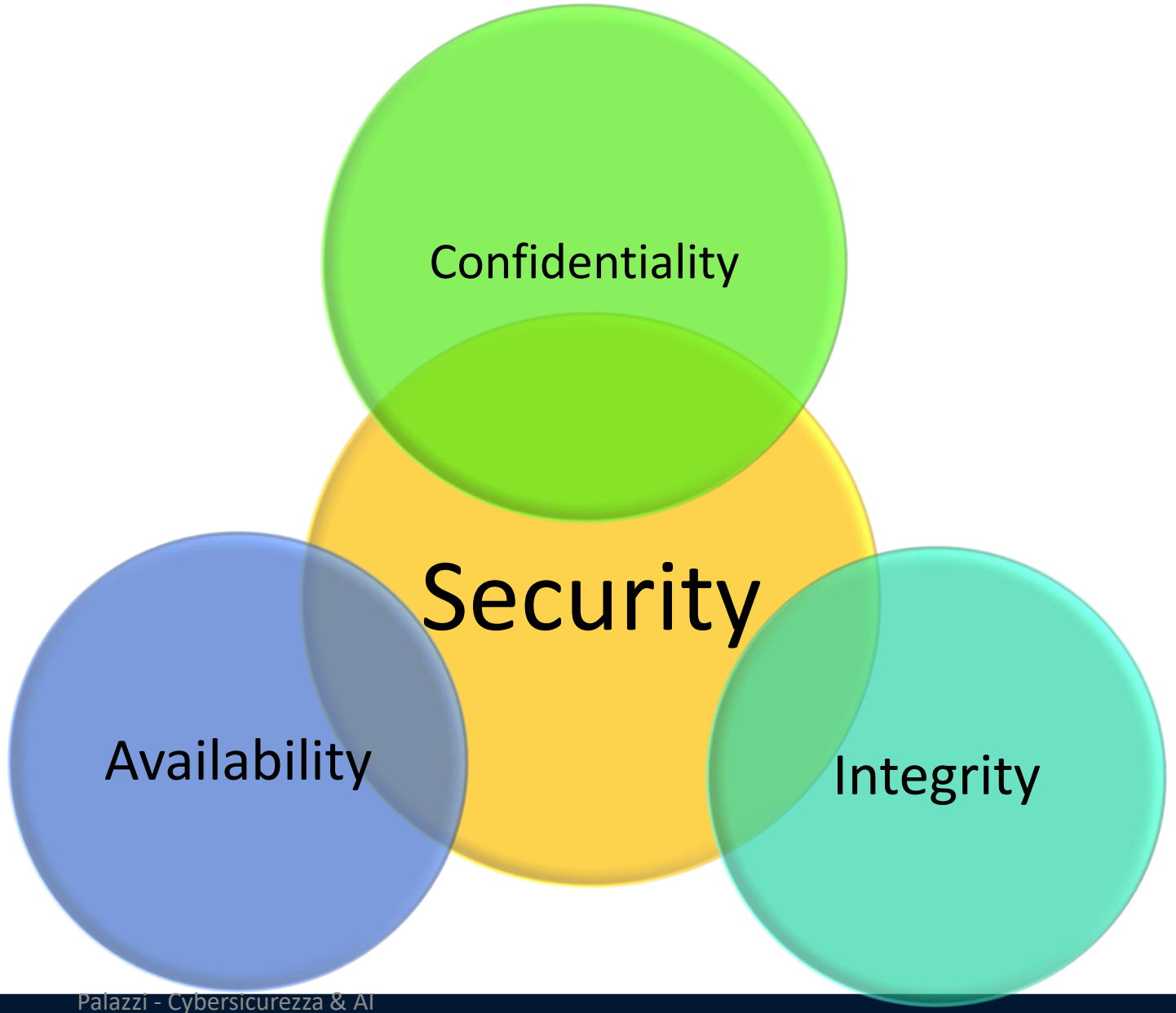
Impedire la divulgazione di informazioni a persone non autorizzate

Integrità - Integrity

Rilevare la manomissione dei dati

Disponibilità - Availability

Garantire
l'accesso ai dati



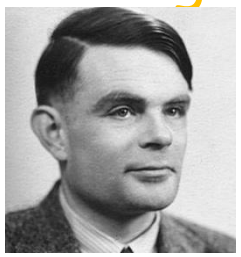
Altre proprietà

- Non ripudio
  - Capacità di assicurare che il mittente di una comunicazione non possa successivamente disconoscerla
- Autenticità
  - Capacità di attribuire la paternità di un'informazione o servizio
- Controllo degli accessi
  - Gestione delle autorizzazioni ai vari soggetti

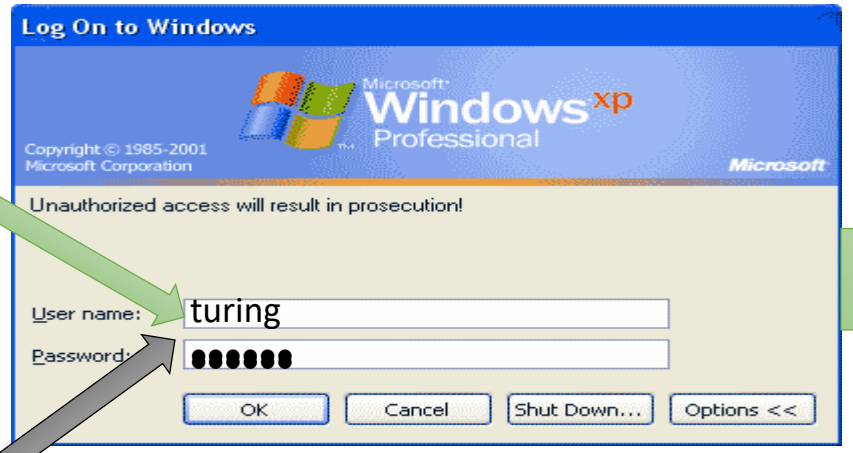
Il controllo degli Accessi

Identificazione

Turing



password



Accesso?

File
DATI
PERSONALI

Autenticazione

Autorizzazione

Fernando Corbato

www.wired.com/2012/01/computer-password/

Mediazione: Security Trade-off

- La sicurezza assoluta contro tutti i possibili avversari è praticamente irrealizzabile
- La sicurezza implica un compromesso/mediazione tra la mitigazione del rischio e il costo di implementazione dei meccanismi di difesa
- Inoltre, devono essere presi in considerazione fattori umani come l'accettazione dell'utente e l'usabilità

Classificazione delle Minacce

TERMINI CHIAVE

ALCUNI TERMINI CHIAVE NELLA CYBERSICUREZZA?

ASSET

Un asset è tutto ciò che ha valore (da intendere come beni tangibili e intangibili) per un'Organizzazione.
Es. I **dati presenti** in un database

MINACCIA

È una potenziale causa di un incidente indesiderato, che potrebbe causare danni ad un sistema o ad un'organizzazione

VULNERABILITÀ

La vulnerabilità è un punto di debolezza in un sistema, processo o controllo che può essere sfruttata da una minaccia per causare danni o violazioni.

ATTACCO

È una azione realizzata da **individui**/ **organizzazioni,** al fine di causare un **danno** o **trarre un vantaggio** mediante **un accesso o uso non autorizzato/previsto di un asset**

RISCHIO

Il **rischio** rappresenta la **probabilità** di un evento imprevisto, con una valutazione dell'**impatto** sulle possibili conseguenze negative

CONTROMISURA

È **un'azione,** oppure uno **strumento, che contrasta una minaccia e mitiga il rischio di attacco.**
Es. la realizzazione di un piano di risposta in caso di attacco

VETTORI D'ATTACCO

VITTIMEt

PERSONALE AMMINISTRATIVO
Personale di un'Amministrazione con mansioni burocratiche o dirigenti

PERSONALE IT
Personale con competenze specifiche in materia di sicurezza delle informazione e delle reti

FORNITORI
Coloro che approvvigionano l'Amministrazione con i propri beni e servizi

CITTADINI
Coloro che usufruiscono dei beni e servizi erogati dall'Amministrazione

VETTORI D'ATTACCO

SOCIAL ENGINEERING


MALWARE


VULNERABILITÀ


PHISHING


DDoS


WEB ATTACK


NON NOTI


ATTACCANTI

ATTIVISTI
Gruppi o singoli hacker che svolgono attacchi al fine di promuovere obiettivi politici o un cambiamento sociale

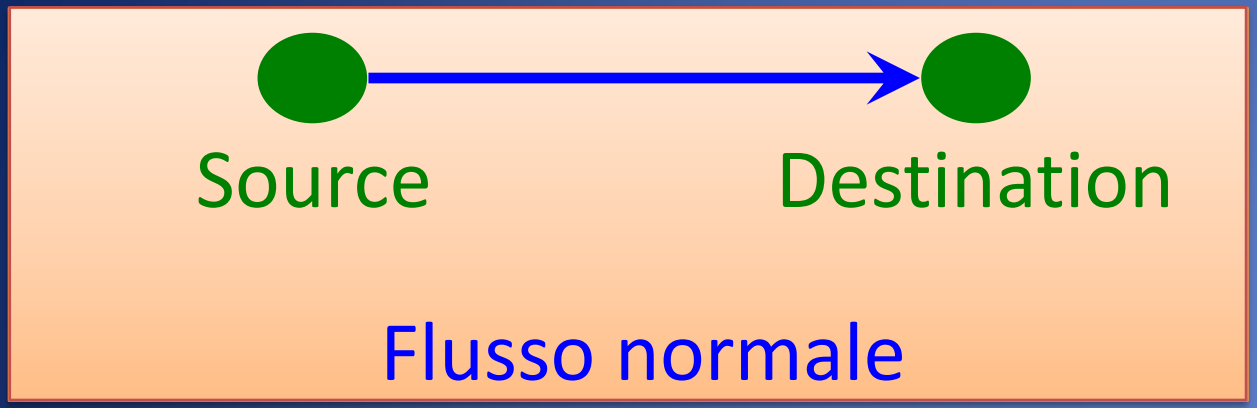
CRIMINALI INFORMATICI
Coloro che promuovono azioni illeciti di attacco con il solo fine di ottenere un vantaggio economico

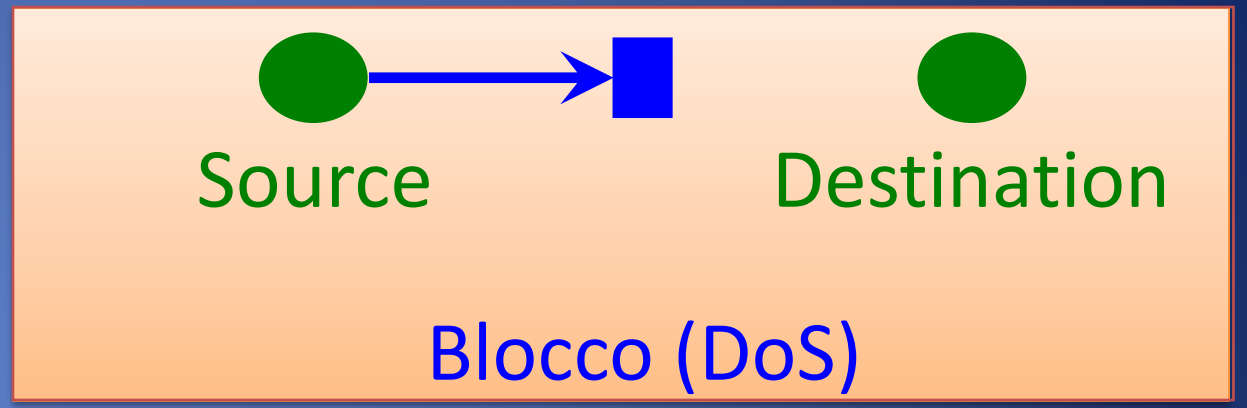
PERSONALE INTERNO
Dipendenti o ex-dipendenti che tentano di danneggiare i dati o i sistemi di un'Amministrazione

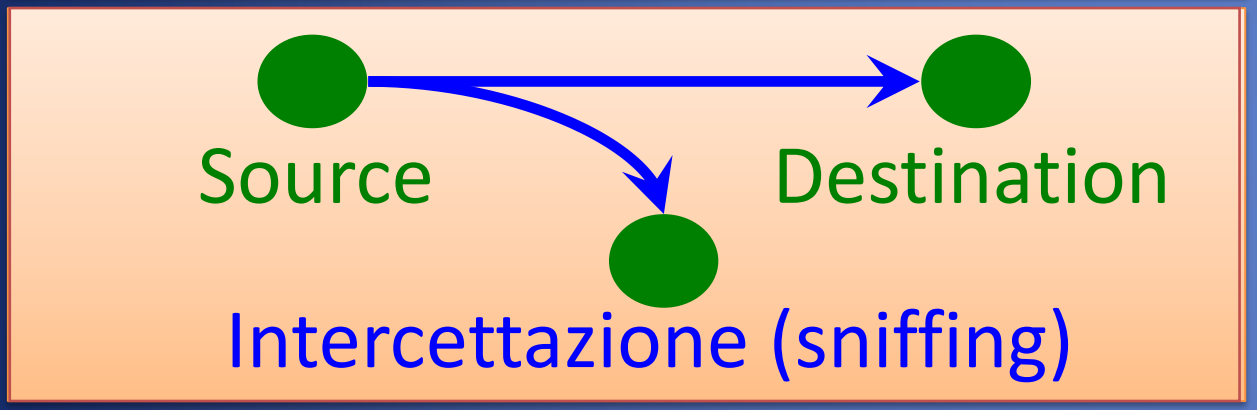
TERRORISTI
Coloro che attaccano per causare danni attraverso l'intimidazione

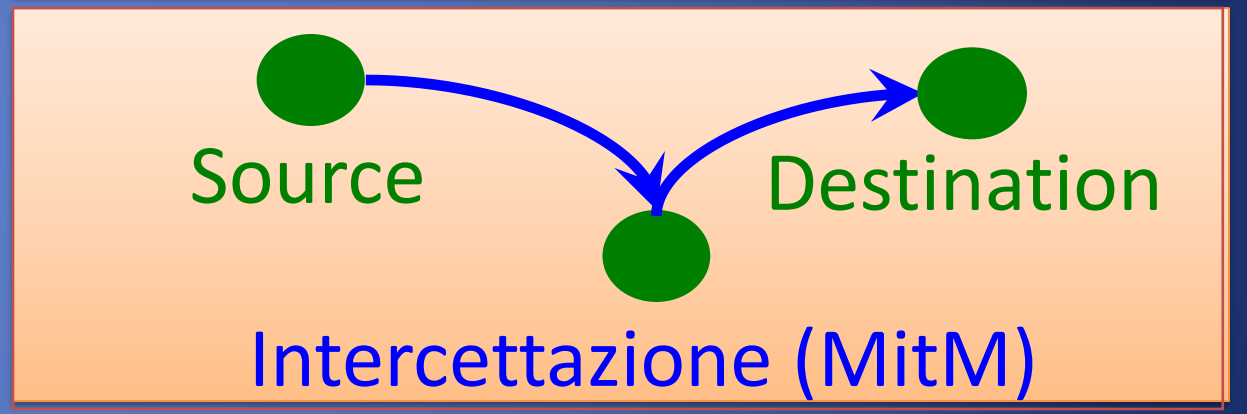
STATO/NAZIONE
Hacker finanziati da uno Stato con il fine di penetrare i computer o i network di un altro Paese per causare danni o interruzioni

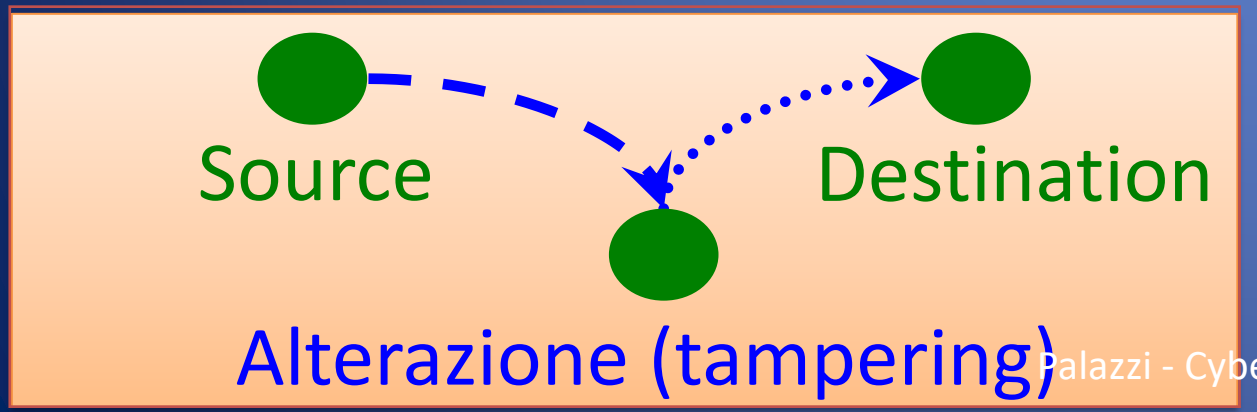
Minacce su flussi di informazioni

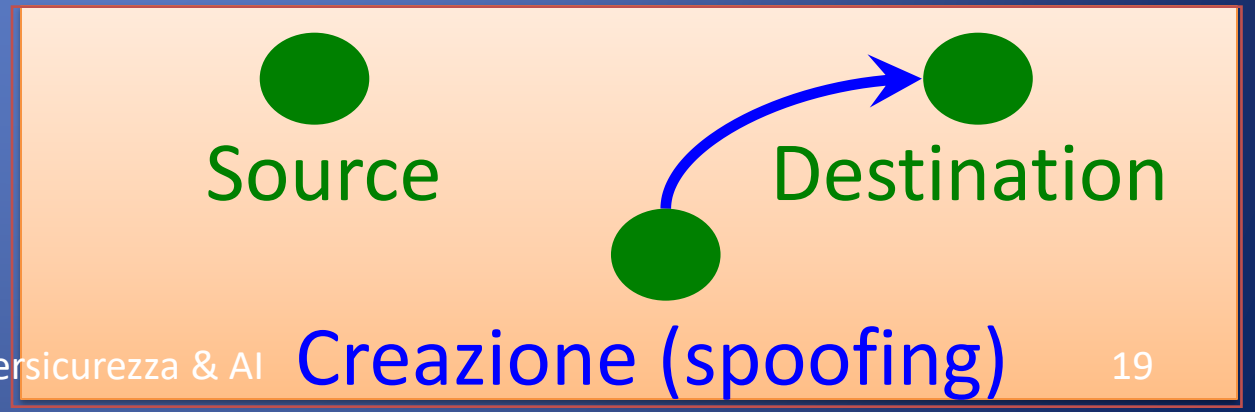












Minacce (STRIDE)	Descrizione	Violazione
Spoofing	Creazione di contenuto impersonificando altro account	Autenticazione
Manomissione (Tampering)	Alterazione dei dati o del sistema	Integrità
Ripudio	Non riconoscere azioni compiute	Non ripudio
Rivelazione di Informazioni	Esporre informazioni a una parte non autorizzata	Riservatezza (Confidenzialità)
Negazione servizio (Denial of Service)	Impossibilità di fruire servizi	Disponibilità (Availability)
Elevazione del privilegio	Possibilità di effettuare di privilegi senza autorizzazione	Autorizzazione

Cos’è la Cybersicurezza in pratica?

- La sicurezza di un sistema, di un'applicazione o di un protocollo non è assoluta ma è sempre relativa a:
  - un insieme di proprietà desiderate
  - un avversario con capacità e obiettivi specifici
- Esempio: Pagamento stipendi tramite NoiPA
  - Proprietà da proteggere: La riservatezza e l’integrità dei dati economici e personali dei dipendenti pubblici (stipendio, IBAN, codice fiscale, indennità particolari, etc.)
  - Avversario ipotetico: Un dipendente interno dell'amministrazione (es. ufficio personale) che ha accesso al sistema ma non è autorizzato a visualizzare o modificare gli stipendi di colleghi di altri uffici

Cos’è la Cybersicurezza in pratica? (2)

- Cosa non garantisce la sicurezza: Un account condiviso tra più operatori, protetto da una sola password o con permessi eccessivamente ampi
- Cosa invece funziona:
  - Account nominativo con credenziali individuali
  - Controllo dei ruoli e dei permessi (es. ogni operatore può agire solo su dipendenti della propria amministrazione)
  - Tracciamento delle attività (log di accesso per consultazione e separazione delle responsabilità per le modifiche)

L’AI introduce nuove criticità:

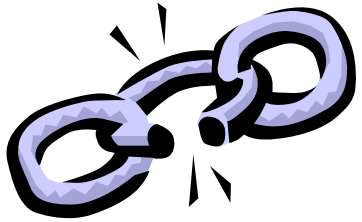
- *L’AI può essere manipolata per rivelare contenuti riservati?*
- *Chi è responsabile se l’AI commette un errore?*
- *L’utente capisce che sta interagendo con un AI?*

La sicurezza informatica è un attitudine mentale…

…è necessario pensare alla sicurezza fin dall'inizio di ogni attività «by design»

Non fare ipotesi restrittive sulle capacità dei possibili attaccanti

Ricordiamoci la metafora della catena e della sicurezza data dall'anello più debole



Tre regole di igiene cibernetica

- Usa password robuste e diverse per lavoro e vita privata
- Evita di connetterti a WiFi pubbliche non protette
- Segnala subito ogni anomalia

LA PASSWORD

- Password robuste
- Come crearle?
- Come gestirle?

123456
Valentina83
ACN2025

Seduto In Quel Caffè Io Non Pensavo A Te

SIQCINPAT)29

WI-FI PUBBLICHE

- Perché sono pericolose?
- Quali sono i rischi?
- Come proteggerci?

SEGNALA OGNI ANOMALIA

- **Quali sono le anomalie a cui prestare attenzione?**
- **A chi segnalarle?**

Tre buone pratiche

- Non aspettare che il problema diventi grave.
- Segnala anche se pensi che non sia importante.
- Non condividere mai link o file sospetti e, se hai dubbi, chiedi sempre conferma.

La sicurezza non è un'opzione: è un'abitudine

GRAZIE!

Valentina Lo Voi