# MISSIONE 1 – COMPONENTE 1 – PNRR, Cybersicurezza e minacce informatiche


PNRR

*Dossier*

# Sommario

# Introduzione

La sicurezza delle reti e dei sistemi informatici costituisce uno dei 7 investimenti previsti dal *Piano Nazionale di Ripresa e Resilienza* (PNRR) nell'ambito delle azioni di *Digitalizzazione della Pubblica Amministrazione*.

La componente 1 della prima Missione 1 del PNRR (alla quale sono destinati circa 9,72 miliardi di euro a cui si sommano 1,40 miliardi del fondo complementare) si propone di sviluppare un'offerta integrata e armonizzata di servizi digitali all'avanguardia orientati a cittadini, residenti e imprese. Il raggiungimento di un tale risultato permetterebbe all'Italia di raggiungere gli ambiziosi traguardi fissati in sede europea dal *Digital Compass 2030*, il quale prevede che entro il 2030 tutti i servizi pubblici chiave siano disponibili *online*. La missione 1 componente 1 deve essere letta in armonia con tale cornice europea nella quale i diritti ed i principi digitali integreranno i diritti esistenti, come quelli sanciti dalla Carta dei diritti fondamentali dell'UE e la legislazione in materia di protezione dei dati e di privacy. In tale ambito si completerà il quadro di riferimento per i cittadini sui loro diritti digitali, nonché orientamenti per gli Stati membri dell'UE e per le imprese che si occupano di nuove tecnologie, con l'obiettivo di aiutare tutti i cittadini dell'UE a trarre il massimo vantaggio dalla trasformazione digitale. A livello macro le persone ed i loro diritti saranno al centro della trasformazione digitale, sostenendo la solidarietà e l'inclusione, garantendo la libertà di scelta online, promuovendo la partecipazione allo spazio pubblico digitale, aumentando in tale prospettiva la sicurezza, la protezione e la responsabilizzazione delle persone, promuovendo altresì la sostenibilità del futuro digitale.

Scendendo nella prospettiva italiana del PNRR, per il comparto della pubblica amministrazione, lo snodo decisivo è rappresentato dal passaggio al digitale che si traduce nello sviluppo di servizi on-line come quelli appena avviati dall'anagrafe nazionale della popolazione residente e nella migrazione su *cloud pubblico* che rappresenta uno degli investimenti più importanti nell'agenda del sistema paese. In tale sguardo è possibile mettere in luce i principali servizi su cui insiste l'intervento programmato nella componente in analisi:

a) l'Identità digitale[1];

b) i pagamenti digitali tra cittadini e Pubblica amministrazione[2];

[1] Con l'obiettivo di raggiungere oltre 40 milioni di Italiani con le piattaforme esistenti per l'identificazione (CIE e SPID) e completando su tutti i comuni l'estensione dell'Anagrafe della Popolazione residente ANPR.
[2] Promuovendo l'adozione di PagoPA in oltre 14.000 amministrazioni locali.

c) le notifiche digitali[3].

Nel dettaglio, il rafforzamento dei servizi pubblici digitali si radica su una serie di interventi *abilitanti*, tra cui la migrazione al cloud delle pubbliche amministrazioni, la diffusione della App "IO" come punto di accesso preferenziale per il cittadino e il ***rafforzamento della cybersecurity nazionale***.

Proprio per ovviare alla necessità di un rafforzamento del generale grado di sicurezza informatica a livello nazionale la Missione 1, Componente 1.1, Investimento 1.5 del PNRR promuove l'implementazione e il potenziamento dei sistemi nazionali di ***cybersecurity*.**

Infatti, la digitalizzazione aumenta nel suo complesso il livello di vulnerabilità della società da minacce *cyber*, su tutti i fronti (ad es. frodi, ricatti informatici, attacchi terroristici, ecc.). Inoltre, la crescente dipendenza da servizi "software" e l'aumento di interdipendenza delle "catene del valore digitali" (PA, aziende controllate dallo Stato, privati) contribuiscono a sottolineare l'estrema importanza di un'attenta valutazione del rischio presente e futuro, e quindi di una risposta adeguata da parte del Paese. L'obiettivo dell'investimento è rafforzare l'ecosistema digitale nazionale potenziando i servizi di gestione della minaccia *cyber*. Il tutto, attraverso una rinnovata capacità di monitoraggio, prevenzione e scrutinio tecnologico a supporto della transizione digitale del Paese.

Il quadro normativo vigente in merito alla *Strategia nazionale di cybersicurezza* prevede, in particolare all'articolo 6 del decreto legislativo 18 maggio 2018, n. 65 che il Presidente del Consiglio dei ministri adotti, sentito il Comitato Interministeriale per la cybersicurezza, la *Strategia nazionale per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale*. In relazione alla Strategia nazionale di cybersicurezza nell'ambito di applicazione del presente decreto, vengono indicati gli obiettivi e le priorità in materia di sicurezza delle reti e dei sistemi informativi. Sono altresì definiti: il quadro di governance per conseguire gli obiettivi; le priorità su cui impattano le misure del PNRR, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti; e le misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato. Vengono inoltre contemplati i programmi di formazione, sensibilizzazione ed istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi, i piani di ricerca e sviluppo e un piano di valutazione dei rischi con l'elenco dei vari attori coinvolti nell'attuazione. Nella prospettiva d'attuazione, **l'Agenzia per la Cybersicurezza Nazionale** (ACN), in stretto contatto con l'Amministrazione titolare, il Dipartimento per la Trasformazione Digitale (DTD), curerà

[3] Tramite la creazione della nuova Piattaforma unica di notifiche digitali per comunicare efficacemente con cittadini e imprese garantendo la validità legale degli atti.

l'attuazione dell'investimento connettendo il mondo della Pubblica Amministrazione, dell'impresa e dei fornitori di tecnologia. La trasformazione digitale della PA contiene anche importanti misure di rafforzamento delle difese *cyber*, a partire dalla piena attuazione della disciplina in materia di "Perimetro di Sicurezza Nazionale Cibernetica". In tale ambito l'Agenzia per la Cybersicurezza Nazionale curerà l'evoluzione dell'infrastruttura e dei servizi per l'attuazione della strategia *cyber* nazionale che si articola su tre pilastri: sviluppare le capacità di ***cyber resilience*** in modo diffuso nel Paese; rafforzare le capacità nazionali di scrutinio e certificazione tecnologica; potenziare le capacità *cyber* della Pubblica Amministrazione. Il piano prevede investimenti incentrati su: capacità di monitoraggio; prevenzione e risposta più efficaci contro le minacce cyber per identificare tempestivamente gli eventi informatici malevoli e mitigarne gli effetti dannosi al fine di conservare in sicurezza dati e servizi della Pubblica Amministrazione; certificazione delle tecnologie *cyber* per una transizione digitale nazionale resiliente. Gli investimenti sono organizzati su quattro aree di intervento principali. In primo luogo, sono rafforzati i presidi di front-line per la gestione degli *alert* e degli eventi a rischio intercettatati verso la PA e le imprese di interesse nazionale. In secondo luogo, sono costruite o rese più solide le capacità tecniche di valutazione ed audit continuo della sicurezza degli apparati elettronici e delle applicazioni utilizzate per l'erogazione di servizi critici da parte di soggetti che esercitano una funzione essenziale. Inoltre, si investe nell'immissione di nuovo personale sia nelle aree di pubblica sicurezza e polizia giudiziaria dedicate alla prevenzione ed investigazione del crimine informatico diretto contro singoli cittadini, sia in quelle dei comparti preposti a difendere il Paese da minacce cibernetiche. Infine, sono irrobustiti gli *asset* e le *unità cyber* incaricate della protezione della sicurezza nazionale e della risposta alle minacce *cyber*. Tutto ciò è svolto in raccordo con le iniziative europee per assicurare la protezione degli interessi comuni dei cittadini e delle imprese.[4] Nell'orizzonte del 2024 tali interventi porteranno al dispiego integrale dei Servizi nazionali di *cybersecurity* con l'attivazione di una rete nazionale integrata di servizi di rilevamento, gestione e mitigazione del rischio *cyber* a supporto della PA e dell'industria nazionale; al completamento della rete dei laboratori a supporto del conseguimento dell'autonomia strategica nazionale nel settore ed alla realizzazione di un piano operativo delle attività di monitoraggio tecnico-organizzativo, con almeno 50 interventi di potenziamento delle capacità *cyber* della PA a protezione dei dati e dei servizi dei cittadini. Specificamente il Piano segnala una serie di criticità che necessitano di adeguate risposte:

[4] https://www.governo.it/sites/governo.it/files/PNRR.pdf

- il crescente livello complessivo di vulnerabilità della società per minacce *cyber*, dovuto alla sempre maggiore diffusione della digitalizzazione in ogni campo del vivere civile;
- la crescente dipendenza da servizi *software*, con la conseguente esposizione alle intenzioni degli sviluppatori/proprietari degli stessi;
- l'aumento di interdipendenza delle *catene del valore digitali*

La trasformazione digitale della PA, come programma nel PNRR, prevede quindi importanti misure di rafforzamento delle difese *cyber*, rendendo *genius loci* il perimetro di Sicurezza Nazionale Cibernetica.

In chiave schematica gli investimenti sono organizzati su quattro aree di intervento principali:

1. Rafforzare i presidi di *front line* per la gestione degli *alert* e degli eventi a rischio intercettatati verso le PA e le imprese di interesse nazionale;
2. Costruire (o rendere più solide) le capacità tecniche di valutazione ed *audit* continuo della sicurezza degli apparati elettronici e delle applicazioni utilizzate per l'erogazione di servizi critici da parte di soggetti che esercitano una funzione essenziale;
3. Investire nell'immissione di nuovo personale sia nelle aree di pubblica sicurezza e polizia giudiziaria, dedicate alla prevenzione ed investigazione del crimine informatico diretto contro singoli cittadini, sia in quelle dei comparti preposti a difendere il Paese da minacce cibernetiche;
4. Irrobustire gli *asset* e le unità *cyber* incaricate della protezione della sicurezza nazionale e della risposta alle minacce *cyber*.

Il **Piano Nazionale di Ripresa e Resilienza**, l'istituzione della nuova **Agenzia per la Cybersicurezza nazionale** ed il **decreto attuativo** del perimetro di sicurezza nazionale cibernetica pongono la *cybersecurity* a fondamento della digitalizzazione della Pubblica Amministrazione e del Sistema Italia. In tale contesto sono necessarie infrastrutture

tecnologiche e piattaforme in grado di offrire a cittadini ed imprese servizi digitali efficaci, sicuri e resilienti. Si evidenzia che la minaccia cibernetica cresce continuamente in quantità e qualità, determinata anche dall'evoluzione delle tecniche di ingegneria sociale volte a ingannare gli utenti finali dei servizi digitali sia interni alla PA che fruitori dall'esterno. Inoltre, si assistite ad un incremento notevole degli attacchi alle *supply chain*, ovvero alla catena dei fornitori di beni e servizi nell'indotto della PA. È necessario quindi per tutte le PA un cambio di approccio in cui la *cybersecurity* non deve essere vista come un costo o un mero adempimento normativo, ma come un'opportunità per la crescita e la trasformazione digitale sia della Pubblica Amministrazione che dell'intero Paese. Questa è la chiave di riflessione del PNRR legata alla *cybersecurity*. Punti focali di questa valutazione sono le tematiche relative al ***Cyber Security Awareness***, in quanto da tale consapevolezza possono derivare le azioni organizzative necessarie a mitigare il rischio connesso alle potenziali minacce informatiche e alle evoluzioni degli attacchi informatici.

La sicurezza delle reti e dei sistemi informatici deve considerare anche lo sviluppo delle infrastrutture digitali, parte integrante della strategia di modernizzazione del settore pubblico, poiché queste sostengono l'erogazione sia di servizi pubblici a cittadini e imprese sia di servizi essenziali per il Paese. Tali infrastrutture devono essere affidabili, sicure, energeticamente efficienti ed economicamente sostenibili. L'evoluzione tecnologica espone, tuttavia, i sistemi a nuovi e diversi rischi, anche con riguardo alla **tutela dei dati personali**. L'obiettivo di garantire una maggiore efficienza dei sistemi non può essere disgiunto dall'obiettivo di garantire contestualmente un elevato livello di sicurezza delle reti e dei sistemi informativi utilizzati dalla Pubblica Amministrazione. Conseguentemente, nella M1C1 si pone l'esigenza di attuare un percorso di razionalizzazione delle infrastrutture per garantire la sicurezza dei servizi erogati dalle amministrazioni mediante la migrazione diretta a *data center* più sicuri e verso infrastrutture e servizi *cloud qualificati*, ovvero conformi a standard di qualità, sicurezza, performance e scalabilità, portabilità e interoperabilità. Le amministrazioni che devono attuare il processo di migrazione potranno avvalersi dei finanziamenti previsti dalla componente richiamata per un ammontare complessivo di 1,9 miliardi di euro, nello specifico con i due investimenti che mirano all'adozione dell'approccio *Cloud first* da parte della PA, ovvero "Investimento 1.1: Infrastrutture digitali" e "Investimento 1.2: Abilitazione e facilitazione migrazione al cloud".

# La Cybersicurezza e le minacce informatiche

## 1. La Cybersicurezza

La *cybersicurezza* può essere definita, in linea generale ed in prima approssimazione, come l'insieme di mezzi, tecnologie, attività e procedure teso a garantire la sicurezza informatica dei computer, server, dispositivi mobili, sistemi elettronici, reti informatiche (con particolare attenzione alla rete internet) in termini di disponibilità, confidenzialità e integrità dei beni o asset informatici. da eventuali attacchi dannosi. Essa, pertanto, è riferita all'insieme di tecnologie, processi e procedure finalizzate alla protezione di reti, dispositivi, programmi e dati da attacchi, danni o accessi non autorizzati.

La pubblica amministrazione (inclusi i corpi militari), le aziende, le organizzazioni sanitarie, le organizzazioni finanziarie, ecc. raccolgono, elaborano e archiviano sui propri dispositivi una quantità sempre crescente di dati, con precisione sempre più capillare. La crescita esponenziale dell'importanza della rete in molteplici attività umane[5], incluse quelle legate alla vita quotidiana, comporta un analogo incremento dei dati presente *on-line*, molti dei quali sensibili o strettamente riservati (es. informazioni sanitarie o personali, dati genetici, dati biometrici, dati finanziari, ecc.). Le organizzazioni, pubbliche e private, nello svolgimento delle proprie attività istituzionali utilizzano le reti e ad altri dispositivi (come ad esempio, la Piattaforma Digitale Nazionale Dati) per la trasmissione e la condivisione con altri soggetti istituzionali (come nei casi della c.d. *cooperazione applicativa*) dei dati in proprio possesso. L'accesso non autorizzato a tali dati, la loro esposizione senza il previo consenso, la loro alterazione o distruzione sono tutti eventi in grado di dare vita a conseguenze negative per il titolare dei dati stessi.

Purtroppo, l'esperienza comune ci insegna che la "crescita" della rete è stata accompagnata da un analogo incremento ed una continua evoluzione delle minacce in rete. Le tecniche utilizzate per portare a segno attacchi *cyber* sono divenute, infatti, sempre più raffinate ed all'avanguardia, al punto da essere in grado, in molti casi, di superare o aggirare i sistemi e le procedure di sicurezza implementate proprio per contrastarle.

È divenuta, dunque, sempre più impellente la necessità di una tutela efficace contro le minacce e gli attacchi di *hacker* e malintenzionati in genere e, quindi, di un rafforzamento dei sistemi

[5] La tendenza verso una sempre maggiore importanza della rete nella società odierna appare sostenuta da due impulsi fondamentali. Da un lato la crescita costante del numero di utenti e, dall'altro, l'incremento dei dispositivi connessi (PC, tablet, smartphone, smart TV, ecc.). Quest'ultimo aspetto sembra destinato ad una crescita sempre maggiore grazie alle nuove frontiere della *domotica* e del c.d. *internet delle cose*.

di sicurezza che coinvolga strumenti, procedure e professionalità coinvolte. Una valida strategia di sicurezza informatica, infatti, riesce ad assicurare un grado adeguato di protezione rispetto agli attacchi dei criminali informatici.

I settori maggiormente colpiti dagli attacchi criminali sono: servizi bancari, servizi medici, rivenditori ed enti pubblici, ma qualunque dispositivo proiettato sulla rete è potenzialmente esposto a rischio di attacchi *cyber*.

## 2. Le diverse tipologie di attacchi informatici

L'attività di vigilanza e di contrasto delle minacce *cyber* è rivolta ha lo scopo di combattere tre diversi tipi di comportamenti illegali:

3. **cybercrimine**: attività sanzionate dall'ordinamento penale, poste in essere per mezzo (e spesso con l'abuso) delle tecnologie dell'informazione e della comunicazione (sia *hardware* che *software*) o, comunque, orientate contro i beni informatici[6]. Il cybercrimine è, pertanto, materia disciplinata dal diritto penale che nel corso del tempo ha delineato lo scenario del cybercrimine, anche in funzione dell'evoluzione tecnologica e del consolidamento di tecniche criminali sempre più raffinate, sia individuando nuove figure criminose sia riconducendo i comportamenti in rete a figure criminose già esistenti[7]. Nello scenario attuale i crimini informatici più diffusi consistono in aggressioni mirate a sistemi aziendali o istituzionali, finalizzati al conseguimento di un vantaggio economico o a provocare l'interruzione di un dato servizio o un'attività aziendale;

4. **cyberattacchi**: azioni, manovre o tentativi posti in essere da individui singoli o organizzazioni verso sistemi informatici, infrastrutture, reti di calcolatori e/o dispositivi elettronici con la finalità diraccogliere, alterare o distruggere dati e informazioni. Le motivazioni alla base degli attacchi informatici possono essere ricondotte essenzialmente a tre categorie principali: politica, criminale e personale. Gli attacchi a sfondo politico sono perpetrati da organizzazioni che intendono sfruttare l'evento per attirare l'attenzione sulle cause portate avanti e quindi, essenzialmente, per avere visibilità. Le aggressioni di tipo criminale sono, invece finalizzate al conseguimento di facili guadagni finanziari grazie al furto di denaro, al furto di dati

[6] Sono considerati, dunque, reati informatici sia la frode o il furto di informazioni riservate realizzate grazie all'utilizzo di dispositivi digitali, sia il danneggiamento di sistemi informatici.
[7] Ad esempio, l'accesso abusivo ad un sistema informatico che è stato assimilato al reato di violazione di domicilio di cui all'art. 614 del Codice penale.

(incluso lo spionaggio industriale) o al danneggiamento o all'interruzione dell'attività di concorrenti commerciali. Le aggressioni animate da motivazioni personali sono riferibili a soggetti che hanno particolari legami con l'organizzazione colpita (es. dipendenti, ex dipendenti, utenti, ecc.) e possono avere motivazioni piuttosto varie che vanno dal furto di dati o di denaro, a meri danneggiamenti spesso animati da risentimenti vari;

3. **cyberterrorismo**: attacchi illegali e minacce rivolti contro sistemi informativi di organizzazioni nazionali messi in atto per intimidire o costringere un governo o il suo popolo ad un dato comportamenti o per ingenerare paura e disorientamento nella società e perseguire, così, obiettivi politici e/o sociali. Gli atti di cyberterrorismo si caratterizzano per la loro attitudine a provocare violenza o a mettere in pericolo persone o beni, provocando danni sufficienti ad ingenerare sentimenti di paura (es. attacchi che determinano esplosioni, incidenti aerei, contaminazione delle condotte idriche acqua, gravi perdite economiche, ecc.).

### *2.1 I Malware*

La minaccia informatica più comune e più diffusa è rappresentata dai *malware*[8]. Con tale termine si intende, genericamente, un programma o un codice dannoso che mette a rischio un sistema informatico danneggiandolo o provocandone il malfunzionamento che si diffonde, normalmente attraverso la diffusione di allegati e-mail non richiesti o *download* in apparenza legittimi.

In particolare, i *malware* si attivano nel momento in cui l'utente apre un collegamento o un allegato apparentemente innocuo che, però, installa sul dispositivo uno o più *software* pericolosi.

I *malware* non sono in grado arrecare danni fisici alle componenti *hardware* dei dispositivi ma, intervenendo sulla componente *software*, possono compromettere le funzioni fondamentali di un terminale (computer, tablet, *smartphone*, ecc.) o spiare le attività degli utenti o, infine, rubare, criptare o eliminare dati.

L'utilizzo dei *malware* è, pertanto, finalizzato ad invadere, danneggiare o disattivare reti, sistemi, e terminali, assumendone parzialmente il controllo. Per questa via i criminali

[8] Il termine *malware* nasce dalla contrazione di "*malicious software*" (*software* malevolo).

informatici, attraverso i *malware* mirano ad ottenere vantaggi (economici o di altro tipo) a danno degli utenti.

Le tipologie di *malware* più comuni sono:

- **virus:** è un *software* che infetta uno o più *file* residenti sul terminale attaccato[9] integrandosi nei codici eseguibili (incluso il sistema operativo) del sistema informatico vittima, senza farsi rilevare dall'utente. Un virus informatico è capace di replicarsi autonomamente, quando vengono eseguiti i programmi infettati, e di diffondersi nell'intero sistema informatico;

- **worm**: si tratta di *malware* simili ai virus che non necessitano, però, di legarsi ad altri programmi eseguibili per diffondersi in quanto utilizza le e-mail o le reti di computer. Solitamente i *worm* danneggiano o distruggono i file dei dispositivi aggrediti;

- **trojan[10] (o cavalli di Troia):** è un tipo di *malware* che solitamente si presenta come un *software* legittimo, ma che consente accessi non autorizzati al computer della vittima. I *trojan* vengono utilizzati per rubare dati finanziari o per installare altre minacce e, più in generale per assumere il controllo remoto del terminale ad insaputa del legittimo proprietario;[11]

- **rootkit**: è un tipo di *malware* che fornisce agli *hacker* l'acceso a dispositivo bersaglio con i privilegi da amministratore. Operano in maniera da rimanere invisibili agli utenti, altri *software* e al sistema operativo stesso. In alcuni casi possono arrivare ad infettare anche il *firmware* dei computer;

- **spyware:** è un *malware* che spia segretamente le attività e i comportamenti dell'utente, al fine di far acquisire ai criminali informatici informazioni utili da sfruttare a proprio vantaggio (es. dati delle carte di credito);

- **keylogger:** sono *malware* che vanno in esecuzione come processi in *background* su computer o altri dispositivi e registrano i tasti premuti dall'utente sulla tastiera, memorizzando le informazioni raccolte e inviandole ai criminali informatici i quali, in

[9] Molto spesso di tratta di file di tipo eseguibile es. *.exe, *.bat, ecc.
[10] Il nome è ispirato all'*Iliade* e alla vicenda della guerra di Troia: in quanto il *trojan* si nasconde all'interno di un altro programma apparentemente utile e innocuo. Un *trojan* può contenere qualsiasi tipo di istruzione malevola. Spesso i *trojan* sono usati come veicolo alternativo ai *worm* e ai *virus* per installare delle *backdoor* o dei *keylogger* sui sistemi bersaglio.
[11] Un particolare tipo di utilizzo dei *trojan*, sempre più diffuso, è rappresentato dal c.d. ***cryptomining dannoso*** (o *drive-by mining* o *cryptojacking*). Attraverso l'installazione di un *trojan* i criminali informatici sono in grado di utilizzare le risorse del computer infettato per "*estrarre*" criptovalute (*mining*) ed inviare, poi, la valuta raccolta ai propri account.

questo modo, ottengono informazioni sensibili come nomi utente, *password*, PIN delle carte di credito, ecc.;

- **ransomware:** si tratta di un *malware* che impedisce all'utente l'accesso al proprio dispositivo o ai dati criptando i file. Solitamente il *ransomware* è associato ad una richiesta di un riscatto per poter sbloccare i file criptati;
- **adware:** *software* indesiderati utilizzati per presentare materiale pubblicitario (spesso all'interno del *browser*) che presentandosi come una componente legittima possono essere utilizzati per diffondere *malware;*
- **botnet**: rete di dispositivi infettati da *malware* (detti *bot* o *zombie*) che i criminali informatici riescono a controllare tramite un unico dispositivo (detto *botmaster*). Il Botnet permette l'esecuzione di *task online* senza l'autorizzazione dell'utente ed aumenta esponenzialmente le capacità offensive di chi ha sferrato l'attacco. Attraverso i dispositivi infettati è possibile lanciare attacchi definiti *Distributed Denial of Service*[12] (attacco DDoS) contro altri sistemi.

### *2.2 Le altre minacce informatiche*

Nel corso del tempo a fianco ai *malware* il crimine informatico ha elaborato anche modalità differenti per utilizzare illegalmente e a proprio vantaggio dati, informazioni e sistemi informatici o per interferire con servizi in rete o un'attività aziendali. Si tratta di condotte criminali abbastanza sofisticate che interferiscono con le modalità di funzionamento dei sistemi di elaborazione o di comunicazione, insinuandosi nei punti di eventuale debolezza dei sistemi stessi. Anche in questo caso gli esempi sono molteplici, ma ci limiteremo a ricordare i più diffusi:

- **immissione di codice SQL**: si tratta di un attacco informatico finalizzato al furto dei dati contenuti in un'applicazione *web* interfacciata con un *database* (tipico esempio sono le pagine *web* degli erogatori di servizi *on line* che richiedono un nome utente e una *password*), attraverso l'inserimento nel *database* stesso di un'istruzione SQL dannosa, che permette l'accesso alle informazioni sensibili contenute nel *database*;

[12] Gli attacchi di tipo *Distributed Denial of Service* (in inglese *attacco distribuito di interruzione del servizio*) determinano l'esaurimento delle risorse di un sistema informatico che fornisce un servizio *on line* attraverso una crescita esponenziale delle richieste (e, più in generale, del traffico dei dati in entrata) rivolte al sistema bersaglio da molte fonti diverse.

- ***phishing***: è una tipica truffa *on line* in cui i criminali informatici, simulando una comunicazione digitale da parte di un ente affidabile (es. e-mail, SMS, ecc.), mirano ad ingannare la persona oggetto di raggiro cercando di convincerla, con messaggi per lo più allarmistici, a fornire le proprie informazioni personali, dati finanziari o codici di accesso. In questo modo i criminali informatici riescono ad accedere agli account di posta elettronica, alle informazioni sulle carte di credito, agli ID, ai conti bancari e ai sistemi interni;
- **attacco *Man-in-the-Middle***: si tratta di una minaccia informatica in cui il criminale informatico intercetta, ritrasmette o altera segretamente le comunicazioni fra due parti che credono di comunicare direttamente tra di loro, allo scopo di sottrarre dati;
- **attacco *Denial of Service***: si tratta di attacchi in cui i criminali informatici cercano di impedire agli utenti l'accesso alla rete, ad un server *web*, FTP o di posta elettronica. Detti attacchi vengono realizzati con l'invio di molti pacchetti di richieste con la finalità di saturare le risorse e di un dato sistema, rendendolo così *instabile* e non disponibile agli altri utenti. Il sovraccarico di reti e server impedisce, infatti, al servizio di soddisfare le richieste legittime;
- **attacco MITM**: è un tipo di attacco in cui il criminale informatico si inserisce nel flusso di informazioni che si instaura tra un utente e una rete Wi-Fi pubblica non protetta. Di norma ciò avviene attraverso un *malware* che consente l'acquisizione fraudolenta di informazioni riservate.

## 3. I contenuti della *Cybersecurity*

La protezione rispetto agli attacchi informatici è rivolta verso tutti i potenziali rischi cagionati da soggetti interni ed esterni all'organizzazione ed operativamente agisce su due livelli principali, il livello di *sicurezza fisica ed ambientale* che attiene alle componenti *hardware* ed alle condizioni in cui delle componenti operano (ad es. la limitazione dell'accesso fisico nei locali in cui sono custoditi *server* ed altre componenti critiche) ed il livello di *sicurezza logica* che attiene, invece, agli strumenti di tipo *software*.

Le attività di *cybersecurity* possono essere classificate in diverse categorie in ragione dello specifico oggetto di protezione:

- **sicurezza di rete**: insieme di strategie, procedure e tecnologie finalizzate a proteggere le reti informatiche dalle azioni dei criminali informatici (come attacchi mirati o

*malware* opportunistici) finalizzate ad accedere a una rete, a modificarla o a violarla. La sicurezza di rete si raggiunge integrando più linee di difesa in corrispondenza delle possibili criticità. In primo luogo, è necessaria un'adeguata policy di controllo degli accessi alla rete che riguardi sia gli utenti autorizzati, sia i dispositivi collegati e i dati immessi. Un'altra linea di difesa di particolare importanza è rappresentata dalla capacità di filtrare, grazie ad appositi dispositivi *hardware* o *software* denominati *firewall*, il traffico in entrata e in uscire dalla rete. Estremamente importante, in quest'ambito, è la capacità di prevenire ed individuare eventuali intrusioni fornendo risposte adeguate;

- **sicurezza delle applicazioni**: protezione di *software* e dispositivi da possibili minacce che potrebbero consentire l'accesso i dati e informazioni meritevoli di protezione o modifiche al codice dall'applicazione da parte di soggetti non autorizzati[13]. Per garantire la sicurezza delle applicazioni si utilizzano *hardware*, *software* e procedure specifici che mirano ad identificare e minimizzare i fattori di vulnerabilità. I processi tesi alla sicurezza delle applicazioni stanno assumendo sempre maggiore importanza a causa del fatto che le applicazioni utilizzate nelle Amministrazioni Pubbliche e nelle imprese, sempre più spesso, vengono rese sono disponibili in ambienti *cloud*, dove emergono rischi specifici, ulteriori rispetto ai normali profili di vulnerabilità delle applicazioni. In primo luogo, il continuo flusso di dati sensibili o, comunque, meritevoli di tutela lungo la rete internet, che l'utilizzo del *cloud* comporta, espone maggiormente queste informazioni al rischio di possibili violazioni e minacce. Inoltre, come è noto, gli ambienti *cloud* mettono a disposizione degli utilizzatori risorse condivise ove è, pertanto, necessario che ciascun utente abbia accesso, nell'ambito delle proprie applicazioni *cloud*, esclusivamente ai dati per cui dispongono delle autorizzazioni. Un ulteriore aspetto, che sta assumendo sempre maggiore interesse, è quello legato alla sicurezza delle applicazioni *web* in quanto coinvolge servizi *on-line* di amministrazioni pubbliche e imprese a cui è possibile accedere tramite l'interfaccia di un *browser* su Internet o utilizzando apposite app. Di norma, le applicazioni *web* risiedono su server remoti, il che comporta un flusso di dati da e verso l'utente veicolato sulla rete internet;
- **sicurezza delle informazioni**: protezione del patrimonio informativo di una organizzazione (tra cui rientrano anche i dati detenuti a titolo temporaneo) da accessi, divulgazioni, utilizzi, alterazioni, interruzioni o distruzioni non autorizzate, al fine di

[13] Per poter massimizzare l'efficacia delle strategie di sicurezza delle applicazioni è necessario che la sua implementazione venga programmata già nella fase di progettazione dell'applicazione stessa.

garantire integrità[14], riservatezza[15] e disponibilità[16]. In altri termini, la sicurezza delle informazioni è orientata alla difesa delle informazioni da minacce sia interne che esterne. La sicurezza delle informazioni copre un campo più ampio della cybersicurezza (che comprende anche le informazioni conservate in modalità cartacee) e si concentra principalmente sulla prevenzione di fughe, distorsioni e distruzione di informazioni;

- **sicurezza operativa**: gestione e protezione degli asset di dati attraverso attente *policy* in tema di autorizzazioni utilizzate dagli utenti per accedere ad una rete e di procedure standardizzate per la memorizzazione o la condivisione dei dati;***disaster recovery* e continuità operativa**: strategie che permettono di rispondere efficacemente a qualsiasi evento che determina una perdita in termini di operazioni o dati (inclusi gli incidenti di *cybersecurity*). La *disaster recovery* individua le procedure utili per ripristinare le operazioni e le informazioni di un'organizzazione e, conseguentemente, la capacità operativa disponibile prima dell'evento. La *continuità operativa* sta ad indicare la capacità di un'organizzazione di mantenere determinati standard nell'erogazione di prodotti e servizi successivamente al verificarsi di un incidente;
- **formazione degli utenti finali**: adeguamento della capacità e della propensione degli utenti al rispetto delle procedure di sicurezza per minimizzare il rischio di introdurre accidentalmente un *malware* o altre minacce in un sistema altrimenti sicuro (es. eliminare e-mail sospette, non inserire unità USB di cui non se ne conosce il grado di sicurezza, ecc.).

## 4. La *Cybersecurity* e le attività dinamiche connesse

Considerando in chiave approfondita il macro-tema della Cybersecurity appare necessaria una valutazione interdisciplinare. In prima istanza appare opportuno considerare **l'analisi euristica**. Nel merito è un'analisi di tipo informatico necessaria per mantenere alto il livello di sicurezza del sistema e individuare eventuali minacce come virus o malware. In ambito scientifico tale processo è utilizzato per formulare un insieme di ipotesi, tecniche e strategie preziose per trovare un concetto, una teoria o un argomento utile per risolvere un problema.

[14] Dati ed informazioni devono essere protetti rispetto ad interventi ed alterazioni illeciti che ne compromettono validità, accuratezza o completezza.
[15] L'accesso alle informazioni deve essere consentito solo agli utenti autorizzati. A tal fine è necessario proteggerle da accessi non autorizzati da parte di soggetti interni ed esterni all'organizzazione.
[16] I soggetti autorizzati devono poter essere disponibili nel momento in cui ne hanno bisogno, secondo i requisiti di servizio stabiliti. Occorre, quindi, che le informazioni siano protette da eventi che possano comprometterne la disponibilità (guasti, interruzioni delle connessioni di rete, ecc.).

In ambito di cybersicurezza è un'analisi approfondita del codice sorgente di una pagina web con l'obiettivo di individuare segmenti infetti o sospetti, anomalie e comandi pericolosi. Concretamente viene analizzato il linguaggio di programmazione e la modalità di scrittura di una applicazione, evidenziando la fonte primaria per eseguire una scansione completa che ne garantisca l'affidabilità e attendibilità.

Tale modalità di analisi consente anche di intercettare facilmente le anomalie e permette di prevenire la comparsa di virus, ostacolando la proliferazione di nuove minacce in una novazione costante e progressiva. Proprio per questo l'analisi euristica è una delle tecniche di base per lo sviluppo dei software antivirus. Nel dettaglio l'analisi euristica consente di poter aumentare il livello di sicurezza informatica raffinando gli strumenti di difesa contro ogni tipo di *cyber attacco*. Spicca in tale valutazione la necessità di un'estrema rapidità, concretamente declinata nella rapidissima identificazione di virus e programmi indesiderati, e la connessa dinamicità di esecuzione. In tale ultima prospettiva, cruciale per la sicurezza informatica, tale forma di analisi assume centralità costruendo nel tempo una memoria strutturata inerente al comportamento dei ***malware.*** In questo modo si dà vita a numerosi database in cui sono presenti tutte le informazioni relative a intere famiglie di *malware*. Queste caratteristiche sono interconnesse con l'economicità e il costante aggiornamento operato dagli sviluppatori, dai programmatori e dai produttori di antivirus. Ulteriore elemento dinamico che afferisce al macro ambito Cybersecurity è il ***pattern recognition*** che declina specialisticamente l'area dell'apprendimento automatico. Per comprendere tale concetto è necessario riflettere sull'analisi computazionale delle immagini e dei modelli più astratti. Nel dettaglio, la tecnologia di ***computer vision*** comporta l'acquisizione di immagini digitali utilizzando sensori di immagine, l'elaborazione e l'analisi delle foto per acquisire una certa comprensione dell'input visivo. La *visione artificiale* è un sottoinsieme dell'*intelligenza artificiale* ed è utilizzata per estrarre informazioni significative dalle immagini. La *computer vision* è un campo dell'apprendimento automatico e dell'intelligenza artificiale che si occupa di come i computer possono essere addestrati a ricavare informazioni significative da immagini o video digitali. Viene utilizzato in un'ampia gamma di aree applicative, come il riconoscimento facciale, il rilevamento dei difetti, la verifica dell'assemblaggio, il rilevamento degli intrusi e sicurezza dei server. Per l'interpretazione delle minacce potenziali e attuali ai sistemi informatici, la *computer vision* è strettamente correlata alla ***pattern recognition***. Il riconoscimento dei modelli o riconoscimento degli schemi è un metodo di analisi dei dati che riconosce modelli e regolarità dei flussi informatici utilizzando algoritmi di apprendimento automatico. È uno studio su come le macchine possono classificare gli oggetti in una serie di categorie e classi similmente a come il cervello umano valuta gli accadimenti esterni.

Specificamente, la *pattern recognition* è una tecnologia che consente alle macchine di rilevare disposizioni di caratteristiche o dati che forniscono alcune informazioni importanti su un dato sistema. Una dinamica di sicurezza informatica attiva radicata nel processo di guardare i dati e cercare di identificare eventuali regolarità all'interno degli stessi. In chiave di sicurezza preventiva, la *pattern recognition* è alla base della risoluzione dei problemi e della progettazione di algoritmi ed ha come obiettivo quello di apprendere un classificatore di dati (*pattern*) basandosi su conoscenza di informazioni statistiche estratte dai pattern stessi. I pattern da classificare sono tipicamente gruppi di misure che definiscono punti in uno spazio multidimensionale (al contrario del *pattern matching*, in cui il pattern è specificato in modo rigido). Da molti anni i motori di analisi euristica e di riconoscimento dei pattern d'azione dei sistemi operano con tali tecnologie per aumentare la protezione e fornire una difesa innovativa in grado di adattarsi alle tante minacce che animano il mondo del web e quello informatico in generale. In una visione interdisciplinare la cybersicurezza si connette con l'**intelligenza artificiale** cioè con l'insieme di tecnologie che combinano dati, algoritmi e potenze di calcolo.

I progressi compiuti nell'ambito del calcolo e la crescente disponibilità di dati sono pertanto fattori determinanti per l'attuale crescita dell'IA. L'impatto dei sistemi di intelligenza artificiale può essere considerato non solo da una prospettiva individuale del cittadino, ma anche dal punto di vista della società nel suo complesso impattando sulle pubbliche amministrazioni e imprese. L'utilizzo di tali tecnologie può svolgere un ruolo significativo nel conseguimento degli obiettivi di sviluppo sostenibile e nel sostegno al processo democratico e dei diritti sociali. In tale sentiero espositivo Libro bianco della Commissione Europea sull'intelligenza artificiale descrive la cornice prospettica di un approccio europeo teso all'eccellenza e alla fiducia. In tale documento si presentano le opzioni strategiche che consentono uno sviluppo sicuro e affidabile dell'IA in Europa, nel pieno rispetto dei valori e dei diritti dei cittadini dell'UE. I principali elementi costitutivi del libro bianco sono i seguenti:

- il quadro strategico che stabilisce misure per allineare gli sforzi a livello europeo, nazionale e regionale. Tramite un partenariato tra il settore pubblico e privato, l'obiettivo di tale quadro è mobilitare risorse per conseguire un "ecosistema di eccellenza" lungo l'intera catena del valore, a cominciare dalla ricerca e dall'innovazione, e creare i giusti incentivi per accelerare l'adozione di soluzioni basate sull'IA, da parte delle amministrazioni pubbliche e da parte delle piccole e medie imprese;

- gli elementi chiave di un futuro quadro normativo per l'IA in Europa, che creerà un "ecosistema di fiducia" unico. A tal fine, deve essere sempre garantito dal legislatore nazionale il rispetto delle norme dell'UE, comprese le norme a tutela dei diritti fondamentali e dei diritti dei consumatori, in particolare per i sistemi di IA ad alto rischio gestiti nell'UE. La costruzione di un ecosistema di fiducia è un obiettivo strategico in sé e dovrebbe dare ai cittadini la fiducia di adottare applicazioni di IA e alle imprese e alle organizzazioni pubbliche la certezza del diritto necessaria per innovare utilizzando l'IA. La Commissione sostiene con forza un approccio antropocentrico basato sulla comunicazione "Creare fiducia nell'intelligenza artificiale antropocentrica"[17]e terrà conto anche dei contributi ottenuti durante la fase pilota degli orientamenti etici elaborati dal gruppo di esperti sull'IA.

Lo sfruttamento della capacità dell'UE di investire nelle tecnologie e nelle infrastrutture di prossima generazione nonché nelle competenze digitali, come l'alfabetizzazione ai dati (*data literacy*), accrescerà la sovranità tecnologica dell'Europa nell'ambito delle tecnologie e infrastrutture abilitanti fondamentali per l'economia dei dati. Le infrastrutture dovrebbero sostenere la creazione di hub europei di dati che consentano lo sviluppo di un'IA affidabile basata su valori e regole europei. L'Europa dovrebbe sfruttare i propri punti di forza per far crescere la propria posizione negli ecosistemi e lungo la catena del valore, da determinati settori della produzione di hardware al software e ai servizi. Inoltre, può contribuire a rafforzare la tecnologia legata alle **soluzioni neuromorfiche**[18], che sono ideali per l'automazione dei processi industriali (industria 4.0) e dei modi di trasporto e possono migliorare l'efficienza energetica di vari ordini di grandezza. Inoltre, i recenti progressi nell'ambito del calcolo quantistico genereranno un aumento esponenziale della capacità di elaborazione[19]favorendo la crescita del comparto legato alla Digitalizzazione, Innovazione e Sicurezza. Parallelamente è necessario considerare le basi algoritmiche dell'IA, creando collegamenti tra discipline che attualmente lavorano separatamente, come l'apprendimento automatico (***machine learning***) e l'apprendimento profondo (***deep learning***), che sono caratterizzati da una limitata interpretabilità e dalla necessità di una grande quantità di dati per addestrare i modelli e apprendere mediante correlazioni, e gli approcci simbolici, in cui le

[17] COM(2019) 168 final
[18] Per soluzioni neuromorfiche si intendono tutti i sistemi di circuiti integrati su larghissima scala (VLSI) che imitano le architetture neurobiologiche presenti nel sistema nervoso
[19] I computer quantistici avranno la capacità di elaborare in un tempo inferiore al secondo set di dati molto più grandi rispetto ai computer attuali con le più alte prestazioni, consentendo lo sviluppo di nuove applicazioni di IA in tutti i settori.

regole sono create mediante l'intervento umano. Combinare il ragionamento simbolico con le reti neurali profonde può aiutarci a rendere maggiormente spiegabili i risultati dell'IA. Migliorare l'accesso ai dati e la gestione degli stessi è una questione fondamentale. In tale prospettiva è opportuno considerare che senza dati lo sviluppo dell'IA e di altre applicazioni digitali è impossibile. Questo enorme volume di nuovi dati rappresenta un'opportunità per le pubbliche amministrazioni europee di assumere una posizione di primo piano nella trasformazione basata sui dati e sull'IA. La promozione di pratiche responsabili in materia di gestione dei dati e la conformità dei dati ai principi FAIR[20] contribuiranno a creare fiducia e a garantire la riutilizzabilità dei dati. Altrettanto importante è investire nelle tecnologie e nelle infrastrutture di calcolo.

## 5. La moderna gestione delle minacce

I sistemi informativi delle moderne organizzazioni (pubbliche amministrazioni, aziende, ecc.) si caratterizzano per un elevato grado di complessità che se da un lato permette il trattamento di una ingente mole di dati e l'erogazione di servizi capillari ed articolati, dall'altro espone tali sistemi informativi a rischi specifici quali *malware* mutevoli[21], APT (*Advanced Persistent Threats* - Minacce avanzate persistenti[22]), minacce interne[23]. Ulteriori momenti di vulnerabilità possono essere legati all'utilizzo di soluzioni *cloud* per il trattamento dei dati e l'erogazione dei servizi e di una forza lavoro (tutto o in parte) remota[24].

[20] *Findable, Accessible, Interoperable and Reusable*, cioè dati reperibili, accessibili, interoperabili e riutilizzabili, come indicato nella relazione finale e nel piano d'azione del gruppo di esperti della Commissione sui dati FAIR, 2018, https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf

[21] Si tratta di particolari *malware* estremamente versatili, in grado di variare il modo in cui si manifesta. Proprio questa capacità di mutare rende estremamente difficile la loro individuazione con soluzioni antivirus basate esclusivamente sull'utilizzo di firme virali, in quanto, per ogni variante del *malware* andrebbe generato un aggiornamento per il *software* antivirus.

[22] La locuzione anglosassone *Advanced Persistent Threat* (in italiano *minaccia avanzata e persistente*), individua una minaccia informatica posta in essere da criminali informatici dotati di elevate competenze tecniche e grandi risorse umane e finanziarie e, per questo, in grado di realizzare attacchi su larga scala, non visibili, protratti per lunghi periodi di tempo. Le APT sono finalizzate ad ottenere informazioni riservate o a rendere inutilizzabili alcuni servizi dell'organizzazione attaccata per motivazioni generalmente politiche o economiche. Gli attacchi APT sono molto utilizzati anche per il cyberspionaggio.

[23] Le minacce interne sono rappresentate da un uso improprio dei dati di un'organizzazione (pubbliche amministrazioni, aziende, ecc.) per cause accidentali o dolose. Le minacce interne sono particolarmente pericolose per la sicurezza informatica di PA e imprese e possono rivelarsi più costose delle minacce esterne.

[24] Di norma i dispositivi utilizzati dai *lavoratori remoti* sono meno protetti rispetto alle reti interne di PA e imprese, e rappresentano perciò uno degli anelli deboli della catena di protezione dalle aggressioni esterne. Occorre, infatti, tener presente che rispetto a tali aggressioni la protezione offerta dai normali *software* antivirus risulta, per lo più, insufficiente.

I più comuni sistemi di gestione delle minacce seguono un'architettura logica di supporto riferita a standard internazionali comuni[25] che individuano cinque funzioni fondamentali:

- ***identificazione***: individuazione dettagliata degli asset e delle risorse più importanti dell'organizzazione quali la gestione delle risorse, la *mission* istituzionale, la *governance*, la valutazione dei rischi, la strategia di gestione dei rischi;
- ***protezione***: messa in atto delle verifiche e dei controlli di sicurezza tecnica e fisica finalizzati allo sviluppo e all'implementazione di livelli di sicurezza efficace e alla protezione di infrastrutture critiche. Rientrano in quest'ambito la gestione delle identità, il controllo degli accessi, la formazione, la sicurezza dei dati, i processi e le procedure di sicurezza delle informazioni, la manutenzione e la tecnologia di protezione;
- ***rilevamento***: perfezionamento di misure in grado di segnalare all'organizzazione i possibili attacchi informatici. L'attività di rilevamento comprende: la segnalazione delle anomalie e degli eventi critici, il monitoraggio continuo della sicurezza e l'implementazione dei processi di rilevamento precoce;
- ***risposta***: reazione appropriata agli attacchi informatici e ad altri eventi di sicurezza informatica. Questa fase comporta la pianificazione della risposta, la comunicazione, l'analisi, la mitigazione del danno e i miglioramenti del sistema di gestione delle minacce;
- ***ripristino***: Implementazione dei piani per la resilienza informatica al fine di garantire la continuità operativa in caso di attacco informatico, violazione della sicurezza o altri eventi di sicurezza informatica.

[25] Nello specifico il riferimento è al *framework* di sicurezza informatica istituito dal *National Institute of Standards and Technology* (NIST) definito nella guida denominata *NIST Cybersecurity Framework* (NIST CF) ove, anche con il ricorso a standard e *best practice*, il NIST fornisce una guida completa per migliorare la sicurezza delle informazioni e la gestione dei rischi relativi alla sicurezza informatica per le organizzazioni del settore privato.

# Il Glossario della Cybersicurezza

**Abilitazione**: provvedimento con il quale l'Agenzia per la cybersicurezza nazionale accerta i requisiti necessari affinché un esperto o un laboratorio di prova possa coadiuvare l'Agenzia nelle attività di vigilanza nazionale o di rilascio dei certificati di cybersicurezza.

***Adware*: *software*** indesiderati utilizzati per presentare materiale pubblicitario (spesso all'interno del *browser*) che presentandosi come una componente legittima possono essere utilizzati per diffondere *malware*.

**Agenzia dell'Unione europea per la cybersicurezza**: Agenzia è incaricata di creare le condizioni per un elevato livello comune di cybersicurezza in tutta Europa.

**Agenzia per la cybersicurezza nazionale**: l'Agenzia di cui all'art. 5 del D.L. 14 giugno 2021, n. 82, convertito, con modificazioni, dalla L. 4 agosto 2021, n. 109, designata dall'art. 7, comma 1, lettera e), del medesimo decreto-legge, per l'Italia, quale autorità nazionale di certificazione della cybersicurezza.

**Attacco distribuito di negazione del servizio**: vedi Attacco Distributed Denial of Service (DDoS).

**Attacco *Distributed Denial of Service* (DDoS)**: attacchi informatici che determinano l'esaurimento delle risorse di un sistema informatico che fornisce un servizio *on line* attraverso una crescita esponenziale delle richieste (e, più in generale, del traffico dei dati in entrata) rivolte al sistema bersaglio da molte fonti diverse.

**Attacco *Man-in-the-Middle***: minaccia informatica in cui il criminale informatico intercetta, ritrasmette o altera segretamente le comunicazioni fra due parti che credono di comunicare direttamente tra di loro, allo scopo di sottrarre dati.

**Autorizzazione**: provvedimento con il quale l'Agenzia accerta il possesso di requisiti specifici o supplementari a cui sono soggetti gli organismi di valutazione della conformità per poter operare nell'ambito di uno specifico sistema europeo di certificazione, in aggiunta

a quanto già previsto nell'allegato del Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019.

**Botnet**: rete di dispositivi infettati da *malware* (detti *bot* o *zombie*) controllata da remoto tramite un unico dispositivo (detto *botmaster*). Il Botnet permette l'esecuzione di *task online* senza l'autorizzazione dell'utente ed aumenta esponenzialmente le capacità offensive dell'attacco sferrato.

**Certificato europeo di cybersicurezza**: un documento rilasciato da un organismo di certificazione che attesta che un determinato prodotto TIC, servizio TIC o processo TIC è stato oggetto di una valutazione di conformità ai requisiti stabiliti da un sistema europeo di certificazione.

**Continuità operativa**: strategia di risposta agli attacchi informatici che permette ad un'organizzazione di mantenere determinati standard nell'erogazione di prodotti e servizi successivamente al verificarsi di un incidente.

**Cryptomining dannoso**: procedura illegale che grazie all'installazione di un *trojan* fornisce ai criminali informatici la possibilità di utilizzare le risorse del computer infettato per "*estrarre*" criptovalute (*mining*) ed inviare, poi, la valuta raccolta ai propri account.

**Cryptojacking**: vedi Cryptomining dannoso.

**Cyberattacchi**: azioni, manovre o tentativi posti in essere da individui singoli o organizzazioni verso sistemi informatici, infrastrutture, reti di calcolatori e/o dispositivi elettronici con la finalità di raccogliere, alterare o distruggere dati e informazioni.

**Cybercrimine**: attività sanzionate dall'ordinamento penale, realizzate per mezzo (e spesso con l'abuso) delle tecnologie dell'informazione e della comunicazione o, comunque, orientate contro i beni informatici.

**Cyberterrorismo**: attacchi illegali e minacce rivolti a sistemi informativi di organizzazioni nazionali messi in atto per intimidire o costringere un governo e/o i cittadini ad un dato comportamenti o per ingenerare paura e disorientamento nella società e perseguire, così, obiettivi politici e/o sociali.

**Dichiarazione UE di conformità**: attestazione di conformità rilasciata da un fabbricante di prodotti
TIC o fornitore di servizi TIC ai sensi dell'art. 53, par. 1, del Regolamento UE 2019/881, a seguito del processo di autovalutazione di conformità previsto dallo stesso articolo.

***Disaster recovery*:** strategia di risposta agli attacchi informatici che individua le procedure utili per ripristinare le operazioni e le informazioni di un'organizzazione e, conseguentemente, la capacità operativa disponibile prima dell'evento.

**ECCG**: vedi Gruppo europeo di certificazione della cybersicurezza.

***Drive-by mining***: vedi Cryptomining dannoso.

**Elenco dei laboratori di prova e degli esperti per le attività di vigilanza nazionale**: registro aggiornato dei laboratori di prova e degli esperti abilitati dall'Agenzia ad effettuare attività di valutazione di sicurezza informatica nell'ambito dei compiti di vigilanza nazionale dell'Agenzia.

**Emittenti delle dichiarazioni di conformità UE**: i soggetti di cui all'art. 53, par. 1, del Regolamento UE 2019/881, ossia fabbricanti o fornitori di prodotti TIC, servizi TIC o processi TIC che presentano un basso rischio corrispondenti al livello di affidabilità *di base*.

**ENISA**: vedi Agenzia dell'Unione europea per la cybersicurezza.

**Formazione degli utenti finali**: adeguamento della capacità e della propensione degli utenti al rispetto delle procedure di sicurezza per minimizzare il rischio di introdurre accidentalmente un *malware* o altre minacce in un sistema altrimenti sicuro.

**Gruppo europeo di certificazione della cybersicurezza**: ai sensi dell'art. 62 del Regolamento.

**Immissione di codice SQL**: attacco informatico finalizzato al furto dei dati contenuti in un'applicazione *web* interfacciata con un *database* attraverso l'inserimento di SQL dannosa, che permette l'accesso alle informazioni sensibili contenute nel *database*.

**Keylogger:** *malware* che avviano un processo in *background* su computer o altri dispositivi e registrano i tasti premuti dall'utente sulla tastiera, memorizzando le informazioni raccolte e inviandole ai criminali informatici. Sono utilizzati per il furto di nomi utente, *password*, PIN delle carte di credito, ecc.

**Incidente**: ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi.

**Laboratorio di prova**: organismo di valutazione della conformità che svolge verifiche documentali e/o prove in base alle norme armonizzate europee ed agli standard e specifiche tecniche nell'ambito del sistema europeo di certificazione in cui è accreditato.

**Livello di affidabilità di base**: livello di affidabilità che soddisfa i requisiti ed è valutato con i criteri specificati al par. 5 dell'art. 52 del Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019.

**Livello di affidabilità elevato**: livello di affidabilità che soddisfa i requisiti ed è valutato con i criteri specificati al par. 7 dell'art. 52 del Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019.

**Livello di affidabilità sostanziale**: livello di affidabilità che soddisfa i requisiti ed è valutato con i criteri specificati al par. 6 dell'art. 52 del Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019.

***Malware*:** un programma o un codice dannoso che mette a rischio un sistema informatico danneggiandolo o provocandone il malfunzionamento che si diffonde, normalmente attraverso la diffusione di allegati e-mail non richiesti o *download* in apparenza legittimi.

**Messa a disposizione sul mercato**: la fornitura di un prodotto TIC o di un servizio TIC per la distribuzione, il consumo o l'uso sul mercato dell'Unione Europea nel corso di un'attività commerciale, a titolo oneroso o gratuito.

**Mercato online:** un servizio digitale che consente ai consumatori ovvero ai professionisti, come definiti rispettivamente all'articolo 141, comma 1, lettere a) e b), del D.lgs. 6 settembre

2005, n. 206, di concludere contratti di vendita o di servizi online con i professionisti sia sul sito web del mercato online sia sul sito web di un professionista che utilizza i servizi informatici forniti dal mercato online.

**Motore di ricerca online**: un servizio digitale che consente all'utente di effettuare ricerche, in linea di principio, su tutti i siti web o su siti web in una lingua particolare sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, frase o di altra immissione, e fornisce i link in cui trovare le informazioni relative al contenuto richiesto.

**Norma**: vedi standard.

**Norma armonizzata**: una norma europea adottata sulla base di una richiesta della Commissione Europea ai fini dell'applicazione della legislazione dell'Unione sull'armonizzazione ai sensi dell'art. 2, par. 1, n. 1, lett. c), del Regolamento (UE) n. 1025/2012.

**OCSI**: vedi Organismo di Certificazione della Sicurezza Informatica.

**Organismo di accreditamento**: l'organismo autorizzato a svolgere l'attività di accreditamento nel territorio dello Stato, ai sensi dell'art. 2, par. 1, n. 11, del Regolamento (CE) 765/2008, designato con decreto del Ministro dello sviluppo economico del 22 dicembre 2009 in attuazione dell'art. 4, comma 2, della L. 23 luglio 2009, n. 99.

**Organismo di certificazione**: organismo di valutazione della conformità che emette certificati europei di cybersicurezza in base alle norme armonizzate europee ed agli standard di riferimento ai sensi dell'art. 54, par. 1, lett. c), del Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019 per il sistema di certificazione in cui è accreditato.

**Organismo di Certificazione della Sicurezza Informatica**: organismo di certificazione dell'Agenzia per la cybersicurezza nazionale, accreditato ai sensi dell'art. 60, par. 2, del Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, istituito ai sensi dell'art. 4 del DPCM 30 ottobre 2003.

**Punto di interscambio internet (IXP)**: un'infrastruttura di rete che consente l'interconnessione di più di due sistemi autonomi indipendenti, principalmente al fine di agevolare lo scambio del traffico internet; un IXP fornisce interconnessione soltanto ai sistemi autonomi; un IXP non richiede che il traffico internet che passa tra qualsiasi coppia di sistemi autonomi partecipanti passi attraverso un terzo sistema autonomo, né altera o interferisce altrimenti con tale traffico.

**Quadro europeo di certificazione**: insieme della regolamentazione eurounitaria comprendente Titolo III del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, ed i successivi sistemi europei di certificazione adottati a norma dell'articolo 49 dello stesso Regolamento.

**Ransomware:** *malware* che impedisce all'utente l'accesso al proprio dispositivo o ai dati criptando i file. Solitamente il *ransomware* è associato ad una richiesta di riscatto per poter sbloccare i file criptati.

**Rappresentante:** la persona fisica o giuridica stabilita nell'Unione europea espressamente designata ad agire per conto di un fornitore di servizi digitali che non è stabilito nell'Unione europea, a cui l'autorità competente NIS o il CSIRT Nazionale può rivolgersi in luogo del fornitore di servizi digitali, per quanto riguarda gli obblighi di quest'ultimo ai sensi del decreto legislativo 18 maggio 2018, n. 65.

**Revoca di un certificato europeo di cybersicurezza:** annullamento di un certificato europeo di cybersicurezza prima della sua scadenza da parte dell'organismo di valutazione della conformità emittente o da parte dell'Agenzia.

**Richiamo:** qualsiasi provvedimento volto ad ottenere la restituzione di un prodotto TIC che è già stato reso disponibile all'utilizzatore finale.

**Rischio:** ogni circostanza o evento ragionevolmente individuabile con potenziali effetti pregiudizievoli per la sicurezza della rete e dei sistemi informativi.

**Ritiro:** qualsiasi provvedimento volto ad impedire la messa a disposizione sul mercato di un prodotto TIC o servizio TIC nella catena della fornitura.

**Rootkit**: *malware* capace di rimanere invisibili agli utenti, altri software e al sistema operativo che fornisce agli *hacker* l'acceso a dispositivo bersaglio con i privilegi da amministratore.

**Phishing**: truffa *online* basata su comunicazioni per lo più allarmistiche, apparentemente (ed in modo simulato) proveniente da un ente affidabile che spinge la vittima del raggiro a fornire le proprie informazioni personali, codici di accesso di account di posta elettronica, informazioni sulle carte di credito, dati di login a conti bancari o a sistemi interni, ecc.

**Servizio di cloud computing:** un servizio digitale che consente l'accesso a un insieme scalabile ed elastico di risorse informatiche condivisibili.
**Sicurezza delle applicazioni:** protezione di *software* e dispositivi da possibili minacce che potrebbero consentire l'accesso i dati ed informazioni meritevoli di protezione.
**Sicurezza delle informazioni:** protezione dell'integrità e della *privacy* dei dati, inclusi quelli detenuti a titolo temporaneo.

**Sicurezza di rete:** difesa delle reti informatiche dalle azioni dei criminali informatici come attacchi mirati o *malware* opportunistici.
**Sicurezza operativa**: gestione e protezione degli asset di dati attraverso attente *policy* in tema di autorizzazioni utilizzate dagli utenti per accedere ad una rete e di procedure standardizzate per la memorizzazione o la condivisione dei dati.

**Sicurezza dei sistemi informativi:** la capacità di una rete e dei sistemi informativi di resistere, a un determinato livello di riservatezza, ad ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi

**Sistema dei nomi di dominio (DNS):** è un sistema distribuito e gerarchico di naming in una rete che inoltra le richieste dei nomi di dominio.

**Specifica:** una specifica tecnica ai sensi dell'articolo 2, primo paragrafo, numero 4), del regolamento (UE) n. 1025/2012

**Spyware:** *malware* che spia segretamente le attività e i comportamenti dell'utente, al fine di far acquisire ai criminali informatici informazioni utili da sfruttare a proprio vantaggio (es. dati delle carte di credito).
**Standard:** una specifica tecnica, adottata da un organismo di normazione riconosciuto ai sensi dell'articolo 2, paragrafo 1, numero 1), del regolamento (UE) n. 1025/2012.

**TIC:** Tecnologia dell'Informazione e della Comunicazione.

**Trattamento dell'incidente:** tutte le procedure necessarie per l'identificazione, l'analisi e il contenimento di un incidente e l'intervento in caso di incidente.

**Trojan (o cavallo di Troia):** *malware* che presentandosi come un *software* legittimo, consente accessi non autorizzati al computer aggredito. I *trojan* vengono utilizzati per rubare dati finanziari o per installare altre minacce e, più in generale per assumere il controllo remoto del terminale ad insaputa del legittimo proprietario.

**Vigilanza del mercato:** le attività svolte ed i provvedimenti adottati dall'Agenzia per la cybersicurezza nazionale e dalle altre autorità pubbliche competenti per garantire che i prodotti TIC, i servizi TIC ed i processi TIC ad essi collegati siano conformi ai requisiti stabiliti dal quadro europeo di certificazione e non pregiudichino la salute, la sicurezza o qualsiasi altro aspetto della protezione del pubblico interesse.

**Virus:** *software* che infetta uno o più *file* residenti sul terminale attaccato, integrandosi nei codici eseguibili ed il sistema operativo del sistema informatico aggredito, non rilevabile dall'utente e capace, infine, di replicarsi autonomamente.

**Worm:** *malware* in grado di danneggiare o distruggere i file dei dispositivi aggrediti senza necessità di legarsi ad altri programmi eseguibili.