Technologies for our future

CONFINDUSTRIA

CYBER SECURITY
E
TRASFORMAZIONE DIGITALE

Rischi e opportunità: l'importanza dell'osservazione e della prospettiva

Giulio Iucci
Presidente ANIE Sicurezza

I FATTORI ABILITANTI DELLA TRASFORMAZIONE

COPERTURA TERRITORIO

Forte proliferazione di sistemi di sicurezza e controllo sul territorio (privato e pubblico) con il risultato di avere una miriade di "sensori a campo" che potenzialmente possono essere connessi e comunicare.

CONVERGENZA TECNOLOGICA

La digitalizzazione ha portato ad un esponenziale processo di convergenza tra Sicurezza Fisica e Sicurezza Informatica, con forte interconnessione tra i settori Security, Safety, Automation (IOT).

SENSIBILIZZAZIONE SOCIALE

Forte attenzione alla sicurezza dei beni materiali, immateriali ed umani, da parte delle istituzioni, delle aziende e dei singoli.

LA TECNOLOGIA È AL CENTRO DEL PROCESSO

SVILUPPO TECNOLOGICO

- Hardware (prestazioni sempre più elevate)
- Software (gestione, comando e controllo degli apparati e dei Sistemi)
- Infrastrutturale (Reti – Cloud)

CONTENIMENTO COSTI

Netta riduzione dei costi dei singoli apparati, a fronte di maggiori prestazioni ed agevolazioni per l'acquisto di impianti di sicurezza.

IL TREND DELL'INTEGRAZIONE

PASSATO: STAND ALONE

- Sistemi stand-alone con interconnessioni individuali.
- Incapacità di scambiare informazioni tra i sistemi.
- Processo decisionale dipendente dall'operatore

ATTUALE: INTEGRAZIONE

- Soluzione di gestione centralizzata che integra tutti i sistemi.
- Eventi e incidenti unificati in un unico processo standard.
- Maggiore capacità nel gestire il rischio e assicurare la conformità.
- Investimenti in soluzioni integrate guidate dal ROI.

FUTURO: CONVERGENZA

- Convergenza della sicurezza IT, fisica e logica in piattaforme unificate.
- Processi decisionali supportati da scenari automatici e dinamici.
- Trasmissione dei dati più veloce ed elaborazione tramite architettura distribuita.

IL NUOVO SCENARIO

LA CONVERGENZA DIGITALE

La **Convergenza Digitale** non è più rimasta solo concettuale e/o di competenza specifica, ma è divenuta "sistemica": questa è la vera svolta e visione del futuro.

Gli **Impianti Speciali** di **automazione**, **sicurezza** di cose e persone, **gestione** dei **dati** e delle **informazioni**, a servizio di una infrastruttura tecnologica complessa di qualunque genere, non possono più essere considerati come entità separate, bensì **elementi appartenenti ad un unico Sistema**.

Inoltre i cittadini sono ormai degli utenti sempre connessi

La sicurezza non può più essere percepita per settori e con un approccio azione-reazione, ma con un approccio "olistico", come un **unico "ambiente"** che consenta la supervisione del tutto, nell'ottica dell'**Early Warning.**

IL NUOVO SCENARIO

LA SICUREZZA FISICA È ANCHE SICUREZZA CYBER

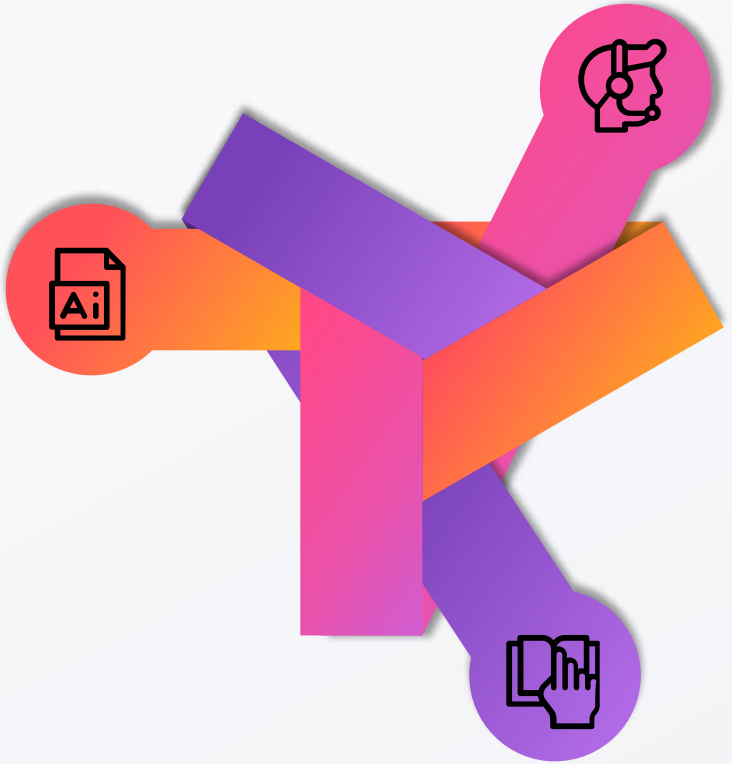
Tutti gli apparati ed i singoli sottosistemi sono, costantemente ed in tempo reale, connessi tra loro ed a loro volta **connessi con gli utenti**, come parte di un unico grande **"organismo"** che può essere "attaccato" non, come in passato, solo direttamente nelle sue "infrastrutture critiche", ma violando qualsiasi suo componente anche apparentemente residuale che faccia poi da "bridge" per entrare nel cuore dell'obiettivo principale.

E' necessario quindi conoscere e comprendere quali siano le criticità portate dalla convergenza tecnologica con relativa connessione globale, utilizzarne tutti i vantaggi, minimizzando i rischi che, in ogni caso, non potranno essere azzerati, ma mitigati adottando le **misure tecnologiche, architetturali e procedurali coerenti e proporzionate al contesto ed al bene da proteggere**, sia esso materiale, immateriale o umano.

IL TRIANGOLO DELLA SICUREZZA

UOMINI

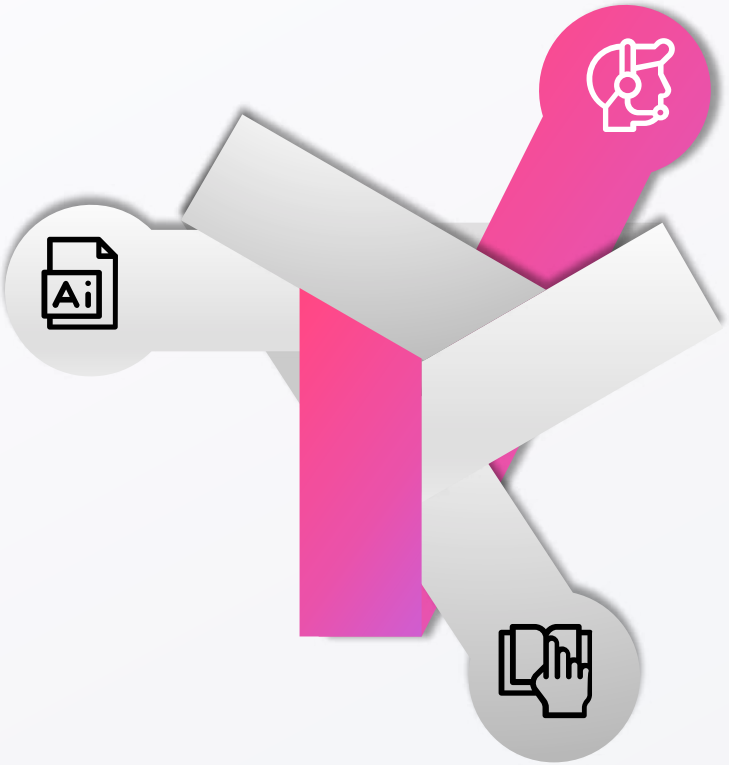
TECNOLOGIA



PROCEDURE

IL TRIANGOLO DELLA SICUREZZA

UOMINI



UOMINI

Nuovo ruolo all'interno del processo;

il fattore umano resta abilitante.

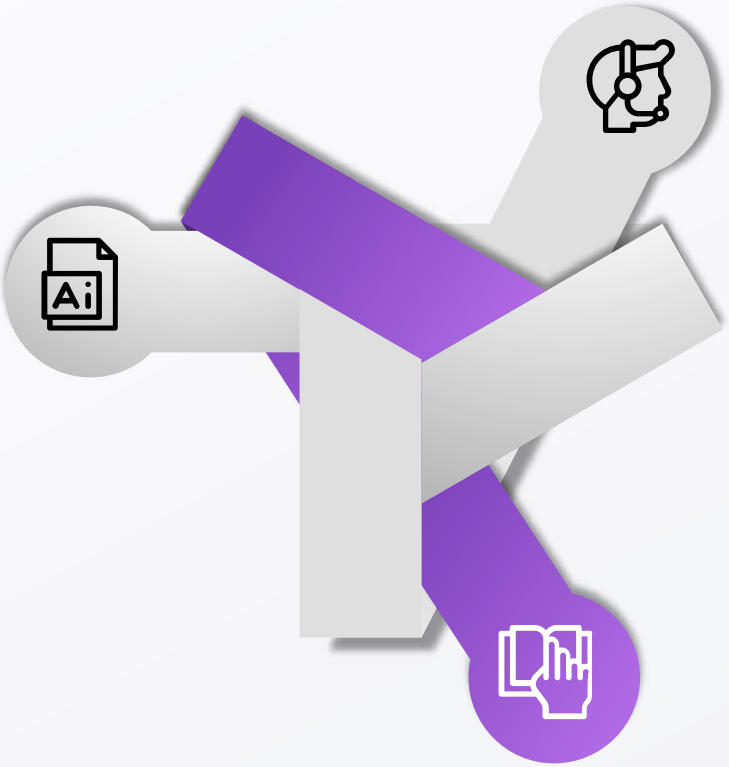
Gli uomini si trovano:

all'inizio - effettuano la risk analysis ed il risk assessment (ingegnerizzano, implementano e indirizzano);

durante - effettuano la manutenzione dei sistemi;

alla fine - decidono, ma con un'elevata velocità.

IL TRIANGOLO DELLA SICUREZZA



PROCEDURE

PROCEDURE

Non più procedure basate su “azione – reazione”, ma un processo più complesso ed elaborato, che gestisca in maniera organica ed in tempo reale, una miriade di informazioni, dando **supporto completo e veloce** all’uomo **sulle decisioni**, attivando tutte le azioni necessarie. Il processo inizia prima con la mappatura del sistema e continua dopo l’evento con l’analisi e la messa a sistema dei risultai attenuti.

IL TRIANGOLO DELLA SICUREZZA

TECNOLOGIA

Le soluzioni integrate richiedono **dati unificati** tra i sistemi, per distribuire **informazioni utili e utilizzabili**, garantendo così una maggiore visibilità degli eventi e il controllo situazionale. Oggi si riescono a governare tantissimi stati, funzioni, allarmi e informazioni, perché è la tecnologia a farlo, mettendo il tutto a disposizione dell'operatore, assistendolo nelle procedure da attivare.

IL FLUSSO DEL COMANDO E CONTROLLO

MONITORARE

Sistemi, sensori, data base, informazioni on line, ecc. (manutenere)

IMPLEMENTARE

Attivare tutte le azioni correttive (operative e tecnologiche) e trasferirle

APPRENDERE

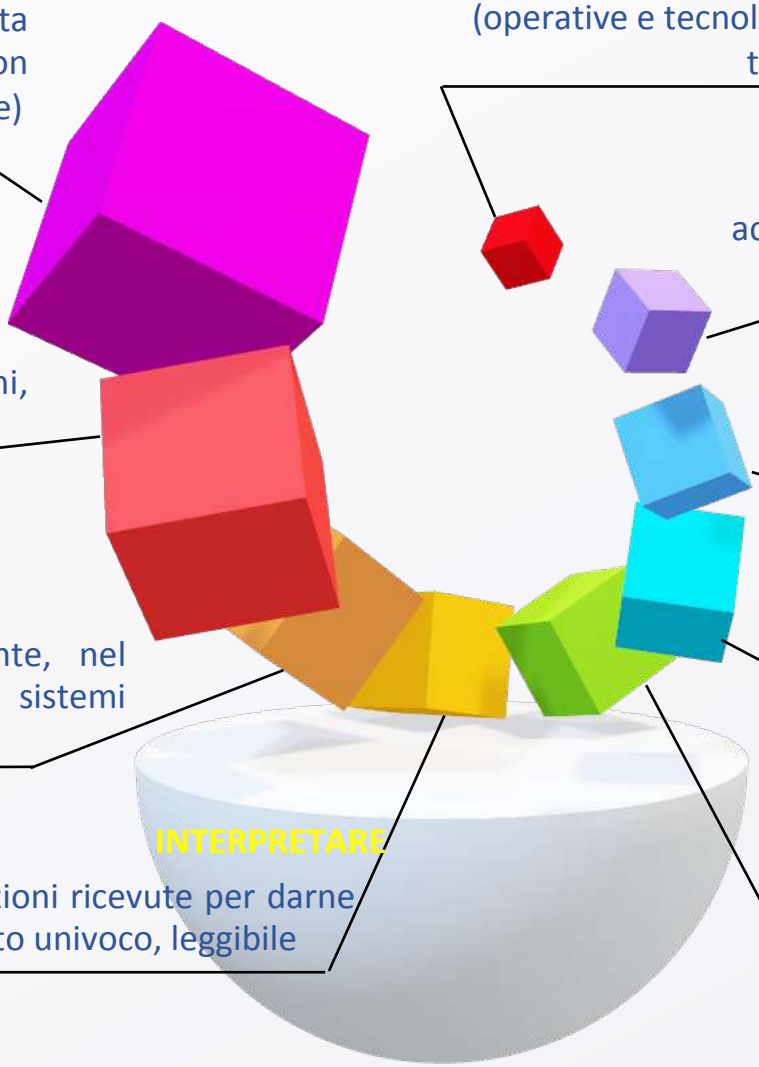
Fare esperienza di quanto accaduto, comprendendone le cause e le dinamiche

INTERCETTARE

Allarmi, informazioni, anomalie, ecc.

RIPRISTINARE

Riattivare e rendere operativo tutto ciò che è stato interrotto e/o danneggiato



CORRELARE

Geograficamente, nel tempo e tra sistemi diversi

CONTENERE

Minimizzare i danni potenziali o già verificatisi

INTERPRETARE

Le informazioni ricevute per darne un significato univoco, leggibile

INTERVENIRE

Attivare le procedure pianificate d'intervento

LA MATRICE COMPLETA DELLE ATTIVITA'

LA PAROLA D'ORDINE È DIVENTATA EARLY WARNING, MA LA FILIERA È PIÙ ARTICOLATA.

MAPPARE	MONITORARE	INTERCETTARE	INTERPRETARE	INTERVENIRE	ANALIZZARE	RE-INSERIRE
CODIFICARE CERTIFICARE	CONNETTERE	INFORMAZIONE PUSH	CORRELARE	PROCEDURE E REGOLE CERTE	ANOMALIE	CAPITALIZZARE
UNIFORMARE	INTERFACCIARE	INFORMAZIONE PULL	SIGNIFICATO ALLE INFORMAZIONI	MITIGARE	NOVITA'	CATEGORIZZARE
INDICIZZARE SEGMENTARE	PROTOCOLLI E TECNOLOGIE DIVERSI	SELEZIONARE E FILTRARE	ESPERIENZA E STATISTICA	RESILIENZA	SIGNIFICATO	CORREGGERE INSERIRE
GEO LOCALIZZARE	LOGICA DEI PROCESSI	DATA BASE	CONTESTO	VIRTUALIZZARE BACK-UP	IMPARARE PER PREVENIRE	METTERE A SISTEMA
COLLAUDARE	CONTROLLARE	SCENARIO GLOBALE	MATRICE DI CONFRONTO	RIPRISTINARE	DATA BASE	SISTEMA ESPERTO
SIMULAZIONI	PENETRATION TEST	MANUTENZIONE	PREDITTIVA	CONSERVATIVA	CORRETTIVA	EVOLUTIVA

IL PROBLEMA È: PRENDERE DECISIONI CORRETTE . . . NEL PIÙ BREVE TEMPO POSSIBILE

LE OPPORTUNITA’

- ✓ Maggiore **comprensione** e **valutazione tempestiva** delle situazioni emergenziali.
- ✓ Gestione **semplificata** di **grandi volumi di dati** e informazioni.
- ✓ Innalzamento globale della **qualità dei servizi** erogati e della **sicurezza**.
- ✓ Possibilità di **aggiungere valore** all’infrastruttura. Contenimento costi.
- ✓ **Semplificazione** ed **automatizzazione** delle procedure operative e di manutenzione.
- ✓ Incremento di **efficienza ed efficacia negli scenari** complessi e nel **processo decisionale**.
- ✓ Dispiego contenuto di **risorse umane**, **bassi costi di esercizio** e maggiore **accuratezza**.

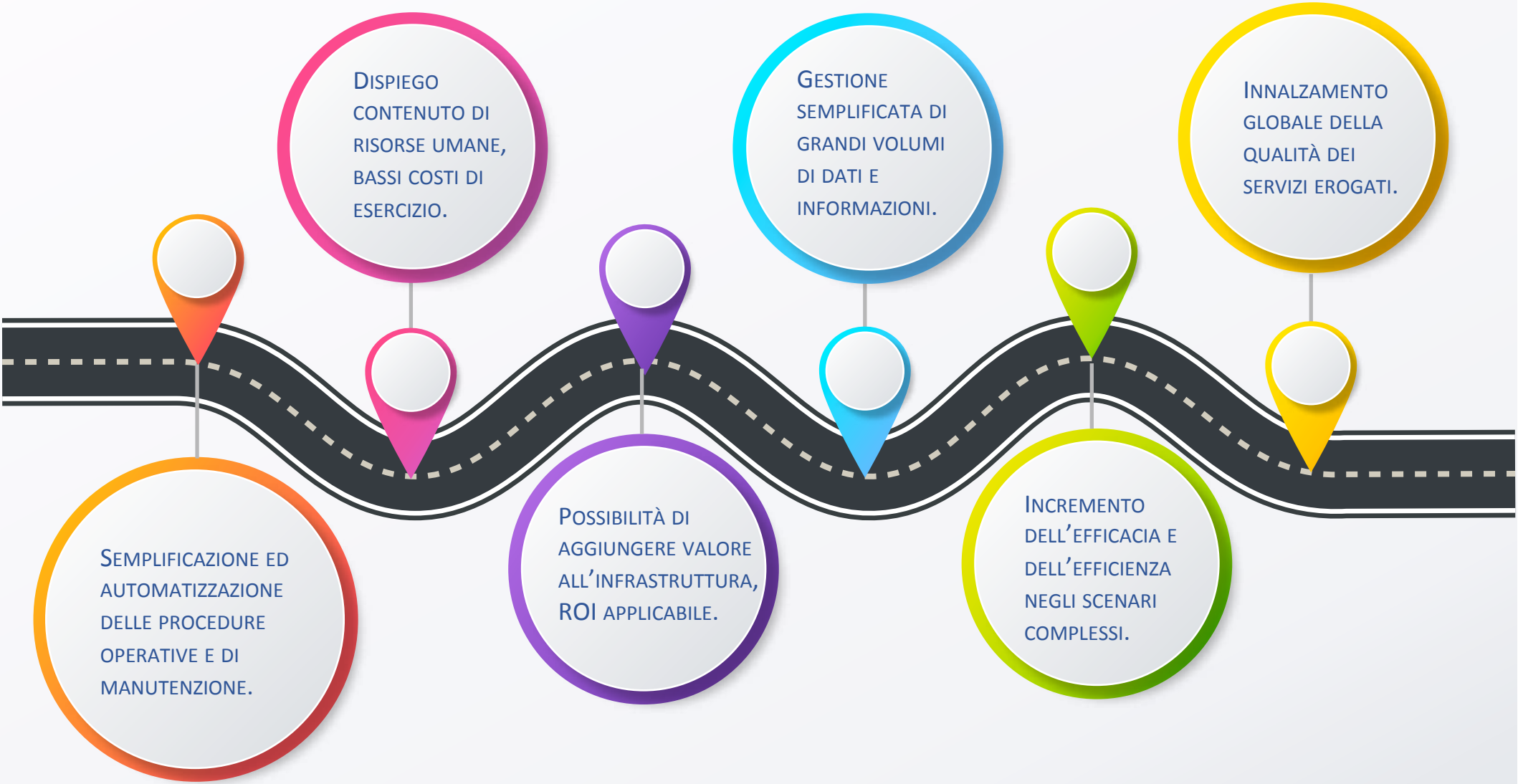
UNA SOLUZIONE UNICA

UNA PIATTAFORMA CON UN FRONT-END UNIFICATO

E UN BACK-END CAPACE DI DIALOGARE CON QUALUNQUE TECNOLOGIA IN CAMPO.

Sistemi, Soluzioni e Servizi integrati che consentono di monitorare gli Asset, velocizzare le informazioni dei sistemi di sicurezza, metterli in matrice automatica di confronto, valutare le contromisure ed operare di conseguenza, applicando un modello di intervento unificato che razionalizzi tutti i flussi operativi di sicurezza fisica ed automazione.

IL SUPPORTO ALLE DECISIONI



LE CRITICITA’

TUTTO È CENTRALE E PRIMARIO, NON ESISTE LA PERIFERIA ED IL RESIDUALE.

Il concetto di sicurezza fisica che prevede sistemi più critici e sensibili, deve essere rivisto in un nuovo paradigma: **tutti i sistemi connessi**, anche residuali, devono essere considerati **potenzialmente critici e sensibili.**

Occorre innanzitutto determinare le **nuove vulnerabilità** introdotte e poi proteggere ciascun elemento che fa parte del sistema e i canali di comunicazione tra essi.

In ogni caso, le regole base per misurare **il rischio**, rimangono invariate ed utilizzano gli stessi parametri macro di riferimento per definire **la probabilità** e **l’entità** di ciò che può accadere.

E’ quindi sempre importante effettuare con chiarezza **un’analisi di contesto** e definire in dettaglio quali siano **i beni da proteggere** e gli eventuali **offender**.

Tutto ciò anche per dare **equilibrio** e **sostenibilità** ad un’azione di **protezione** e **prevenzione** che sia **coerente** con i reali rischi e conseguenze di un’azione criminosa.

LA SICUREZZA DEI SISTEMI

Convenzionalmente si indicano tre caratteristiche fondamentali per la sicurezza dei sistemi: ***riservatezza*, *integrità* e *disponibilità*.**

Da un contesto di ***computer security*** a uno di ***network security***, anche le proprietà di ***autenticità*** e ***non ripudiabilità*** assumono un ruolo essenziale.

Possono quindi essere definite cinque caratteristiche fondamentali:

01 **Riservatezza**
02 **Integrità**
03 **Autenticità**
04 **Non-ripudio**
05 **Disponibilità**

LA SICUREZZA DEI SISTEMI

01

Riservatezza

Le informazioni/dati memorizzati in un sistema o scambiate tra due entità devono essere **protette da letture non autorizzate** ed essere accessibili solo ai soggetti ed ai processi che ne hanno diritto, in base alle policy definite nel Sistema.
La *segretezza* o *confidenzialità*, si ottiene soprattutto mediante tecniche crittografiche.

LA SICUREZZA DEI SISTEMI

02

Integrità

Le informazioni/dati memorizzati in un sistema o scambiate tra due entità devono essere **protette da modifiche non autorizzate** (alterazione, cancellazione o aggiunta).
L'integrità può essere garantita da meccanismi di *checksum (sequenza di bit utilizzata per verificare l'integrità di un dato)*, da tecniche crittografiche (es. firma digitale, meccanismi di controllo dell'accesso ai dati).

03

Autenticità

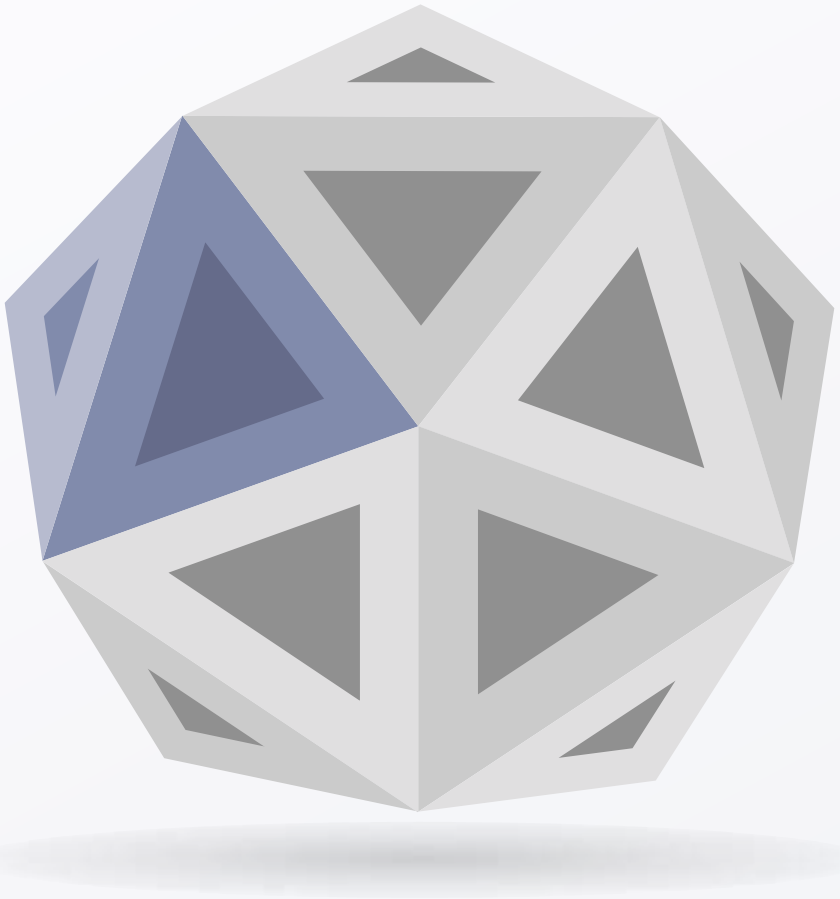
Identificazione certa della provenienza di una informazione/ dato: **verificare l'identità dell'origine**. Le informazioni sul mittente devono essere garantite da tecniche crittografiche.
Per l'**autenticazione,** al fine di ottenere l'accesso ad un servizio, è necessario dimostrare preliminarmente la propria identità presso il sistema che ospita tale servizio.

04

Non - Ripudiabilità

Chi genera ed invia un dato **non deve poter negare** successivamente di averlo generato ed inviato, né deve poterne negare il contenuto. Allo stesso modo, chi riceve un dato, non deve poter negare di averlo ricevuto, né deve poterne negare il contenuto.
Nell'ICT la non ripudiabilità è ottenuta attraverso tecniche crittografiche.

LA SICUREZZA DEI SISTEMI



05

Disponibilità

Risorse, servizi e dati di un sistema devono essere **sempre accessibili** agli utenti legittimi. I sistemi devono risultare funzionanti con il livello di prestazioni prestabilito e nessuno deve essere in grado di minacciare il loro funzionamento regolare. Es. attacchi denial of service *(malfunzionamento dovuto ad attacco informatico in cui si fanno esaurire le risorse di un sistema che fornisce un servizio)*, ma anche disastri naturali (cali di tensione, guasti all'hardware).

TIPOLOGIE DI ATTACCHI

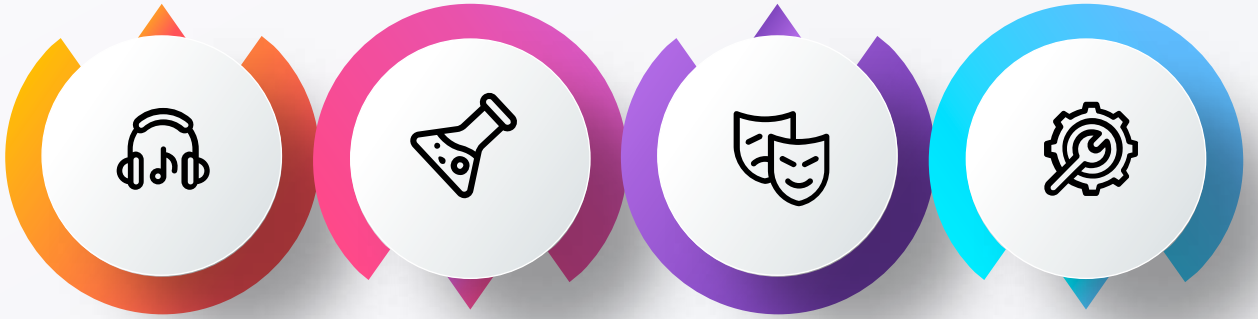
Di seguito vengono forniti alcuni semplici esempi dei più ricorrenti **attacchi** che costituiscono una *violazione delle proprietà di sicurezza* sopra descritte

INTERCETTAZIONI

Violano la proprietà di riservatezza dell'informazione

FALSIFICAZIONI

Violano i requisiti di autenticità e di non-ripudio



ALTERAZIONI

Violano il requisito di integrità

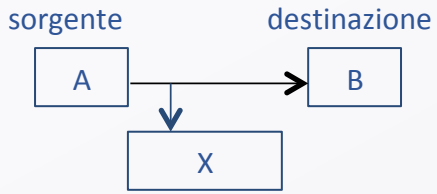
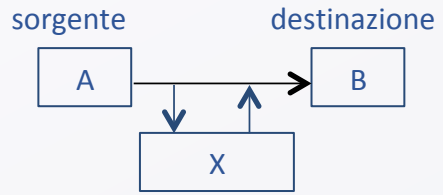
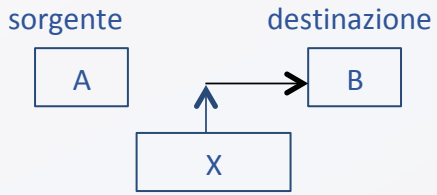
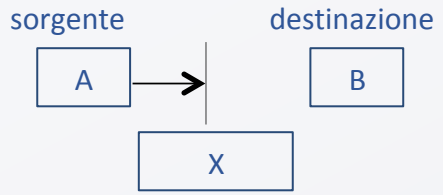
SABOTAGGI O INTERRUZIONI

Minacciano la disponibilità del sistema

Nella Tabella seguente sono elencate le caratteristiche delle principali categorie di attacco.

TIPOLOGIE DI ATTACCHI

CATEGORIE DI ATTACCO: CARATTERISTICHE PRINCIPALI

Attacco	Schema	Azione
Flusso standard di informazione		▪ Invio pacchetto IP ▪ Invio mail ▪ Accesso WEB ▪ Accesso Data Base
Intercettazione		▪ Sniffing pacchetti di rete ▪ Furto dati (crittoanalisi) ▪ Furto dati (analisi del traffico) ▪ Furto dati (covert channel)
Alterazione		▪ Modifiche non autorizzate a file o programmi ▪ Attacchi “man in the middle” ▪ Azioni di disturbo del canale di comunicazione
Generazione		▪ Masquerading ▪ Spoofing ▪ Intrusioni } identità fittizia per accesso non autorizzato alle informazioni
Interruzione		▪ Denial of service: negazione del servizio ▪ Flooding, resource starvation, mail storm ▪ Crashing di applicazioni ▪ Sabotaggio linee di comunicazione ▪ Danneggiamenti fisici } traffico in entrata

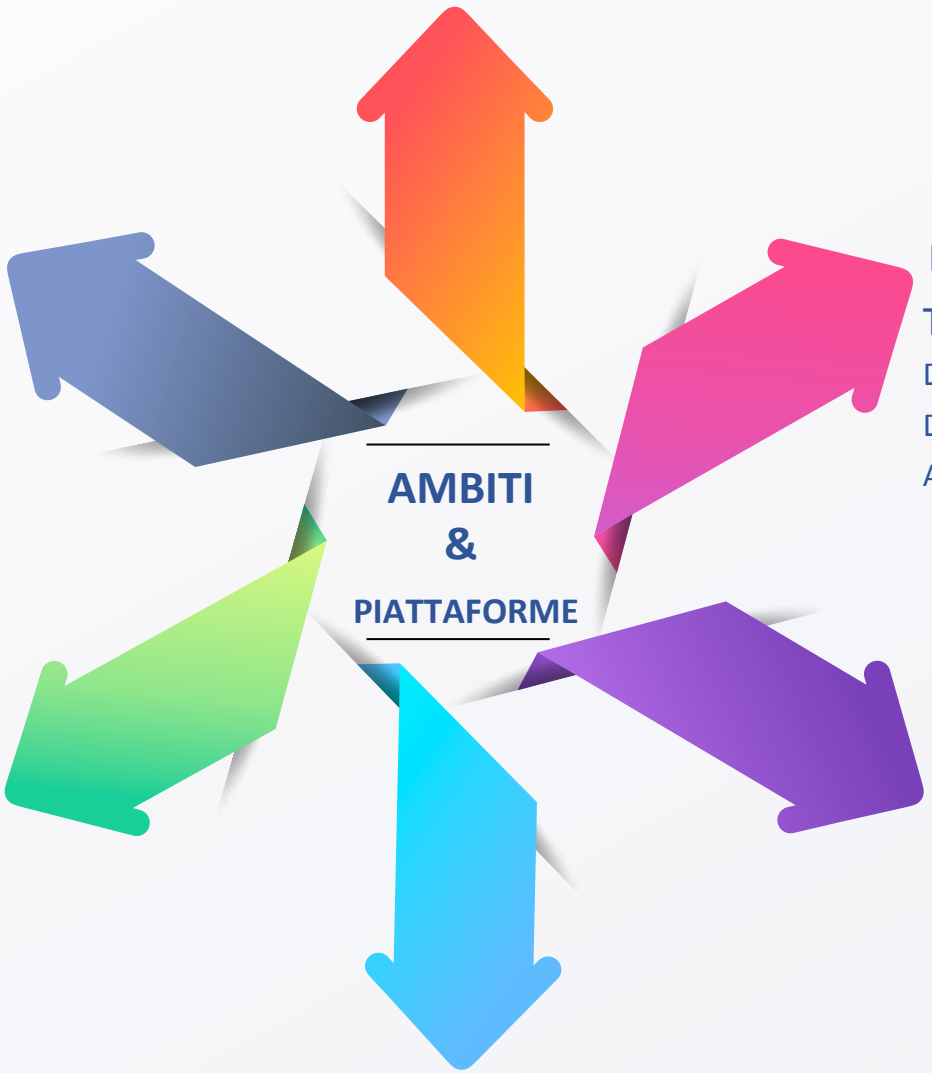
ANIE FEDERAZIONE
Technologies for our future
CONFINDUSTRIA

IT (FIREWALL)

PREROGATIVE DI ACCESSO / VALIDAZIONE -
SICUREZZA PORTE DI ACCESSO AI SINGOLI SISTEMI

RESILIENZA (BACKUP)

PROTEZIONE E SEGMENTAZIONE
RESILIENZA / BCRS
VIRTUALIZZAZIONE / BACKUP



NETWORK LINK

TRASMISSIONI SICURE / ALGORITMI
DI CRITTOGRAFIA / AUTENTICAZIONE
DATI - PROTEZIONE E RICHIESTA
ACCESSO RETE DA REMOTO

PROCEDURE

LOGICHE DI ACCREDITAMENTO, DI
ACCESSO E DI INTERVENTO.
AGGIORNAMENTI E PENETRATION
TEST PERIODICI

ARCHITETTURA DI SISTEMA

SUDDIVISIONE IN ZONE (FISICHE
E LOGICHE) ISOLATE TRA LORO
E, OVE POSSIBILE, CON IL
MONDO ESTERNO

SISTEMI DI MONITORAGGIO

ALLARMI/ANOMALIE - SUPERVISIONE E MONITORAGGIO
PSIM - DATA ANALYTICS
ARTIFICIAL INTELLIGENCE (PREDITTIVITÀ)

I PUNTI DI ATTENZIONE

IN GENERALE

- Cultura
- Informazione
- Formazione
- Norme e Procedure
- Certificazioni
- Test e Controlli
- Incentivazioni
- Politiche Europee
- Investimenti Nazionali

DI DETTAGLIO

- Supervisione e Monitoraggio (PSIM – Data Analytics – Artificial Intelligence)
- Protezione e Segmentazione
- Prerogative di Accesso / Validazione
- Protezione e richiesta accesso rete da remoto
- Sicurezza porte di accesso ai singoli sistemi
- Suddivisione in zone isolate tra loro
- Trasmissioni sicure / Algoritmi di Crittografia / Autenticazione dati
- Aggiornamenti e Penetration Test periodici
- Virtualizzazione / Backup
- Resilienza / BCRS

IL TREND DELLA CERTIFICAZIONE

CYBER SECURITY ACT

I LIVELLI DI SICUREZZA:

- FONDAMENTALE (Base) – Autocertificazione volontaria
- SOSTANZIALE – Verifica/monitoraggio da parte di un ente terzo
- ALTO (Servizi essenziali: Energia/Trasporto/Banche/Infrastrutture Sanitarie, Digitali, ecc.) Ente terzo esegue dei test (audit)

ATTIVITA':

- RISK ANALISYS
- RISK ASSESMENT
- SCHEMI DI CERTIFICAZIONE (Prodotti – Processi – Servizi)

SCHEMI DI CERTIFICAZIONE:

- Prodotto
- Processo (azienda costruttrice)
- Procedure (back-up, penetration test, ecc.)
- Architettura di sistema
- Rete e connessioni (interne – esterne)
- Resilienza (capacità di resistere) intervenire – mitigare – ripristinare

AGENTI INTELLIGENTI

INTERNET DELLE COSE (IOT) o INTELLIGENZA ARTIFICIALE (A.I.)?

Internet Of Things - "Internet delle cose" - E' l'espressione utilizzata per definire la rete di apparecchiature, sensori e dispositivi, **diversi dai computer**, connessi a Internet.
Possono essere sensori per automobili, radio, impianti di vario tipo, ma anche elettrodomestici, lampadine, telecamere, pezzi d'arredamento, container per trasporto merci, ecc.
In generale qualunque dispositivo elettronico equipaggiato con un software che gli permetta di scambiare dati con altri oggetti connessi.

Artificial Intelligence - "Intelligenza Artificiale" - E' la capacità di un sistema hardware di risolvere problemi o svolgere compiti e attività tipici della mente e dell'abilità umane.
Nel settore informatico, l'AI è la disciplina che si occupa di realizzare macchine (hardware e software) in grado di "agire" autonomamente (risolvere problemi, compiere azioni, ecc.).
Le capacità di ragionamento o di comportamento di un sistema intelligente si misurano determinando il grado di similitudine o il risultato ottenuto, paragonandolo con il comportamento umano o il comportamento ideale, attraverso il modo di agire.

L'INTELLIGENZA ARTIFICIALE

AGIRE UMANAMENTE

01

IL RISULTATO DELL'OPERAZIONE COMPIUTA DAL SISTEMA INTELLIGENTE NON È DISTINGUIBILE DA QUELLA SVOLTA DA UN UMANO.

PENSARE UMANAMENTE

IL PROCESSO CHE PORTA IL SISTEMA INTELLIGENTE A RISOLVERE UN PROBLEMA RICALCA QUELLO UMANO. QUESTO APPROCCIO È ASSOCIATO ALLE SCIENZE COGNITIVE.

02

PENSARE RAZIONALMENTE

03

IL PROCESSO CHE PORTA IL SISTEMA INTELLIGENTE A RISOLVERE UN PROBLEMA È UN PROCEDIMENTO FORMALE CHE SI RIFÀ ALLA LOGICA.

AGIRE RAZIONALMENTE

IL PROCESSO CHE PORTA IL SISTEMA INTELLIGENTE A RISOLVERE IL PROBLEMA È QUELLO CHE GLI PERMETTE DI OTTENERE IL MIGLIOR RISULTATO ATTESO DATE LE INFORMAZIONI A DISPOSIZIONE.

04

L'INTELLIGENZA ARTIFICIALE

GLI AGENTI INTELLIGENTI HANNO IMPLICAZIONI ETICHE?

Sì, riguardano ad esempio la capacità degli oggetti connessi o della rete stessa di prendere decisioni.

- Se una vettura senza conducente ha come unica alternativa all'investire un bambino, che sta attraversando la strada, quella di puntare verso un marciapiede dove camminano dei pedoni, che scelta farà, o meglio, dovrà fare?
- Se la medesima autovettura si trova davanti un pedone che attraversa la strada fuori dalle strisce pedonali, sarà giusto investirlo, salvaguardando la vita della persona che trasporta?

Quale sarà la scelta GIUSTA'? E CHI la decide?

Chi sarà il responsabile per quella scelta? Chi valuta le priorità legali, umane, sociali e le relative ripercussioni dell'azione? Il programmatore che ha scritto il codice di controllo dell'auto? Il produttore? Un organismo apposito? Oppure nessuno?

Oggi, tali azioni sono competenza e responsabilità dell'uomo e sono chiaramente normate ed in ogni caso, spesso non hanno un problema etico, in quanto dipendono dall'istinto dell'uomo (come negli esempi espressi) e non da una programmazione fatta a priori con regole certe.

In futuro, con l'applicazione e l'intervento dell'IA, con la capacità intrinseca della macchina di imparare dalla propria esperienza, quale modello di esperienza da fare sarà quello GIUSTO?

RIASSUMENDO


ANIE
FEDERAZIONE
Technologies for our future
CONFINDUSTRIA
LA
TECNOLOGIA
È AL CENTRO

GRAZIE

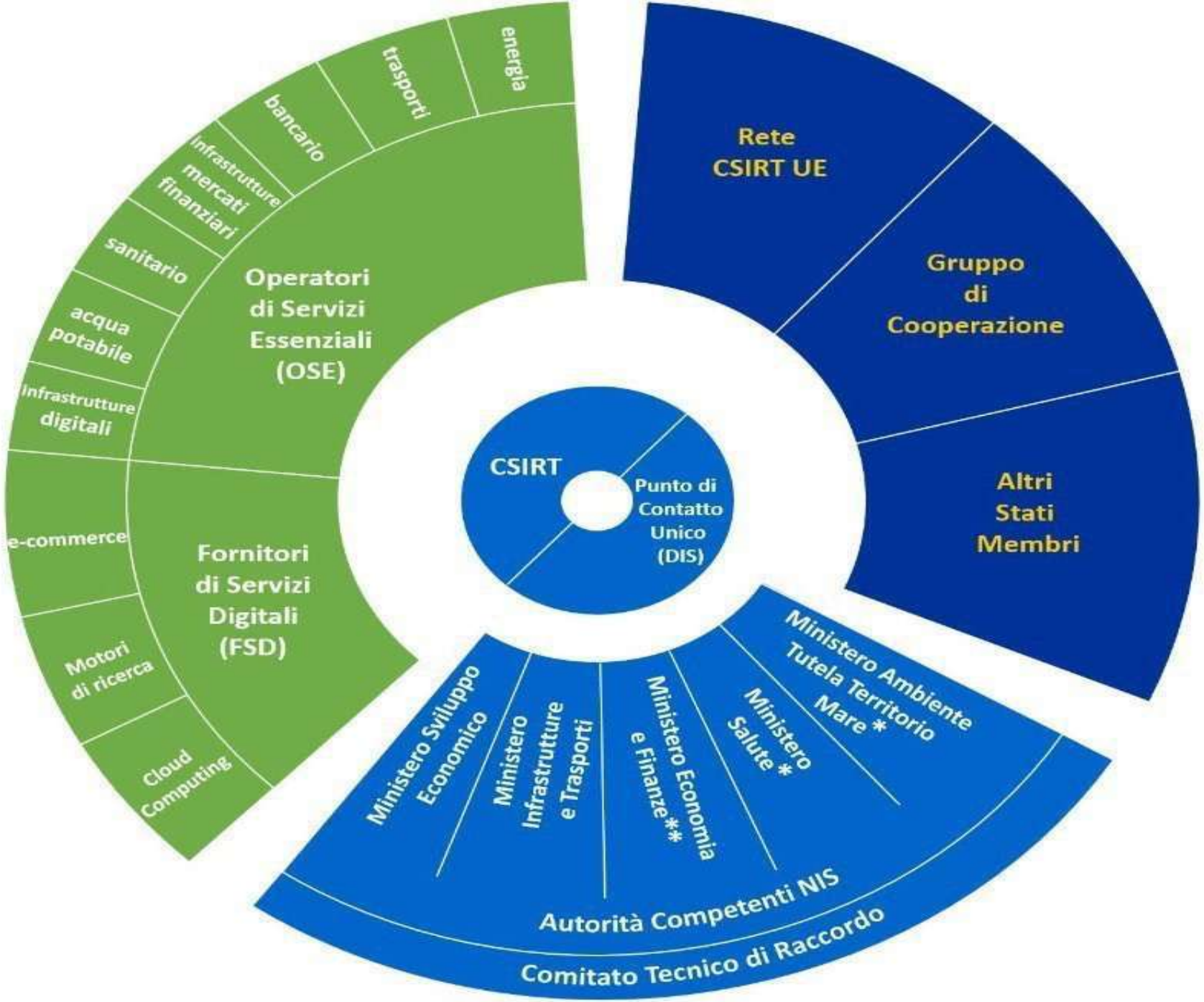
Giulio Iucci

CARNELUTTI
LAW FIRM

Sicurezza Cibernetica: Disciplina Europea e Italiana

Avv. Stefano Mele

La Direttiva NIS



Servizi interessati

Attori governativi NIS

Meccanismi della cooperazione europea

* più regioni e province autonome di Trento e di Bolzano

** in collaborazione con le autorità di vigilanza di settore, Banca d'Italia e Consob

Direttiva NIS e Operatori di Servizi Essenziali (OSE)

La creazione di obblighi di sicurezza e di notifica per gli operatori di servizi essenziali (*art. 12*) richiede che le società:

- **adottino misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano nelle loro operazioni**
- **adottino misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali, al fine di assicurare la continuità di tali servizi**
- **notifichino al CSIRT italiano e, per conoscenza, all'Autorità competente NIS, senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti. Le notifiche includono le informazioni che consentono di determinare un eventuale impatto transfrontaliero dell'incidente**

Direttiva NIS e Operatori di Servizi Essenziali (OSE)

Le autorità competenti NIS valutano il rispetto da parte degli operatori di servizi essenziali degli obblighi previsti, nonché i relativi effetti sulla sicurezza della rete e dei sistemi informativi (*art. 13*), richiedendo di fornire:

- **le informazioni necessarie per valutare la sicurezza della loro rete e dei loro sistemi informativi, compresi i documenti relativi alle politiche di sicurezza**
- **la prova dell'effettiva attuazione delle politiche di sicurezza, come i risultati di un *audit* sulla sicurezza svolto dall'autorità competente o da un revisore abilitato e, in quest'ultimo caso, metterne a disposizione dell'autorità competente i risultati, inclusi gli elementi di prova**

A seguito della valutazione delle informazioni o dei risultati degli *audit* sulla sicurezza, l'autorità competente NIS può emanare istruzioni vincolanti per gli operatori di servizi essenziali al fine di porre rimedio alle carenze individuate

Il Perimetro di Sicurezza Nazionale Cibernetica

Il perimetro di sicurezza nazionale cibernetica

L'obiettivo del perimetro di sicurezza cibernetica è quello di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale

Il perimetro di sicurezza nazionale cibernetica

In via preliminare, occorre fin da subito evidenziare come l'intento del legislatore italiano non sia quello di estendere l'applicazione del Perimetro di Sicurezza Nazionale Cibernetica ad ogni operatore nazionale, sia esso pubblico o privato, bensì di sensibilizzare verso una cultura della gestione dei rischi cibernetici e di garantire la segnalazione degli incidenti informatici solo da parte di quei soggetti:

1. **che abbiano una sede nel territorio nazionale;**
2. **da cui dipenda l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per gli interessi dello Stato**

e, all'interno di questo alveo, solo nel caso in cui:

3. **dal malfunzionamento o interruzione – anche parziali – o dall'utilizzo improprio delle loro reti, dei sistemi informativi e dei servizi informatici possa derivare un pregiudizio per la sicurezza nazionale**

Cosa occorrerà fare?

Predisporre, aggiornare con cadenza annuale e inviare al Ministero dello Sviluppo Economico un elenco delle reti, dei sistemi informativi e dei servizi informatici di pertinenza, comprensivo della relativa architettura componentistica

(I criteri in base ai quali la Società dovrà predisporre e aggiornare con cadenza almeno annuale questo elenco saranno disciplinati con Decreto del Presidente del Consiglio dei ministri (DPCM) entro 4 mesi dall'entrata in vigore della legge di conversione del decreto)

Cosa occorrerà fare?

Adottare le misure di sicurezza elaborate dal Ministero dello sviluppo economico volte a garantire un elevato livello di sicurezza delle reti, dei sistemi e dei servizi rilevanti

(L'elaborazione di tali misure sarà disciplinata nei termini e nelle modalità attuative con un Decreto del Presidente del Consiglio dei ministri (DPCM) entro 10 mesi dall'entrata in vigore della legge di conversione del decreto)

Cosa occorrerà fare?

Notificare al CSIRT italiano eventuali incidenti aventi impatto sulle reti, i sistemi e i servizi rilevanti

(Le procedure utili per la notifica al CSIRT italiano saranno disciplinate con Decreto del Presidente del Consiglio dei ministri (DPCM) entro 10 mesi dall'entrata in vigore della legge di conversione del decreto)

Cosa occorrerà fare?

Dare comunicazione al Centro di valutazione e certificazione nazionale (CVCN) ogni volta in cui dovrà procedere all'affidamento di forniture di beni, sistemi e servizi ICT destinati ad essere impiegati sulle reti, sui sistemi e per l'espletamento dei propri servizi rilevanti, diversi da quelli necessari per lo svolgimento delle attività di prevenzione, accertamento e repressione dei reati

Il CVCN potrà imporre condizioni e test di hardware e software a carico della società (45 giorni + 15, altrimenti silenzio assenso). In tal caso, i relativi bandi di gara o contratti dovranno essere integrati di clausole che subordinano l'affidamento della fornitura o del servizio al rispetto delle condizioni e all'esito favorevole dei test

(Le procedure, le modalità e i termini previsti saranno disciplinati da un regolamento, adottato entro 10 mesi dalla data di entrata in vigore della legge di conversione del decreto)

I poteri del Presidente del Consiglio in caso di crisi cibernetica

Il Perimetro di Sicurezza Nazionale Cibernetica prevede anche alcune attribuzioni emergenziali in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi e servizi

In tali casi, su deliberazione del Comitato Interministeriale per la Sicurezza della Repubblica (CISR), il Presidente del Consiglio dei ministri può disporre, ove indispensabile e per il tempo strettamente necessario all'eliminazione dello specifico fattore di rischio o alla sua mitigazione, secondo un criterio di proporzionalità, la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati


MEDIUM | HIGH
SECURITY

CARNELUTTI
LAW FIRM

Attori e scenari nel mercato della cyber security

Filippo Cavallarin

Come vengono scoperte le vulnerabilità?

Aziende

Aziende

Ricercatori

Ricercatori

Gloria

Lucro

Ricercatori

Gloria

Disclosure

Viene risolta
la vulnerabilità

Lucro

Ricercatori

Gloria

Disclosure

Viene risolta
la vulnerabilità

Lucro

1

Aziende che comprano 0day

2

I criminali che comprano 0day
(vari blackmarket)

Ricercatori

Gloria

Disclosure

Viene risolta
la vulnerabilità

Lucro

1

Aziende che comprano 0day

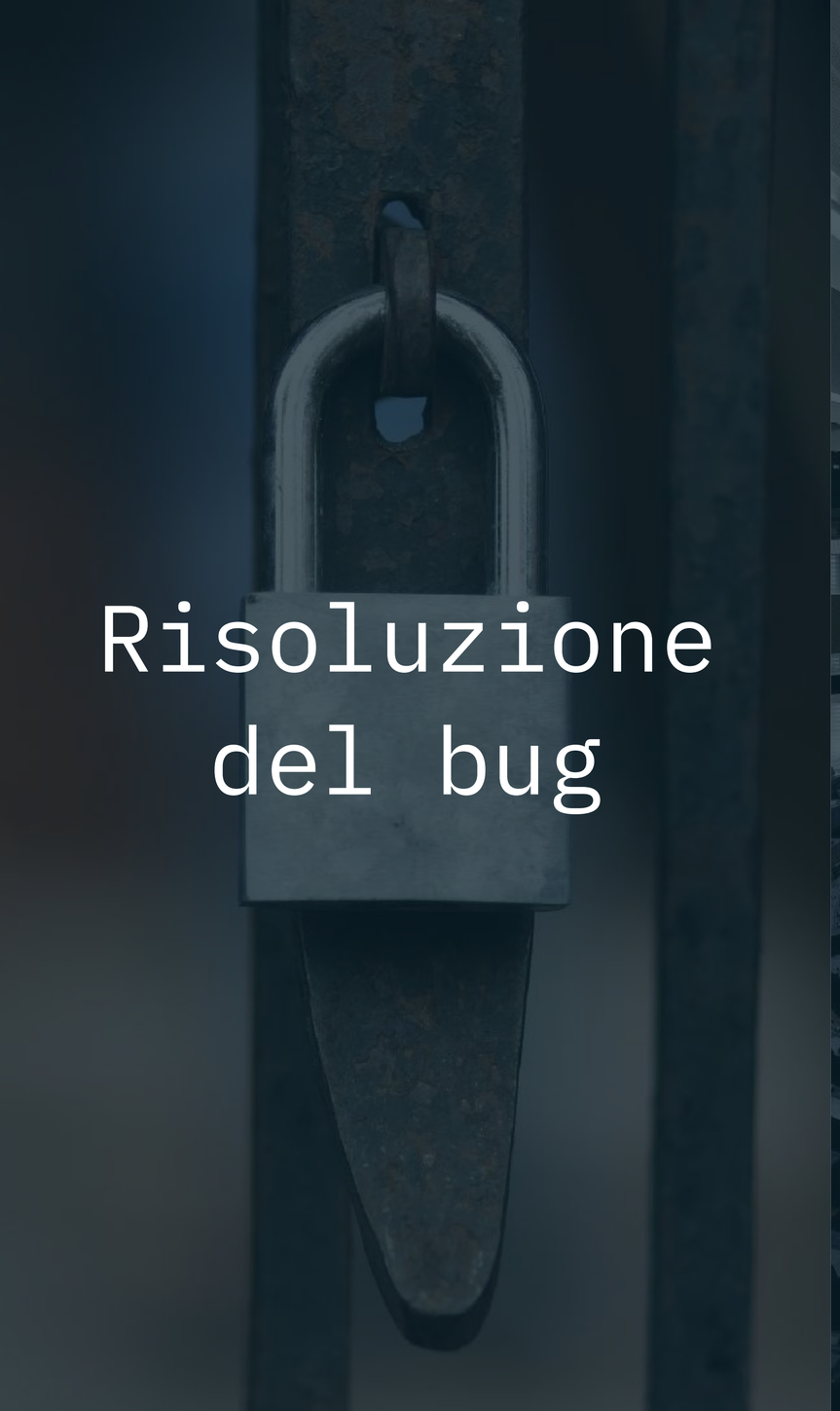
2

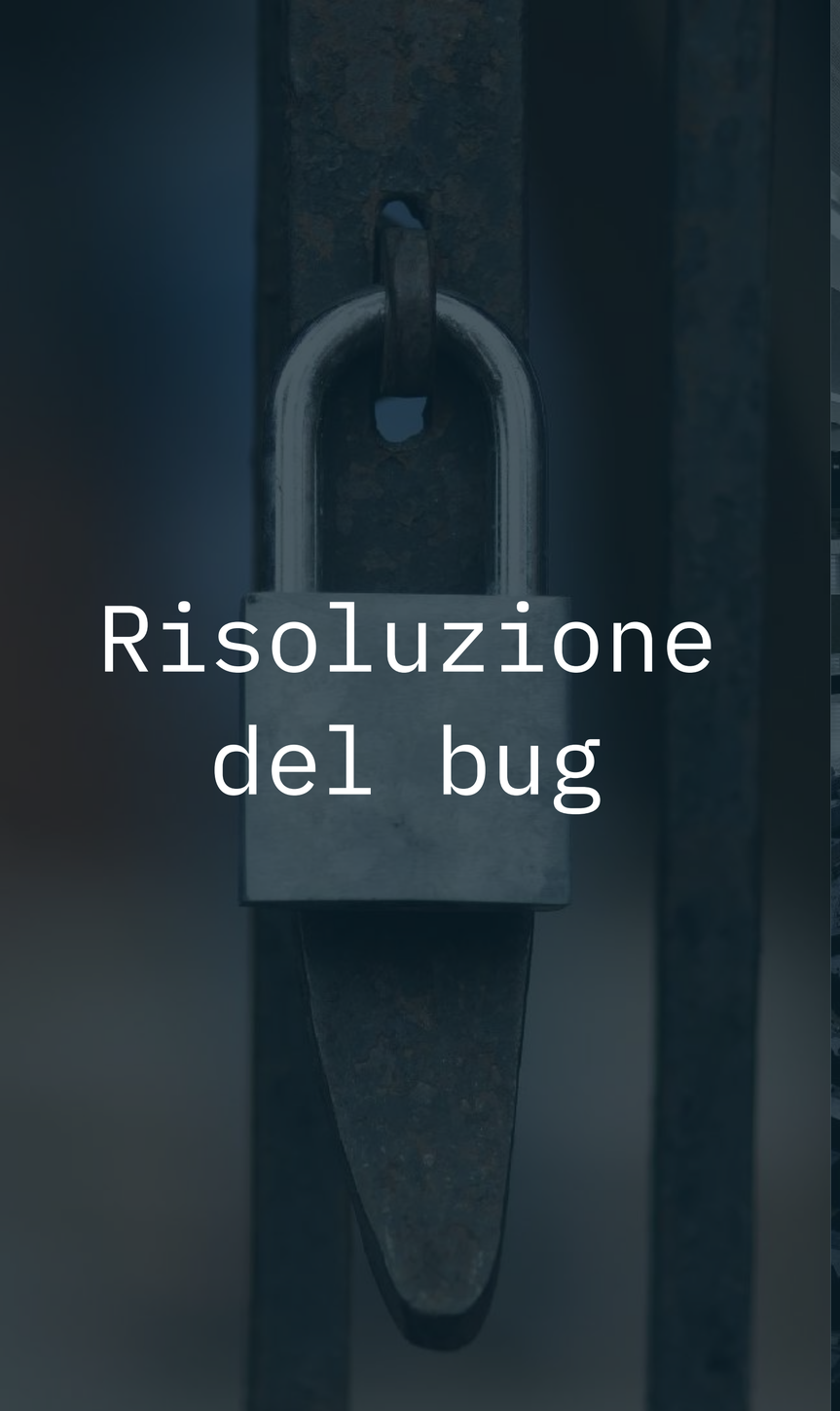
I criminali che comprano 0day
(vari blackmarket)

La vulnerabilità resta
in mano a pochi

Come viene usata una vulnerabilità?

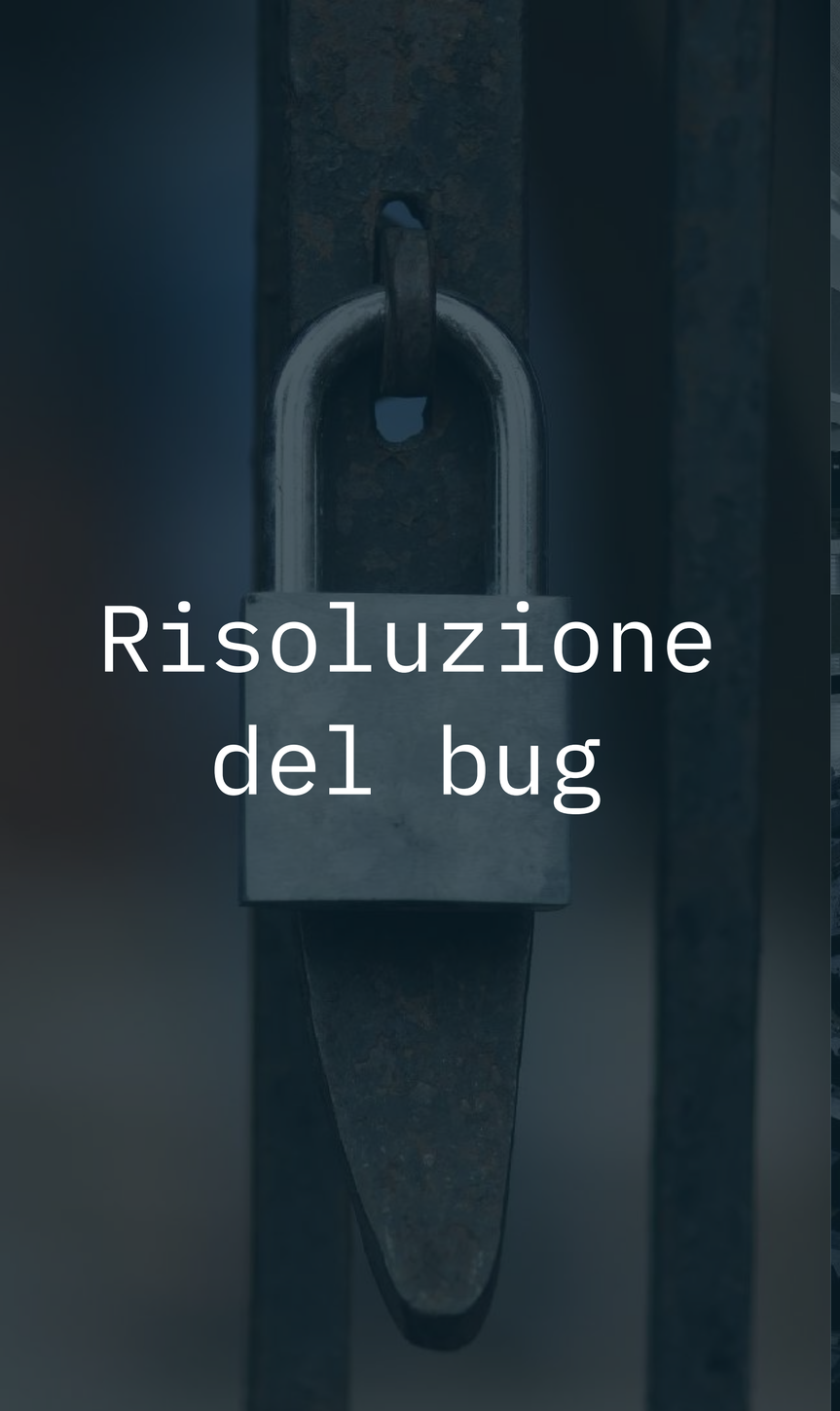
Risoluzione del bug





Risoluzione
del bug

Governi
e forze
dell'ordine



Risoluzione del bug

Governi e forze dell'ordine

Cyber criminali

Quali mercati esistono?

Bounty

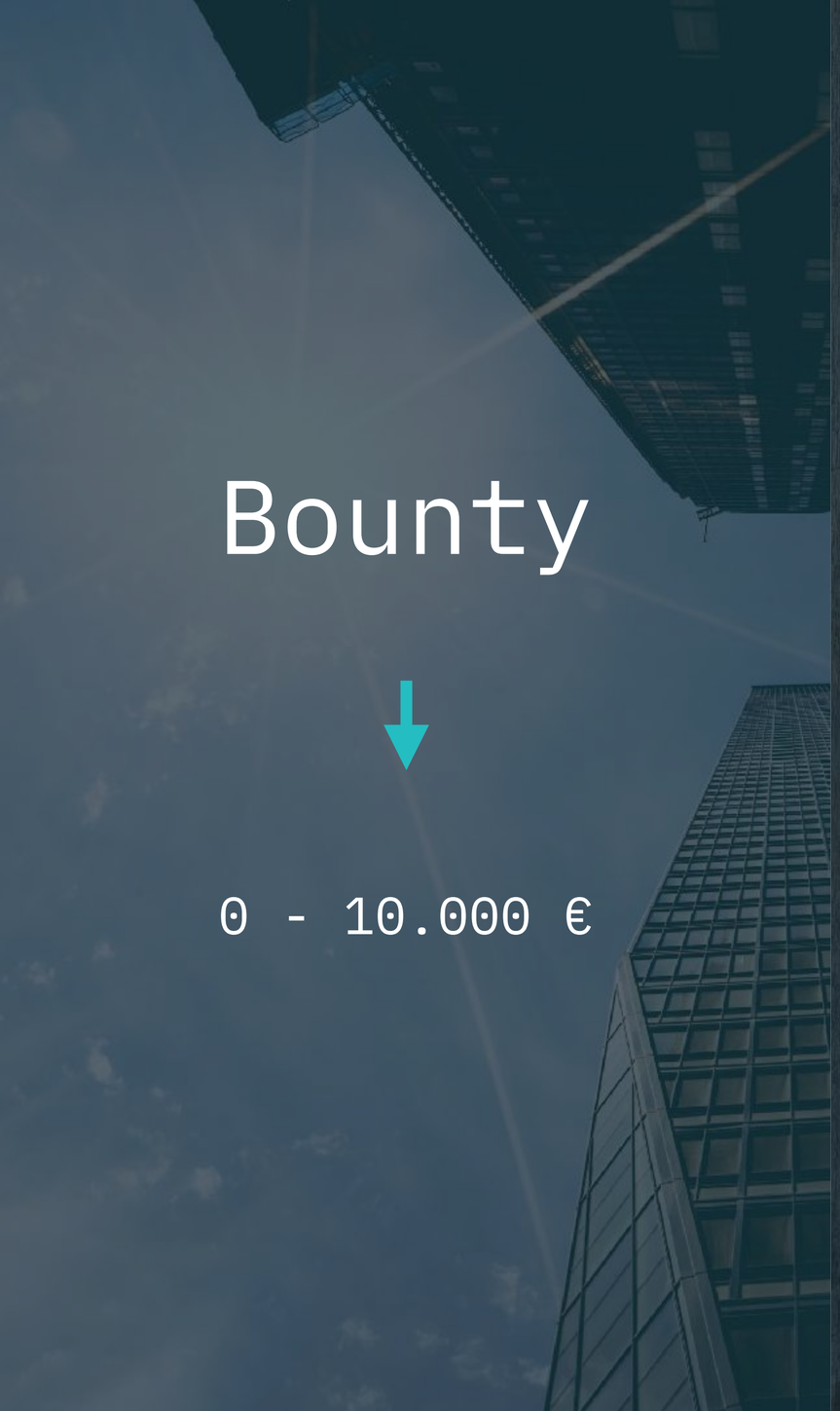
0 - 10.000 €

Bounty

0 - 10.000 €

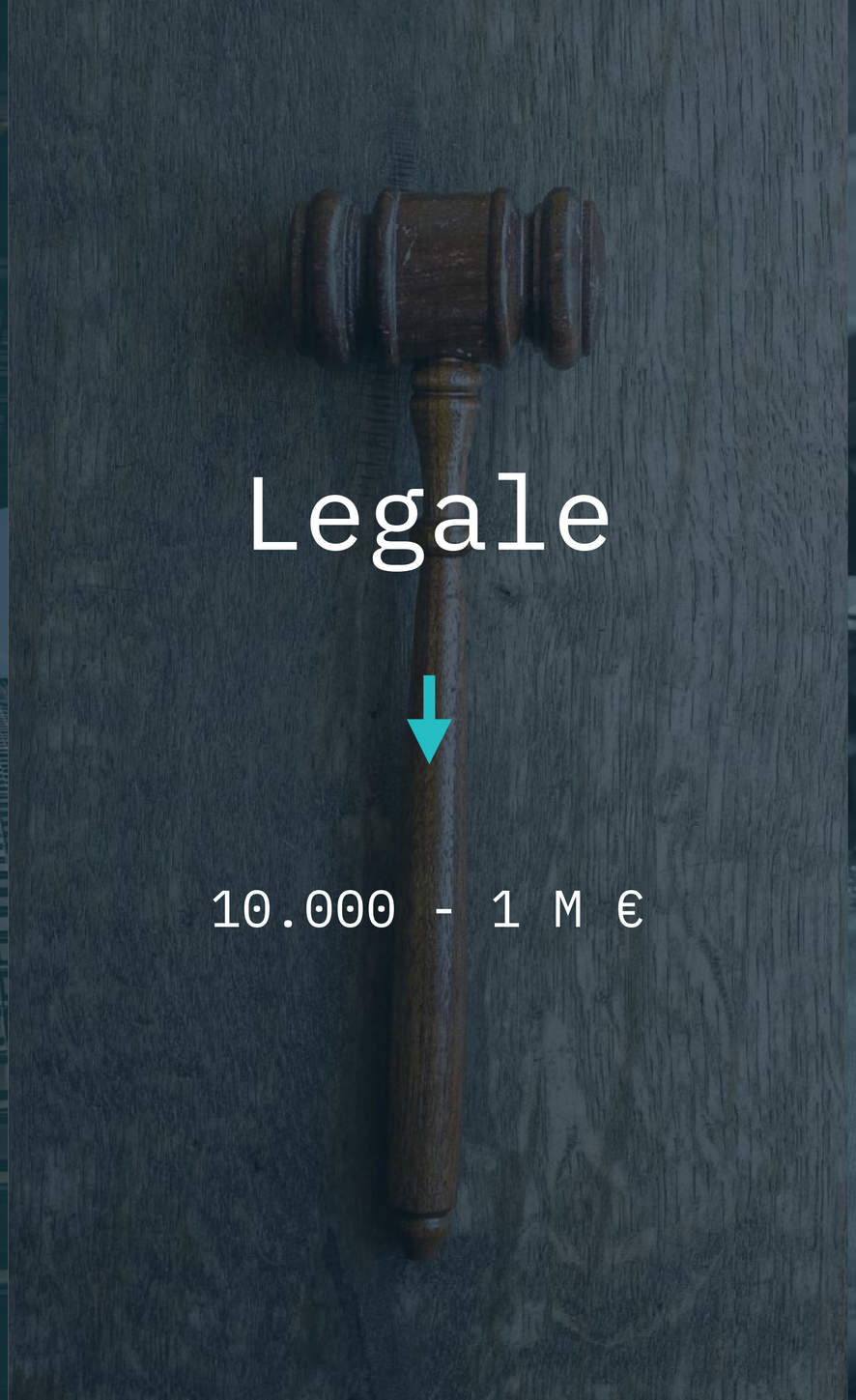
Legale

10.000 - 1 M €



Bounty

0 - 10.000 €



Legale

10.000 - 1 M €

Illegale

Non ci sono dati

Chi ha in mano queste armi?

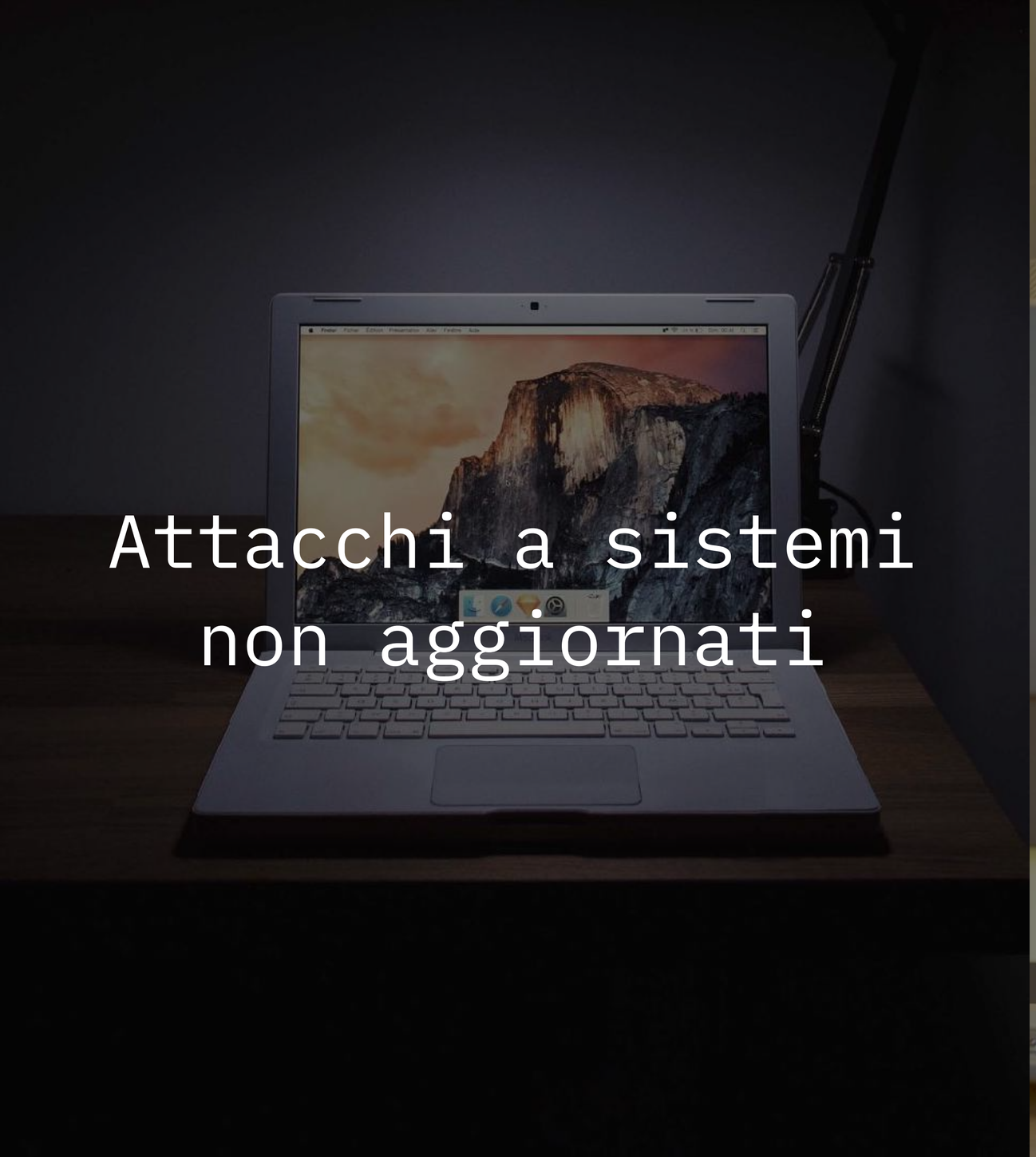
Gruppi di hacker

Gruppi
di hacker

Governi

Che rischio corrono le aziende?

Attacchi a sistemi non aggiornati



Attacchi a sistemi non aggiornati

Attacchi a persone

Che strumenti esistono per difendersi?

Strumenti

Antivirus

Firewall

IDS

Honeypot

Strumenti

Antivirus

Firewall

IDS

Honeypot

Procedure

Update dei sistemi

Security assessments

Penetration tests

Formazione del personale

FILIPPO CAVALLARIN

filippo@fcvl.net

Referenze

https://www.zdnet.com/article/the-scariest-hacks-and-vulnerabilities-of-2019/

https://www.zdnet.com/article/google-finds-malicious-sites-pushing-ios-exploits-for-years/

https://twitter.com/ihackbanme/status/1064400858245402625

https://zerodium.com/program.html

GRUPPO TIM

CYBER SECURITY E TRASFORMAZIONE DIGITALE

Milano, 2 dicembre 2019

Dalla mistica dell'incidente all'organizzazione

Guido Allegrezza
Resp. Compliance, Governance & Security

TrustTechnologies

Abbiamo sempre fatto così, ovvero nulla è peggio che cambiare

Da:
https://commons.wikimedia.org/wiki/File:Libya_4924_Pictograms_Tadrart_Acacus_Luca_Galuzzi_2007_cropped.jpg
- Licenza CCA-Condividi allo stesso modo 2.5 Generic

Non è mai successo niente, ovvero l’ottimismo dell’incoscienza

J. G. Fragonard, The Swing– Immagine di dominio pubblico da https://commons.wikimedia.org/wiki/File:Fragonard,_The_Swing.jpg

Com’è potuto accadere? ovvero la mistica dell’incidente

A. Sanquirico, scena per L’utimo giorno di Pompei di G. Pacini,– Immagine di dominio pubblico da https://upload.wikimedia.org/wikipedia/commons/b/bd/Eruption_of_Vesuvius_from_Pacini%27s_opera_L%27ultimo_giorno_di_Pompei.jpg

Chi è stato?

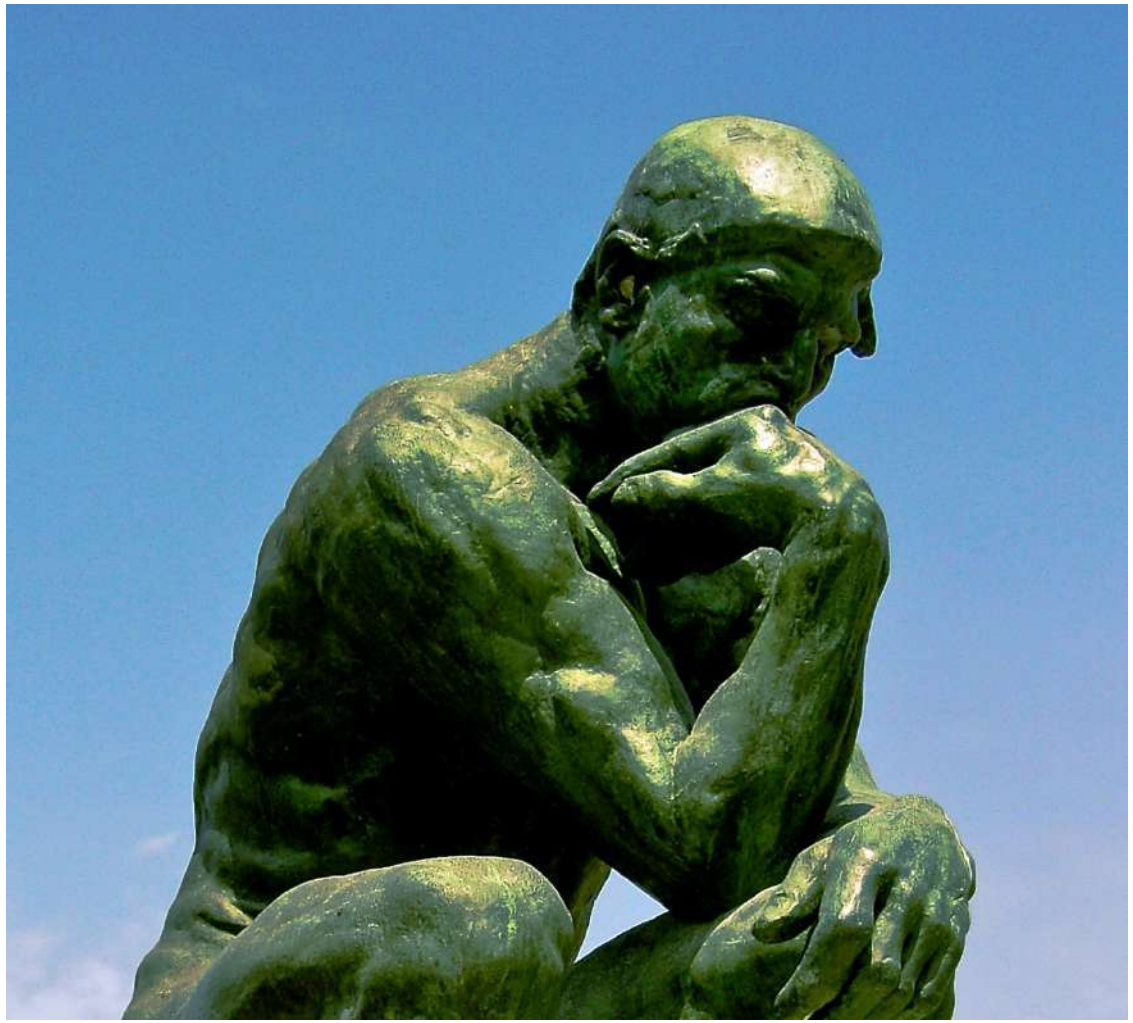
ovvero

le gioie

dell’auditor

Jean-Leon Gerome, Pollice Verso - Pubblico dominio, da https://commons.wikimedia.org/w/index.php?curid=12278

A meno di dolo o negligenza grave, non sarebbe meglio…



- **… chiedersi in cosa abbiamo sbagliato, invece che chiedersi come è potuto accadere?**
  Sembra una banalità, ma per la cyber security vale l'equazione «migliorare=prevenire»
- **… chiedersi se abbiamo pianificato, realizzato, verificato e modificato, invece di chiedersi chi è stato?**
  I sistemi complessi richiedono affinamenti e controlli, ma spesso ci si passa sopra
- **… chiedersi se lavorare sereni sia più produttivo che creare un clima di «terrore»?**
  Può sorprendere, ma niente come la cyber security è questione di cultura e valori dell'organizzazione, piuttosto che di *technicalities*

Auguste Rodin, Le Penseur- Pubblico dominio, da Andrew Horne
https://commons.wikimedia.org/wiki/File:The_Thinker,_Rodin.jpg

Lo sparambio è l'anima der guadambio, ma l'avarizia non paga

Quello che ci costa un «incidente di security» è formato da:

- **Costo degli interventi correttivi immediati, che possono facilmente essere pari o superiori a un buon investimento iniziale**
- **Ritardi nelle attività pianificate, che possono produrre danni prolungati nel tempo**
- **Danni reputazionali, che spesso sono veramente difficili da calcolare, ma si prolungano nel tempo**
- **Sanzioni, che possono esser peggiori dell'Apocalisse (ad esempio, quelle previste dal GDPR)**

I costi e gli investimenti per il miglioramento e la prevenzione, che avremmo dovuto fare per tempo e che ci avrebbero consentito di risparmiare gli altri!

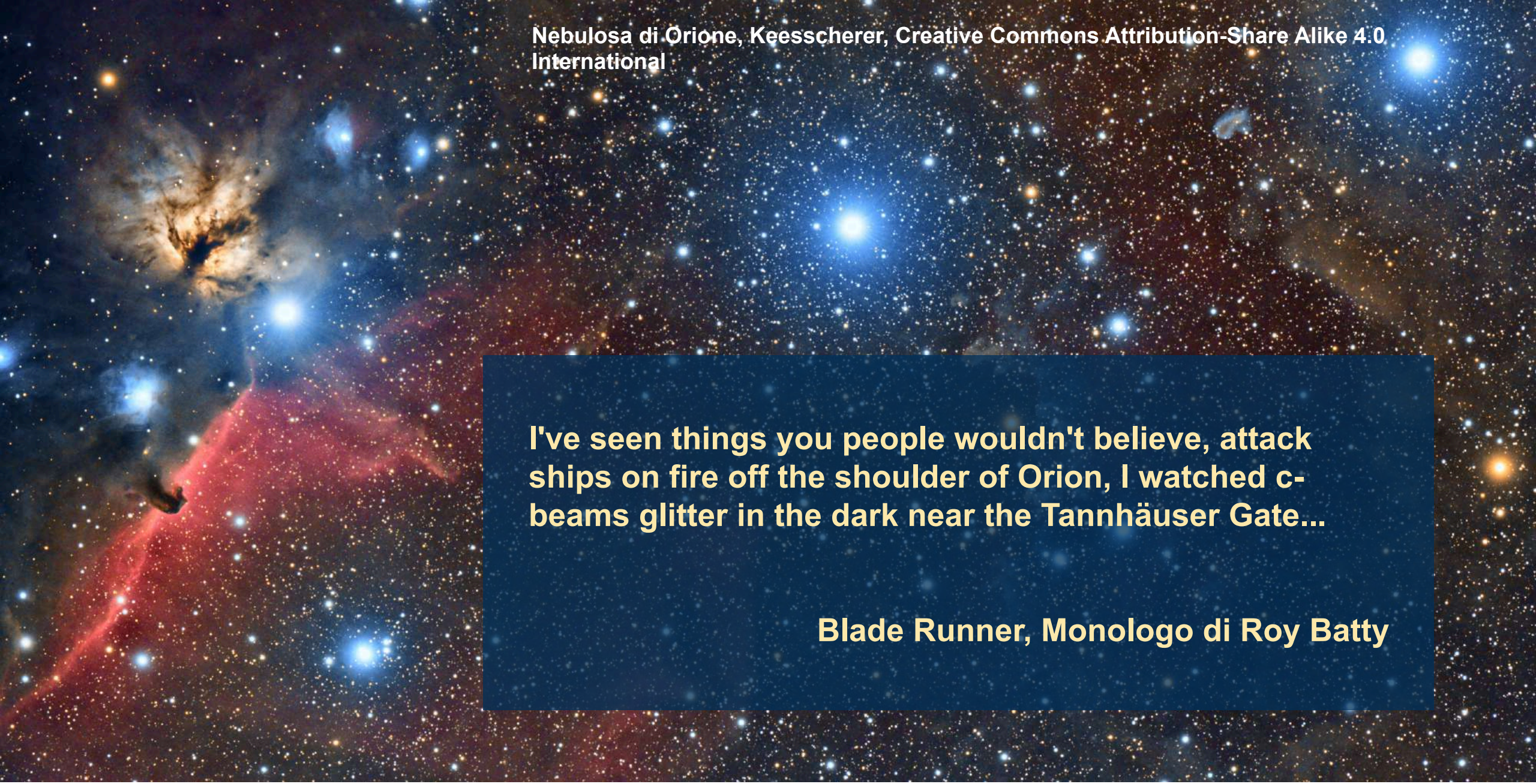
Alberto Sordi, L'avaro – Diritti non determinabili, da http://www.pieropiccioni.com/film.php?movie=14

Per concludere…

- L'errore umano è alla base dell'80-90% degli incidenti di sicurezza: un fattore che si conferma un anello debole del **sistema** → O la cyber security viene percepita e funziona «nel sistema» o rimarrà sempre qualcosa «da esperti» → Occorre lavorare sui **processi** (*)
- Il 63% delle organizzazioni è indietro rispetto alla **formazione** cyber security, ma è un problema aziendale, non tecnico → Occorre lavorare su **cultura**, **valori** e **clima**, ma anche sul **cliente** (**)
- Quando ci sono, i programmi di security awareness sono percepiti come "**obblighi aziendali**" e non riescono ad attivare percorsi di cambiamento (*)

(*) Rapporto CLUSIT 2019, Università la Sapienza; (**) Studio annuale dei professionisti di cyber security ISSA e ESG

San Giorgio, Raffaello Sanzio - Google Cultural Institute maximum zoom level, Public Domain, https://commons.wikimedia.org/w/index.php?curid=22173993



Nebulosa di Orione, Keesscherer, Creative Commons Attribution-Share Alike 4.0 International

I've seen things you people wouldn't believe, attack ships on fire off the shoulder of Orion, I watched c-beams glitter in the dark near the Tannhäuser Gate...

Blade Runner, Monologo di Roy Batty

La presentazione può contenere materiali acquisiti tramite ricerche on line per i quali non è stato possibile comunicare, con eventuali detentori di diritti, che possono fare riferimento all'autore per eventuali omissioni o inesattezze nella citazione delle fonti.

I contenuti della presentazione costituiscono un'elaborazione personale dell'autore e non costituiscono in alcun modo una posizione ufficiale delle aziende del Gruppo TIM

Grazie per la vostra attenzione!

guido.allegrezza@telecomitalia.it

BOOLEBOX
SECURE SHARING

BooleBox:la sicurezza militare applicata alla protezione dei dati aziendali

Valerio Pastore
CTO e Founder BooleBox

Chi siamo

Boole Server – profilo aziendale

BooleBox è azienda innovativa nel settore della protezione datacentrica, file sharing sicuro e gestione degli accessi.

*LA MISSIONE DI **BOOLEBOX** È QUELLA DI SVILUPPARE SOLUZIONI DEDICATE ALLA PROTEZIONE **DELLE INFORMAZIONI**.*

L’idea innovativa

La gestione degli accessi ai documenti TOP SECRET negli ambienti militari ha caratteristiche molto rigorose:

1. Sono conservati in stanze blindate
2. Una guardia controlla i permessi e l’identità di chi entra
3. Una seconda guardia all’interno controlla:
   - Che la consultazione riguardi il documento per cui si possiedono i permessi
   - La durata della consultazione del documento
   - Che non vengano fotografate parti del documento
   - Che non vengano copiate parti del contenuto del documento
4. La guardia all’ingresso controlla che la persona all’uscita non porti fuori nessun documento

L’Idea Innovativa

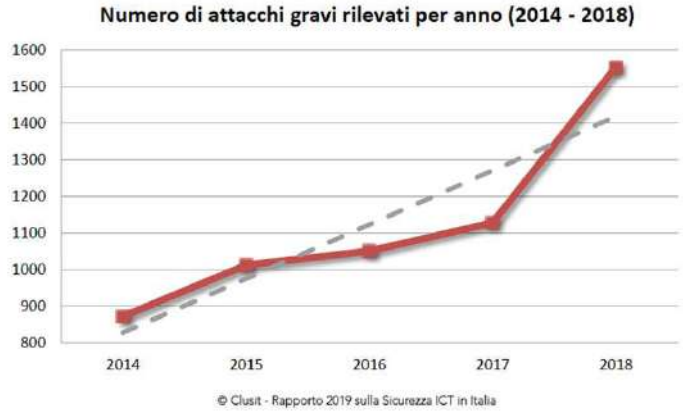
La «protezione di livello militare» di BooleBox per i dati aziendali o personali: il documento non viene più spedito al destinatario.
Il destinatario viene invitato ad accedere alla data room per poter consultare i documenti protetti:

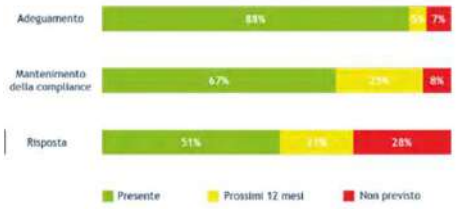
- CIFRATURA DI LIVELLO MILITARE
- AUTENTICAZIONE BIOMETRICA (IMPRONTA DIGITALE)
- PERMESSI SUI SINGOLI FILE O CARTELLE
- PERMESSI PERSONALIZZABILI SULLE OPERAZIONI CONSENTITE
- PERMESSI CON SCADENZA TEMPORALE
- ANTI SCREEN CAPTURE / DETER PHOTO SHOT
- BLOCCO DEL COMANDO COPIA/INCOLLA
- BLOCCO DEI COMANDI DOWNLOAD / STAMPA / SALVA CON NOME

Cybersecurity: trend e investimenti

Nel 2018 gli attacchi con impatto significativo sono aumentati a livello globale del 38% con una media di 129 al mese . Poco più di quattro al giorno, e si tratta solo di quelli gravi e conosciuti

Aumento dei casi di spionaggio cyber +57%
- spionaggio geopolitico
- spionaggio industriale
- furto di proprietà intellettuale





Aumento degli investimenti

La normativa sta aiutando, basti pensare al GDPR e, a breve, al Cybersecurity ACT:
le imprese e le pubbliche amministrazioni costrette a stanziare budget importanti per
- compliance
- sicurezza dei dati e delle informazioni

Fonte: © Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

Il valore dei dati

«I dati diventeranno la materia prima più importante del futuro.»

Peter Altmaier, Ministro dell'economia tedesco

Infatti **i dati sono la materia prima** dell'economia digitale ed alimentano l'intelligenza artificiale.

Valore di mercato di Facebook $ 502,376,053,193: asset = dati degli utenti

Trasformazione digitale

Come utilizziamo il tempo online

I servizi più utilizzati:

Servizi (a volte anche gratuiti) in cambio di **DATI PERSONALI**

Abbiamo la percezione del valore dei nostri dati?

I rischi per i nostri dati: Cloud Act

CLOUD ACT (firmato il 23.03.2018, Stati Uniti):

- Autorità statunitensi
- Forze dell'ordine
- Agenzie di intelligence

possono **acquisire i nostri dati informatici (personali e aziendali) depositati su server di operatori di servizi di cloud computing** a prescindere dal posto dove questi dati si trovano; quindi anche in Europa

E' sufficiente che questi operatori siano **Americani**

Esiste la possibilità, tecnicamente, di accedere ai nostri file, aprirli, consultarli, copiarli e utilizzarli.

I rischi per i nostri dati: Back-up

Backup

Servizi di archiviazione in Cloud di dati personali / progetti di lavoro: come funzionano

1. I dati vengono "consegnati" e **archiviati** all'interno del nostro spazio cloud offerto dal service provider selezionato

2. Vengono fatte più **copie di backup dei nostri file** e salvate su diversi server geograficamente dislocati per garantirne la disponibilità

3. Le nostre informazioni saranno **conservate** anche dopo che le avremo eliminate dalla piattaforma.
   E il diritto all'oblio?

Esigenza: Sovranità dei dati

Gaia-X

Istituzioni, Forze dell'ordine, Istituti scolastici, Ospedali **utilizzano service provider Americani che possono accedere a dati strategici!**

Nel caso di una guerra commerciale potrebbero essere bloccati:

- parti delle istituzioni
- servizi fondamentali ai cittadini
- produzione

La protezione datacentrica

BOOLEBOX
SECURE SHARING

CIFRATURA
DI LIVELLO MILITARE

CHIAVI DI CIFRATURA
PERSONALI

Il nuovo standard
di sicurezza

CONTROLLO
DEL DATO

SISTEMI DI
AUTENTICAZIONE
AVANZATI

BooleBox

1

LA PIATTAFORMA

BooleBox è la piattaforma di **Archiviazione, collaborazione, condivisione e sincronizzazione dati** progettata per **proteggere contenuti e informazioni sensibili**.

ENCRYPTION SUITE

2

Gmail Outlook

OneDrive SharePoint Windows

BooleBox si integra con le applicazioni cloud più usate per permetterti di creare una zona sicura all'interno di esse. **Una cassaforte per i tuoi file** senza cambiare il tuo metodo di lavoro.

Le tue esigenze, le nostre risposte

1 LA PIATTAFORMA

Cifratura file anche in fase di lettura e di modifica

Condivisione sicura grazie a limitazioni nella condivisione di file e cartelle o invio di e-mail

Automatizzazione delle limitazioni operative per utenti su singoli progetti

Collaborazione in tempo reale con Office 365 e lo strumento «task e commenti»

Tracciabilità dettagliata di tutte le operazioni eseguite sui documenti

Accesso protetto da ogni device con possibilità di imporre l'autenticazione biometrica

BooleBox

1

LA PIATTAFORMA

BooleBox è la piattaforma di **Archiviazione, collaborazione, condivisione e sincronizzazione dati** progettata per **proteggere contenuti e informazioni sensibili**.

ENCRYPTION SUITE

2

Gmail Outlook OneDrive SharePoint Windows

BooleBox si integra con le applicazioni cloud più usate per permetterti di creare una zona sicura all'interno di esse. **Una cassaforte sicura per i tuoi file** senza cambiare il tuo metodo di lavoro.

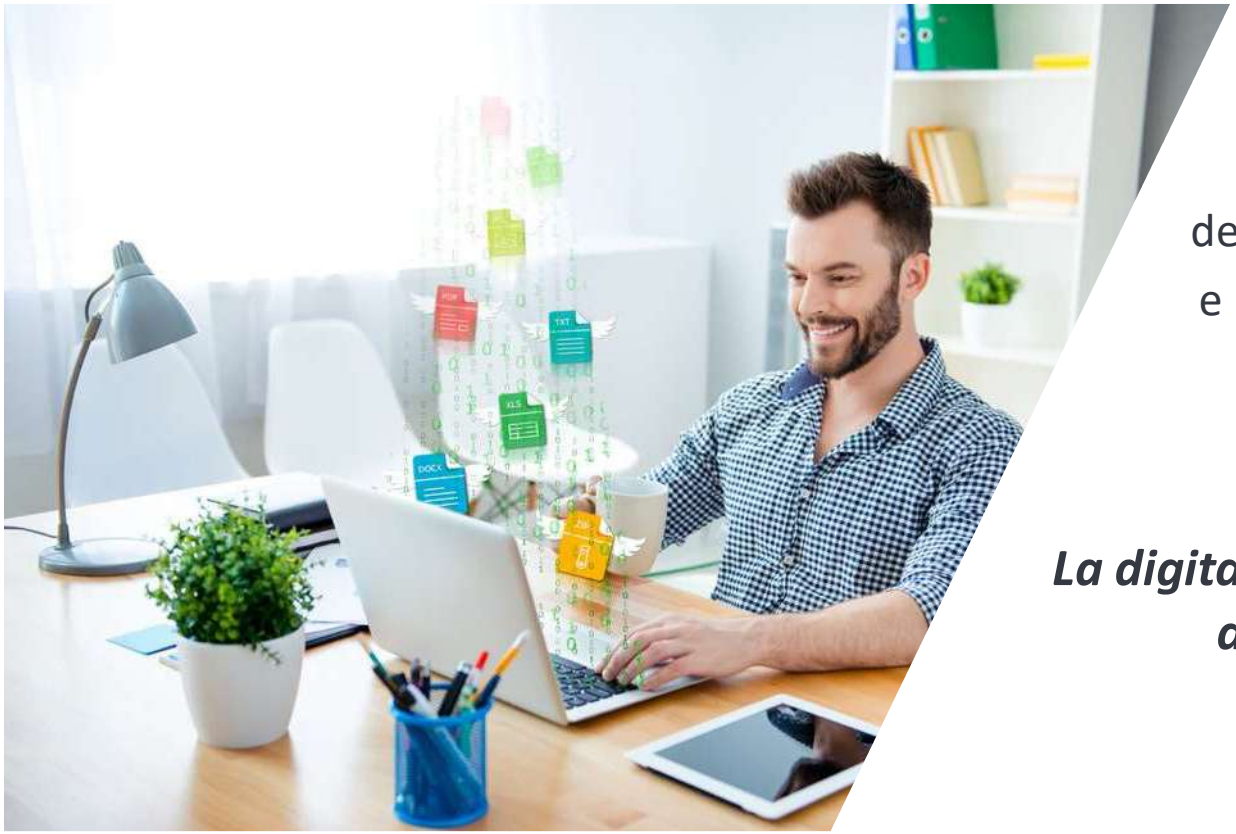
BooleBox: protezione dei dati riservati ovunque si trovino

BooleBox fornisce una unica
piattaforma di protezione
ovunque siano archiviati i tuoi dati

BOOLEBOX
SECURE SHARING


BooleBox è sicura per i tuoi dati
come Fort Knox:
diventano inespugnabili!

Il messaggio



Manca la reale percezione
del furto del documento digitale
e la sensibilità sulla necessità di
proteggere dei nostri dati

La digitalizzazione implica sempre anche la protezione

Grazie per l'attenzione

www.boolebox.it