

"Cybersecurity: un quadro complesso con impatti profondi sulla società"

Ing. Georgia Cesarone
Responsabile Innovazione e Formazione
START4.0

START 4.0 è uno degli 8 Competence Centre creati dal MISE e ha tra i suoi principali obiettivi quello di essere promotore della diffusione di innovazione, trasferimento tecnologico e progetti 4.0 sicuri all'interno dei diversi ecosistemi siano essi pubblici o privati.

La sintesi tra una guida pubblica, il supporto dei grandi enti di ricerca e il coinvolgimento di grandi società operanti su mercati internazionali è un'operazione sfidante che ha come fine ultima quello di alzare il livello di consapevolezza sull'importanza del digitale per il sistema Paese.



8 Centri nazionali

(Genova, Torino, Milano, Padova, Bologna, Pisa, Roma, Napoli)

Valore della rete nazionale:

45 milioni di euro

400+ imprese coinvolte

60+ Università coinvolte

40+ Enti pubblici coinvolti

Il partenariato di START 4.0

START4.0





ENERGY

Cybersecurity strategies for power distribution infrastructures



TRANSPORT

Information security management in the context of rail and naval transport



WATER SYSTEM

Solution for recovery and monitoring of reservoir and of distribution networks



MANUFACTURING

Digitalization and increase of technological maturity levels of industrial processes



PORT

Freight and people safety, related flows data management related flows

La cybersecurity è un tema complesso con profondi impatti sulla società per diverse ragioni:

- ❑ **Dipendenza dalla tecnologia:** La nostra società moderna è fortemente dipendente dalla tecnologia e dall'informazione digitale per svolgere attività quotidiane, come comunicare, lavorare, fare acquisti e gestire le nostre finanze. Gli attacchi informatici possono compromettere queste attività e minacciare la nostra sicurezza e privacy.
- ❑ **Interconnessione globale:** L'interconnessione globale delle reti informatiche significa che un attacco condotto in una parte del mondo può avere conseguenze su scala mondiale. Questo amplifica gli impatti negativi degli attacchi informatici e rende la cybersecurity una sfida globale.
- ❑ **Dati sensibili e personali:** Le informazioni personali e sensibili sono sempre più archiviate in formato digitale, sia da individui che da organizzazioni. La violazione della sicurezza dei dati può portare a gravi conseguenze, come il furto di identità, la frode finanziaria e la violazione della privacy.

- ❑ **Infrastrutture critiche:** Le infrastrutture critiche, come l'elettricità, le telecomunicazioni, i trasporti e la sanità, sono sempre più interconnesse e dipendenti dalla tecnologia informatica. Un attacco informatico mirato a queste infrastrutture può avere conseguenze devastanti sulla società e sull'economia.
- ❑ **Evoluzione delle minacce:** Gli attaccanti informatici sono sempre più sofisticati e creativi nel trovare nuovi metodi per compromettere la sicurezza informatica. Questo richiede un costante adattamento e miglioramento delle difese cybersecurity per proteggere efficacemente sistemi e dati.

La cybersecurity è cruciale per garantire la sicurezza, la privacy e il corretto funzionamento della società.

**La sua complessità dipende dalle componenti inerenti ai 3 pilastri relativi a:
tecnologie, processi e persone**

L'insieme delle risorse informatiche e dei siti web che possono essere visitati simultaneamente da milioni di persone tramite reti di computer, e in cui avvengono scambi comunicativi di varia natura.

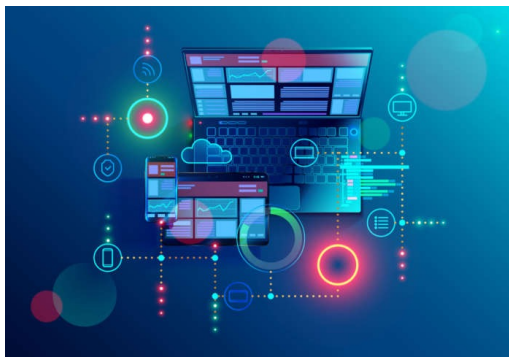
- **Realtà astratta** che connette ad un'unica rete i computer di tutto il mondo consentendo agli utenti che ne fanno uso di interagire tra loro.
- Non è un mondo puramente virtuale, **richiede la presenza di oggetti fisici**. Dietro a tali dispositivi vi sono degli **individui** che influenzano e plasmano questo mondo, che condividono informazioni e che, a loro volta, vengono **“formati”** da esso e stimolati al progresso tecnologico.



Nel cyberspazio **coesistono tre diversi elementi:**

- ***the human layer***, vale a dire le risorse umane dedite all'utilizzo dei sistemi di informatizzazione e comunicazione;
- ***the logical layer***, ossia i programmi/software, i sistemi operativi e le varie applicazioni e, infine, i bit che viaggiano nell'etere;
- ***the physical layer***, ovvero le infrastrutture e le apparecchiature fisiche mobili o fisse, che rendono possibile la trasmissione di dati





DATI

Informazioni non ancora sottoposte a elaborazione.
(collezione di numeri, testi o immagini non elaborate).

elaborando i dati si ottengono



INFORMAZIONI

Risultato dell'utilizzo dei dati e della loro eventuale modifica in modo da renderli significativi per la persona che li riceve



RISERVATEZZA

Garanzia che essi siano accessibili esclusivamente a chi è autorizzato ad accedervi



INTEGRITA'

Garanzia che essi e i processi necessari alla loro gestione siano esatti e completi in ogni loro parte

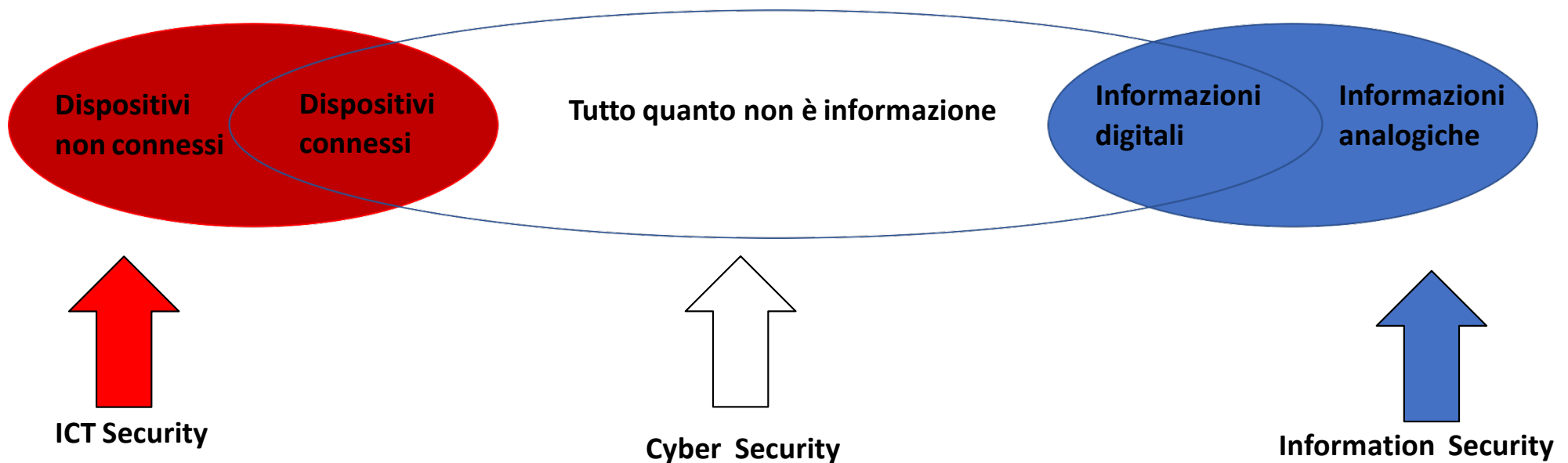


DISPONIBILITA'

Garanzia che gli utenti autorizzati abbiano accesso ad essi ogni qualvolta è necessario

Una serie di azioni pensate per difendere sistemi elettronici, reti, server e dispositivi da attacchi hacker.

Si tratta, in buona sostanza di una serie di azioni e provvedimenti pensati per la sicurezza informatica e delle informazioni.

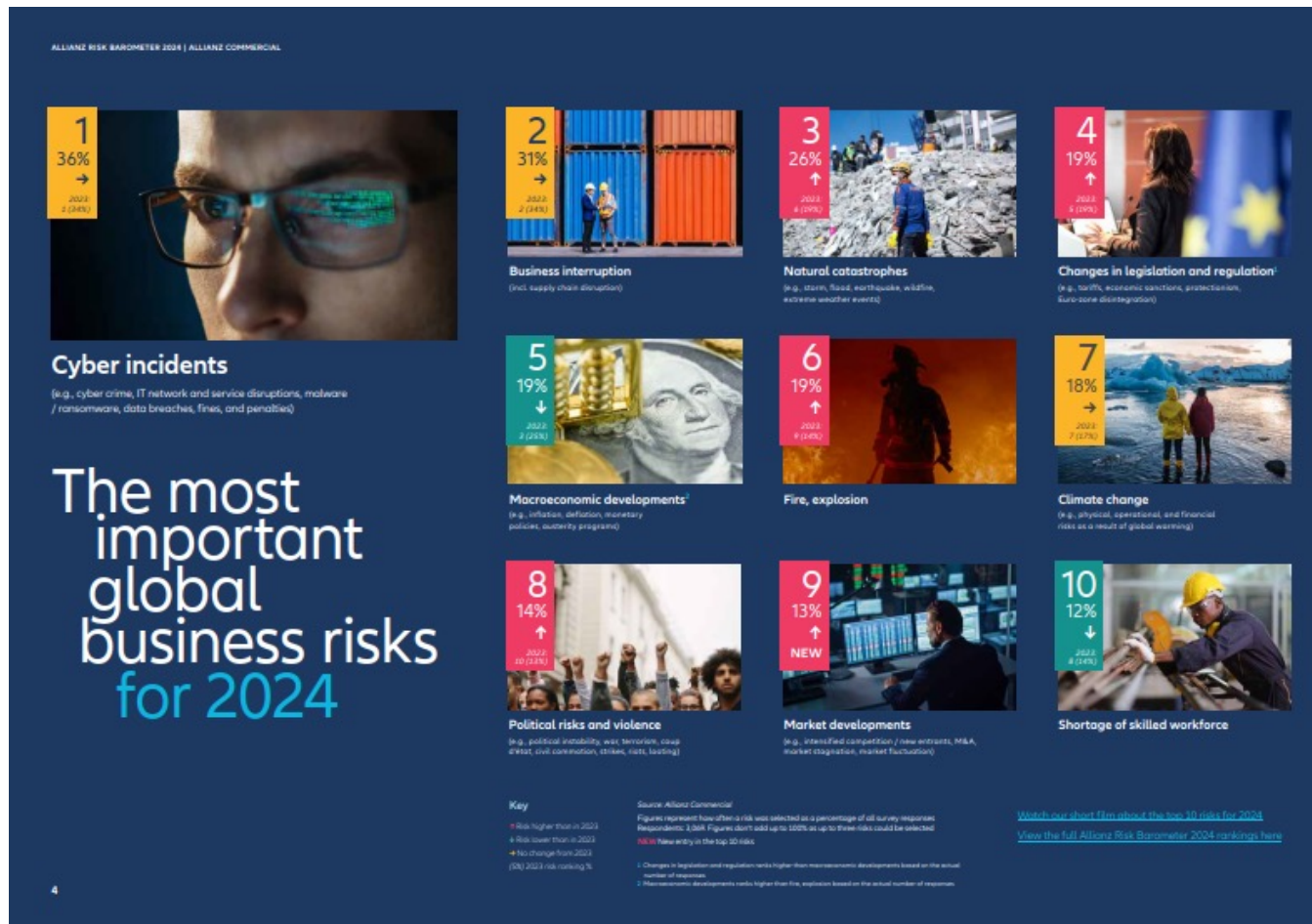


- **Minacce (*threats*)** possono essere portate da una molteplicità di **agenti ostili (*threat actors*)**, quali ad esempio, nazioni, criminali (singoli o organizzati in gruppi), **attivisti** (ad es. il gruppo anonymous), o un **dipendente infedele (*insider*)**.
- **Vulnerabilità:** difetti delle infrastrutture tecnologiche, delle procedure o dei processi aziendali che consentono l'esecuzione di comportamenti indesiderati nelle infrastrutture IT e/o OT. Gli **agenti ostili** sfruttano (*exploit*) le vulnerabilità per lanciare **attacchi cyber**.
- **Impatto:** conseguenza di un attacco cyber, quali la perdita finanziaria, il danno reputazionale, l'interruzione del servizio, la sottrazione di segreti industriali, e la divulgazioni di dati sensibili.
 - L'impatto è normalmente legato alla violazione di una o più delle proprietà di **confidenzialità (*confidentiality*)**, **integrità (*integrity*)** e **disponibilità (*availability*)** delle risorse digitali (*digital assets*) dell'organizzazione



- Il **rischio informatico**, o **cyber risk**, è un *rischio di tipo operativo* associato alle perdite economiche inflitte a una organizzazione dalla **mancata confidenzialità, disponibilità di integrità di informazioni e/o sistemi informativi, propri o di terzi**.
- La sua origine può essere:
 - **Accidentale**: si tratta di eventi che si verificano indipendentemente dalla volontà di tutti i soggetti coinvolti (es.: spegnimento server)
 - **Deliberata** (es.: cyber crime): sono eventi che derivano da azioni volontarie di soggetti allo scopo di raggiungere obiettivi personali di varia natura (es. furto dati sensibili)
 - Ulteriore caratteristica è che il **rischio cyber può avere una dimensione sistemica**, al pari del rischio finanziario.





Attacchi in Italia

(Clusit rapporto 2024 marzo su sicurezza ICT)

START4.0

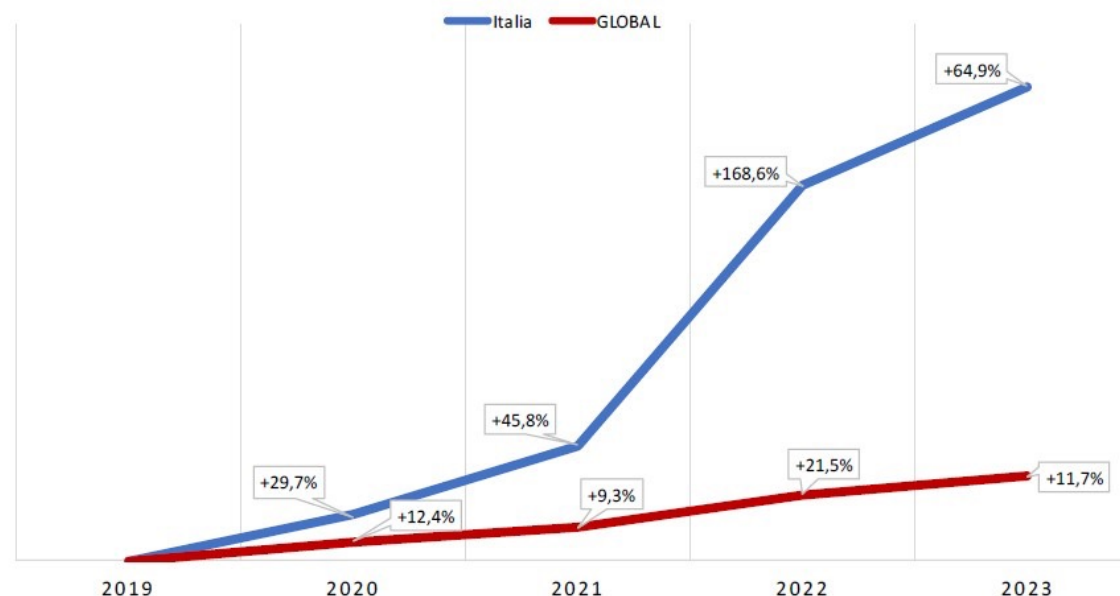
CONFRONTO CRESCITA % ITALIA VS GLOBAL

+65%

è la crescita degli
incidenti
informatici in Italia
nel 2023

11,2%

è la quantità di
incidenti censiti in
Italia rispetto al
resto del mondo



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia



Distribuzione della severity degli attacchi

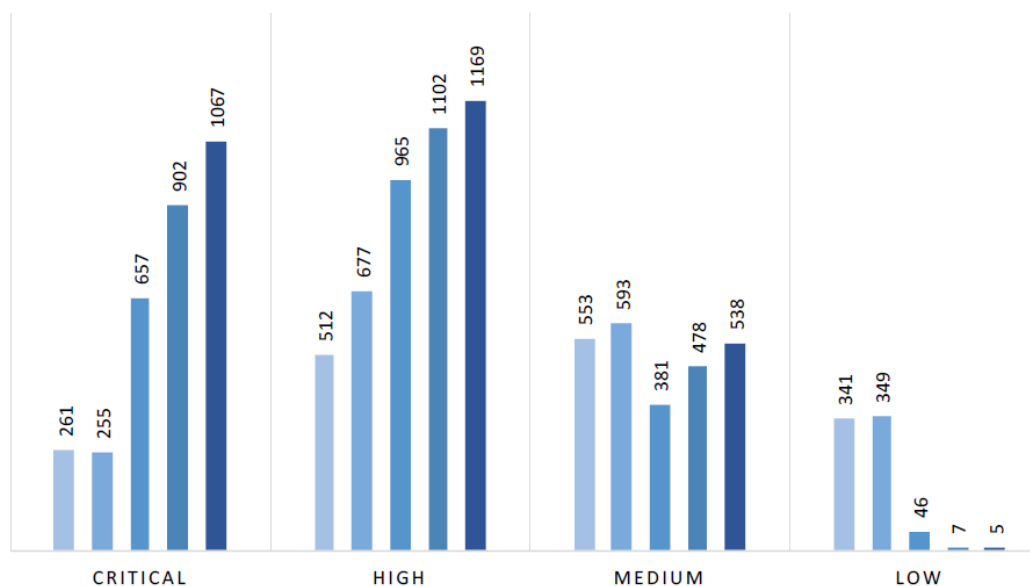
(Clusit rapporto 2024 marzo su sicurezza ICT)

START4.0

- In 4 casi su 5 l'impatto degli attacchi rientra nelle due categorie massime (**high e critical**).
- Scomparsa la voce riguardante gli incidenti con impatto "low".
- 5 attacchi su 2779

SEVERITY 2019 - 2023

■ 2019 ■ 2020 ■ 2021 ■ 2022 ■ 2023



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia



21

Distribuzione delle vittime in Italia

(Clusit rapporto 2024 marzo su sicurezza ICT)

START4.0

+30%

È la crescita
del numero degli
incidenti a danno del
settore HealthCare

+50%

gli incidenti al
settore GOV negli
ultimi 5 anni

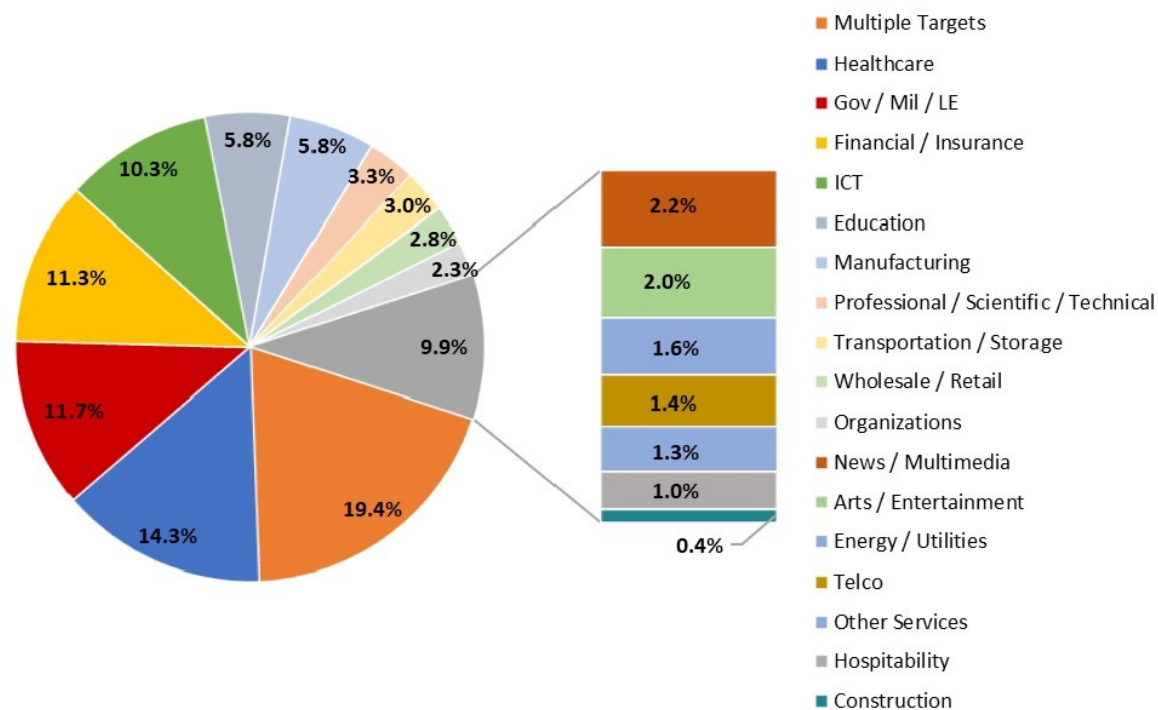
+62%

è la crescita
degli incidenti a
danno dei settori
Financial/Insurance

+25%

è la crescita
degli incidenti a
danno del settore
Manufacturing

DISTRIBUZIONE DELLE VITTIME 2023



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia



16

Distribuzione delle vittime in Italia

(Clusit rapporto 2024 marzo su sicurezza ICT)

START4.0

TECNICHE DI ATTACCO IN ITALIA 2023

DDoS

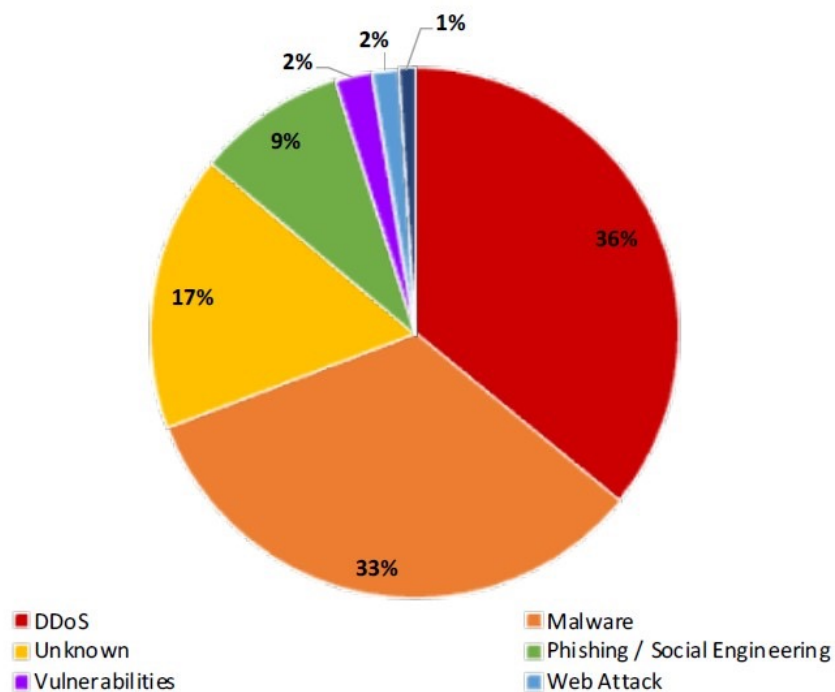
è la principale
tecnica di attacco
in Italia

+4%

è la crescita degli
attacchi basati su
Malware in Italia

+87%

è la crescita degli
attacchi phishing e
social engineering
in Italia



© Clusit - Rapporto 202 sulla Sicurezza ICT in Italia



31

“Come per larga parte delle Nazioni Occidentali, per l’Italia il 2023 è stato un anno di pesanti e diversificate aggressioni alla sicurezza cyber, che spesso hanno proceduto in parallelo ai conflitti in corso in Ucraina e in Medio Oriente”.

Alfredo Mantovano, Autorità Delegata per la sicurezza della Repubblica, nella Prefazione che dà inizio alla Relazione Annuale al Parlamento 2023.





Council of the EU



PRESS RELEASE
367/24
03/05/2024

Cyber: Statement by the High Representative on behalf of the EU on continued malicious behaviour in cyberspace by the Russian Federation

The European Union and its Member States, together with international partners, strongly condemn the malicious cyber campaign conducted by the Russia-controlled Advanced Persistent Threat Actor 28 (APT28) against Germany and Czechia. Today, Germany has shared publicly its assessment on APT28 compromise of various e-mail accounts of the German Social Democratic Party executive. At the same time, Czechia announced its institutions have been a target of this cyber campaign. State institutions, agencies and entities in Member States, including in Poland, Lithuania, Slovakia and Sweden have been targeted by the same threat actor before. In 2020, the EU imposed sanctions on individuals and entities responsible for the APT28 attacks targeting the German Federal Parliament in 2015.

The malicious cyber campaign shows Russia's continuous pattern of irresponsible behaviour in cyberspace, by targeting democratic institutions, government entities and critical infrastructure providers across the European Union and beyond.

This type of behaviour is contrary to the UN norms of responsible state behaviour in cyberspace, such as impairing the use and operation of critical infrastructure. Disregarding international security and stability, Russia has repeatedly leveraged APT28 to conduct malicious cyber activities against the EU, its Member States and international partners, most notably Ukraine.

The EU will not tolerate such malicious behaviour, particularly activities that aim to degrade our critical infrastructure, weaken societal cohesion and influence democratic processes, mindful of this year's elections in the EU and in more than 60 countries around the world. The EU and its Member States will continue to cooperate with our international partners to promote an open, free, stable and secure cyberspace.

The EU is determined to make use of the full spectrum of measures to prevent, deter and respond to Russia's malicious behaviour in cyberspace.

Press office - General Secretariat of the Council of the EU
Rue de la Loi 175 - B-1048 BRUSSELS - Tel.: +32 (0)2 281 6319
press@consilium.europa.eu - www.consilium.europa.eu/press

La situazione israelo-palestinese

- **7 ottobre, ore 6.35:** le sirene avvertono del lancio dei **primi razzi di Hamas**.
- **6.33/7.04:** il gruppo hacker Anonymous Sudan lancia **attacchi contro due app, Tzeva Adom e RedAlert**, utilizzate per diramare messaggi di allerta alla popolazione israeliana su attacchi imminenti
- **9.46:** gli aerei israeliani iniziano a colpire Gaza.
- **16.18: Anonymous Sudan** attacca il sito del **Jerusalem Post**, con un'altra azione DDoS, facendolo crollare per 12 ore.
- **Punto importante:** sabotare sistemi di allerta alla cittadinanza e canali di informazione può essere considerata un'azione di guerra collaterale.
- **18.10:** un altro gruppo hacker, **Cyber Av3ngers**, manda offline il sito della **Israel Electric Corporation**.

La situazione israelo-palestinese

- **Secondo giorno di guerra**, dalla notte inizia a dipanarsi uno degli attacchi più significativi della cyberwar.
- **8 ottobre, ore 1.29: il gruppo AnonGhost** annuncia di aver trovato una vulnerabilità. Invece di una notifica di pericolo in tempo reale, **gli hacker fanno comparire su molti telefonini israeliani il messaggio «fuck Israel»**. Poco dopo, diffondono il codice di vulnerabilità su un gruppo Telegram, mettendo l'arma a disposizione di altri. **In giornata creeranno tensione inviando messaggi su «imminenti eventi nucleari»**.
- **10.58: il sito di Hamas viene attaccato da Indian Cyber Force (esempio di controffensiva).**
- **14.52: Cyber Av3ngers** afferma di aver **compromesso la centrale elettrica Dorad** (il sito non è raggiungibile).
- **16.59: Killnet attacca il sito del governo israeliano.**
- **17.18: Anonymous Sudan** fa una chiamata alle armi sul proprio canale Telegram. Questo è il livello meno sofisticato, ma comunque di forte impatto, della guerra cibernetica: **proselitismo, disinformazione, diffusione di fake news.**

La situazione israelo-palestinese

- **Dal 7 al 17 ottobre**, gli analisti della società di sicurezza informatica Swascan hanno individuato **178 gruppi di attivisti cyber** che stanno partecipando al conflitto a diversi livelli.
- **Circa 150 sono pro Hamas**, e hanno basi (dichiarate) in uno scenario molto ampio rispetto al teatro di guerra: Marocco, Yemen, Iran, Sudan, Malesia, Indonesia, Russia, Bangladesh, Emirati Arabi.
- **Poco più di 20 gruppi sono pro Israele**, con basi nella stessa Israele e in India.

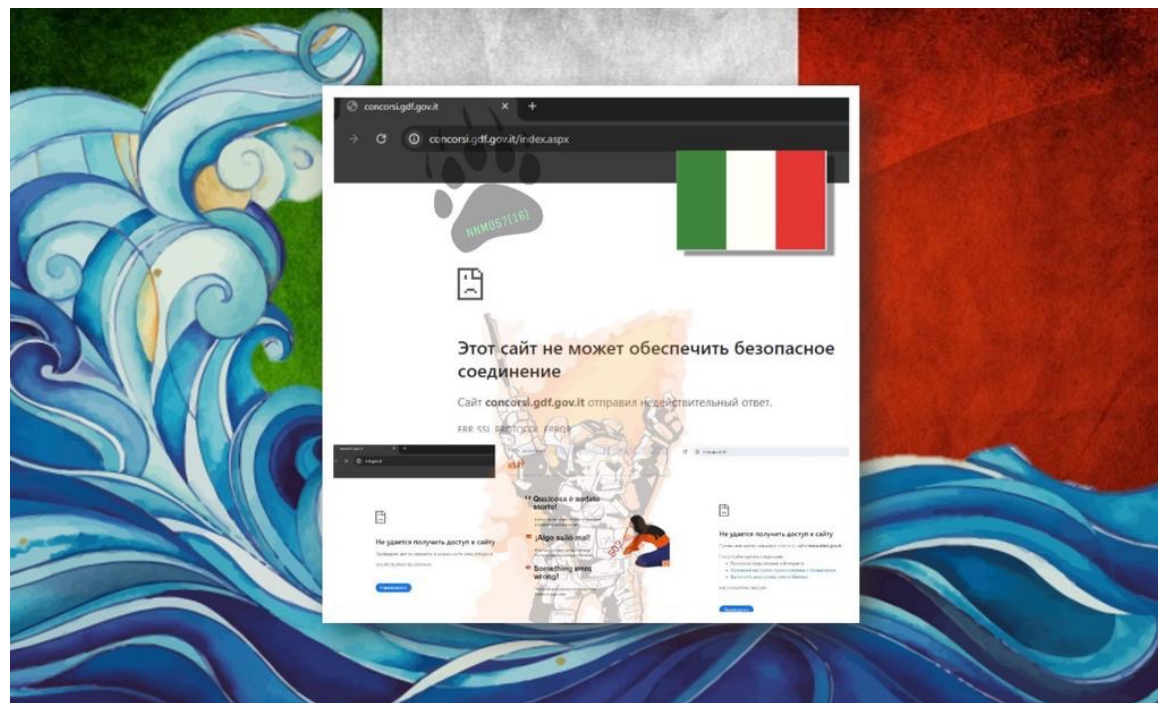
**Dichiarazione sottosegretario alla Presidenza del Consiglio
Alfredo Mantovano a Radio 24.**

Le minacce cyber e ibride si sono moltiplicate ma il sistema è attrezzato a fronteggiare queste minacce. Ne aspettiamo altre da qui alle Europee perché **questa è la nuova frontiera della guerra**

MIMIT, Guardia di Finanza e MIT, sito della Presidente del Consiglio presi di mira dal gruppo di hacktivisti filorussi di NoName057

START4.0

- Riportato all'interno del loro canale Telegram quanto segue:
- Continuiamo il nostro viaggio attraverso l'Italia e mettiamo a tacere i dossiers di questo paese 🐾 ❌ Il Ministero dello Sviluppo Economico italiano (morto sul ping) `check-host.net/check-report/190ecd82kad5`
- ❌ Il Ministero italiano delle Infrastrutture e dei Trasporti `check-host.net/check-report/190e4ee8k77f` Sottodominio della Polizia finanziaria `check-host.net/check-report/190e529dk37f`
- ❌ Il sito di Giorgia Meloni, capo del governo italiano, è inattivo e si limita a segnalare problemi tecnici. Tradotto con DeepL.com (versione gratuita)

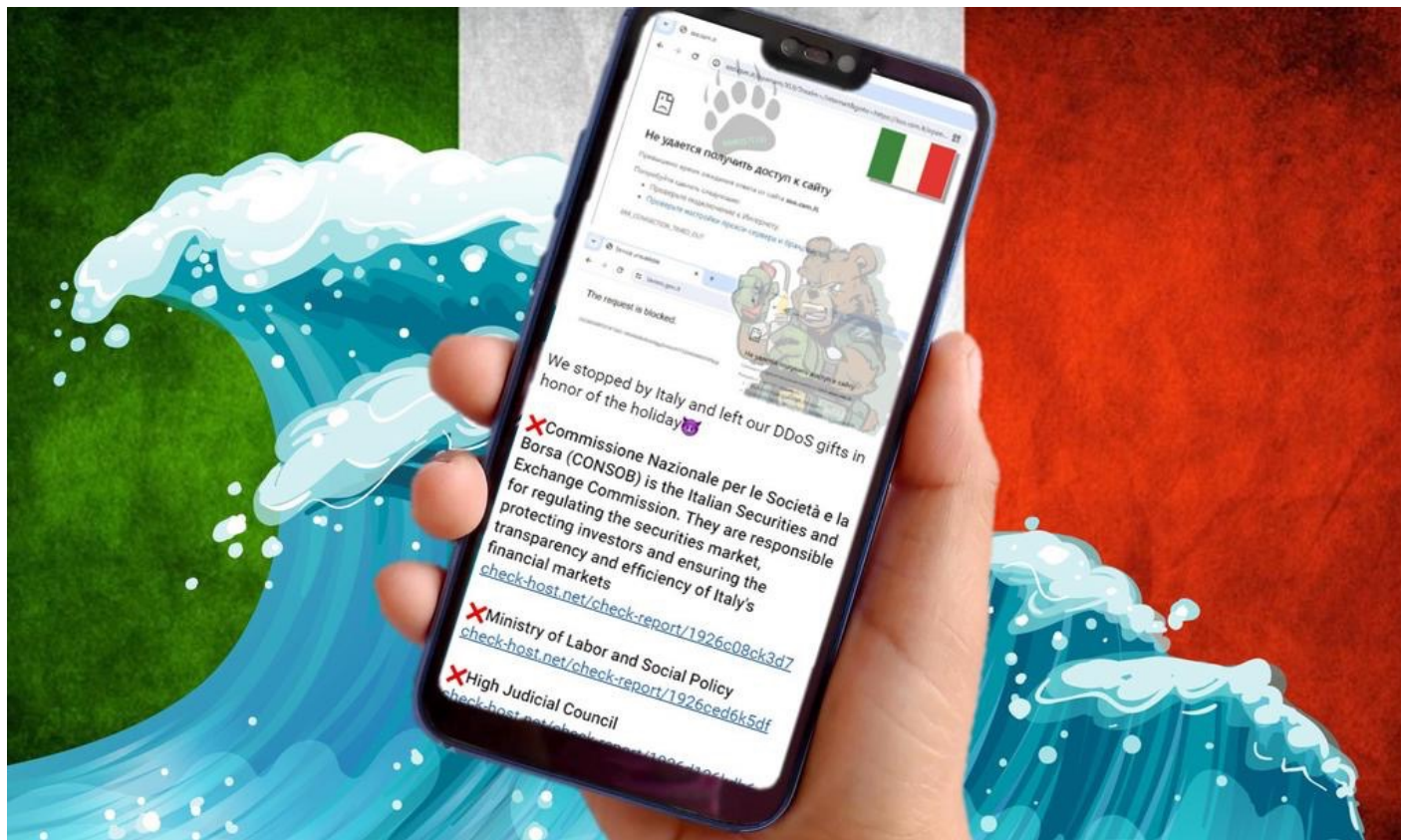


Redazione RHC
7 Maggio 2024
ore 13:24

Altro giorno altro DDoS!

- Ministero del Lavoro e delle Politiche Sociali
- Consiglio superiore della magistratura
- Commissione Nazionale per le Società e la Borsa

Redazione RHC
9 Maggio 2024
ore 11:44

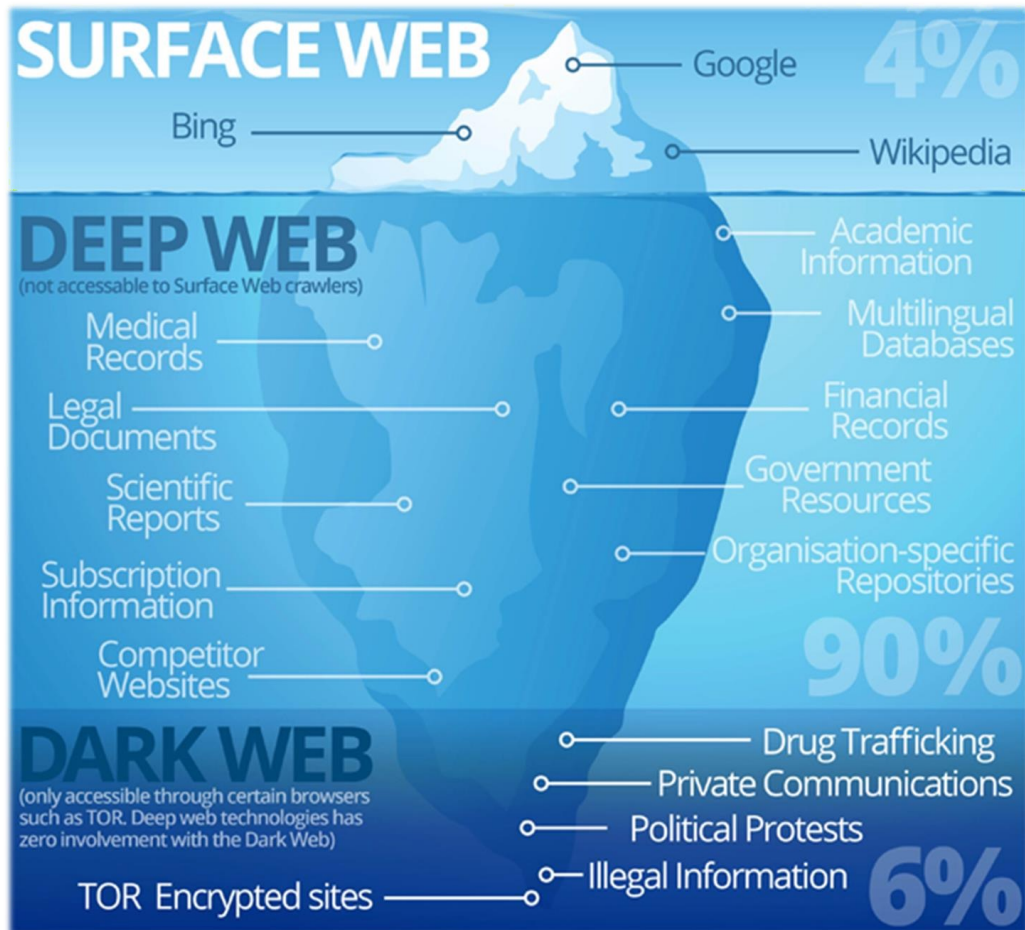


- **Gli eventi accidentali.** Si tratta delle conseguenze di eventi non ponderabili e legati a elementi casuali quali, ad esempio, gli eventi atmosferici che determinano l'interruzione dell'erogazione di energia elettrica e possono avere delle conseguenze sui sistemi operativi e sui dati.
- **Gli eventi indesiderati.** Sono le operazioni compiute da soggetti intenzionati a danneggiare il funzionamento dei dispositivi o a sottrarre informazioni e dati. In questo caso possiamo, distinguere ulteriormente tra:
 - ✓ **attacchi malevoli**, finalizzati a intaccare il funzionamento dei sistemi,
 - ✓ **accesso ai dispositivi da parte di soggetti non autorizzati** e finalizzati alla sottrazione di dati e informazioni.

L'insieme delle azioni commesse in violazione della legislazione internazionale o nazionale (laddove presente) che implicano l'utilizzo di computer o reti informatiche.



- Solitamente i **cyber crimes** perseguono interessi privati, in particolare l'interesse economico per i loro responsabili a differenza di quanto accade nel caso di **cyber attack**.
- La caratteristica principale di un **cyber attack** è quella di essere il **prodotto di una condotta attiva**, sia che si parli di offesa sia che si parli di difesa.
- Ogni **azione aggressiva** commessa sia da un **attore statale** sia da uno **non statale** e diretta a colpire la sicurezza nazionale di un Paese deve ritenersi un **attacco informatico**.
- Qualsiasi attacco che non persegua tale scopo, ad es. la pirateria informatica non rientra in questa definizione.



Al giorno d'oggi, un utente malintenzionato non ha bisogno di essere un abile hacker.

Può facilmente acquistare hacking capabilities 'As a Service' sul dark web.

Malware: Software dannoso progettato per danneggiare o compromettere computer, reti o dispositivi.

Phishing: Tentativi di ottenere informazioni personali, come nomi utente, password e informazioni finanziarie, fingendosi di essere entità affidabili tramite e-mail, messaggi di testo (smishing) o chiamate telefoniche (vishing).

Attacchi di ingegneria sociale: Manipolazione psicologica degli individui per ottenere informazioni riservate o per indurli a compiere azioni non sicure, come rivelare password o installare software dannosi.

Attacchi ransomware: Blocco o crittografia dei dati da parte di malware che richiede un pagamento (ransom) per ripristinare l'accesso ai dati.

Attacchi di tipo Denial-of-Service (DoS) e Distributed Denial-of-Service (DDoS): Tentativi di rendere un servizio o un'applicazione non disponibile per gli utenti legittimi sovraccaricandolo con un numero eccessivo di richieste.

Vulnerabilità del software (zero-days): Sfruttamento di falle di sicurezza in software, applicazioni o sistemi operativi per ottenere accesso non autorizzato o per eseguire azioni dannose.

Europol, nel suo rapporto IOCTA sugli otto trend del cyber crime nel 2016, li ha classificati in:

- **crime-as-a-service**: il crimine diventa una commodity che si compra al “supermercato” (nero) criminale;
- **i ransomware**, la nuova edizione dell’estorsione;
- **l’uso criminale dei dati** nelle forme di truffe od estorsioni più sofisticate;
- **le frodi nei pagamenti**, che stanno velocemente sostituendo le “cartiere”;
- **la pedopornografia** online e gli abusi;
- **l’abuso di darknet** per attività illecite;
- **il social engineering**, ora rivolto anche ai vertici aziendali per frodi articolate;
- **l’uso distorto delle valute virtuali**, divenute lo strumento di pagamento degli illeciti.



Hacker: Individui esperti nell'uso di computer e software per accedere a dati o sistemi senza autorizzazione.

Cracker: Hackers che si dedicano principalmente a compromettere la sicurezza informatica, spesso con intenti malevoli.

Script Kiddies: Individui con conoscenze informatiche limitate che utilizzano software predefiniti per condurre attacchi informatici.

Spie informatiche: Individui che lavorano per organizzazioni governative o private per ottenere informazioni sensibili da reti o sistemi informatici di altre organizzazioni.

Cyberterroristi: Individui o gruppi che utilizzano attacchi informatici per causare danni fisici, danneggiare infrastrutture critiche o diffondere il terrore.

Insiders: Dipendenti, ex dipendenti o partner commerciali che sfruttano la propria posizione per compiere atti dannosi all'interno di un'organizzazione.

Hacktivist: Individui o gruppi che conducono attacchi informatici per motivi politici o sociali.

*Un'efficace strategia di **cyber security** richiede, allora, un'analisi delle **minacce**, delle **vulnerabilità** e dei **rischi associati** all'impiego di sistemi informatici nonché l'attuazione di **adeguate e specifiche misure difensive**.*

Quando parliamo di misure di **cyber security** è bene ricordare che queste possono consistere tanto in **misure di prevenzione**, le quali agiscono riducendo la probabilità di realizzazione di una minaccia, quanto in **misure di protezione**, le quali agiscono riducendo la gravità del danno prodotto da un attacco o da un crimine informatico.



- **Responsabilità** in merito chiaramente identificate e assegnate a una determinata figura aziendale
- **Impegno e leadership** mostrati dal management nel sostenere la sicurezza
- **“Buy-in” dei dipendenti**, i quali devono ricevere una comunicazione efficace e una formazione adeguata sulla sicurezza informatica e sui protocolli da rispettare
- **Consapevolezza e formazione dei dipendenti**, quanto alle minacce e contromisure attuabili
- **Policy di sicurezza informatica**
- **Gestione delle terze parti** (vaglio preliminare, verifiche ecc.)

- ***Audit periodici***
- ***Pianificazione e risposta*** agli incidenti di sicurezza
- ***Utilizzo di accessi centralizzati e corretta gestione delle password***
(preferite le *passphrase*, ad es. di tre parole casuali)
- ***Patch e aggiornamenti software*** regolari e automatizzati
- ***Protezione dei dati personali***, ai sensi della normativa in materia

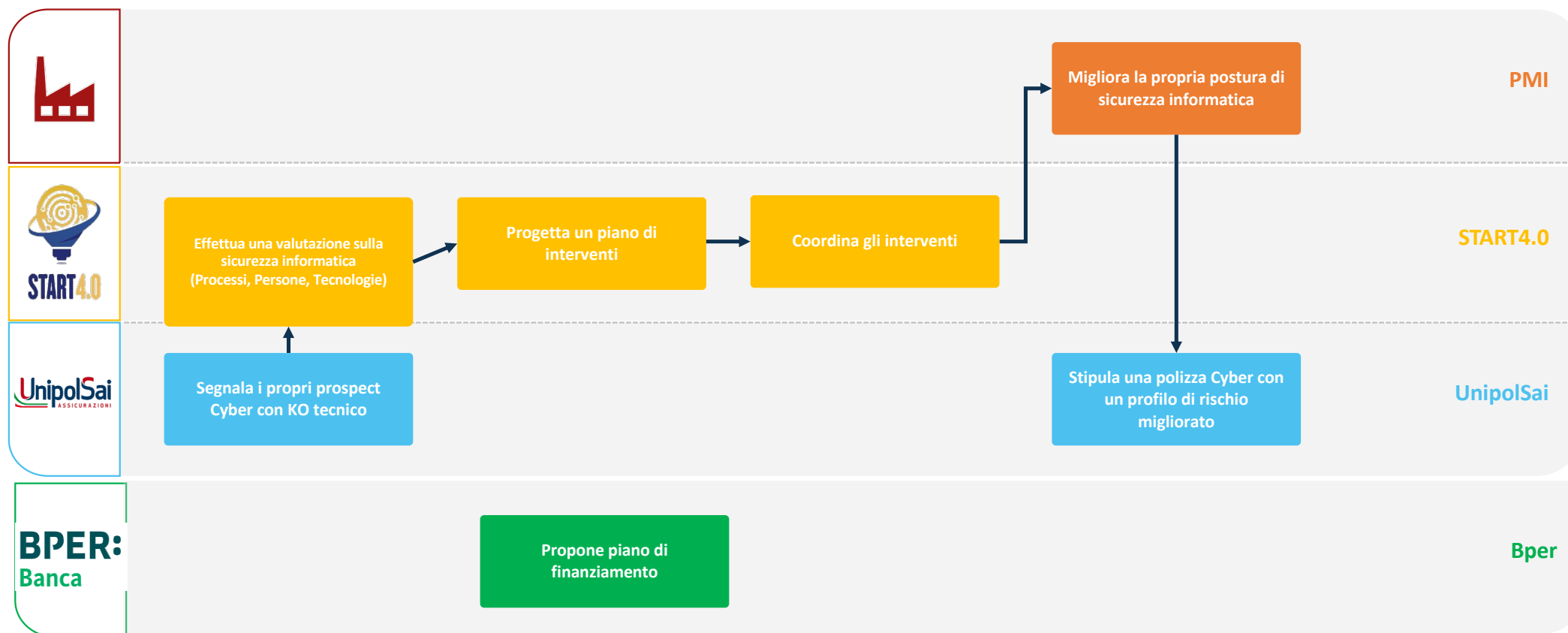
- **Sicurezza delle reti** (in particolare, tramite **firewall**)
- **Antivirus** su tutti i dispositivi ed endpoint
- Utilizzare **strumenti di protezione della posta elettronica e della navigazione web** – in **abbinamento a formazione e consapevolezza**
- **Crittografia applicata** a più livelli possibili (in particolare, utilizzando VPN per le connessioni)
- **Monitoraggio della sicurezza**, registrando l'attività dei sistemi anche per fini di manutenzione e risoluzione dei problemi, segnalando attività sospette
- **Sicurezza fisica** degli ambienti e dispositivi utilizzati
- **Backup** sicuri (soprattutto a tutela dagli attacchi **ransomware**), il più possibile separati, regolari, automatizzati e crittografati;
 - in merito ENISA ricorda la “**Regola 3-2-1**”:
conservare tre copie dei dati – archivarle in due archivi/media diversi – avere almeno un backup esterno al perimetro logico-fisico aziendale.

- A miglior specifica, l'ENISA come detto ha prodotto un'apposita **infografica riassuntiva** dei dodici punti fondamentali, utile anche per la formazione e consapevolezza interna alle aziende.
- Contestualizzando il tutto al **contesto pandemico**, l'ente aggiunge alcune specifici suggerimenti più che attuali:
 - rivedere le strutture di **accesso remoto**;
 - rivedere i **rapporti con i servizi cloud** (richiamando anche le già citate linee guida ENISA per l'uso del cloud);
 - implementare una **corretta gestione dei dispositivi mobili**;
 - condurre **un'adeguata formazione sulla consapevolezza** circa i temi di sicurezza, specie quelli di maggiore allarme nel periodo pandemico;
 - implementare **siti web sicuri**;
 - **condividere informazioni** a livello nazionale e internazionale, specie sugli attacchi subiti.

- A miglior specifica, l'ENISA come detto ha prodotto un'apposita **infografica riassuntiva** dei dodici punti fondamentali, utile anche per la formazione e consapevolezza interna alle aziende.
- Contestualizzando il tutto al **contesto pandemico**, l'ente aggiunge alcune specifici suggerimenti più che attuali:
 - rivedere le strutture di **accesso remoto**;
 - rivedere i **rapporti con i servizi cloud** (richiamando anche le già citate linee guida ENISA per l'uso del cloud);
 - implementare una **corretta gestione dei dispositivi mobili**;
 - condurre **un'adeguata formazione sulla consapevolezza** circa i temi di sicurezza, specie quelli di maggiore allarme nel periodo pandemico;
 - implementare **siti web sicuri**;
 - **condividere informazioni** a livello nazionale e internazionale, specie sugli attacchi subiti.

START4.0, quale Soggetto Attuatore nell'ambito dell'**Intervento 2.3 “Potenziamento ed estensione tematica e territoriale dei centri di trasferimento tecnologico per segmenti di industria”** della **Missione 4 “Istruzione e ricerca”, Componente 2 “Dalla ricerca all'impresa”** del Piano Nazionale di Ripresa e Resilienza – Next Generation EU, eroga alle imprese, a costi agevolati, servizi tecnologici nel rispetto della normativa nazionale ed europea sugli aiuti di Stato, alimentando le banche dati nazionali relative agli aiuti di Stato e il sistema informatico (ReGiS) di cui all'articolo 1, comma 1043, della legge 30 dicembre 2020, n. 178, per supportare il Ministero, congiuntamente a tutti i centri di trasferimento tecnologico, nel raggiungere i seguenti Target nazionali entro il quarto trimestre 2025





Ing. Georgia Cesarone

georgia.cesarone@start4-0.it

START4.0