Quaderno di Polizia Cibernetica

Prevenire – Contrastare – Proteggere

A cura di:
Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica

Nr. 1 - Anno 2025

powered by:
KPMG

Prefetto Vittorio Pisani – Capo della Polizia
Direttore Generale della Pubblica Sicurezza

Viviamo in un'epoca in cui la rivoluzione digitale sta investendo tutta la nostra realtà quotidiana.

Le tecnologie dell'informazione rappresentano oggi non solo un formidabile strumento di progresso ma anche un terreno di confronto delicato, in cui si misurano la resilienza dei sistemi e la sicurezza dei nostri asset più strategici (come la salute, la mobilità, l'informazione).

Parallelamente, la dimensione digitale offre delle potenzialità inedite alla criminalità organizzata, con la maggioranza dei fenomeni criminali che ha assunto anche una connotazione virtuale, laddove, però, sono tristemente reali per le vittime le conseguenze delittuose.

Non è più soltanto l'identità fisica ad essere esposta al rischio di essere offesa o aggredita: è anche l'identità digitale di ciascuno a poter essere trafugata, sostituita, illecitamente utilizzata. E le azioni aggressive ibride generano un nuovo senso di insicurezza: il cittadino si può trovare smarrito in un mondo digitale ove i tradizionali strumenti di difesa non sono più adeguati.

Si tratta di nuove sfide che richiedono un'avanguardia di pensiero e invocano una nuova strategia in cui la sicurezza cibernetica rappresenta una delle dimensioni in cui si declina la pubblica sicurezza e quindi la sicurezza nazionale: esercizio complesso che richiede professionalità specializzate, strumenti adeguati e una visione sistemica e integrata dell'azione di prevenzione e di contrasto.

L'operatività della Direzione Centrale dedicata alla Sicurezza Cibernetica risponde a questa sfida, ponendo la Polizia di Stato nelle condizioni di affrontare con serietà, costanza ed efficacia le minacce che arrivano dalla rete. Un presidio essenziale, concepito per proteggere le infrastrutture digitali del Paese, garantire la continuità dei servizi essenziali, tutelare i dati sensibili dei cittadini e rafforzare la fiducia nella capacità dello Stato di presidiare quei diritti inviolabili garantiti dalla Costituzione, anche quando si esprimono in rete.

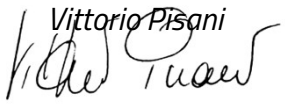
Il primo Quaderno di Polizia Cibernetica è il risultato di un'intensa attività di polizia, ma anche del necessario studio, del produttivo confronto e della divulgazione scientifica, che ha coinvolto accademici, esperti del settore privato e operatori di polizia, con l'obiettivo di valorizzare le esperienze maturate sul campo, offrire uno strumento concreto per la formazione e la sensibilizzazione su temi centrali della nostra contemporaneità.

In un tempo in cui le minacce digitali si evolvono con rapidità, l'elemento umano resta il fattore decisivo. La qualità della nostra risposta dipende dalla preparazione, dalla capacità di aggiornamento e quindi dalla dedizione dei nostri operatori. A loro, ai poliziotti, spesso primo presidio alla sicurezza cibernetica, va il mio più sincero ringraziamento. Con il loro lavoro quotidiano, silenzioso e qualificato, contribuiscono a garantire la protezione dei diritti, delle libertà e del sistema democratico.

In un tempo segnato da incertezze globali, la Polizia di Stato sente la responsabilità di costituire un presidio solido ed operativo a tutela del cittadino e delle Istituzioni.

Rivolgo, dunque, un plauso convinto a coloro che hanno contribuito alla realizzazione di questo Quaderno, auspicando che possa costituire non solo un utile strumento di approfondimento tecnico, ma anche un segno tangibile delle competenze che la Polizia di Stato offre quotidianamente, al servizio del Paese.

Vittorio Pisani



Premessa

Primo Dirigente Tecnico Andrea Carnimeo

Gentili relatori e stimati colleghi,

Questo Quaderno specialistico, frutto del lavoro congiunto di apprezzati professori e professionisti del settore, si propone di analizzare, in dettaglio, le tecniche di formazione e le competenze richieste per rispondere adeguatamente ai rischi legati alla cybersicurezza, con particolare riferimento alle esigenze specifiche dei nostri operatori che lavorano per la protezione delle infrastrutture critiche in Italia. Attraverso approfondimenti, *case studies* e *best practices*, ci siamo prefissi l'obiettivo di offrire un quadro completo e pratico per supportare la formazione di nuove generazioni di colleghi e costruire una difesa solida e preparata ad affrontare le minacce cibernetiche in continuo mutamento.

Tutto ciò nella consapevolezza che investire nella formazione specialistica degli operatori di sicurezza cibernetica non è più una scelta facoltativa, ma una necessità inderogabile per garantire la protezione dei sistemi critici e il buon funzionamento delle infrastrutture digitali che sostengono il sistema economico - sociale. Solo con professionisti altamente qualificati e preparati sarà possibile affrontare con successo le sfide di un mondo sempre più vulnerabile agli attacchi informatici e offrire una protezione adeguata ai beni essenziali della nostra collettività. In questo senso, l'istituzione della nuova Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica si inserisce in un più generale contesto normativo, all'interno del quale viene quotidianamente posto l'accento sulla necessità di garantire adeguati livelli di formazione e continuo aggiornamento degli operatori specialisti della cybersicurezza per far fronte ad una minaccia sempre più strutturata e pervasiva. Nel panorama globale, invero sempre più interconnesso e digitalizzato, in questi anni in cui si assiste alla nascita della intelligenza artificiale, la sicurezza cibernetica rappresenta una delle sfide più rilevanti per le organizzazioni pubbliche e private. Attacchi informatici sempre più sofisticati minacciano la protezione delle infrastrutture critiche, dei dati sensibili e dei servizi essenziali che costituiscono il motore della nostra società moderna. La formazione specialistica non si limita alla conoscenza tecnica degli strumenti di difesa, ma implica anche una comprensione profonda delle dinamiche del cyberspazio, delle politiche di sicurezza e delle normative che regolano il settore.

Il motto della Polizia di Stato, “Esserci Sempre” significa per noi rappresentare anche in questo settore un punto di riferimento per il cittadino, per accrescere e migliorare la postura di sicurezza del sistema Italia.

La linea è tracciata. Come ogni inizio lo scoglio più duro è compiere il primo passo, la Polizia di Stato si sta dimostrando ancora una volta in grado di mutare dinamicamente la propria pelle, segno di maturità e solidità di una istituzione democratica che ha una grande passato e un altrettanto grande futuro.

Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica

Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica

Dirigente Generale Luigi Rinella
Direttore Centrale per la Polizia Scientifica e la Sicurezza Cibernetica

Gentilissimi relatori,

porgo i miei più sentiti apprezzamenti per la conclusione dell'iter formativo dei seminari on-line, che si sono svolti con l'intervento di docenti appartenenti al mondo accademico ed esponenti del settore privato, complimentandomi per l'ottima l'iniziativa e il prezioso contributo fornito, che ha riscosso enorme interesse e partecipazione da parte di tutto il personale della Polizia per la Sicurezza Cibernetica.

In questo particolare momento storico, in cui si susseguono continui eventi critici che generano un diffuso allarme sociale, è preciso dovere della Polizia salvaguardare il mondo della sicurezza informatica, mettendo a disposizione le proprie risorse e capacità tecniche.

Il contesto che si è delineato negli ultimi tempi impone la massima attenzione alla sfera Cyber, in funzione della tutela di tutta la collettività. Per tali ragioni, non posso che esprimere un particolare elogio al progetto di realizzazione di un "Quaderno di Polizia Cibernetica" della nuova Direzione Centrale per la Polizia Scientifica e Sicurezza Cibernetica che - raccogliendo in sintesi gli incontri didattici - racchiude in sé un enorme valore tecnico e di divulgazione scientifica nel settore.

La Direzione Centrale che guido si compone di un Servizio Affari Generali, del Servizio per la Polizia Scientifica, del Servizio Polizia Postale e per la Sicurezza Cibernetica e del Servizio per la Sicurezza Cibernetica del Ministero dell'Interno, che - pur nei differenti settori di intervento - agendo tra loro in modo coordinato con autorevolezza, solidità e professionalità, costituiscono, anche sotto il profilo tecnico, il settore di avanguardia della Polizia di Stato.

Sono certo che la vostra professionalità, l'impegno e la dedizione, uniti ad un non comune spirito di servizio, saranno ricompensati da un importante risultato, che verrà tramandato in futuro anche grazie alla diffusione didattica ad opera dell'Ispettorato delle Scuole della Polizia di Stato, che saprà farne tesoro, fornendo un enorme contributo specialistico alla formazione dei colleghi.

Con l'auspicio che possiate sempre continuare a distinguervi, rinnovo le mie più vive congratulazioni per l'iniziativa.

Dirigente Superiore Ivano Gabrielli
Direttore del Servizio Polizia Postale e della Sicurezza Cibernetica

Gentilissimi relatori,

condividendo le parole espresse dal Direttore Centrale, ci tengo ad esprimere il più vivo apprezzamento per questa importante attività formativa, che si inserisce nel più ampio contesto delle iniziative didattiche programmate annualmente per la crescita professionale dei nostri operatori.

È stato un momento di arricchimento professionale che ha permesso alle articolazioni territoriali dipendenti dal Servizio Polizia Postale e per la Sicurezza Cibernetica di confrontarsi con le professionalità più avanzate del settore privato e pubblico, per proseguire nel cammino di progresso che oggi vede questa struttura, nella sua globalità, quale principale e più importante agenzia di *law enforcement* all'interno dell'architettura di sicurezza nazionale.

Il rinnovato assetto determinatosi dopo la nascita della Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica ha imposto un ripensamento, già ideato da tempo, della articolazione interna della stessa struttura, che in qualità di Organo Centrale del Ministero dell'Interno garantisce la sicurezza e la regolarità dei servizi di comunicazione.

Al riguardo, il Servizio Polizia Postale si compone di nr. 5 Divisioni e di nr. 3 Centri a competenza nazionale (il Commissariato di P.S. Online, il Cnaipic e il Cncpo), nonché a livello territoriale di nr. 18 Centri Operativi per la Sicurezza Cibernetica e di nr. 82 Sezioni Operative, di cui n. 9 a competenza distrettuale.

È innegabile la presenza di una minaccia cibernetica sempre più ramificata e persistente, perpetrata da organizzazioni criminali più strutturate in grado di sferrare attacchi informatici che si rivelano al contempo dirompenti in danno delle infrastrutture critiche del nostro Paese quanto silenti, nascondendosi all'interno dei sistemi bersaglio, per carpire i dati essenziali alla costruzione di una rete informativa estesa che permette agli attori ostili di insinuarsi all'interno dei sistemi e controllare le sfere più importanti della realtà socio-economica.

Elogio l'impegno mostrato per illustrare e far comprendere le più attuali tecniche e tattiche utilizzate per gli attacchi informatici, la cui approfondita conoscenza diventa l'elemento fondante di una difesa strutturata, efficace in grado di aumentare la postura di sicurezza e anticipare l'evento dannoso o mitigarne per tempo gli effetti una volta verificatesi nella realtà.

La consapevolezza in una materia così tecnica eleva il personale specialista per divenire un interlocutore qualificato degli altri attori istituzionali che si affacciano sulla scena del mondo cyber a cui negli ambiti di competenza vengono riconosciuti sempre maggiori sfere di intervento e azione, connesse ad importanti attribuzioni legislative. La dislocazione dei nostri Uffici, insieme alla funzione di coordinamento e di azione diretta svolta dal Servizio e dai 3 Centri specialistici in esso presenti, permette quella vicinanza al cittadino e alle strutture essenziali presenti sul territorio per rispondere in maniera tempestiva al verificarsi di un evento dannoso.

In questo contesto, il continuo aggiornamento delle procedure di azione permette di tenere il passo all'evolversi della minaccia cibernetica e di sopperire con professionalità alle limitazioni imposte dalla natura stessa dell'azione malevola (combattendo contro il fattore temporale e perseguendo la necessità di conservare le tracce informatiche).

Allo stesso tempo, la diffusione di una cultura sulla sicurezza cibernetica permette di far luce sull'esistenza non solo di falle tecniche di sistema (siano esse conosciute o meno dai programmatori stessi) ma soprattutto di aumentare la consapevolezza sui comportamenti umani, che costituiscono sempre più spesso la porta di ingresso dei criminali all'interno dei sistemi.

La costituzione di una rete di salvaguardia tra gli operatori specialistici mediante una sinergia e l'acquisizione di un comune bagaglio professionale costituisce la più forte contromisura ed il più sicuro governo degli eventi malevoli, strumento necessario per arginare la velocità, la diffusione e la potenza di un attacco informatico, nonché per garantire la sicurezza delle risorse online, essenziali per l'ordinato svolgersi della vita odierna.

Dirigente Superiore Tecnico Gianpaolo Zambonini
Direttore del Servizio per la Sicurezza Cibernetica del Ministero dell'Interno

Carissimi relatori,

unendomi alle parole del Sig. Direttore Centrale, ci tengo ad esprimere i miei più sinceri ringraziamenti per l'importante iniziativa svolta.

Dal momento in cui ho assunto la direzione dell'Ufficio condivido con i funzionari assegnati lo sviluppo e il coordinamento della struttura, "Servizio per la Sicurezza Cibernetica del Ministero dell'Interno", che rappresenta un importante snodo strategico della costituita "Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica". L'Ufficio garantisce la sicurezza delle reti, dei sistemi informativi e delle infrastrutture informatiche in uso al Ministero dell'Interno, avvalendosi di due importanti centri: il Computer Emergency Response Team (di seguito C.E.R.T.) e il Centro di Valutazione (di seguito C.V.).

Il C.E.R.T., ai sensi della normativa vigente, svolge attività di prevenzione e gestione degli incidenti informatici, assumendone il governo, occorsi ai danni delle reti e dei sistemi informativi del Dicastero. Invece, il C.V. valuta l'idoneità dei prodotti e servizi di Information and Communication Technology (ICT), destinati ad essere impiegati sulle reti e sui sistemi informativi del Ministero dell'Interno, ed inseriti nel perimetro di sicurezza nazionale cibernetica, il quale è stato istituito dall'art. 1 del D.L. n. 105/2019.

I recenti fatti di cronaca in materia di attacchi informatici ed esfiltrazione dati hanno richiamato ancor di più l'attenzione della collettività sulla sicurezza cibernetica, che oggi assume carattere prioritario all'interno delle agende politiche, ove si percepisce nitidamente la necessità e l'urgenza di porre un argine alla criminalità informatica. Conoscere e comprendere una materia di carattere così tecnico e specifico, come questa, diviene il compito che siamo chiamati istituzionalmente ad assolvere, nonché la fondamentale leva per poter trovare soluzioni idonee a rassicurare i cittadini con la nostra presenza e vicinanza a tutela della sicurezza pubblica. Al riguardo è innegabile il pregio di questo lavoro, e i relatori con la loro intuitiva lungimiranza hanno centrato l'obiettivo, rendendo concetti difficili facilmente comprensibili. Avvertiamo la necessità di condividere questo sapere anche con i giovani colleghi, affinché possano approcciarsi alle tematiche, sicuramente affascinanti, con consapevolezza ed una preparazione di base, per operare facilmente nel settore.

Ai docenti del mondo accademico e delle aziende private intervenuti rinnovo la mia disponibilità ad una piena collaborazione, che permette di individuare e condividere, anche in tempo reale, preziose e strategiche informazioni utili alla prevenzione degli attacchi informatici, sia di matrice criminale, comune che terroristica, ai danni dei sistemi critici e sensibili del nostro Paese.

Mi auguro che questo strumento consentirà una sempre maggiore consapevolezza sul tema, per dare il giusto valore alle procedure di sicurezza ed assumere un atteggiamento strategicamente proattivo, che si traduce in un'operatività concreta ed efficiente nel rilevare e prevenire gli attacchi informatici.

Infine, desidero esprimere un sincero ringraziamento a ciascuno dei miei collaboratori per il loro contributo, tanto sul piano tecnico quanto su quello organizzativo, che ha avuto un ruolo fondamentale nel successo dell'evento.

Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica

Dirigente Superiore Fabiola Mancone
Direttore del Servizio di Polizia Scientifica

Gentili relatori,

il Servizio Polizia Scientifica, incardinato nella Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica, rappresenta un punto di riferimento per gli accertamenti forensi in ambito biologico, chimico, fisico e dattiloscopico nonché nell'applicazione delle tecnologie più avanzate all'analisi delle tracce digitali, affrontando, con competenza e rigore, le sfide poste da un settore sempre più complesso e in continua evoluzione.

Negli ultimi anni, sono stati compiuti significativi investimenti nello sviluppo e nell'applicazione delle metodologie di Intelligenza Artificiale (IA). L'avvento di tali tecnologie, infatti, ha portato alla creazione di nuovi e complessi strumenti di sofisticazione criminale, come i deepfake: contenuti audio, immagini e video generati artificialmente in grado di replicare la realtà con una fedeltà tale da risultare praticamente indistinguibili da quelli autentici, rappresentando una minaccia significativa per l'affidabilità delle prove digitali. La Polizia Scientifica è all'avanguardia nel contrastare tali minacce, sviluppando applicativi e metodologie innovative in grado di rilevare contenuti manipolati, garantendo così la sicurezza e l'integrità delle evidenze forensi.

Già partire dal 2018, infatti, il Servizio Polizia Scientifica ha progettato e implementato il sistema nazionale di riconoscimento facciale noto come SARI (Sistema Automatico di Riconoscimento delle Immagini), uno strumento investigativo basato su algoritmi di intelligenza artificiale e tecniche di apprendimento profondo (deep learning) che permette di effettuare ricerche di volti sconosciuti all'interno della banca dati AFIS, che contiene oltre 19 milioni di immagini di soggetti fotosegnalati dalle FF.OO, raccolte in conformità alla normativa vigente.

Recentemente, inoltre, è stato sviluppato e reso operativo il portale AIM4SIE (Artificial Intelligence Methods for Smart Investigation of Evidences), una piattaforma integrata che offre accesso a diversi strumenti di IA appositamente progettati per supportare le attività investigative, come il miglioramento delle immagini, l'elaborazione di identikit, la simulazione dell'invecchiamento dei volti (c.d. age progression), l'elaborazione dell'audio e l'impiego di modelli linguistici basati su IA di ultima generazione (c.d. Large Language Models - LLM).

Questi strumenti, combinati con l'expertise e la professionalità degli operatori, rafforzano significativamente le capacità tecniche e operative della Polizia Scientifica, consentendole di affrontare con efficacia le sfide poste dalle indagini moderne e di cogliere le opportunità offerte dalle tecnologie emergenti.

Diventa, pertanto, essenziale riuscire a trasferire questo patrimonio di conoscenze ai giovani colleghi, preparandoli ad affrontare, con consapevolezza, un settore tanto complesso quanto stimolante: ed è proprio questo il grande valore di questo lavoro.

Desidero, infine, esprimere un particolare ringraziamento ai collaboratori del Servizio per il contributo a questo Quaderno.

Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica

Dirigente Superiore Tiziana Liguori
Direttore del Servizio Affari Generali della Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica

Gentili relatori

nel corso di questi ultimi anni la tecnologia è diventata parte integrante del nostro vivere quotidiano. L'evoluzione della rete e la facilità della connessione rappresentano sicuramente punti di forza per il miglioramento delle attività umane. L'utilizzo del web è un diritto fondamentale che deve essere garantito a tutti e in sicurezza.

Le risorse informatiche sono indispensabili anche per gli Stati, essendo ormai dimostrato come la competitività di un Paese sia fortemente condizionata dal livello di digitalizzazione raggiunto dalla sua Pubblica Amministrazione. Le tecnologie digitali, infatti, costituiscono oggi un potente motore di innovazione e gli stessi progressi della ricerca sarebbero impensabili senza un uso intensivo delle risorse informatiche.

È, pertanto, evidente come nello scenario attuale, la garanzia dei diritti e delle libertà non possa prescindere da un'adeguata capacità degli Stati di contrastare le minacce cibernetiche, in costante espansione ed evoluzione.

Nella criticità del quadro sopra delineato, l'iniziativa in argomento e l'encomiabile sforzo profuso dai relatori per rendere fruibile a tutti gli operatori del settore una tematica così complessa, assumono una rilevanza strategica.

È, infatti, un obiettivo imprescindibile consolidare la professionalità del personale della Polizia di Stato dedicato al contrasto del cybercrime attraverso una formazione specialistica e qualificata, ed è in tale tracciato che si muove il pregevole progetto del Quaderno di Polizia Cibernetica, tenuto conto anche dell'elevata capacità delle organizzazioni criminali di utilizzare le tecniche sempre più sofisticate e all'avanguardia per perseguire le loro finalità.

Indice

Indice

Indice

Architettura Nazionale di Sicurezza Cibernetica

Autore: Federico Barone

Normativa PSNC

Il mondo digitale è ormai **centrale** nella vita quotidiana e nella politica internazionale, ma rappresenta anche uno spazio dove proliferano **attività illecite**, spesso condotte da organizzazioni criminali transnazionali, incluse le **mafie**, che sfruttano la rete per enormi profitti illeciti.

L'Italia, in modo pionieristico, ha creato un sistema normativo e organizzativo per affrontare le minacce informatiche, basato su **un'Architettura Nazionale della Sicurezza Cibernetica**, che coinvolge vari attori istituzionali in sinergia. Tale architettura affronta la cybersecurity sotto quattro **dimensioni principali**.

01. CYBER DEFENSE

Ministero della Difesa

Risponde ad attacchi militari esterni condotti da **attori statuali** (State-Sponsored Attackers) contro l'integrità nazionale.

02. CYBER INTELLIGENCE

Dipartimento delle Informazioni per la Sicurezza (DIS)

Previene **minacce** alla sicurezza nazionale e **contrasta** il **cyber-espionage.**

01. CYBER RESILIENCE

Agenzia per la Cybersicurezza Nazionale (ACN)

Garantisce la sicurezza dei sistemi informatici **strategici**, prevenendo la **paralisi** di servizi **essenziali**.

01. CYBER CRIME

Polizia Postale

Previene e **reprime** i reati informatici, in coordinamento con altre forze di **law enforcement** europee e nazionali.

L'obiettivo del sistema italiano è reagire prontamente alla **mutevolezza** delle minacce informatiche, garantendo la **sicurezza** e la **continuità operativa** dei sistemi essenziali.

L'**Architettura Nazionale di Sicurezza Cibernetica** è il risultato di un lungo percorso normativo iniziato con l'istituzione del **Servizio Polizia Postale** nel 1998, per il contrasto del crimine informatico. Il sistema ha evoluto gradualmente con leggi e decreti, inclusa la **Legge sull'Intelligence** del 2007, che ha istituito il **Sistema di Informazione per la Sicurezza della Repubblica**, e ha affidato la responsabilità della sicurezza cibernetica al Presidente del Consiglio.

Alcune **tappe principali** di questo percorso includono:

DPCM 2013 (Decreto Monti)

definisce l'architettura istituzionale per la protezione delle infrastrutture critiche e istituisce il **Nucleo per la Sicurezza Cibernetica (NSC)**.

DPCM 2017 (Decreto Gentiloni)

rivede la struttura, assegnando la presidenza dell'NSC al **Dipartimento delle Informazioni per la Sicurezza (DIS)** e riconoscendo un ruolo importante al **CNAIPIC** (organo di contrasto al crimine informatico).

Decreto Legislativo 65/2018

recepisce la **Direttiva NIS europea**, introducendo misure per migliorare la cooperazione tra Stati membri e la sicurezza delle reti cibernetiche, e confermando il ruolo del CNAIPIC.

Decreto Legge 105/2019

istituisce il **Perimetro di Sicurezza Nazionale Cibernetica** per proteggere le infrastrutture e i servizi essenziali per lo Stato, con un regolamento attuativo (**DPCM 2020**) che definisce le modalità per l'inclusione dei soggetti da proteggere.

L'architettura nazionale si è sviluppata per garantire una risposta **efficace** alle minacce **cibernetiche**, coinvolgendo vari attori **istituzionali** e puntando a rafforzare la **protezione** delle infrastrutture **critiche** nazionali.

Il Perimetro di Sicurezza Nazionale Cibernetica (PSNC)

Il Perimetro di Sicurezza Nazionale Cibernetica, istituito dal **Decreto-legge n. 105/2019**, identifica soggetti pubblici e privati rilevanti per la sicurezza nazionale in **settori strategici** come governo, difesa, energia, telecomunicazioni, trasporti, servizi digitali, ed economia. I soggetti inclusi devono predisporre elenchi annuali dei **beni ICT essenziali**, documentarne la sicurezza e adottare misure tecniche e organizzative per prevenire e gestire incidenti cibernetici.

Il **DPCM 2021** definisce le **tipologie di incidente** e le modalità di **notifica**:

- Entro **6 ore** per incidenti considerati **meno gravi**.
- Entro **1 ora** per **incidenti gravi**.

Le notifiche e la gestione dei beni ICT sono supervisionate dal **CSIRT Italia** e dall'**ACN**, istituita nel 2021 per coordinare la **sicurezza cibernetica nazionale**. L'ACN garantisce **innovazione** tecnologica per la Pubblica Amministrazione.

Per la verifica delle forniture ICT intervengono il **CVCN** e i laboratori di accreditamento, che analizzano la sicurezza. La normativa centralizza il **coordinamento** e **rafforza** la **resilienza** cibernetica.

L'Agenzia per la Cybersicurezza Nazionale (ACN) svolge funzioni chiave per la sicurezza cibernetica italiana, tra cui: **tutela degli interessi nazionali**, **prevenzione e mitigazione** degli attacchi informatici, gestione del **CSIRT Italia** e del **CVCN**, e **promozione di competenze industriali e tecnologiche per l'autonomia strategica**. L'ACN è l'**interlocutore unico** per la sicurezza di **reti**, **sistemi** e **comunicazioni** e collabora con il Centro Europeo di competenza per la cybersicurezza.

La Direttiva **NIS2**, attuata nel 2024, amplia i soggetti coinvolti includendo anche le **PMI critiche** e introduce un quadro normativo più strutturato per la notifica degli incidenti significativi. Le notifiche devono seguire tempi precisi: una prenotifica **entro 24 ore** e una notifica completa **entro 72 ore**, con relazioni intermedie e finali su richiesta. Queste misure mirano a rafforzare la **resilienza** cibernetica nazionale.

La normativa in materia di cybersicurezza vede una crescente integrazione e sovrapposizione tra la Direttiva **NIS**, orientata alla tutela del **mercato comune europeo**, e il **Perimetro nazionale di sicurezza cibernetica**, che protegge la sicurezza **nazionale** e le funzioni **essenziali** dello Stato. Questa contiguità crea sfide nella co-applicabilità delle norme e nel coordinamento tra gli enti coinvolti. La Direttiva **NIS2** introduce obblighi dettagliati per la **gestione della cybersicurezza**, tra cui procedure rigorose per la segnalazione degli incidenti, che devono rispettare tempistiche stringenti e includere dettagli su minacce, misure adottate e potenziali implicazioni penali.

Il **Decreto del 7 febbraio 2024** istituisce la **Direzione Centrale** per la **Polizia Scientifica** e la **Sicurezza Cibernetica,** con il Servizio per la **Sicurezza Cibernetica** del **Ministero dell'Interno**. Questo Servizio coordina il **CERT**, che gestisce il **monitoraggio** e la risposta agli incidenti informatici, e il **Centro di Valutazione**, che si occupa della **certificazione** e **ispezione** di sistemi ICT critici. Entrambi operano per rafforzare la **resilienza** e la **sicurezza** delle reti e delle infrastrutture del **Ministero dell'Interno**, attraverso **analisi delle vulnerabilità**, **piani di rischio**, **direttive tecniche** e **formazione del personale**.

Autore

Federico Barone

Attualmente ricopre il ruolo di Funzionario Tecnico presso il Servizio per la Sicurezza Cibernetica del Ministero dell'Interno, con il ruolo di responsabile della Sezione Monitoraggio & Analisi Cyber e della Sezione Cybersecurity Governance & Operation Technology, dove sovrintende, le attività di prevenzione, monitoraggio e gestione degli incidenti di sicurezza cibernetica del Ministero dell'Interno, ovvero le attività di verifica, valutazione e certificazione dei sistemi ICT critici.

Cyber Threat Intelligence e Supply Chain

Autori: Dario Amoruso e Stefano Dibisceglia

L'evoluzione delle minacce nella supply chain

Introduzione

Negli ultimi anni, la crescente complessità delle **supply chain globali** ha messo in evidenza quanto un **punto debole** nella catena possa mettere a rischio intere organizzazioni. Un fornitore o un partner terzo con misure di sicurezza **inadeguate** rappresenta una **porta** d'ingresso per i cybercriminali, che sfruttano le **vulnerabilità** per accedere ai sistemi critici di aziende ben più grandi.

Recenti attacchi informatici hanno evidenziato le **gravi vulnerabilità** nella sicurezza delle supply chain digitali. Tra i casi emblematici, il data breach del Ministero della Difesa britannico (MOD) nel maggio 2024 ha esposto i dati di 270.000 membri del personale, attraverso una falla in un appaltatore responsabile dei pagamenti, sollevando dubbi sulla sicurezza delle infrastrutture critiche e possibili legami con il cyber-spionaggio statale, forse cinese.

Ad aprile 2024, un attacco al fornitore **Sisense** ha **compromesso** il repository **GitLab**, esponendo credenziali sensibili per servizi Amazon S3 e minacciando i clienti che utilizzano le sue soluzioni di business intelligence. Questi eventi dimostrano come falle nella filiera possano causare **effetti domino**, con gravi conseguenze **operative**, **finanziarie**, **reputazionali** e **normative**. La sicurezza delle supply chain è ora una **priorità** assoluta per aziende e governi.

La nascita della Cyber Threat Intelligence: dalle origini alla maturità

La Cyber Threat Intelligence (**CTI**), o intelligence sulle **minacce informatiche**, è il risultato di decenni di evoluzione nel campo della sicurezza informatica. Le sue radici affondano negli anni '90, quando le aziende iniziarono a capire che non bastava più reagire agli attacchi informatici, ma era necessario anticiparli. In quegli anni, le **minacce** erano relativamente semplici: **virus informatici** creati per scopi spesso amatoriali o vandalici, che raramente avevano impatti significativi sulle operazioni aziendali. Con l'avvento del nuovo millennio, però, gli attacchi iniziarono a diventare sempre più **mirati** e sofisticati. Gruppi di hacker sponsorizzati **da** stati o organizzazioni criminali iniziarono a sfruttare vulnerabilità informatiche per scopi economici, politici o strategici. Gli attacchi non erano più limitati ai singoli individui o alle grandi aziende tecnologiche; anche le supply chain, con la loro intrinseca complessità e interdipendenza, divennero un bersaglio primario.

È in questo contesto che la **CTI** si è sviluppata come **disciplina**. Inizialmente utilizzata principalmente da governi e grandi aziende tecnologiche, la CTI si basa sulla raccolta, l'**analisi e la condivisione di informazioni** relative alle minacce informatiche. L'obiettivo è quello di fornire un quadro chiaro e aggiornato dei rischi,

permettendo alle organizzazioni di prendere decisioni informate e proattive.

La CTI si distingue per la sua **natura dinamica**: non si limita ad identificare minacce già conosciute, ma cerca di prevedere quelle future attraverso l'analisi di tendenze, comportamenti e tecniche utilizzate dai **cybercriminali**. Questo approccio è particolarmente rilevante per le supply chain, dove un singolo punto di debolezza può avere conseguenze catastrofiche.

IL RUOLO DELLA CTI NELLA PROTEZIONE DELLE SUPPLY CHAIN

Le supply chain moderne rappresentano un intricato sistema di interdipendenze globali. La crescente digitalizzazione ha portato enormi benefici in termini di efficienza e scalabilità, ma ha anche aperto nuove vulnerabilità che possono essere sfruttate da attaccanti informatici. In questo contesto, la **Cyber Threat Intelligence (CTI)** si è rivelata uno strumento strategico per identificare, prevenire e mitigare i rischi in modo proattivo, proteggendo non solo i singoli anelli della catena di approvvigionamento, ma anche l'intera rete di relazioni commerciali.

Un approccio proattivo basato sui dati

La CTI si basa su un approccio proattivo che raccoglie, analizza e distribuisce informazioni utili sui rischi e sulle minacce emergenti.

A differenza degli approcci tradizionali alla sicurezza informatica, che tendono a concentrarsi sulla risposta agli attacchi già in corso, la CTI permette alle aziende di **anticipare potenziali minacce prima che queste si concretizzino**. Questo è particolarmente importante nelle supply chain, dove un attacco ad un piccolo fornitore può avere ripercussioni devastanti su scala globale.

Un esempio concreto è rappresentato dall'attacco subito nel **2020 da SolarWinds**. Gli **hacker** hanno compromesso un aggiornamento del software di gestione utilizzato da migliaia di aziende e governi. Questo attacco ha dimostrato come una vulnerabilità in un singolo fornitore possa propagarsi rapidamente in tutta la supply chain. Se le aziende coinvolte avessero adottato strumenti di **CTI** per monitorare i **comportamenti anomali** del software e delle reti, avrebbero potuto individuare e contenere l'attacco in tempi molto più rapidi.

Monitoraggio continuo dei partner e dei fornitori

Uno degli **aspetti chiave della CTI** è il monitoraggio costante delle terze parti e di tutte le entità coinvolte nella supply chain. Questo tipo di analisi consente di valutare in tempo reale il livello di rischio associato a ciascun attore della catena. Ad esempio, la CTI può identificare fornitori che non rispettano gli standard minimi di sicurezza informatica o che presentano vulnerabilità note nei loro sistemi.

Grazie a queste informazioni, le aziende possono **prendere decisioni basate sui dati**, come sospendere temporaneamente le transazioni con un fornitore compromesso, richiedere audit di sicurezza o implementare misure compensative per **ridurre il rischio.**

Un esempio pratico è l'utilizzo di strumenti CTI per **verificare le credenziali** pubbliche dei fornitori su piattaforme del dark web, un'attività che può rivelare dati esposti a seguito di un attacco informatico.

Analisi predittiva e prevenzione delle minacce

L'aspetto predittivo della CTI rappresenta un elemento di svolta nella protezione delle supply chain. Utilizzando tecniche avanzate come il machine learning e l'intelligenza artificiale, i **sistemi di CTI sono in grado di analizzare grandi volumi di dati** per identificare schemi e anomalie che potrebbero indicare una minaccia in evoluzione. Ad esempio, un aumento del traffico di rete verso un determinato sistema può essere un segnale di un attacco imminente, come un **tentativo di esfiltrazione di dati** o di distribuzione di malware.

Questa capacità di **anticipare gli eventi** consente alle aziende di adottare misure preventive, come isolare i sistemi a rischio o rafforzare le difese in punti strategici della rete. Inoltre, l'analisi predittiva permette di identificare gli attori della minaccia e le loro modalità operative. Ad esempio, un attacco basato su tecniche di spear phishing può essere prevenuto analizzando i modelli di comunicazione degli attaccanti e implementando **filtri specifici**.

Gestione del rischio e classificazione delle minacce

La CTI è fondamentale per una gestione efficace del rischio nelle supply chain Attraverso un processo di analisi dettagliata delle **minacce**, le aziende possono classificare i rischi in base alla loro probabilità e al potenziale impatto.

Questa classificazione consente di allocare risorse in modo più efficiente, concentrandosi sulle vulnerabilità che rappresentano una maggiore minaccia per la continuità operativa.

Ad esempio, **se la CTI rileva che un determinato settore è oggetto di attacchi mirati da parte di gruppi di cybercriminali**, le aziende appartenenti a quel settore possono rafforzare le proprie difese e adottare strategie di mitigazione mirate. Nel settore manifatturiero, un attacco a un fornitore di componenti critici può avere effetti a cascata su tutta la supply chain. La CTI permette di valutare questi scenari e di implementare soluzioni proattive per ridurre il rischio.

Condivisione delle informazioni

La condivisione delle informazioni è un altro elemento cruciale della CTI. Le aziende non operano in isolamento, ma fanno parte di un ecosistema **interconnesso**.

Attraverso la condivisione di informazioni sulle minacce con **fornitori**, **partner** e **clienti**, le organizzazioni possono migliorare la sicurezza complessiva della supply chain. Ad esempio, piattaforme come **ISAC (Information Sharing and Analysis Centers)** o **TLP (Traffic Light Protocol)** facilitano la diffusione di informazioni sensibili sulle minacce in modo sicuro.

Queste piattaforme consentono alle aziende di condividere dettagli sugli attacchi subiti, sui metodi utilizzati dagli hacker e sulle soluzioni adottate per **mitigare i rischi**. Un caso concreto è rappresentato dal settore finanziario, dove l'uso di reti di condivisione delle informazioni ha permesso di ridurre significativamente l'impatto degli attacchi informatici.

Automazione e rilevazione in tempo reale

La tecnologia gioca un ruolo centrale nella CTI. Strumenti avanzati di automazione consentono di rilevare e rispondere alle **minacce in tempo reale**. Ad esempio, **sistemi di monitoraggio basati sull'intelligenza artificiale** possono identificare comportamenti anomali nei **flussi di dati**, segnalando tentativi di compromissione o attività sospette. Questi strumenti sono particolarmente **utili** per le **supply chain globali**, dove la complessità delle interazioni rende difficile individuare manualmente i segnali di un attacco.

Un esempio pratico è l'utilizzo di strumenti di CTI per monitorare le reti di comunicazione tra fornitori.

Se un sistema rileva un traffico insolito verso un server esterno non autorizzato, può automaticamente bloccare la connessione e inviare un avviso al team di sicurezza. Questo approccio non solo migliora la **velocità di risposta**, ma riduce anche il rischio di errore umano.

INCIDENT RESPONSE E RIDUZIONE DEI TEMPI DI RECUPERO

Oltre alla prevenzione, la CTI gioca un ruolo **fondamentale** nella **gestione degli incidenti** informatici. In caso di compromissione, le informazioni fornite dalla CTI possono essere utilizzate per identificare rapidamente la **causa dell'attacco**, isolare i sistemi compromessi e ripristinare le operazioni.

Ad esempio, un'azienda che utilizza la CTI può ricevere in tempo reale informazioni su un attacco in corso, comprese le indicazioni sulle **modalità di mitigazione più efficaci**. Nel caso di un ransomware, ad esempio, la CTI può fornire dettagli su come bloccare la diffusione del malware e recuperare i dati senza pagare il riscatto.

RIFERIMENTI NORMATIVI E INCENTIVI ALLA CTI

Negli ultimi anni, gli attacchi informatici alla **supply chain** sono diventati sempre più frequenti e sofisticati, dimostrando quanto una vulnerabilità in un fornitore possa avere conseguenze devastanti per un'azienda. Compromettere un partner esterno consente ai criminali informatici di infiltrarsi nei sistemi di più organizzazioni contemporaneamente, sfruttando connessioni fidate e aggirando le difese di sicurezza tradizionali. Per rispondere a queste minacce crescenti, l'Unione Europea ha introdotto la Direttiva **NIS2**, con l'obiettivo di rafforzare la resilienza digitale delle infrastrutture critiche e delle imprese strategiche, ponendo particolare attenzione proprio ai rischi connessi alla catena di approvvigionamento. La supply chain è diventata un **obiettivo privilegiato** per gli attaccanti perché rappresenta un punto di accesso indiretto a molte aziende. Ogni organizzazione si affida a fornitori esterni per servizi essenziali, come cloud computing, software di gestione o infrastrutture di rete. Se uno di questi fornitori viene compromesso, l'effetto può propagarsi rapidamente, generando danni a cascata lungo tutta la catena.

La **NIS2** impone quindi alle aziende non solo di proteggere i propri sistemi, ma anche di adottare misure concrete per valutare e mitigare i rischi legati ai loro fornitori, richiedendo maggiore attenzione e responsabilità nella gestione della sicurezza informatica. In questo contesto, la **Cyber Threat Intelligence** assume un ruolo cruciale. Grazie alla capacità di raccogliere, analizzare e condividere informazioni sulle minacce emergenti, la CTI consente alle aziende di monitorare la sicurezza della propria supply chain in modo proattivo. Attraverso l'intelligence delle minacce, è possibile **individuare** segnali di compromissione prima che un attacco possa avere conseguenze dirette, **valutare** il livello di esposizione dei fornitori ed **intervenire** tempestivamente per ridurre i rischi. Inoltre, la CTI aiuta le aziende a rispondere rapidamente agli incidenti informatici, garantendo una gestione più efficace delle emergenze e una maggiore conformità ai requisiti imposti dalla NIS2. La nuova direttiva europea ha reso evidente che la sicurezza non può più essere confinata ai perimetri aziendali tradizionali. Proteggere i propri sistemi non è più sufficiente, è necessario estendere la difesa lungo tutta la catena di fornitura, adottando strumenti avanzati per anticipare e contrastare le minacce. La Cyber Threat Intelligence rappresenta la chiave per affrontare questa sfida, permettendo alle aziende di migliorare la propria **resilienza**, ridurre i rischi operativi e garantire la continuità del business in un contesto sempre più interconnesso e vulnerabile.

Il futuro della sicurezza delle supply chain dipende dalla capacità di adattarsi rapidamente alle nuove sfide. La CTI, con il supporto di normative e tecnologie sempre più avanzate, sarà il fulcro di questa trasformazione.

Autori

Dario Amoruso

Associate Partner di KPMG Advisory S.p.A. – Cyber and Tech Risk

Stefano Dibisceglia

Service Manager di KPMG Open Platform S.r.l. – Cyber and Tech Risk

Il valore della Cyber Threat Intelligence per la Sicurezza Nazionale

Autore: Mattia Siciliano

01. La natura della Cyber Threat Intelligence

La Cyber **Threat Intelligence (CTI)** è un ambito sempre più critico nel panorama della sicurezza informatica. Si focalizza sulla prevenzione e mitigazione di minacce mediante la raccolta, analisi e contestualizzazione di dati provenienti da fonti differenti. A causa dell'aumento delle cyber-minacce, la CTI è diventata essenziale per la sicurezza nazionale e per la protezione delle infrastrutture critiche. La CTI si basa su una combinazione di dati empirici e modelli predittivi che permettono di anticipare e comprendere le minacceLa CTI si articola in vari livelli di intelligence, coprendo campi chiave come i **Threat Feeds**, che forniscono informazioni basilari su malware, sistemi di comando e controllo (C&C), e altre minacce che minano la sicurezza nazionale e aziendale.
Alcuni esempi pratici dell'utilizzo di feed di intelligence includono:

- **Feed di Malware e Dispositivi Mobile**: Monitorano e analizzano il traffico di malware per dispositivi mobili, identificando indirizzi IP compromessi, valori hash di malware, e altre metriche utili per mitigare attacchi su larga scala.
- **Brand Reputation**: Monitorano l'uso improprio di marchi e identità aziendali sui social network e sul dark web per prevenire rischi reputazionali.
- **Analisi Antifrode e Anti-Riciclaggio (AML)**: Questi feed permettono di tracciare URL di phishing, account compromessi, e transazioni sospette, rendendo più efficaci le misure di protezione per il settore bancario e finanziario.

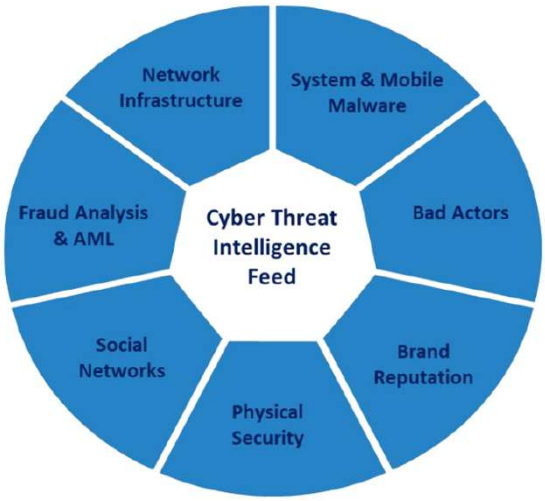


Figura 1 – Feed Maps

Grazie a tali feed, le organizzazioni possono raccogliere indicatori di compromissione (IoCs) e altre informazioni critiche che consentono di agire tempestivamente per prevenire e contrastare minacce emergenti.

02. Condivisione e Classificazione delle Informazioni

Un elemento chiave per la CTI è la **condivisione delle informazioni**, in quanto le minacce informatiche richiedono risposte coordinate e rapide. La classificazione dei dati, come nel caso del protocollo **TLP (Traffic Light Protocol)**, consente di categorizzare le informazioni in base al livello di sensibilità, assicurando che ogni partner riceva dati rilevanti senza compromettere la sicurezza.
Per esempio, dati classificati come 'TLP Red" ' sono condivisi solo con individui specifici, mentre 'TLP white ' permette una condivisione pubblica.

Classification of Information for sharing it is designed to improve the flow of information between individuals, organizations or communities in a controlled and trusted way. The ***Traffic Light Protocol*** (TLP) is based on the concept of the originator labeling information with one of four colors to indicate what further dissemination, if any, can be undertaken by the recipient. The recipient must consult the originator if wider dissemination is required.

TLP:RED = Not for disclosure, restricted to participants only. Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In most circumstances, TLP:RED should be exchanged verbally or in person.

TLP:AMBER = Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.

TLP:GREEN = Limited disclosure, restricted to the community. Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not released outside of the community.

TLP:WHITE = Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Figura 2 - TLP Mapping

La **Cyber Threat Intelligence Sharing** rappresenta un elemento d'innovazione significativa nel campo della cybersecurity, in quanto permette la condivisione rapida e sicura di informazioni tra diverse organizzazioni e istituzioni. In combinazione con i processi di CTI Sharing esistono le piattaforma di **Cyber Threat Intelligence (TIP)**. Questi sistemi rispondono alla crescente necessità di difendersi da minacce avanzate e coordinate, spesso troppo complesse per essere affrontate da una singola entità. Attraverso queste piattaforme, enti governativi, aziende private e fornitori di servizi critici possono scambiarsi dati su attacchi in corso, tecniche di attacco emergenti, e indicatori di compromissione (IoCs), come indirizzi IP sospetti, hash di malware e vulnerabilità specifiche.
L'elemento distintivo di queste piattaforme è la capacità di facilitare una **difesa collettiva** contro attacchi sofisticati, rendendo le informazioni disponibili in tempo reale e migliorando la capacità di risposta delle organizzazioni partecipanti. Per garantire che le informazioni condivise siano sfruttabili in modo efficace, le piattaforme di CTI utilizzano protocolli di classificazione come il Traffic Light Protocol (TLP), che distingue i dati in base a livelli di riservatezza (ad es., TLP per dati estremamente sensibili). Questo approccio permette alle organizzazioni di decidere con quali enti condividere le informazioni, migliorando la sicurezza complessiva delle operazioni senza compromettere dati sensibili.

Esempio: ICS/SCADA e Sicurezza Industriale

Nell'ambito della sicurezza industriale, le TIP sono particolarmente utili per proteggere infrastrutture critiche come i sistemi ICS (Industrial Control Systems) e SCADA. (Supervisory Control and Data Acquisition), utilizzati per il controllo di reti elettriche, impianti idrici, e stabilimenti industriali. Poiché i sistemi ICS/SCADA sono spesso obiettivi di attacchi cibernetici devastanti – come è avvenuto con il malware Stuxnet, che ha colpito le centrifughe nucleari iraniane – la condivisione di informazioni su vulnerabilità specifiche e tentativi di attacco rappresenta una linea di difesa essenziale.
Le TIP consentono inoltre agli operatori di ICS/SCADA di ottenere dati aggiornati su vulnerabilità software e hardware, dettagli di attacchi noti e tecniche utilizzate dagli aggressori. Ad esempio, se una centrale elettrica individua un tentativo di intrusione basato su una vulnerabilità di sistema, può informare altre infrastrutture critiche della rete condivisa, permettendo loro di implementare immediatamente le misure preventive. Questo scambio di informazioni contribuisce a ridurre i tempi di risposta agli attacchi e a limitare i danni potenziali, rendendo i sistemi industriali più resilienti.

Benefici e Sfide

Le TIP offrono numerosi benefici, tra cui una maggiore consapevolezza delle minacce, una migliore collaborazione tra settore pubblico e privato, e una più rapida capacità di risposta. Tuttavia, esistono anche delle sfide. Uno dei principali ostacoli è la **fiducia tra le parti**: le organizzazioni devono essere disposte a condividere informazioni critiche, comprese vulnerabilità proprie, senza timore di compromettere la propria reputazione o di violare regolamenti di privacy. Inoltre, la quantità e la qualità delle informazioni raccolte devono essere gestite con attenzione per evitare sovraccarichi informativi e garantire che solo i dati rilevanti siano utilizzati

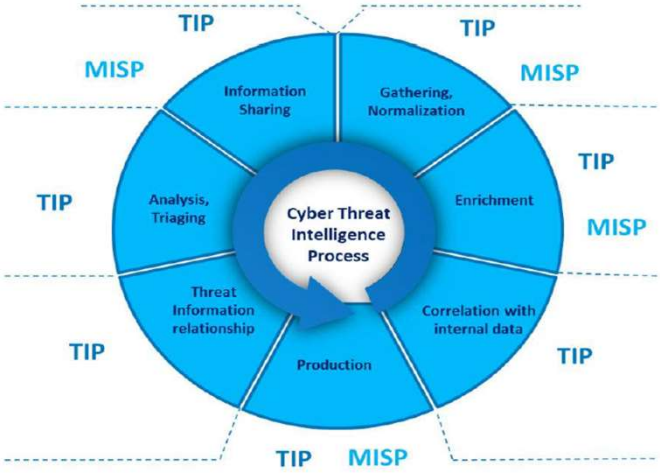


Figura 3 – TIP Process Mapping

In conclusione, le TIP svolgono un ruolo cruciale nella costruzione di una difesa cibernetica più robusta e collettiva, rendendo le infrastrutture critiche meno vulnerabili a minacce emergenti e aiutando le organizzazioni a operare in un ambiente sempre più sicuro e cooperativo.

03. Le minacce ibride e il ruolo della CTI

Le minacce ibride rappresentano una delle maggiori sfide nel panorama della sicurezza moderna, combinando elementi convenzionali e non, come attacchi cibernetici, guerra psicologica e spionaggio economico. Un esempio emblematico è la campagna di attacchi contro l'Ucraina da parte di gruppi come Fancy Bear e EMBER BEAR, che hanno condotto attacchi di tipo **phishing** per ottenere accesso a email sensibili e operazioni distruttive come il WhisperGate wiper malware. Questo tipo di minaccia, che utilizza metodi di sabotaggio informatico e disinformazione, richiede capacità avanzate di CTI per anticipare le mosse degli aggressori. Un esempio e' rappresentato nella figura 4.
Nell'ambito del conflitto in Ucraina, la CTI ha svolto un ruolo cruciale nel monitorare attività cibernetiche sospette e nell'identificare potenziali tattiche di guerra ibrida, fornendo dati preziosi per contrastare azioni di spionaggio o cyber-attacchi distruttivi. L'abilità di monitorare e analizzare in tempo reale le azioni degli attori di minacce ibride permette di prendere decisioni informate e prevenire gravi conseguenze sulle infrastrutture e sulla sicurezza pubblica.

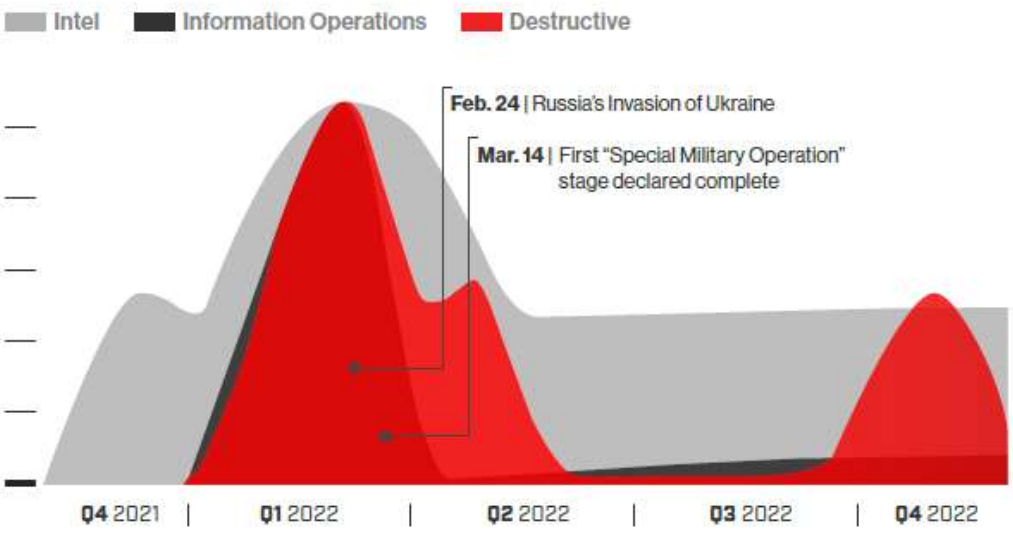


Figura 3 – Russian and Ukranian War Cyber Operation approach

04. L'impatto dell'Intelligenza Artificiale sulla CTI

L'Intelligenza Artificiale (IA) sta rivoluzionando la CTI sia in termini di difesa che di attacco. Strumenti come **FraudGPT** e **WormGPT** vengono utilizzati da gruppi criminali per condurre attacchi socialmente ingegnerizzati e campagne di phishing su vasta scala, superando le difese tradizionali. Questi strumenti, presenti su forum e canali di comunicazione underground, rendono la risposta delle difese cibernetiche particolarmente difficile poiché le IA criminali sono in grado di adattarsi e reagire rapidamente a nuovi schemi di difesa.
D'altro canto, l'IA supporta anche la CTI nelle operazioni di difesa, grazie alla sua capacità di processare grandi quantità di dati in tempo reale, individuando anomalie e schemi sospetti che potrebbero rappresentare minacce4. L'adozione di modelli di machine learning consente ai sistemi di sicurezza di identificare in modo proattivo potenziali attacchi, analizzando comportamenti non convenzionali nei flussi di dati aziendali. Questo supporto avanzato migliora la capacità di difesa, come evidenziato dai sistemi di intelligenza artificiale impiegati per proteggere le reti critiche e individuare tempestivamente tentativi di accesso non autorizzato.
Un ulteriore esempio è il crescente interesse nella manipolazione di modelli di linguaggio di grandi dimensioni (LLM), come ChatGPT, da parte di cybercriminali, che tentano di aggirare le restrizioni di sicurezza per usare questi strumenti a scopo dannoso, come nel caso di WolfGPT e DarkBARD.

05. Conclusioni

La Cyber Threat Intelligence rappresenta una componente essenziale per la protezione delle infrastrutture nazionali e globali. Essa permette di anticipare le minacce grazie alla raccolta e all'analisi di dati provenienti da fonti diversificate. La costante evoluzione delle tecniche di attacco, inclusa l'introduzione dell'IA nel campo criminale, pone nuove sfide alla difesa cibernetica, ma la CTI fornisce un vantaggio strategico, consentendo risposte più rapide e coordinate. L'integrazione di strategie di intelligence condivisa e il costante aggiornamento delle tecniche di difesa, combinate alle tecnologie di AI, contribuiscono a una maggiore sicurezza cibernetica globale, offrendo a governi e aziende la capacità di rispondere proattivamente alle minacce e di proteggere in modo efficace le infrastrutture critiche.

Autore

Mattia Siciliano

Mattia Siciliano è un leader dinamico nel campo della cybersecurity e delle soluzioni digitali, con oltre 15 anni di esperienza focalizzata sul miglioramento delle performance organizzative attraverso l'implementazione di soluzioni innovative e di alta qualità. Attualmente ricopre il ruolo di Co-Direttore del Corporate Cybersecurity HUB presso la Luiss Business School, dove guida iniziative strategiche per potenziare la sicurezza informatica nelle organizzazioni

La Cyber Intelligence nella Gestione degli Incidenti Informatici

Autore: Francesco Schifilliti

Le principali fasi che compongono il processo di Incident Response (IR) e le funzioni operative strettamente correlate a tali attività sono elementi essenziali per garantire l'efficacia nella gestione degli incidenti di sicurezza. Tra queste funzioni, la *cyber threat intelligence* svolge un ruolo sempre più centrale, fornendo informazioni strategiche che arricchiscono le fasi di Detection & Triage e di Analysis dell'IR, integrandosi con i dati provenienti dai sistemi di sicurezza perimetrale.

Il **NIST SP 800- 61** definisce un incidente informatico come « una violazione o una minaccia imminente di violazione delle politiche di sicurezza informatica, delle politiche di utilizzo accettabile o delle pratiche di sicurezza standard».
In base a questa definizione, possiamo considerare come incidente diverse tipologie di attacchi informatici, come ad esempio: l'invio, da parte di un attaccante tramite una **botnet**, di un elevato volume di richieste a un server con l'obiettivo di causarne un disservizio; l'inoltro di un'e-mail contenente un codice malevolo progettato per stabilire una connessione con un server esterno; oppure l'**esfiltrazione** di dati riservati di un'organizzazione accompagnata dalla minaccia di renderli pubblici in caso di mancato pagamento di un **riscatto**.
In particolare, possiamo vedere un progredire del concetto di evento fino a quello di attacco come segue:

- un ***cyber security event*** è una modifica alla sicurezza informatica che potrebbe avere un impatto sulle operazioni organizzative (inclusa la missione, le capacità o la reputazione);
- un ***cyber security incident*** è un evento che compromette effettivamente, o potenzialmente, la riservatezza, l'integrità o la disponibilità di un sistema informativo o delle informazioni che il sistema elabora, memorizza o trasmette, oppure che costituisce una violazione o una minaccia imminente di violazione delle politiche di sicurezza, delle procedure di sicurezza o delle politiche di utilizzo accettabile;
- un ***cyber attack*** è qualsiasi tipo di attività malevola che tenta di raccogliere, interrompere, negare, degradare o distruggere le risorse di un sistema informativo o le informazioni stesse.

Lo **scopo principale** del processo di Incident Response è di rimuovere efficacemente una minaccia dall'infrastruttura IT di una organizzazione, riducendo al minimo i danni e ripristinando le normali operazioni il più rapidamente possibile. Questo obiettivo primario si articola in diversi aspetti, tra cui: verificare che un incidente si sia effettivamente verificato o documentare che non si è verificato; mantenere o ripristinare la continuità aziendale riducendo l'impatto dell'incidente; identificare le cause dell'incidente; minimizzare l'impatto di eventuali incidenti futuri; migliorare la sicurezza e la pianificazione della risposta agli incidenti; e applicare le lezioni apprese per perfezionare il processo.

È evidente che l'indirizzamento di tutte le sotto-attività di un Incident Response presuppongono che si stabiliscano delle collaborazioni tra il gruppo incaricato della risoluzione dell'incidente con diverse altre parti quali, ad esempio, nuclei di polizia giudiziaria e agenzie governative, Internet Service Provider, software vendor, etc.

Figura 1: Principali Stakeholders in un Incident Response.

Nella Figura 2 è mostrato il processo di riferimento dell'IR presentato nello **Special Publication 800-61 del NIST** che abbraccia un classico approccio PICERL (Prepare, Identify, Contain, Eradicate, Recover and Lessons Learned):

Figura 2: Schema di riferimento di un Incident Response lifecycle

Sebbene le fasi del processo sopra indicato rimangano invariate, le modalità, le metodologie e gli strumenti con cui svolgerle si sono modificate e adeguate all'evolversi delle minacce.
Nella Figura 3 sono mostrate le principali interazioni con le altre funzioni che oggi può prevedere un'attività di risposta ad incidente quali la Digital Forensics, la Malware Analysis, il Security Monitoring e la Cyber Threat Intelligence.

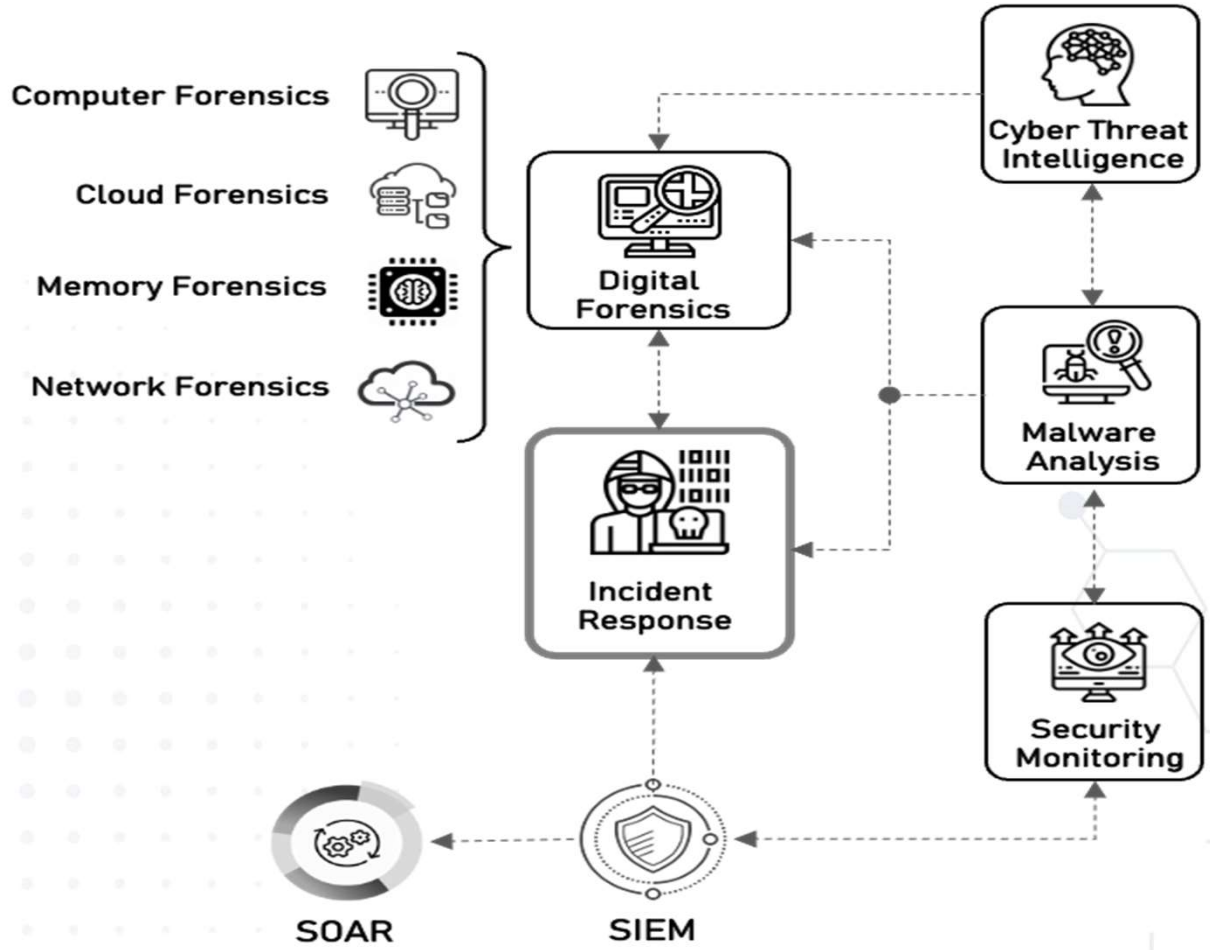
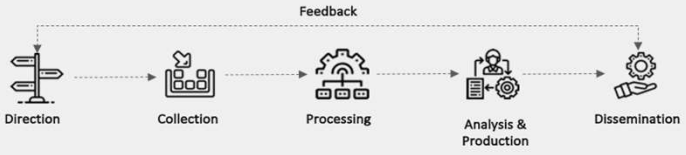
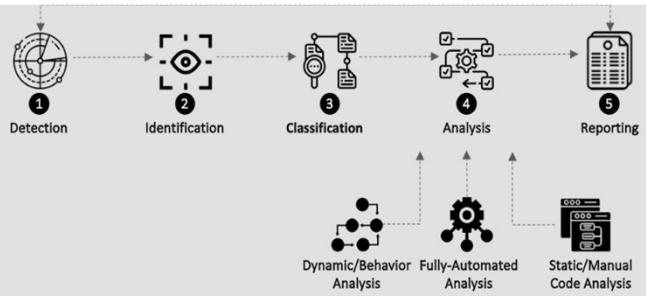


Figura 3: Schema di riferimento di un Incident Response lifecycle

Nella tabella seguente sono riportati, per ognuna delle **tre funzioni principali** che supportano l'Incident Response, i processi base di riferimento:

Descrizione Funzione	Processo base
La Digital Forensics gioca un ruolo cruciale nell'indagine sui crimini informatici, inclusi il furto di proprietà intellettuale, la cyber spionaggio e il possesso non autorizzato di contenuti. Coinvolge l'analisi di artefatti digitali come sistemi di file, dump della memoria e file di log per ricostruire gli eventi, identificare i colpevoli e raccogliere prove.	
Threat Intelligence implica la raccolta di informazioni su attaccanti attuali e potenziali per comprendere le loro motivazioni, tattiche e tecniche. Si basa sulla raccolta di dati da varie fonti, inclusi log, fonti pubbliche e piattaforme specializzate di threat intelligence.	
	

L'analisi dei malware è il processo di esame del software maligno per comprendere il suo comportamento, le capacità e l'impatto potenziale. Il malware assume varie forme, inclusi virus, cavalli di Troia e ransomware. L'analisi dei malware aiuta gli esperti di sicurezza a comprendere i meccanismi interni del malware, a sviluppare contromisure e a potenziare le difese della cybersecurity complessiva.	

Tab. 1 - Processi base della Digital Forensics, della Cyber Threat Intelligence e della Malware Analysis

In generale, queste funzioni possono essere anche viste -in un contesto più ampio e articolato- all'interno di un **Security Operation Center (SOC) intelligence-driven**:

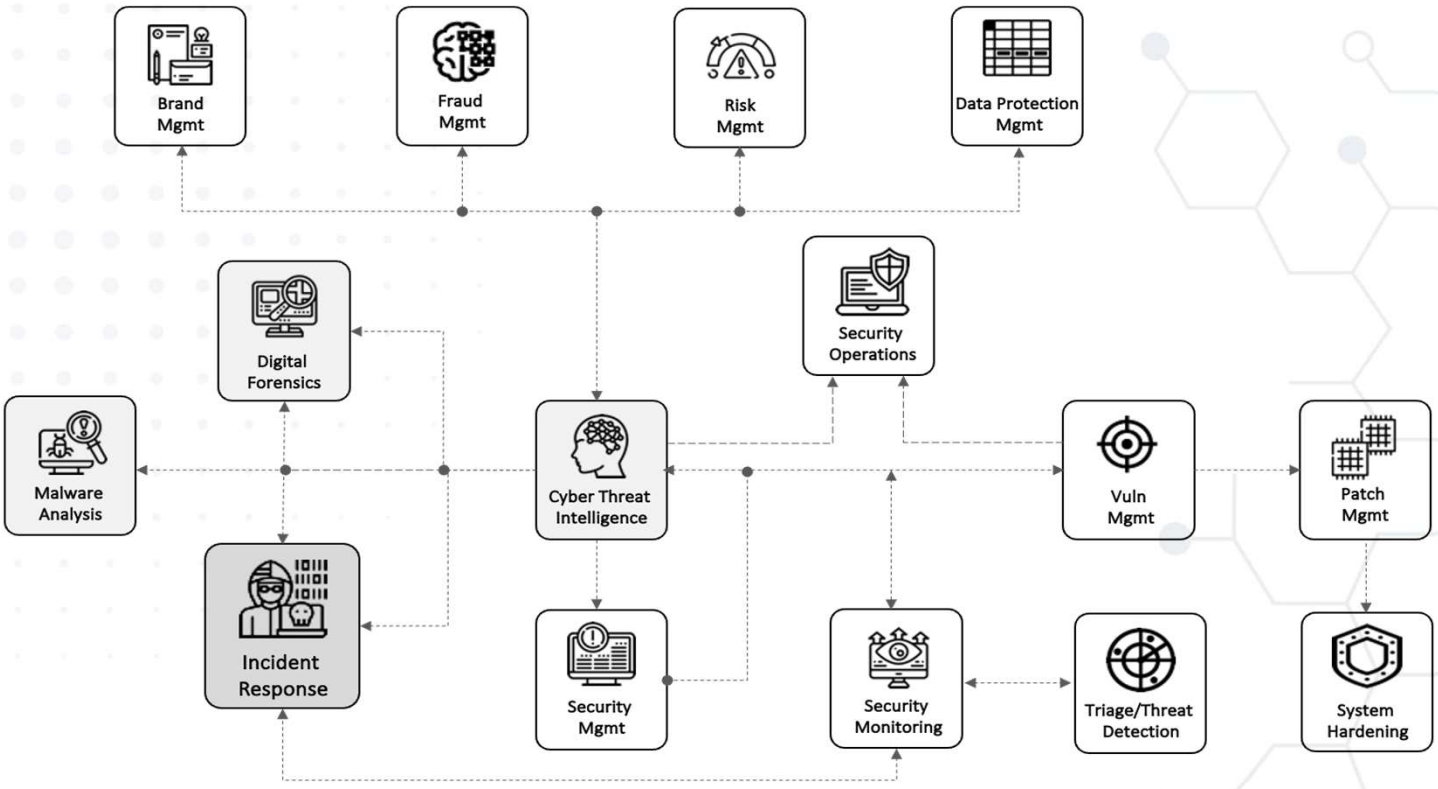


Figura 4: Principali funzioni presenti in un SOC intelligence-driven

I Security Operations Center (SOC) sono progettati e mantenuti con l'obiettivo di migliorare la qualità della sicurezza operativa di una organizzazione, migliorarne le protezioni e ridurre l'esposizione alle minacce. Questi obiettivi si possono ottenere attualmente passando dal rilevamento reattivo delle minacce al miglioramento proattivo dei processi e questo approccio richiede spesso la ridefinizione del ruolo del SOC.

Sulla base delle funzioni che sono potenzialmente utilizzate in un Incident Response, possiamo considerare come riferimento il seguente processo di IR:

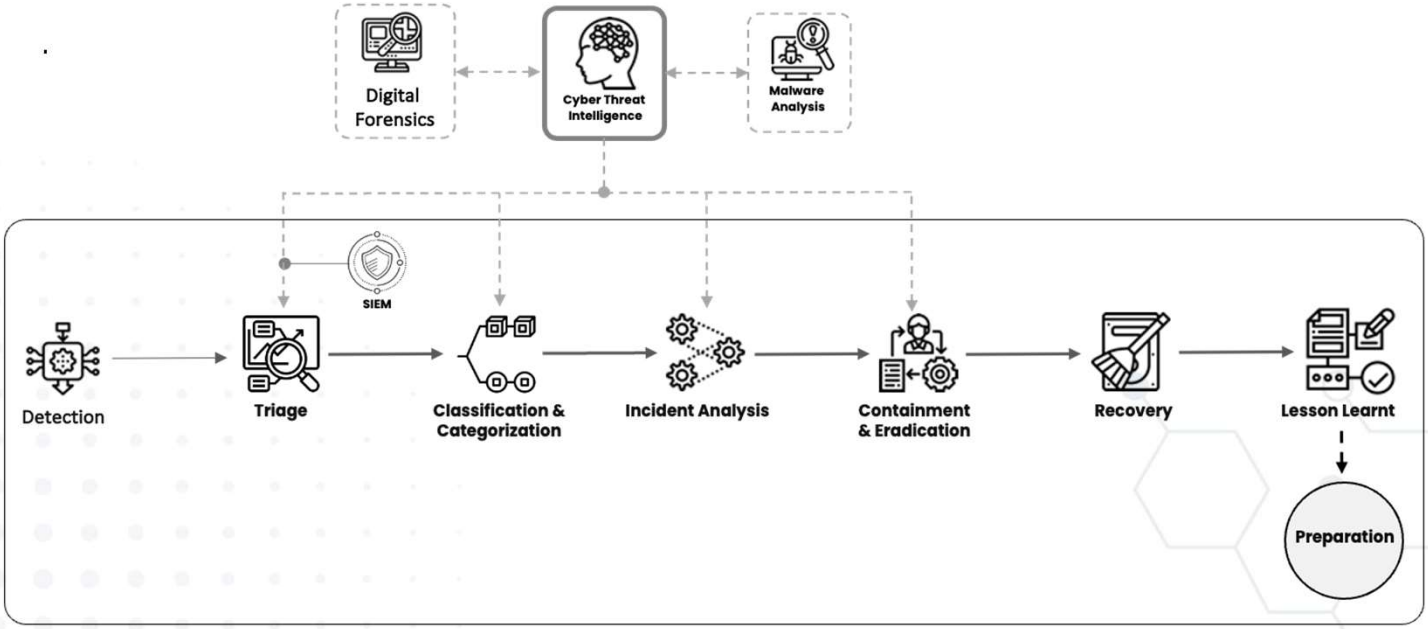


Figura 5: Processo complessivo di un Incident Response

Le fasi iniziali di **detection** e **triaging** sono cruciali per **identificare**, **analizzare** e **gestire** gli incidenti di sicurezza informatica. In particolare, gli obiettivi della detection sono il **monitoraggio continuo** dei sistemi per rilevare **anomalie** o **eventi** potenzialmente dannosi, minimizzare la finestra temporale tra l'inizio di un **evento malevolo** e la sua **identificazione** e registrare dati utili per supportare l'analisi e il triaging successivo.

Per raggiungere tali obiettivi, vengono impiegate tecniche che integrano monitoraggio, analisi avanzata e gestione degli incidenti. Strumenti come il **SIEM** consentono di **aggregare** e **analizzare** log e avvisi per rilevare anomalie o pattern di attacco, supportati da **regole di rilevamento** e **aggiornamenti continui**. La **threat intelligence** arricchisce gli **indicatori di compromissione** e individua **nuove minacce**, mentre le segnalazioni, sia manuali che automatiche, forniscono ulteriori spunti investigativi. Tecnologie avanzate, come algoritmi di **machine learning** e **analisi comportamentale**, migliorano il rilevamento delle attività sospette. Una volta individuato un **potenziale incidente**, viene valutata la gravità per determinarne l'**impatto** e definire le **priorità di intervento**, decidendo se è necessaria una risposta immediata.

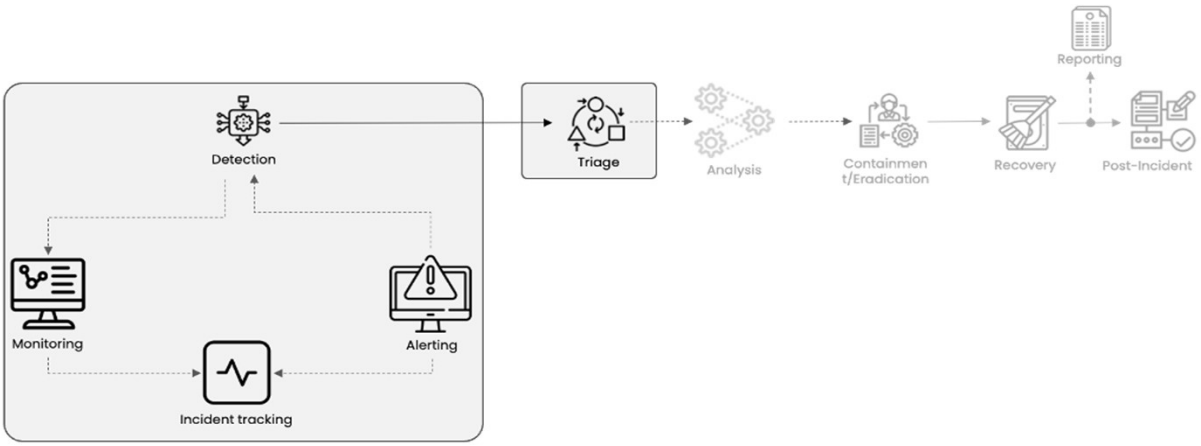


Figura 6: Fasi di Detection e Triaging nel processo di Incident Response

Una volta **rilevato** un incidente, il team avvierà la fase di **analisi** iniziando con la raccolta in **live acquisition** degli elementi dinamici e/o volatili di interesse quali la memoria **RAM**, i **registri di sistema**, le **connessioni di rete** ed esecuzione di **processi software**, fino agli **elementi statici** in post-mortem acquisition delle immagini forensi ottenute attraverso l'acquisizione di hard drive o delle immagini di dischi di macchine virtuali, log/eventi, etc.

A seconda del tipo di incidente, gli analisti dovranno individuare nella fase di identification le **fonti** di prova necessarie per la **comprensione** e l'**analisi** degli artifact. Naturalmente, le fasi di identificazione e acquisizione sono da considerarsi attività che possono essere svolte in maniera ciclica a seconda dell'avanzamento della fase di acquisizione.

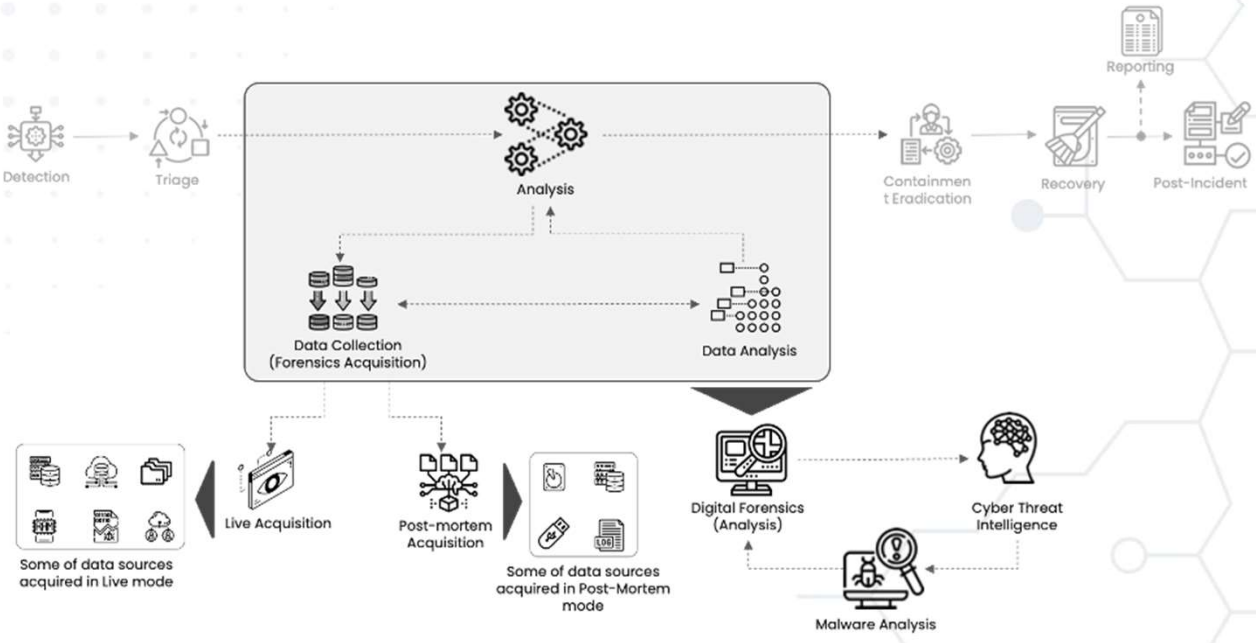
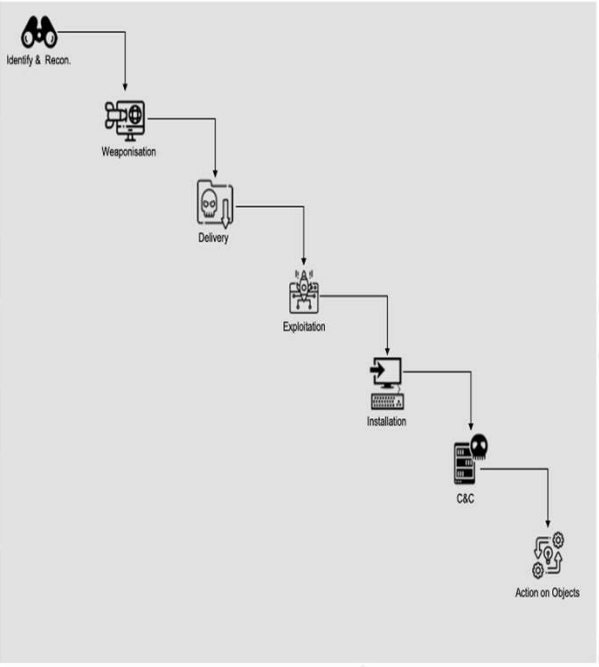


Figura 7: Fasi di Analysis nel processo di Incident Response

Un aspetto fondamentale nella fase di analisi che determina quali fonti di dati acquisire ed esaminare è lo **stato dell'incidente**. In generale, una volta che un IR team inizia la sua attività deve stabilire lo stato dell'incidente, ovvero se l'attaccante ha **completato** l'attacco oppure se questo è ancora **in corso**. La **Cyber Kill Chain** (CKC) è un modello di sicurezza che può essere utilizzato per descrivere sia lo **stato dell'attacco** (dal punto di vista dell'attaccante) e ,se non ancora completato, suggerire una contromisura per bloccare l'attacco. Infatti, il CKC ricorda che un attacco non è mai un evento atomico e se si è in grado di fermare in una delle sue fasi, allora lo si può interrompere.
Ecco una descrizione sintetica delle fasi principali del CKC:

Nome Fase	Descrizione Fase	Processo base del CKC
Identify & Reconnaissance	Questa fase coinvolge l'identificazione del bersaglio e la raccolta di informazioni preliminari. Gli attaccanti analizzano il target per scoprire vulnerabilità nei sistemi, nelle infrastrutture di rete o nel comportamento umano, utilizzando fonti aperte o tecniche più sofisticate per mappare la sicurezza avversaria.	
Weaponisation	Gli attaccanti sviluppano malware o payload nocivi specificamente progettati per sfruttare le vulnerabilità identificate sull'infrastruttura target, modificare o creare nuovi exploit, impacchettare il malware in documenti o altri file che sembrano innocui per facilitarne la consegna, etc.	
Delivery	Il malware o l'exploit viene spedito al target attraverso e-mail di phishing, siti web compromessi, download indesiderati o dispositivi fisici come USB infette, etc.	
Exploitation	Il malware attiva il suo payload una volta che è stato inoculato sul sistema target. Questo stadio include l'esecuzione di codice malevolo che sfrutta le vulnerabilità software o hardware per guadagnare l'accesso non autorizzato.	
Installation	Dopo la fase di exploitation, il malware esegue il codice per rendersi persistente sul sistema ospite. Questo può includere la creazione di backdoors, il download di ulteriori payload, etc.	
Command & Control (C&C)	Il malware stabilisce un canale di comunicazione tra il sistema infetto e l'attaccante, permettendo a quest'ultimo di gestire il malware, esfiltrare dati, spostarsi lateralmente nella rete o eseguire ulteriori azioni maligne.	
Action on Objectives	Questa è la fase finale in cui gli attaccanti realizzano i loro obiettivi, che possono includere furto di dati, distruzione di infrastrutture, spionaggio, o qualsiasi altro scopo specifico dell'attacco. In questa fase, possono anche cercare di mantenere l'accesso per operazioni future o per garantire un vantaggio a lungo termine.	

Tab. 2 - Processo base del modello Cyber Kill Chain

Nella fase di **contenimento** si effettuano le attività di **isolamento** dei dispositivi compromessi dalla rete. L'obiettivo che si persegue in questa fase è quello di **mitigare la causa** principale dell'incidente di sicurezza per prevenire ulteriori **danni** o **esposizioni**. Durante questa fase, il team di cyber security può implementare controlli, se necessario, per limitare i danni derivanti da un incidente di sicurezza. L'eradicazione è il processo di rimozione degli effetti dell'attacco informatico. Questo processo inizia una volta che i **sistemi compromessi** possono essere messi **offline** per permettere l'**eradicazione**. Esempi di attività di eradicazione sono la rimozione dei file e l'inversione delle modifiche al registro e alla configurazione apportate dal malware e dagli aggressori durante l'attacco.
Una volta identificate e isolate tutte le macchine interessate, l'azienda può affrontare le cause iniziali che sono state sfruttate dagli attaccanti per avviare l'attacco.

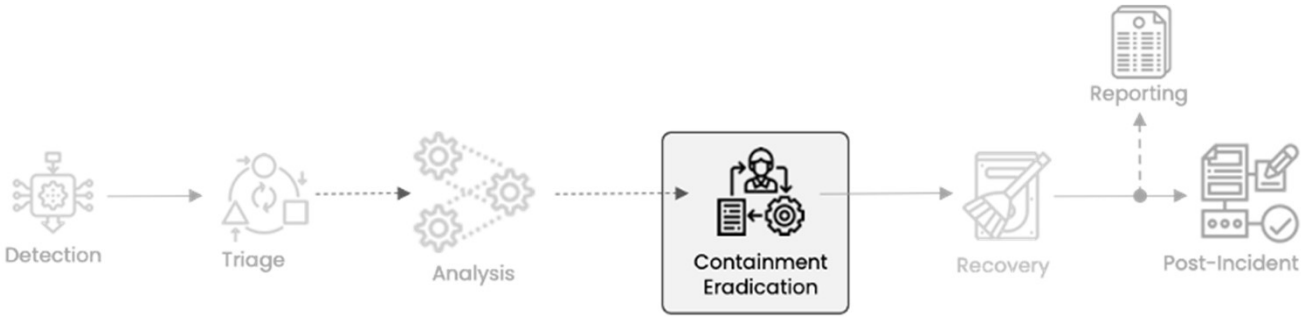


Figura 8: Fasi di Containment e di Eradication nel processo di Incident Response

Le attività di recupero sono strettamente allineate a quelle previste nei piani di continuità operativa o di *disaster recovery* di un'organizzazione. In questa fase del processo, le organizzazioni possono, ad esempio, reinstallare sistemi operativi o applicazioni, eseguire il ripristino dei dati sui sistemi locali dai backup, e controllare, se non già fatto nelle fasi precedenti, gli account utente e amministratore esistenti, per assicurarsi che non siano stati creati account abusivi dagli avversari durante il **lateral movement**.

Infine, l'attività di **post-incidente** (o *lesson learned*) comprende una revisione completa di tutte le azioni intraprese durante l'incidente. Questo processo include la valutazione di ciò che ha **funzionato** e, soprattutto, l'analisi di ciò che non ha funzionato, identificando le debolezze sfruttate dagli attaccanti.
Questa fase riveste un ruolo cruciale nel pianificare e implementare attività mirate al rafforzamento della postura di sicurezza, con l'obiettivo di prevenire futuri attacchi della stessa tipologia. Tutte le valutazioni effettuate devono quindi confluire come feedback per alimentare la fase di Preparation (o Readiness).

Figura 9: Fasi di Recovery e di Post-Incident nel processo di Incident Response

In conclusione, è stato evidenziato come l'adozione di un **modello classico** per il processo di Incident Response, basato sul paradigma PICERL, presenti alcune limitazioni, non tenendo conto di aspetti ormai consolidati nella gestione operativa degli incidenti. Sebbene il modello PICERL offra il vantaggio di essere semplice da personalizzare, esistono approcci più avanzati progettati per integrare nativamente pratiche operative fondamentali. Questi includono, ad esempio, il monitoraggio continuo della rete, l'aggregazione dei log e l'espansione dell'ambito di raccolta e analisi dei dati, non solo per i sistemi chiaramente compromessi, ma anche per quelli su cui sono stati rilevati indicatori di compromissione. Tali modelli permettono di affrontare gli incidenti in modo più completo ed efficace.

Un modello che, ad esempio, approccia le diverse attività attinenti ciascuna fase è quello che fornisce un approccio **Dinamico alla Risposta agli Incidenti** (DAIR) mostrato nella figura seguente:

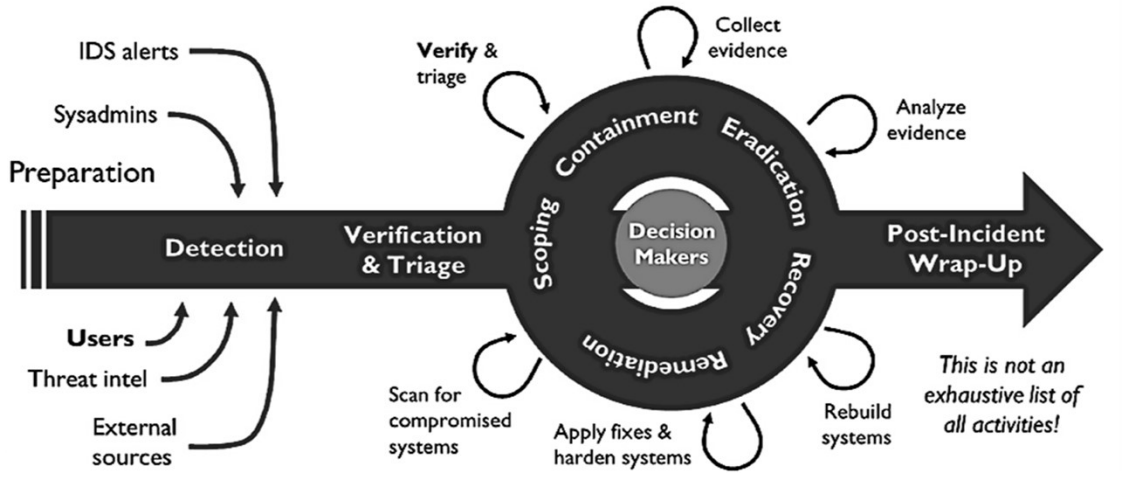


Figura 10: Modello dinamico di Incidente Response (DAIR)

L'approccio dinamico, rispetto a quello lineare, si distingue per una **maggiore fluidità** e un focus orientato ai risultati. In questo modello, la risposta agli incidenti non viene più percepita come una sequenza rigida di passaggi, ma come un insieme di punti di **transizione**, **obiettivi** da raggiungere e **attività** da svolgere, adattandosi in modo più flessibile alle esigenze operative.

Autore

Francesco Schifilliti

Francesco Schifilliti è un consulente altamente specializzato in diversi ambiti della sicurezza informatica, con una consolidata esperienza nelle indagini forensi digitali, nella gestione degli incidenti e nell'intelligence sulle minacce informatiche. Ha collaborato con le forze dell'ordine, fornendo supporto in delicate operazioni investigative, e ha affiancato aziende in indagini interne complesse. Nel corso della sua carriera, ha ricoperto il ruolo di manager nei Forensic Technology & Discovery Services di EY, occupandosi di progetti sia a livello nazionale che internazionale. Le sue competenze spaziano dalla Digital Forensic all'Incident Response, passando per le indagini su Data Breach, l'e-Discovery e la Forensic Data Analytics. Tiene regolarmente presentazioni sulle nuove tendenze del settore e delle minacce informatiche, oltre a svolgere attività didattiche. Ha infatti tenuto lezioni su digital forensics, memory forensics e malware analysis in corsi di dottorato e programmi formativi destinati alle forze dell'ordine italiane.

Ethical Hacking

Autore: Sebastiano Michele Militti

01. Introduzione e cenni storici

L'**Ethical Hacking** ha avuto inizio negli anni'50, quando studenti del **Tech Model Railroad Club** coniarono il termine «Hack» per indicare soluzioni tecniche ingegnose. Negli anni '60 i «**phone phreakers**» scoprirono alcune vulnerabilità nei sistemi telefonici aprendo la strada all'hacking moderno. Negli anni '70 e '80 con la diffusione dei **personal computer**, il termine «hacker» acquisì sia connotazioni positive (**white hat**) sia negative (**black hat**). Nel 1984 **Steven Levy** formalizzò il termine **ethical hacker** nel libro «**Hackers gli eroi della rivoluzione informatica**», come un'attività basata sull'**accesso libero** alle informazioni. Negli anni '90 l'Ethical Hacking divenne una professione riconosciuta, con iniziative come i primi programmi di **penetration testing** della **NSA**, la conferenza **Black Hat** del 1996, e la certificazione **CISSP** del 1999. Dal 2000 in poi l'**ethical hacking** è diventato un elemento fondamentale della **sicurezza informatica**, con la nascita delle certificazioni **CEH** e **OSSTTM**, la standardizzazione del framework **OWASP** e la diffusione dei programmi «**big bounty**». Oggi gli ethical hacker rappresentano figure fondamentali per le attività di **testing dei sistemi**, identificazione delle **vulnerabilità** e protezione delle **infrastrutture critiche,** affrontando sfide legate a nuove tecnologie come l'**intelligenza artificiale,** l' **IoT** e il **Cloud Computing**.

In Italia la cultura hacker mosse i primi passi all'inizio degli anni '80, diffondendosi principalmente attraverso le **BBS** (Bulletin Board System).

Le piattaforme pioniere furono «**Decoder BBS**» di Milano appartenente a «**Cybernet**», la «**ECN**» (European Counter Network), la «**Avana BBS**» di Roma, Mc-Link, Agorà e Galactica BBS per quanto riguarda i primi accessi a Internet. Il movimento hacker italiano si sviluppò come un fenomeno underground, ispirandosi alla **cultura cyberpunk** e alla filosofia del **software libero**. L'**Italian Crackdown** del 1994 fu un momento cruciale nella storia dell'hacking italiano. Si trattò di una vasta operazione di polizia che colpì la comunità hacker e telematica italiana. Questo episodio viene oggi ricordato come un momento di svolta che, paradossalmente, contribuì a legittimare e professionalizzare la comunità hacker italiana, portando alla nascita della prima associazione culturale telematica Italiana, **Metro Olografix**.

In sintesi...

L'**ethical hacking** è passato da una **nicchia underground** a una professione rispettata e necessaria, giocando un **ruolo cruciale** nella sicurezza dei sistemi e dei dati in un mondo sempre più digitalizzato.

02. Il Cyber Risk nel panorama dei rischi globali

La **Cyber Security** rappresenta oggi un aspetto cruciale per tutti i **settori industriali**, data la sua capacità di influenzare profondamente le operazioni aziendali e la stabilità economica. Il **World Economic Forum**, nel suo Global Risk Report 2024, evidenzia che la sicurezza informatica rappresenta una delle principali minacce tecnologiche a livello globale. Tra i rischi percepiti per i prossimi due anni, l'insicurezza cyber si colloca tra quelli considerati più gravi, assieme a problematiche come la **disinformazione**, gli **eventi meteorologici estremi** (alluvioni, terremoti, etc.), e le **tensioni geopolitiche**.

Di seguito viene riportato il costo di una **violazione di dati** in diversi settori critici:

11 Mln €

Stima del costo medio di una violazione dei dati per aziende nel **settore sanitario.**

5 Mln €

Stima del costo medio di una violazione dei dati per Società nel **settore finanziario.**

4-5 Mln €

Stima del costo medio di una violazione dei dati per aziende nel **settore farmaceutico.**

4-5 Mln €

Stima del costo medio di una violazione dei dati per Società nel **settore energetico.**

Questi dati evidenziano chiaramente come la **Cyber Security** non sia più una preoccupazione circoscritta a un unico settore, ma rappresenti una sfida **globale** e **trasversale** che coinvolge una molteplicità di aree industriali. Ogni comparto, dalle infrastrutture critiche al commercio digitale, si trova oggi ad affrontare minacce sempre più sofisticate che richiedono risposte tempestive, coordinate e innovative. La **protezione dei dati sensibili** non è solo una questione tecnica, ma anche **strategica**, che richiede un approccio condiviso e collaborativo tra aziende, istituzioni e professionisti del settore. In questo contesto, la Cyber Security si configura come una **priorità imprescindibile** per garantire la **resilienza** e la **competitività** nel panorama economico globale.

03. Cos'è il Cybercrime e come agiscono i criminali informatici

Il Cybercrime si riferisce ad attività criminali commesse utilizzando la **tecnologia digitale**, come computer, reti e Internet, comprendendo un'ampia gamma di attività illegali, tra cui hacking, phishing, attacchi malware, furto di identità e frodi online. Gli attacchi informatici possono essere classificati in diverse categorie a seconda delle modalità operative e degli obiettivi. Gli attacchi finalizzati all'ottenimento di un accesso non autorizzato ai sistemi informatici utilizzano metodi come il brute force, il **dictionary attack** e il credential stuffing. Gli attacchi di **privilege escalation** cercano di aumentare i privilegi di un account compromesso, mentre gli attacchi di rete includono tecniche di **Denial of Service (DoS)** e **Man-in-the-Middle**. Gli attacchi web sfruttano vulnerabilità come la **SQL Injection** e il **Cross-Site Scripting (XSS),** che consentono l'iniezione di script malevoli per rubare informazioni e dati. Il malware si presenta in diverse forme, tra cui virus, trojan e ransomware, ognuno con obiettivi specifici come il furto di dati o la richiesta di un riscatto. Il **social engineering** manipola psicologicamente le vittime attraverso tecniche come il phishing e il vishing. Gli attacchi hardware sfruttano emanazioni fisiche e possono richiedere accesso diretto all'hardware, mentre gli attacchi wireless compromettono **reti Wi-Fi** e dispositivi **Bluetooth**. Per contrastare le attività dei criminali informatici è stata sviluppata la **Cyber Kill Chain**, un modello che descrive le varie fasi di un attacco informatico.

Le sette fasi della Cyber Kill Chain

1. Ricognizione (Reconnaissance)

L'attaccante raccoglie informazioni sulle potenziali vittime attraverso la ricerca su Internet e altre fonti.

2. Armamento (Weaponization)

L'attaccante sviluppa il malware o l'arma informatica da utilizzare, come un virus o un trojan.

3. Consegna (Delivery)

L'attaccante invia l'arma alla vittima. I metodi di consegna includono email di phishing, chiavette USB infette, ecc.

4. Sfruttamento (Exploitation)

L'attaccante sfrutta una vulnerabilità nel sistema della vittima per eseguire il codice e avere accesso al sistema

5. Installazione (Installation)

Dopo lo sfruttamento, il malware o l'attacco viene installato nel sistema della vittima.

6. Command and Control

L'attaccante stabilisce una comunicazione con il sistema per controllarlo da remoto.

7. Actions on objectives

L'attaccante realizza il suo scopo finale, come ad esempio furto di dati, distruzione di informazioni, ecc.

04. Penetration Testing

Il Penetration Testing, o *pentest*, è una pratica utilizzata per valutare la sicurezza di un sistema informatico o di una rete. Si tratta di **simulare** attacchi reali per identificare e correggere eventuali vulnerabilità. A condurre queste attività sono gli ethical hacker, professionisti esperti che, grazie a creatività e competenze tecniche, utilizzano metodi e strumenti avanzati per aiutare le organizzazioni a migliorare le loro difese.

Esistono diverse metodologie per condurre un penetration test:

Black Box Testing	White Box Testing	Grey Box Testing	Red Teaming
Il tester non ha alcuna informazione preliminare sul sistema target, simulando così un attacco esterno.	Il tester ha un accesso completo alle informazioni del sistema e può effettuare un'analisi approfondita	Il tester ha un accesso limitato alle informazioni del sistema, bilanciando realismo e profondità dell'analisi.	Gruppo di esperti che simula attacchi persistenti e sofisticati per testare la resilienza del sistema

Vi sono delle considerazioni **etiche** da rispettare per condurre un penetration test. Prima di tutto, occorre un'autorizzazione scritta da parte dell'organizzazione target. Inoltre, il penetration tester deve operare nel rispetto delle normative vigenti, garantire la riservatezza dei dati raccolti e assicurarsi di non causare danni permanenti ai sistemi.

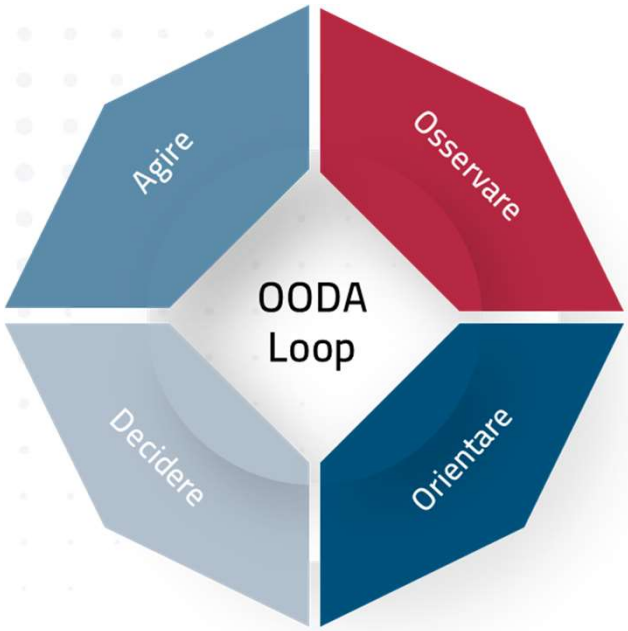
Affinchè un penetration test sia efficace, è fondamentale definire chiaramente l'**ambito** e il **perimetro** dell'attività, seguire metodologie standard riconosciute come **OWASP**, **PTES**, o **NIST SP-800-115**, e documentare accuratamente ogni fase. Il risultato finale dell'attività è un report dettagliato che riassume le vulnerabilità riscontrate e aiuta a migliorare la sicurezza informatica dell'organizzazione, oltre ad identificare la professionalità dei penetration tester.

Infine, per condurre queste analisi si utilizzano spesso distribuzioni specifiche come **Kali Linux**, molto popolare tra gli esperti grazie ai suoi numerosi strumenti preinstallati, ma anche **Parrot OS** e **BackBox**

05. Agire proattivamente attraverso informazioni di Intelligence

La **proattività difensiva** è un elemento chiave nella cybersecurity, e viene indirizzata attraverso attività di intelligence. L'intelligence utilizza un ciclo strutturato detto **ciclo di intelligence**, per valutare dati provenienti da diverse fonti.

Una volta consolidate le informazioni di intelligence, uno dei concetti più utilizzati durante un attacco informatico è l'**OODA** che sta per «**osservare**, **orientare**, **decidere** e **agire**». L'OODA rappresenta il processo mentale che un incident responder adotta durante un **incidente informatico** quando raccoglie informazioni d'intelligence e decide come utilizzarle.



La principale *disciplina d'intelligence nel* campo della cybersecurity è **l'OSINT (Open Source Intelligence)**, che si concentra sulla raccolta e analisi di informazioni disponibili pubblicamente.

Per svolgere attività di OSINT si utilizzano **strumenti** specifici e sistemi operativi progettati per garantire anonimato e protezione dei dati:

- **Kali Linux**: sistema operativo per attività di intelligence e cybersecurity;
- **Qubes OS**: basato sulla virtualizzazione, progettato per isolare le applicazioni;
- **Tails**: garantisce privacy attraverso una distribuzione Linux;
- **Tor** e **VPN**: permettono la navigazione anonima;
- **OnionShare**: condivisione anonima di dati tramite rete Tor;
- **Maltego**: software per la visualizzazione delle relazioni tra dati;
- **DNSdumpster.com**: permette di ottenere informazioni su domini e sottodomini;
- **ClamAV**: scansione di file e sistemi per rilevare malware;
- **Netcraft**: Fornisce dettagli su server web.

Attraverso l'utilizzo di queste tecnologie, l'intelligence diventa cruciale per una **strategia di cybersecurity proattiva**.

Autore

Sebastiano Michele Militti

Head of Security Intelligence & Blue Team presso BIP CyberSe, dove guida con esperienza e competenza il team dedicato alla protezione delle infrastrutture digitali.

Phishing-as-a-Service (PhaaS)

Autore: Pierluigi Paganini

01. Introduzione

Il phishing rappresenta una delle **minacce informatiche** più insidiose e in continua evoluzione del panorama della cybersecurity. Con il termine "phishing" si fa riferimento a un insieme di tecniche di ingegneria sociale volte a ingannare le vittime, inducendole a compiere azioni potenzialmente dannose, come la divulgazione di credenziali di accesso, dati personali o informazioni finanziarie. Gli attacchi di phishing si concretizzano principalmente attraverso messaggi **e-mail**, **SMS** (smishing) o **messaggistica istantanea** (vishing) in cui gli attaccanti si spacciano per enti, aziende o individui fidati.

Negli ultimi anni, il fenomeno ha conosciuto una crescita esponenziale sia in termini di volume sia di sofisticazione degli attacchi. La crescente digitalizzazione dei servizi e la diffusione del lavoro da remoto hanno ampliato la superficie di attacco, esponendo milioni di utenti e organizzazioni a nuove forme di minacce. Questo contesto ha favorito l'emergere di modelli di crimine informatico più complessi, tra cui il modello di **Phishing-as-a-Service (PhaaS)**, un paradigma in cui il phishing è reso disponibile come "servizio" acquistabile sul dark web o in forum dedicati. In questo modello, i cybercriminali possono accedere a kit di phishing preconfigurati e strumenti avanzati per lanciare attacchi con facilità, anche senza disporre di conoscenze tecniche specifiche.

Il PhaaS si inserisce nell'ambito più ampio del **Cybercrime-as-a-Service (CaaS)**, un ecosistema in cui strumenti, servizi e competenze necessarie per condurre attacchi informatici vengono offerti a noleggio o vendita. Questa nuova forma di "democratizzazione" del crimine informatico consente a chiunque, anche a individui senza particolari **competenze tecniche**, di organizzare attacchi di phishing su larga scala. La diffusione di piattaforme PhaaS ha quindi ridotto la barriera di accesso al cybercrime, portando a un aumento della frequenza e della gravità degli attacchi.

Nel contesto italiano, il settore finanziario è uno dei più colpiti. Secondo i **dati** del **2023**, il numero di pagine di phishing attive e operative giornalmente ha registrato una **media** di **3,6 unità**, con un aumento significativo rispetto agli anni precedenti. Questo trend conferma la necessità di un approccio proattivo e strutturato alla protezione delle organizzazioni e degli utenti contro le minacce di phishing.

Le piattaforme PhaaS si distinguono per la loro capacità di offrire strumenti e funzionalità avanzate, come modelli predefiniti di e-mail fraudolente, pagine web di phishing personalizzabili e strumenti analitici per monitorare l'efficacia delle campagne. Attraverso le piattaforme **PhaaS**, i cybercriminali possono **automatizzare** l'**invio** di **campagne** di phishing, selezionare obiettivi specifici e raccogliere dati in modo centralizzato e automatizzato.

02. Il panorama del Phishing

Il phishing rappresenta una delle minacce più persistenti e pericolose nell'ambito della cybersecurity. Con il termine "**phishing**" si indica una pratica di attacco informatico volta a ingannare le vittime, inducendole a compiere azioni dannose, come la divulgazione di informazioni sensibili, **credenziali** di **accesso** o **dati finanziari**.

Le tecniche di phishing sono in costante evoluzione, passando da e-mail generiche e messaggi SMS a campagne mirate (**spear phishing**) indirizzate a specifici individui o organizzazioni. I messaggi di phishing sono studiati per sembrare autentici e spesso imitano comunicazioni di enti affidabili, come istituzioni finanziarie, fornitori di servizi o aziende note.

Tra le principali **caratteristiche** degli **attacchi** di Phishing troviamo:

Ingegneria Sociale

Gli attaccanti sfruttano la **psicologia umana** per indurre le vittime a cliccare su **link dannosi** o scaricare allegati compromessi.

Uso di URL malevoli

Le pagine di phishing imitano **siti web legittimi**, spesso con **domini simili** o **caratteri speciali** che ingannano l'utente.

Tempistica attacchi

Molti attacchi vengono lanciati verso la **fine della settimana** lavorativa, sfruttando il minor supporto disponibile.

Durata dell'attacco

La maggior parte delle pagine di phishing resta attiva **per meno di 48 ore**, rendendo difficile il **rilevamento tempestivo**.

Un fenomeno recente è rappresentato dalle **Phishing Factory**, organizzazioni criminali strutturate che producono un elevato numero di pagine di phishing in breve tempo. Questo approccio consente ai cybercriminali di colpire molteplici obiettivi contemporaneamente e con maggiore frequenza. Nel contesto italiano, il settore finanziario è uno dei più bersagliati, con una media di 3,6 nuove pagine di phishing al giorno nel 2023. Inoltre, il **99,5%** delle **URL** di **phishing** utilizza il protocollo **HTTPS**, ingannando ulteriormente gli utenti, che tendono a fidarsi dei siti con il "**lucchetto**".

Le tecniche di rilevamento e blocco devono quindi evolversi per tenere il passo con le tattiche sempre più sofisticate adottate dai criminali. La consapevolezza e la formazione degli utenti giocano un ruolo fondamentale nella prevenzione del phishing.

03. Funzionamento delle piattaforme Phaas

Le piattaforme di Phishing-as-a-Service (PhaaS) rappresentano una delle evoluzioni più significative nel panorama del crimine informatico. Queste piattaforme offrono ai criminali informatici la possibilità di accedere a strumenti, kit di attacco e funzionalità avanzate per creare, gestire e lanciare campagne di phishing con facilità e su vasta scala. Le **piattaforme PhaaS** operano come veri e propri servizi commerciali, in cui gli utenti possono registrarsi, accedere a un'interfaccia grafica intuitiva e scegliere i servizi necessari per le loro campagne. Spesso, il pagamento dei servizi avviene in criptovalute per garantire l'anonimato.

Le principali caratteristiche di queste piattaforme includono:

Interfaccia intuitiva

L'interfaccia è progettata per essere user-friendly, anche per utenti con competenze tecniche limitate.

Modelli predefiniti

Gli utenti hanno accesso a template preconfigurati per e-mail e pagine di phishing.

Strumenti di personalizzazione

Possibilità di personalizzare il contenuto dei messaggi e delle pagine web, compresi loghi, testi e grafiche.

Il processo di creazione di una campagna su una piattaforma PhaaS si articola in diverse fasi, che includono la selezione del target, la personalizzazione dei contenuti e l'invio automatizzato.

La piattaforma consente il **monitoraggio continuo** delle campagne, con la possibilità di ottimizzare le strategie in tempo reale.

Il modello PhaaS ha **democratizzato** l'accesso alle tecniche di phishing, consentendo anche a utenti privi di competenze avanzate di organizzare attacchi sofisticati. Le autorità devono quindi affrontare una sfida complessa nel rilevare e bloccare tali attività.

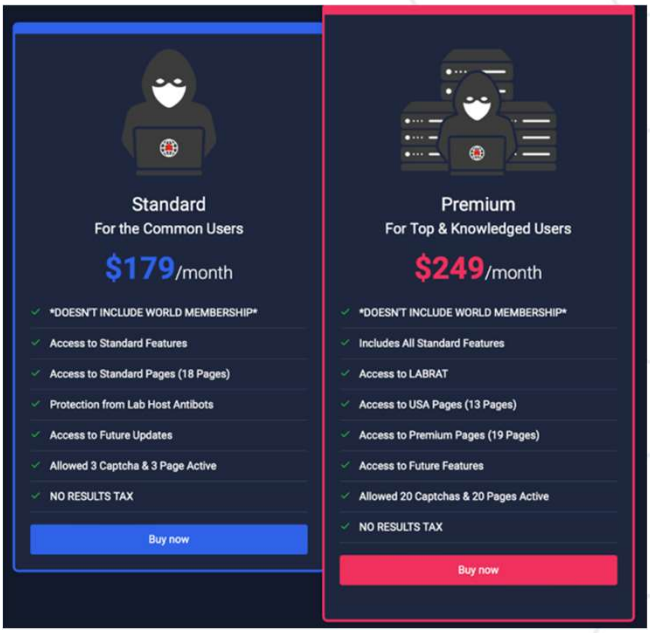


Figura 1: Esempio di piani di abbonamento ad una piattaforma PhaaS.

04. Phishing Kit

I phishing kit rappresentano uno degli strumenti centrali nel panorama del crimine informatico. Si tratta di **pacchetti preconfezionati di strumenti e risorse** progettati per semplificare la creazione e il lancio di **campagne di phishing**. Grazie a questi kit, anche utenti con competenze tecniche limitate possono condurre attacchi sofisticati.

Che cos'è un Phishing Kit?

Un phishing kit è una raccolta di **file** e **script** che consente di **replicare siti web legittimi**, come portali di login per servizi di posta elettronica, banche o piattaforme di pagamento online. Questi kit includono tutto il necessario per costruire una pagina di phishing, tra cui:

- Modelli di **pagine web**: copie identiche di pagine di login di servizi legittimi.
- **Script** per la raccolta dei dati: meccanismi per raccogliere e inviare credenziali rubate al criminale informatico.
- **Elementi grafici**: loghi, immagini e stili grafici per rendere la pagina più credibile.
- **File** di **configurazione**: parametri personalizzabili per adattare il kit a specifici obiettivi o lingue.

Questi kit possono essere trovati nei mercati del **dark web**, venduti a prezzi variabili in base alla complessità e alle funzionalità incluse.

Come funzionano i Phishing Kit?

I phishing kit sono spesso dotati di funzionalità avanzate per aumentare l'efficacia degli **attacchi** e **ridurre** le **probabilità** di **rilevamento**. Il funzionamento di un phishing kit è piuttosto semplice e può essere suddiviso in alcune fasi principali:

Installazione e configurazione

Il kit viene caricato su un server compromesso o su un dominio appositamente registrato. Il criminale configura le impostazioni per specifici obiettivi o gruppi di vittime.

Distribuzione URL Phishing

Gli attaccanti inviano e-mail o messaggi di testo alle vittime contenenti i link alla pagina di phishing creata con il kit.

Interazione con la vittima

Quando l'utente (vittima) visita la pagina, crede di trovarsi su un sito legittimo e inserisce le proprie credenziali.

Raccolta ed invio dei dati

I dati inseriti dall'utente vengono raccolti dal kit e inviati al server del criminale, spesso in tempo reale.

Evoluzione dei Phishing Kit

Negli ultimi anni, i phishing kit si sono evoluti significativamente, introducendo funzionalità sempre più avanzate per evitare il rilevamento e migliorare le probabilità di successo. Alcuni esempi di evoluzione includono il **Multi-factor phishing**, un kit in grado di rubare anche i codici di autenticazione a due fattori (2FA) attraverso attacchi man-in-the-middle.

I phishing kit vengono spesso utilizzati all'interno delle **piattaforme Phishing-as-a-Service (PhaaS).** Queste piattaforme forniscono l'accesso ai kit e la possibilità di condurre campagne di phishing personalizzate, complete di analisi delle prestazioni e supporto tecnico. Attraverso le piattaforme PhaaS, anche criminali con poche competenze tecniche possono accedere a kit sofisticati e gestire operazioni su larga scala. Alcuni kit di phishing hanno ottenuto **notorietà** a causa della loro diffusione o della complessità delle loro funzionalità. Tra i più noti possiamo citare:

Kit per Office 365

I portali di login di Office 365 sono tra i più imitati nei **kit di phishing**, data la loro diffusione in contesti aziendali.

Tycoon 2FA Kit

Un esempio di kit in grado di **superare l'autenticazione a due fattori**, rendendo gli attacchi molto più pericolosi.

Impatto e rischi

L'utilizzo di phishing kit ha aumentato la frequenza e l'efficacia degli attacchi di phishing. Questi kit permettono a criminali con competenze tecniche limitate di lanciare **campagne sofisticate**, **automatizzate** e **mirate**.

Gli attacchi condotti con kit di phishing possono portare al furto di credenziali di accesso, dati finanziari e altre informazioni sensibili, con conseguenze devastanti per le **vittime**. L'impatto per le organizzazioni può essere estremamente grave, con costi diretti e indiretti significativi. Le aziende possono subire danni economici derivanti da frodi finanziarie, perdita di dati critici e costi di recupero delle operazioni. Inoltre, vi è il rischio di danni reputazionali, poiché le violazioni di sicurezza spesso minano la fiducia dei clienti e degli stakeholder. La perdita di fiducia può portare a una riduzione dei ricavi e a un aumento delle spese legate alla gestione delle crisi e alle attività di comunicazione.

Le organizzazioni devono quindi adottare misure preventive per mitigare questi rischi, come l'uso di strumenti di rilevamento avanzati, campagne di sensibilizzazione del personale e tecnologie di autenticazione forte (come l'autenticazione a due fattori) per ridurre l'efficacia di questi attacchi. La formazione del personale è cruciale, poiché gli utenti rappresentano spesso l'anello più debole della catena di sicurezza.

05. Generative AI e Phishing

L'evoluzione delle tecnologie di intelligenza artificiale (**AI**) ha avuto un impatto significativo sul panorama delle minacce informatiche, in particolare nel contesto del phishing. L'introduzione di **modelli di intelligenza artificiale generativa** (Generative AI) ha reso gli attacchi di phishing più sofisticati, personalizzati e difficili da rilevare.

L'AI generativa consente ai criminali informatici di **automatizzare** la **creazione** di **contenuti** personalizzati su larga scala. Grazie a tecnologie di machine learning e modelli linguistici avanzati, è possibile generare testi, immagini e persino video credibili e altamente persuasivi.

Applicazioni dell'AI Generativa per lo svolgimento di attacchi Phishing

Email di Phishing personalizzate. I modelli di AI possono generare e-mail **personalizzate** con contenuti specifici per la vittima, aumentando le probabilità di successo.

Produzione di Deepfake. L'AI può generare **video** e **audio** falsificati per simulare la voce e l'immagine di una persona fidata, come un CEO o un manager.

Superamento dei filtri antispam. I testi generati dall'AI possono **eludere** i filtri **antispam**, rendendo gli attacchi più efficaci.

Rischi associati all'utilizzo dell'AI Generativa per gli attacchi Phishing

L'uso dell'AI generativa nel phishing presenta rischi significativi per le organizzazioni e gli individui. Uno dei principali rischi è l'aumento della frequenza e della qualità degli attacchi. I criminali possono lanciare campagne di phishing su larga scala con **messaggi personalizzati** e altamente convincenti, sfruttando i dati personali disponibili online. Grazie all'AI, è possibile generare e-mail di phishing su misura per ciascun destinatario, rendendo gli attacchi più difficili da identificare e prevenire.

Un altro rischio importante è la maggiore difficoltà di rilevamento. Poiché i messaggi generati dall'AI sono unici e non corrispondono a modelli predefiniti, i sistemi di sicurezza tradizionali che si basano su firme o modelli statici hanno maggiori difficoltà a rilevarli. Questo rende necessario un approccio più dinamico e adattivo nella rilevazione delle minacce.

L'uso delle deepfake rappresenta un rischio ancora più elevato. L'AI è in grado di generare video e audio falsificati in cui viene simulata la voce e l'immagine di una persona fidata, come un CEO o un dirigente aziendale. Questa tecnica è spesso utilizzata negli attacchi di Business Email Compromise (BEC), in cui i truffatori convincono i dipendenti a effettuare trasferimenti di denaro a conti bancari controllati dagli attaccanti.

06. Contromisure e difese

Per contrastare le minacce del phishing e delle piattaforme PhaaS, è fondamentale combinare **soluzioni tecnologiche** e **misure organizzative**. Di seguito sono presentate cinque soluzioni tecnologiche e cinque misure organizzative per una difesa completa.

Soluzioni Tecnologiche	Misure Organizzative
Rilevamento e risposta agli attacchi (EDR e XDR) consente di identificare e rispondere agli attacchi in tempo reale, analizzando il comportamento delle minacce di tipo Phishing.	La formazione e la sensibilizzazione del personale aiutano i dipendenti a riconoscere e segnalare le e-mail di phishing, riducendo il rischio di errore umano.
L'autenticazione multi-fattore (MFA) aggiunge un ulteriore livello di sicurezza, richiedendo una verifica aggiuntiva per accedere ai sistemi e quindi a informazioni e dati.	Le simulazioni di phishing permettono di testare la capacità dei dipendenti di riconoscere le e-mail malevole e identificare le aree in cui è necessaria una maggiore formazione.
I filtri avanzati per e-mail rilevano e bloccano e-mail di phishing utilizzando intelligenza artificiale e algoritmi di apprendimento automatico per identificare messaggi sospetti.	La segnalazione delle minacce consente ai dipendenti di informare il reparto IT delle e-mail sospette, facilitando un intervento tempestivo e migliorando la risposta alle minacce.
L'analisi preventiva dei link e il *sandboxing* consentono di eseguire i link in ambienti sicuri prima che l'utente acceda al contenuto, rilevando comportamenti dannosi.	L'adozione del principio del "privilegio minimo" limita l'accesso degli utenti solo alle risorse necessarie, riducendo la superficie di attacco e l'impatto di eventuali compromissioni.

La combinazione di queste soluzioni tecnologiche e misure organizzative offre una difesa multilivello contro le minacce di phishing e le piattaforme di Phishing-as-a-Service (PhaaS). Un approccio integrato migliora la **capacità di rilevamento**, **risposta** e **prevenzione**, riducendo al minimo i rischi per le organizzazioni.

07. Conclusione

Il phishing e il modello di Phishing-as-a-Service (PhaaS) rappresentano una minaccia crescente nel panorama della cybersecurity. L'evoluzione delle tecniche di attacco, supportata dall'uso di **intelligenza artificiale generativa** e strumenti di automazione avanzati, ha reso gli attacchi di **phishing** più sofisticati e difficili da rilevare. Tuttavia, con un approccio integrato e multilivello, le **organizzazioni** possono ridurre significativamente il rischio di compromissione. L'adozione di tecnologie avanzate, come **EDR**, **XDR** e sistemi di threat intelligence, offre una protezione proattiva e tempestiva. Parallelamente, le misure organizzative, come la formazione del personale e la segnalazione delle minacce, completano la difesa e rafforzano la resilienza aziendale. Per affrontare efficacemente queste minacce, le organizzazioni devono considerare la **sicurezza** come un processo continuo e dinamico, non come una soluzione una tantum. La collaborazione tra enti governativi, forze dell'ordine e il settore privato è essenziale per smantellare le piattaforme PhaaS e ridurre l'accesso alle risorse utilizzate per condurre attacchi.

In definitiva, l'adozione di una **strategia di difesa multilivello** basata su tecnologie avanzate, misure organizzative e conformità normativa rappresenta la via più efficace per mitigare le minacce di phishing. Solo attraverso un approccio coordinato e una vigilanza costante sarà possibile ridurre l'impatto di queste minacce sulle organizzazioni e sugli individui.

Autore

Pierluigi Paganini

Pierluigi Paganini è Ceo di **CYBHORUS** e Membro del Gruppo **Ad-Hoc Working Group on Cyber Threat Landscape dell'agenzia europea ENISA**. E' **Adjunct Professor** in Cyber Security presso l'Università Luiss Guido Carli e Coordinatore scientifico del Master in Cyber Security del Sole24Ore Formazione. Ha fondato **Cybaze**, uno dei principali poli privati di cyber security poi acquisito dal gruppo **Tinexta**. Pierluigi Paganini è fondatore di Security Affairs, tra i primi blog al mondo di Cyber Security e collabora con le principali testate giornalistiche nazionali ed internazionali. Gestisce la rubrica "**Sicuri nella Rete**" per la Repubblica ed è autore per la rubrica VERIFIED dell'agenzia ANSA. Nel 2017 è stato membro del gruppo italiano «**Ise-Shima Cyber Group**» (ISCG) in occasione del G7 Italia, un nuovo Working Group del **G7** sulle tematiche che riguardano il Cyberspace. E' co-autore della dichiarazione di Lucca, approvato dai Ministri del G7, concernente la dichiarazione sulle norme di comportamento degli stati nel **Cyberspace**.

Il Ruolo dell'IA nella Sicurezza Informatica

Autore: Annalisa Appice

01. Introduzione

La progressiva digitalizzazione dei processi e dematerializzazione dei documenti ha contribuito, nell'ultimo decennio, a cambiare drasticamente le pratiche e relazioni sociali, economiche e culturali della società moderna producendo un grande volume di informazioni digitali facilmente accessibili e manipolabili. Queste informazioni hanno reso disponibile un patrimonio di dati strutturati e non strutturati pronti per essere elaborati grazie alle sempre più potenti tecnologie di **Intelligenza Artificiale (IA)**. Pertanto, la trasformazione digitale e l'IA sono oggi considerate complementari, poiché la trasformazione digitale fornisce i dati necessari all'IA per l'analisi e l'apprendimento, mentre l'IA contribuisce a migliorare l'efficienza e l'efficacia dei processi di digitalizzazione. Tuttavia, la trasformazione digitale ha anche aperto le porte a minacce informatiche di dimensioni e complessità senza precedenti.

Con l'aumentare della dipendenza della nostra società ed economia dalla tecnologia, è cresciuta l'urgenza di proteggere il nostro ecosistema digitale da malintenzionati. Negli ultimi anni, l'IA ha quindi guadagnato un ruolo sempre più importante nella sicurezza informatica, grazie alla capacità di analizzare grandi volumi di dati per apprendere i modelli del funzionamento "**normale**" di **un'organizzazione**. Per esempio, gli strumenti di IA possono apprendere modelli di quando e dove gli utenti accedono ai dati o servizi erogati, delle tendenze e dei volumi di traffico dati attesi e degli strumenti cloud comunemente usati Una volta appreso un modello del funzionamento atteso, è possibile identificare anomalie che richiedano un approfondimento di investigazione. Pertanto, i moderni sistemi di sicurezza usano sempre più strumenti di IA, basati principalmente su tecniche di machine learning e deep learning, per identificare non solo minacce già note (per esempio, malware), ma anche varianti di minacce esistenti e, possibilmente, nuove tipologie di minacce. Questa capacità degli strumenti di IA contribuisce a incrementare l'accuratezza e la resilienza dei sistemi di sicurezza, oltre a fornire la conoscenza necessaria per identificare e risolvere le minacce più rapidamente. È importante notare che l'IA non mira a **sostituire i professionisti della sicurezza**, ma opera in modo simbiotico supportandoli nel loro lavoro in modo da renderlo più efficace ed efficiente. Le applicazioni che oggigiorno fanno un uso sistematico degli strumenti di IA per la sicurezza variano dalla scoperta di minacce nel traffico di rete, alla sicurezza delle applicazioni, all'analisi delle e-mail, al monitoraggio dei sistemi di revisione di servizi e prodotti ed ai sistemi anti-malware. Tuttavia, l'IA non è solo uno strumento difensivo al servizio dei professionisti della sicurezza. Infatti, viene sempre più spesso utilizzata in maniera offensiva da attori malintenzionati (cyber-hacker) per trarre vantaggio dalle eventuali vulnerabilità dei sistemi di IA e creare minacce che sfuggono ai sistemi di IA o li avvelenino, portando a errori nella fase di apprendimento del modello.

L'AI offensiva rappresenta oggi una crescente preoccupazione per la sicurezza delle organizzazioni, motivando l'investimento nello sviluppo di una IA difensiva finalizzata a creare contromisure contro l'IA offensiva, scoprire le vulnerabilità dei sistemi di sicurezza e incrementare la robustezza delle **misure di difesa**. Sebbene sia ancora in fase di sviluppo, l'IA difensiva è considerata una strategia promettente per costruire una tecnologia di mitigazione responsabile ed etica. In riferimento all'etica dell'IA, la trasparenza delle decisioni prese con algoritmi di IA è oggi un **serio problema da non trascurare**, in particolare, quando i risultati coinvolgono esseri umani.

Il resto del capitolo è organizzato come segue:

- **Sezione 2** presenta una breve panoramica degli sviluppi recenti nell'ambito dell'IA, dei principali paradigmi di apprendimento e dei rudimenti alla base delle tecniche di machine learning e deep learning.
- **Sezione 3** descrive alcune delle applicazioni che usano comunemente tecniche di machine learning e deep learning per la sicurezza.
- **Sezione 4** analizza la dicotomia tra IA offensiva ed IA difensiva con cenni alla questione etica nell'IA.
- **Sezione 5** affronta il diritto alla spiegazione delle decisioni prese con il contributo di sistemi di IA.
- **Sezione 6** traccia le conclusioni e lezioni apprese.

02. Che cos'è l'Intelligenza Artificiale

L'**IA** (Ertel, 2025) nasce come disciplina scientifica nel secolo scorso. Ufficialmente, la sua origine è datata al 1950, quando, in un articolo pubblicato sulla rivista «Mind», A.M. Turing descrisse un test per stabilire quando una macchina potesse essere definita "intelligente" (il test di Turing). Subito dopo gli esordi della disciplina, furono formulate le prime teorie sulle reti neurali che solo oggigiorno hanno trovato un'ampia applicazione nell'ambito nelle tecniche d**i deep learning**. Si passò quindi alla formalizzazione dei principi di una IA forte in contrapposizione a una IA debole. L'IA forte denota una macchina intelligente che ha coscienza di sé ed è in grado di apprendere da sola. Mentre l'IA debole caratterizza una macchina che è in grado di risolvere solo problemi di un certo tipo. I notevoli progressi degli ultimi cinquant'anni ci hanno mostrato come oggi sia possibile realizzare sistemi effettivi di IA debole grazie agli sviluppi tecnologici e scientifici conseguiti nell'apprendere dai dati con tecniche di machine learning e deep learning. Con queste tecniche, una macchina è programmata per analizzare dati storici e apprendere da essi la conoscenza necessaria per svolgere determinati compiti migliorando i risultati futuri in base a quelli passati.

Un esempio sono i sistemi che imparano a prevedere le abitudini di acquisto degli utenti di un e-commerce basandosi sui dati raccolti dagli acquisti precedenti.

Con le **reti neurali**, l'ingegnerizzazione dei dati cessa di essere un processo separato, ma diventa parte integrante dell'**addestramento** della **rete**.

In particolare, una rete neurale è addestrata direttamente da dati grezzi andando a minimizzare la funzione di perdita (intesa come una misura dell'errore) attraverso il calcolo della derivata di tale funzione e provvedendo ad aggiustare di conseguenza i parametri del modello.

Maggiore è la quantità di dati elaborati, migliore è la comprensione che la tecnica di deep learning riesce ad acquisire senza intervento umano. In generale, il vantaggio delle tecniche di deep learning sulle tecniche di machine learning diventa evidente con l'aumentare della mole di dati raccolta per l'addestramento del modello.

Tecniche di Machine Learning: richiedono un passo di ingegnerizzazione dei dati finalizzato a estrarre una rappresentazione intelligente dei dati grezzi da cui apprendere conoscenza.

Tecniche di Deep Learning: sono tecniche di machine learning basate su reti neurali artificiali, in grado di elaborare grandi moli di dati simulando il comportamento dei neuroni umani

Rete Neurale: utilizza molti livelli di processi matematici interconnessi per creare motori decisionali non lineari.

I principali **paradigmi** di apprendimento che guidano lo sviluppo delle tecniche di **machine learning** e **deep learning** sono quattro:

1. Supervisionato

Per individuare **pacchetti** o **connessioni** che potrebbero indicare intrusioni di vario tipo.

2. Non Supervisionato

I dati non sono etichettati e l'obiettivo è apprendere una "**descrizione**" dei dati (per esempio, associazioni frequenti o raggruppamenti di esempi in **cluster**).

3. Semi Supervisionato

Gli algoritmi sono usati per **apprendere un modello di predizione** a partire da esempi solo parzialmente etichettati. Questo tipo di apprendimento è utile quando esistono molti dati non etichettati.

4. Apprendimento per Rinforzo

Si apprende adattandosi alle regole dell'ambiente. L'algoritmo riceve una **ricompensa per le azioni corrette**, che cerca di massimizzare, mentre applica una penalizzazione per le azioni errate.

Di seguito, vengono riportati alcuni **esempi** di **machine learning supervisionato**: Decision Tree, Random Forest, Support Vector Machine, XGBoost, K-Nearest Neighbour, Logistic Regression, Naive Bayes.

Inoltre, la supervisione o meno la ritroviamo anche per le **reti neurali.**

Esempi di Reti Neurali addestrate in maniera supervisionata:

Deep Neural Network, Convolutional Neural Network, Long Short-Term Network, Transfromer e Graph Neural NetworkSono.

Esempi di Reti Neurali addestrate in maniera non supervisionata:

Autoencoder e Generative Adversarial Network.

03. L'Intelligenza Artificiale nella Cyber Security

L'Intelligenza Artificiale ha numerose applicazioni nella sicurezza.

Si riportano alcuni esempi di casi d'uso.

Analisi del traffico di rete

Per individuare pacchetti o connessioni che potrebbero indicare intrusioni di vario tipo**.**

Malware Discovery

Attraverso l'apprendimento di modelli di comportamento malevolo, andando oltre il semplice confronto.

Analisi delle e-mail

Attraverso l'utilizzo di algoritmi di machine learning e deep learning per scoprire spam e tentativi di phishing**.**

Sicurezza delle Applicazioni

Individua anomalie riconducibili ad accessi non autorizzati e abuso di privilegi.

Analisi delle Revisioni

Riconosce, tra quelle pubblicate online dagli utenti, revisioni spammer o scritte con intenti malevoli.

Cloud Security

Garantisce la corretta configurazione delle autorizzazioni del cloud, controlli e accessi.

I **Large Language Model (LLM)** sono sempre più frequentemente utilizzati nell'analisi delle e-mail e delle revisioni e nella sicurezza delle applicazioni, mentre algoritmi di machine learning o deep learning per la classificazione trovano ampio impiego nell'analisi del traffico di rete, nella scoperta di malware e nell'analisi delle e-mail o delle revisioni.

Tuttavia, la difficoltà e il costo nel reperire dati correttamente etichettati spostano sempre più spesso l'attenzione verso algoritmi non supervisionati, come quelli per la scoperta di associazioni, il **clustering** o la scoperta di anomalie. Inoltre, usando l'IA nelle diverse applicazioni di sicurezza informatica si deve tenere conto dei naturali cambiamenti attesi nella distribuzione dei dati (per esempio, a causa dell'emergere di nuove tipologie di malware o della riduzione della frequenza di alcuni tipi). Di conseguenza, i modelli di classificazione devono essere periodicamente riaddestrati (Andresini et al., 2021).

04. AI Offensiva ed AI Difensiva

AI Offensiva

L'IA *offensiva* si riferisce a sistemi che usano l'IA per **eseguire attività malevole**. Esempi concreti di utilizzo di IA offensiva includono l'impiego di IA generativa, spesso in combinazione con tecniche di ingegneria sociale, per creare software, video, vocali malevoli e e-mail di phishing personalizzate che appaiono autentici e credibili, in grado di manipolare individui o sistemi ignari, inducendoli a rivelare informazioni riservate o a fornire accessi ed autorizzazioni in modo inappropriato. Oggi l'IA offensiva rappresenta una minaccia reale alla sicurezza delle organizzazioni pubbliche e private, come anche dei singoli utenti. Essa può trarre vantaggio dalle vulnerabilità di sistemi di IA progettati per garantire la sicurezza del cyberspazio, generando esempi avversari in grado di eludere il modello di decisione o avvelenare i dati di addestramento. La vulnerabilità dei sistemi di IA è stata teorizzata nel 2014, quando Szegedy et al. dimostrarono che un modello addestrato per la classificazione di immagini, anche se addestrato con avanzate tecniche di deep learning, poteva essere facilmente ingannato con una lieve alterazione dei dati, impercettibile all'occhio umano. Da allora, l'IA offensiva è emersa come una grave minaccia per le organizzazioni, rendendo evidente la necessità di sviluppare normative e quadri giuridici rigorosi per regolarne l'uso. A tal proposito, il Regolamento Europeo sull'IA, che è ufficialmente una legge dell'Unione, dopo la sua pubblicazione in Gazzetta il 12 luglio 2024, è l'ultimo di una lunga serie di normative a livello comunitario che regolano l'uso dei dati e il loro impiego nella creazione di algoritmi di IA (generativa e non solo). Trasparenza, responsabilità ed equità sono i principi cardine che le organizzazioni devono adottare nella progettazione e nell'uso dell'IA. In questa prospettiva, l'IA offensiva viene studiata anche per individuare preventivamente le vulnerabilità dei sistemi di IA, al fine di sviluppare sistemi accurati e robusti contro attacchi avversari.

AI Difensiva

L'IA *difensiva* è uno strumento cruciale nella strategia per contrastare l'IA offensiva e migliorare la capacità di sistemi di sicurezza

e contrastare rapidamente le cyber-minacce (Carrasco et al., 2024). Le aziende dovrebbero aggiornare i protocolli di sicurezza con piani di risposta agli incidenti e strategie di condivisione di informazioni sulle minacce. A tal scopo, si stanno sviluppando strumenti etici di IA offensiva per identificare in modo preventivo quali siano le vulnerabilità dei sistemi. Ad esempio, per contrastare la minaccia dei malware Windows PE, sono state recentemente sviluppate tecniche per generare varianti di malware Windows PE che mantengono comportamenti malevoli ma riescono a eludere modelli di classificazione addestrati con l'IA (Demetrio et al., 2022). Costruire esempi avversari in fase di sviluppo permette di adottare strategie di difesa per rafforzare i sistemi di IA. Una **strategia difensiva** è *l'adversarial training*, che riaddestra un modello di classificazione includendo anche esempi avversari (Angioni et al., 2024, Imran et al., 2024). Altre strategie difensive consistono nell'aggiungere un fattore di regolarizzazione nella funzione di perdita rispetto a un rumore specifico, senza creare nuovi esempi. In alternativa, è possibile addestrare un modello di classificazione in grado di rispondere «non so» o «questo esempio non può essere classificato in modo affidabile», creando così una nuova classe da predire (Costa et al., 2024).

Un'ulteriore strategia consiste nell'identificare caratteristiche dei dati più robuste ad attacchi avversari e utilizzare tali caratteristiche nell'apprendimento del modello di classificazione (Wang et al, 2024).

05. Spiegabilità dell'Intelligenza Artificiale

Spiegare le decisioni di un sistema di IA può aiutare a trasformare le previsioni in azioni, migliorando la resilienza della difesa. In particolare, le spiegazioni possono evidenziare fattori misurabili relativi alle caratteristiche di un campione che influenzano la previsione di uno stato futuro del campione e la loro importanza relativa (Rjoub et al. 2023). Questi fattori possono fornire ai professionisti della sicurezza una comprensione più approfondita del motivo per cui viene attivato un avviso. Inoltre, spiegare l'effetto di alcune caratteristiche dei dati analizzati sulle predizioni può facilitare la trasformazione delle decisioni suggerite dal sistema di IA in conoscenza del dominio, favorendo la fiducia nei sistemi decisionali dalle parti interessate del processo (Andresini et al., 2022).

La richiesta di avvisi di sicurezza spiegabili, come per qualsiasi altra decisione basata sull'IA, è in linea con la visione emergente dell'Unione Europea, che estende il diritto alla spiegazione delineato dal GDPR anche all'IA e, in particolare, alle soluzioni basate su deep learning (Sartor & Lagioia, 2020), anche nel settore della sicurezza informatica. Attualmente, diverse tecniche di **eXplainable Artificial Intelligence (XAI) -** per esempio, SHAP, DALEX, LIME, Integrated Gradients, Grad-CAM e Attention - sono state esplorate nel campo della sicurezza informatica per spiegare decisioni (De Rose et al., 2024) e migliorare l'accuratezza dei sistemi di rilevamento delle minacce (*Andresini et al. 2022, Al-Essa et al., 2024*).

Inoltre, alcuni studi recenti hanno esaminato i progressi della XAI nell'ambito dell'IA offensiva (Kuppa & Le Khac, 2021) e, di conseguenza, dell'IA difensiva (Imran et al., 2024). Sebbene le tecniche XAI possano contribuire in modo sostanziale a migliorare l'accuratezza dei sistemi di IA per il rilevamento delle minacce e a fornire conoscenze utili sulle possibili firme degli attacchi informatici, aiutandoci a prevenire nuove minacce, i recenti progressi nell'ambito dell'IA offensiva hanno evidenziato vulnerabilità in diverse tecniche XAI, sollevando interrogativi sulla loro sicurezza e affidabilità. Negli ultimi anni, gli studi sulle vulnerabilità delle tecniche XAI stanno rapidamente attirando l'attenzione della comunità di IA e sicurezza. Alcuni ricercatori hanno iniziato lo sviluppo di metodi di difesa per mitigare le vulnerabilità di alcune **tecniche XAI** utilizzando approcci multipli, come la regolarizzazione di reti neurali, forzando la rete a rimanere invariata in presenza di perturbazione dei dati, aggregando spiegazioni prodotte da più metodi, introducendo una procedura di regolarizzazione per forzare attribuzioni robuste o tenere conto della robustezza nel processo di apprendimento e spiegazione (*Baniecki & Biecek, 2023*).

06. Conclusione

L'IA riveste oggi un ruolo cruciale nella sicurezza digitale, sia per le organizzazioni che per i singoli individui, grazie ai notevoli sviluppi conseguiti nel machine learning e deep learning che consentono l'analisi di grandi volumi di dati e la conoscenza utile per identificare e gestire comportamenti malevoli. Pertanto, l'IA è diventata uno **strumento indispensabile** a cui i professionisti della sicurezza non possono rinunciare. Tuttavia, non si tratta di una tecnologia che sostituisce tali professionisti bensì di un **approccio simbiotico** che prevede una collaborazione attiva **tra esperti di sicurezza** e **strumenti di IA** all'interno delle soluzioni di cybersecurity. L'obiettivo che ricerca, industria e governance deve continuare a perseguire è lo sviluppo di una tecnologia di IA difensiva in grado di identificare e disarmare l'IA offensiva non appena quest'ultima inizierà a eludere o avvelenare i modelli di IA. L'IA difensiva deve essere in grado di adottare micro-decisioni intelligenti per bloccare ogni tipo di attività sospetta, incluso quella creata con IA offensiva. Un altro elemento fondamentale per uno sviluppo etico dell'IA

Autrice

Annalisa Appice

Annalisa Appice è professoressa ordinaria di **Sistemi di Elaborazione dell'Informazione** all'Università di Bari Aldo Moro, dove insegna **Artificial Intelligence for Security**, **Analisi dei Dati per la Sicurezza** e **Metodi Avanzati di Programmazione**. È membro dei laboratori di ricerca **KDDE** e **CINI** su Cybersecurity, AI e Data Science.
Ha un dottorato in Informatica (2005) e ha svolto ricerca presso l'Università di Bristol e l'Istituto Jozef Stefan. I suoi interessi includono AI, Machine Learning, Deep Learning, Explainable AI e sicurezza informatica, con oltre 200 pubblicazioni su riviste e conferenze di alto livello. Infine, ha ricoperto ruoli di leadership in conferenze internazionali come ECML-PKDD, ISMIS e DS.

Riconoscimento automatico del volto e confronto in ambito forense

Autore: Giovanni Tessitore

01. Introduzione

I sistemi automatici di riconoscimento del volto hanno assunto un ruolo fondamentale nella nostra quotidianità. Si pensi al loro utilizzo nello sblocco degli smartphone, nel controllo automatico dei passaporti negli aeroporti o all'accesso sicuro ai conti bancari. Queste tecnologie non solo semplificano le nostre azioni, ma contribuiscono anche a garantire una maggiore sicurezza e protezione nelle transazioni e negli ambienti sensibili.

Rispetto alle attività condotte dalle forze di polizia, la costante diffusione dei sistemi di video-sorveglianza, installati soprattutto nelle aree urbane, ha reso sempre più frequente il potenziale impiego dei sistemi di riconoscimento per attribuire un' identità ad un volto ignoto o per la ricerca di un sospettato.

Nello specifico, esistono diversi scenari applicativi nei quali le forze di polizia possono impiegare sistemi automatici di riconoscimento facciale.

Il primo scenario, che chiameremo **Ricerca off-line** (o Confronto uno-a-molti), si concretizza quando, a seguito della commissione di un reato, le forze dell'ordine recuperano immagini dell'autore del reato da un sistema di video-sorveglianza che ha ripreso l'evento criminoso e ricercano queste immagini all'interno di una banca dati di soggetti con identità nota. Nello specifico, come vedremo nel seguito, la ricerca può essere effettuata all'interno della banca dati AFIS1 contenente le foto dei volti dei soggetti foto-segnalati a norma di legge. Il secondo scenario è la **Ricerca in tempo reale,** che si concretizza, ad esempio, per l'individuazione fisica di un soggetto sospettato di un grave reato, come un attacco terroristico o un omicidio. In questo contesto, un sistema di riconoscimento facciale - in tempo reale - può essere collegato alle telecamere di una zona circoscritta, come un aeroporto, e le foto disponibili del sospettato possono essere utilizzare per costruire una watch-list.

Il sistema di riconoscimento confronta, in tempo reale, i volti rilevati dalle telecamere con quelli presenti nella watch-list. Se un volto individuato nei video risulta sufficientemente simile a uno della lista, in base a un livello di somiglianza configurabile, viene generato un Alert.

Come vedremo, questi sistemi sono quelli che hanno sollevato negli ultimi anni le maggiori preoccupazioni in tema di privacy e diritti individuali e sono soggetti a restrizioni previste dal Regolamento UE sull'Intelligenza Artificiale (Artificial Intelligence Act).

Nella figura 1 è riportato uno schema riassuntivo degli scenari applicativi appena descritti.

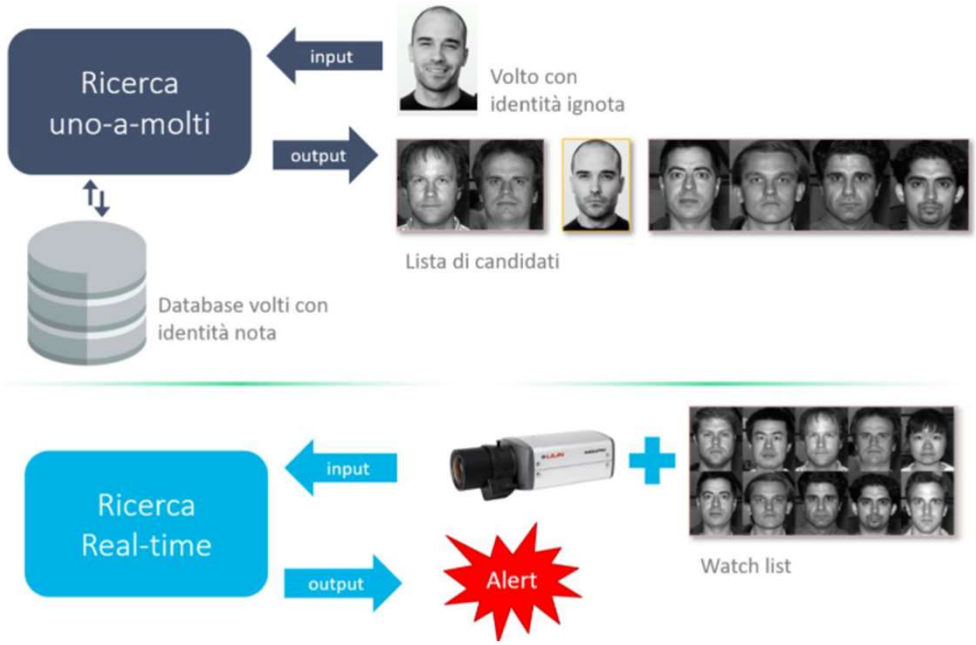


Figura 1: Nella ricerca off-line (confronto uno-a-molti) la singola foto di un soggetto di interesse viene ricercata all'interno di una banca dati di voti con identità nota. Nella ricerca real-time, invece, tutti i volti presenti in uno o più flussi video vengono confrontati in tempo reale e in maniera continua con i volti presenti in una Watch-list. Nel caso in cui uno dei volti del video raggiunga un punteggio di somiglianza rispetto a quelli presenti nella Watch-list superiore ad una certa soglia il sistema genera un Alert.

02. Il progetto S.A.R.I.

A partire dal 20162, il Servizio Polizia Scientifica ha sviluppato il progetto S.A.R.I. - Sistema Automatico Riconoscimento Immagini. Il progetto ha previsto la creazione di due componenti distinte e separate: SARI Enterprise e SARI Real-Time.

Il sistema SARI Enterprise permette di effettuare un confronto uno-a-molti attraverso la ricerca della foto del volto di un soggetto ignoto all'interno della banca dati AFIS della Polizia di Stato, costituita, ad oggi, da circa 20 milioni di foto (presenti sui cartellini fotosegnaletici) e circa 10 milioni di soggetti acquisite in adesione alla normativa vigente.

La soluzione SARI Enterprise è stata avviata in esercizio nel settembre del 2018 a seguito del provvedimento favorevole del Garante per la protezione dei dati personali n. 440 del 26.07.20183. È opportuno evidenziare che tale sistema non è connesso a telecamere di video-sorveglianza e le immagini da ricercare devono essere preventivamente individuate ed estrapolate dalle forze di polizia per poter essere successivamente ricercate.

Il SARI utilizza due algoritmi di riconoscimento facciale, di cui uno presente nella lista degli algoritmi testati dal NIST (National Institute of Standard Technology), denominato NeuroTechnology. Così come avviene nel caso di altri sistemi che sfruttano parametri biometrici (come le impronte digitali), il risultato di una ricerca uno-a-molti, effettuata mediante il SARI, è una lista di candidati ovvero una serie di

volti – in genere 50 – ordinati secondo un valore di similarità (score) rispetto al volto del soggetto di interesse.

È bene precisare che lo score non ha alcuna validità ai fini dibattimentali e la lista dei candidati è sempre verificata da un operatore, con specifica formazione, per individuare l'eventuale presenza di un soggetto con caratteristiche facciali assimilabili a quelle del volto ignoto. L'eventuale corrispondenza non ha alcuna conseguenza automatica, ma viene utilizzata dagli uffici operanti per il proseguo dell'attività investigativa.

Affinché una potenziale corrispondenza possa assumere valore probatorio, è necessario procedere ad un ulteriore accertamento tecnico chiamato comparazione fisionomica, descritto nel paragrafo successivo.

Un recente caso di cronaca - in cui il S.A.R.I. è stato impiegato con successo - è relativo all'individuazione del responsabile di un accoltellamento ai danni di una ragazza israeliana avvenuto nel 2022 all'interno della Stazione Termini di Roma. Il volto dell'aggressore fu ripreso dalle telecamere del sistema di videosorveglianza della stazione e, tramite il SARI, fu effettuata una ricerca all'interno della banca dati dei soggetti fotosegnalati. La lista di candidati fu analizzata dall'operatore di Polizia ed ha permesso di individuare, tra i cinquanta candidati restituiti dal sistema, l'identità del presunto responsabile. In questo caso, è risultato fondamentale sia il contributo dell'intelligenza artificiale presente negli algoritmi di ricerca del SARI, sia il contributo dell'operatore che è riuscito a individuare una potenziale corrispondenza.

03. Il confronto uno-a-uno (confronto fisionomico)

Nel contesto forense, il confronto fisionomico (o confronto del volto uno-a-uno) è un accertamento tecnico atto a stabilire il livello di corrispondenza tra due volti ed è eseguito manualmente da un operatore esperto, seguendo procedure internazionali basate su una tecnica nota come analisi morfologica.

Questo accertamento permette di valutare il grado di corrispondenza tra il volto di un individuo ignoto e quello di un sospettato (in genere con identità nota), esprimendo un giudizio soggettivo su una scala di valori [ENFSI 2018]. Sebbene il riconoscimento facciale sembri un'abilità comune, vi è una grande differenza tra il riconoscere (e quindi confrontare) volti familiari (parenti, amici, celebrità) e volti non familiari, per i quali l'accuratezza è generalmente bassa [Bruce et al. 1999].

Nel contesto forense, metodi come il confronto olistico, che implica semplicemente "guardare" due volti nel loro insieme, la sovrapposizione e l'analisi antropometrica basata sul confronto delle misurazioni delle diverse parti del volto, sono sconsigliati [ENFSI 2018]. Si preferisce, invece, la comparazione morfologica, che analizza singolarmente le caratteristiche facciali evidenziandone somiglianze e differenze. Per strutturare e documentare il processo, si utilizza una checklist di caratteristiche, come quella sviluppata dal *Facial Identification Scientific Working Group* (FISWG), adottata in Europa e negli Stati Uniti. Studi empirici confermano che questo approccio migliora l'accuratezza del confronto [Towler et al. 2017]. Dal 2018, la Polizia Scientifica ha uniformato a livello nazionale le proprie linee guida per il

confronto fisionomico, basandosi sulle Best Practices ENFSI. Il giudizio finale si esprime su una scala di sette livelli: tre positivi, tre negativi e uno inconcludente.

Scala di Valutazione del Confronto Fisionomico		
+3	Sostegno estremamente forte	**Ipotesi Accusatoria** (immagini del volto ignoto e del sospettato appartenente allo stesso soggetto)
+2	Sostegno forte	
+1	Sostegno moderato	
0	Nessun sostegno	
-1	Sostegno moderato	**Ipotesi Difensiva** (immagini del volto ignoto e del sospettato appartenenti a soggetti diversi)
-2	Sostegno forte	
-3	Sostegno estremamente forte	

04. I sistemi biometrici remoti real-time

La componente SARI Real-Time permette l'analisi - in tempo reale - dei flussi video provenienti da una o più telecamere, al fine di generare un Alert nel caso in cui uno dei volti presenti nei video analizzati sia sufficientemente simile ad uno dei volti caricati nella c.d. watch-list. Quest'ultima contiene un elenco di foto di soggetti da attenzionare.

Riguardo al sistema SARI Real-Time va specificato che si tratta di un'unica soluzione tecnologica, completamente separata da altri sistemi (compreso il SARI Enterprise), da installare temporaneamente e in una zona spazialmente limitata. L'impiego di tale sistema sarebbe sempre circoscritto ad un periodo limitato nel tempo e ad un'area di interesse ristretta e ben delineata, ove sarebbero state installate, in maniera momentanea e disgiunta da qualsiasi altro impianto di videosorveglianza, un numero massimo di 10 telecamere connesse direttamente all'infrastruttura. In esito all'esame della "valutazione di impatto sulla protezione dei dati personali (DPIA)", il Garante, con provvedimento n. 127 del 25.03.2021, ha espresso parere negativo all'utilizzo del sistema; conseguentemente, il sistema SARI Real-Time non mai è entrato in esercizio.

I sistemi di riconoscimento facciale real-time rientrano nella categoria dei sistemi di identificazione biometrica remota (RBI). Questi sistemi quando impiegati in luoghi pubblici e per scopi di Law Enforcement sono classificati, dal regolamento europeo sull'intelligenza artificiale,4 come pratica di AI proibita. Tuttavia, sono previste delle eccezioni che ne permettono comunque

'impiego sebbene limitato nel tempo e nel luogo nei casi di: ricerche mirate di vittime (rapimento, traffico, sfruttamento sessuale), prevenzione di una minaccia terroristica specifica e attuale, o localizzazione o identificazione di una persona sospettata di aver commesso uno dei reati specifici menzionati nel regolamento (tra cui terrorismo, traffico di esseri umani, omicidio, stupro). Va specificato che è prevista una preventiva autorizzazione da parte dell'autorità giudiziaria.

05. Conclusioni

L'impiego dei sistemi di riconoscimento facciale in ambito forense rappresenta un'evoluzione tecnologica di grande rilevanza per le attività investigative, ma solleva al contempo questioni di natura tecnica, giuridica ed etica. Strumenti come il SARI Enterprise hanno già dimostrato la loro utilità nel supportare le forze di polizia nell'identificazione di sospettati, garantendo sempre la verifica umana. Il confronto fisionomico rimane un elemento chiave per assicurare che le analisi biometriche condotte - attraverso il SARI - siano affiancate da una valutazione esperta, evitando decisioni automatizzate prive di controllo. Per quanto riguarda l'impiego di sistemi di riconoscimento facciale in tempo reale - come nel caso del SARI Real-Time -, negli ultimi anni le valutazioni negative del Garante per la Protezione dei Dati Personali ne hanno impedito l'uso. Tuttavia, la recente approvazione del Regolamento UE sull'Intelligenza Artificiale riapre la possibilità di utilizzo di tali sistemi. La normativa europea impone restrizioni severe sull'uso delle tecnologie di riconoscimento facciale (in tempo reale) negli spazi pubblici per finalità di law enforcement, ma prevede alcune eccezioni che ne permettono l'utilizzo in situazioni particolari, pur sempre con l'autorizzazione dell'autorità giudiziaria

Nel prossimo futuro, le principali sfide riguarderanno l'affidabilità e la trasparenza di questi sistemi, in particolare per quanto concerne l'interpretabilità degli algoritmi di deep learning alla base del riconoscimento facciale. La necessità di bilanciare sicurezza, diritti fondamentali e garanzie procedurali sarà cruciale per garantirne un utilizzo etico e conforme alle normative vigenti.

Autore

Giovanni Tessitore

Giovanni Tessitore, con una laurea in Informatica e un dottorato di ricerca in Scienze Computazionali e Informatiche conseguito presso l'Università degli Studi di Napoli "Federico II", ha maturato esperienza nell'elaborazione di immagini e nell'apprendimento statistico durante gli studi di dottorato e i successivi anni di ricerca presso la stessa università.

Attualmente ricopre il ruolo di **Direttore della Sezione Investigazioni Elettroniche della IV Divisione del Servizio di Polizia Scientifica**, dove sovrintende, tra le altre responsabilità, alle attività di analisi ed elaborazione di immagini e video, tra cui la comparazione facciale e antropometrica, il miglioramento di immagini e video e l'implementazione di sistemi di riconoscimento facciale automatico.

Caratteristiche dei Firewall

Autore: Fabrizio D'Amore

01. Introduzione

Un **firewall** è un **sistema di sicurezza** fondamentale per proteggere le reti informatiche, sia a livello **personale** che **aziendale**. Esso funge da difesa primaria contro una vasta gamma di minacce provenienti dall'esterno, assicurando che i dati sensibili e le risorse della rete rimangano protetti. La sua funzione principale è quella di agire come una barriera tra una rete interna, come una rete aziendale, scolastica o domestica, e il mondo esterno, rappresentato da Internet e altre reti non affidabili. Questo sistema analizza, filtra e regola il flusso di traffico in base a criteri specifici, assicurando che solo le connessioni sicure e autorizzate possano attraversare i confini della rete.

Il controllo effettuato dal firewall avviene attraverso una serie di regole configurabili, che definiscono quali tipi di traffico possono essere accettati o rifiutati. Queste regole possono essere personalizzate per adattarsi alle esigenze specifiche di un'organizzazione o di un individuo, offrendo un elevato grado di flessibilità e sicurezza. Ad esempio, è possibile bloccare determinati indirizzi **IP**, porte o protocolli che potrebbero rappresentare una minaccia o limitare l'accesso a siti web non appropriati o potenzialmente pericolosi.

Oltre al semplice filtraggio del traffico, i firewall moderni offrono una serie di funzionalità avanzate che vanno ben oltre il loro scopo originario. Possono includere la rilevazione e prevenzione delle intrusioni (**IDS/IPS**), la protezione contro malware e attacchi di tipo **DDoS** (**Distributed Denial of Service**) e il controllo delle applicazioni. Questi strumenti aggiuntivi rendono il firewall una componente essenziale di qualsiasi **strategia** di **sicurezza informatica**, contribuendo non solo a proteggere la rete, ma anche a monitorarla e gestirla in modo proattivo. In un mondo sempre più interconnesso, in cui le minacce informatiche sono in costante evoluzione, l'implementazione di un firewall efficace è diventata una **necessità imprescindibile**.

Controllo del Traffico

un firewall **monitora** e **regola** tutto il traffico che transita tra una rete interna e una rete esterna, **bloccando** o **consentendo** il passaggio in base a regole definite.

Limitazioni

I firewall, pur essendo utili, **non offrono una protezione completa**: non possono bloccare attacchi interni senza configurazioni specifiche e non contrastano malware mirati senza aggiornamenti delle regole.

02. Tipologie di Firewall

I firewall non sono tutti uguali e funzionano in modi diversi per rispondere a esigenze specifiche di sicurezza.

Di seguito vengono analizzati le **principali tipologie** di firewall.

Packet Filtering Firewall

È il tipo di firewall più semplice. Funziona controllando ogni pacchetto dati che entra o esce dalla rete in base a criteri specifici come l'indirizzo IP, porte e protocolli utilizzati.

Questa tipologia è veloce ed efficace per compiti base, ma poco sofisticato, poiché non considera lo stato delle connessioni e potrebbe non rilevare attacchi camuffati da traffico legittimo.

Stateful Inspection Firewall

Questa tipologia di firewall funziona tenendo traccia delle connessioni attive, verificando che il traffico in entrata sia effettivamente autorizzato. Questo lo rende più sicuro rispetto ai semplici filtri di pacchetti, ma il monitoraggio continuo delle connessioni può consumare risorse, causando rallentamenti su reti molto grandi.

Application Level Gateway

Questa tipologia di firewall funziona a un livello superiore rispetto ai firewall tradizionali, analizzando i dati all'interno delle connessioni per garantirne la sicurezza. Offre un'elevata sicurezza, grazie alla capacità di esaminare il contenuto del traffico e richiedere autenticazioni, ma è complesso da configurare, richiede molta potenza di calcolo e può rallentare il traffico.

Circuit Level Gateway

Questo firewall verifica la validità delle connessioni, permettendo solo quelle autorizzate a livello di circuito. Offre vantaggi come basso overhead e controllo sufficiente per molte esigenze, ma manca di un'analisi approfondita del contenuto, rendendolo meno sicuro contro certi attacchi.

Firewall Basato su Host

Questo firewall protegge singoli dispositivi indipendentemente dalla rete utilizzata. Offre dunque protezione personalizzabile per ciascun dispositivo ma non è in grado di proteggere l'intera rete o modificare le regole di un firewall centrale.

03. IPtables

Nel panorama Linux uno degli strumenti più utilizzati è **iptables**, un software open source per amministratori di sistema/rete che può essere usato in quasi tutte le distribuzioni per rispondere ad esigenze di *firewalling* e non solo. Iptables rappresenta il meccanismo attraverso il quale possiamo definire regole di sicurezza che controllano il traffico di rete in entrata, in uscita e in transito attraverso un dispositivo. Di seguito, vengono riportate le principali funzionalità dello strumento iptables.

Controllare l'accesso al sistema: Attraverso l'uso di regole, possiamo determinare quali tipi di connessioni possono essere stabilite verso o dal sistema.

Traffic filtering: Le regole di iptables possono definire criteri dettagliati per accettare o bloccare pacchetti di dati basati su parametri come l'indirizzo IP di origine, l'indirizzo di destinazione, il protocollo utilizzato e le porte.

Iptables utilizza una tabella (filter) con catene di regole: INPUT, FORWARD, e OUTPUT, che gestiscono il traffico in entrata, di transito e in uscita. Le regole nelle catene vengono esaminate in sequenza; se un pacchetto corrisponde a una regola, viene eseguita l'azione associata (ad esempio, **ACCEPT** o **DROP**). Se nessuna regola corrisponde, si applica la politica predefinita della catena.

Di seguito vengono riportati alcuni esempi pratici di configurazione tramite iptables:

Bloccare il traffico su un'interfaccia

Iptables- A FORWARD –i eth0 –j DROP: blocca il traffico su eth0

Consentire connessioni già stabilite

iptables -A FORWARD -i eth0 -m state --state ESTABLISHED -j ACCEPT: consente pacchetti di connessioni autorizzate

Abilitare traffico HTTP verso un server

iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.58 -o eth1 -p TCP --dport 80 -j ACCEPT: connessioni HTTP verso un server

Limitare richieste ICMP

iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/s -i eth0 -j ACCEPT: accetta massimo un ping al secondo

Regole stateful per connessioni TCP

Iptables –A INPUT –P tcp –dport 80 –m state –state NEW, ESTABLISHED –J ACCEPT: permette connessioni sulla porta 80

Consentire traffico di loopback

iptables -A INPUT -i lo -j ACCEPT: consente traffico interno alla macchina

04. Problemi e sfide dei firewall

Di seguito vengono riportate alcune problematiche e sfide inerenti ai firewall:

- **Configurazioni complesse**: aumentano il rischio di errori di configurazione che possono compromettere la sicurezza.
- **Software vulnerabile:** i firewall non correggono falle di sicurezza del software installato sulla rete interna, come bug che possono essere sfruttati per eseguire attacchi.
- **Attacchi di tipo Denial-of-Service (DoS)**: i firewall offrono solo una protezione limitata contro questo tipo di attacchi, specialmente se il traffico di attacco riesce a sovraccaricare il firewall stesso.

In conclusione, i firewall sono strumenti essenziali per la sicurezza di rete, offrendo un'ampia gamma di funzionalità per controllare il traffico e proteggere le reti interne. Tuttavia, la loro efficacia dipende dalla corretta configurazione e dalla capacità di adattarsi alle nuove tecnologie.

Autore

Fabrizio D'Amore

Fabrizio D'amore è **professore universitari**o di **sistemi di elaborazione delle informazioni** presso l'Università «La Sapienza> di Roma. Esperto di **algoritmi** e **sicurezza**, dirige il master di secondo livello in **Sicurezza Informatica e Informazione Strategica**, in collaborazione con il **DIS** della Presidenza del Consiglio dei Ministri. Esperto in tutti i temi della cybersecurity, negli ultimi anni è stato spesso ingaggiato come **consulente di supporto** al management su temi informatici, semplificando i dettagli puramente tecnici e sottolineando le questioni più importanti per i decisori. Ha assistito le più importanti aziende **pubbliche** e **private** nella definizione di **strategie** per la sicurezza informatica, la **privacy** e la **protezione dei dati**. Esperto di **crittografia**, **protezione delle email**, **watermarking** dei documenti, aiuta le aziende a definire piani operativi per la sicurezza, nel rispetto del GDPR per evitare le onerose sanzioni previste in caso di **data breach**. Fabrizio D'Amore ha riconosciute capacità **divulgative** ed è un esperto formatore su ogni aspetto dell'informatica. Opera come **libero professionista** con partita IVA (con incarico diretto previa autorizzazione dell'Università) o tramite l'Università con una maggiorazione del 25%, come referente di quest'ultima, avvalendosi eventualmente di altri professionisti altamente qualificati.

Incidenti cyber in ambienti Enterprise

Autore: Mario Beccia

01. Introduzione

La **trasformazione digitale**, proponendo un aumento di produttività basato sulla maggiore automazione di processo, ha generato un più che corrispondente aumento della dipendenza dal cyberspazio nelle società occidentali. Questa dipendenza ha generato un aumento esponenziale del rischio cyber: le reti informatiche divengono di importanza cruciale per la vita privata e per il business.

Il cyberspazio è caratterizzato da una forte asimmetria fra **attaccante** (ovvero un operatore con intenti malevoli) e **difensore** (ovvero un operatore che controlla e difende una rete informatica). In altri termini, l'investimento di un difensore (in termini di tempo e risorse) è superiore di diversi ordini di grandezza rispetto a quello di un attaccante. Questa asimmetria comporta **diversi effetti collaterali**, quali ad esempio: la relativa semplicità degli **skill** necessari per un attaccante rispetto alla complessità di quelli necessari per un difensore; la quantità di risorse finanziarie necessarie per portare attacchi efficaci rispetto a quelle (**enormemente superiori**) necessarie per assicurare una security posture adeguata; la semplicità con cui un attaccante può nascondere le proprie tracce rispetto alla **complessità dell'analisi forense** e dell'attribuzione di attacchi informatici. Questo articolo esplora le complessità della gestione di incidenti di cyber su larga scala in organizzazioni pubbliche o private di grandi dimensioni, fornendo una panoramica completa delle problematiche più comuni e delle strategie per affrontarle.

Vengono esaminati alcuni **aspetti tecnici** della risposta agli incidenti, ma lo scopo è di guardare specificamente a questioni organizzative, comunicative e strategiche che spesso sono cruciali per il successo o il fallimento della gestione di un incidente.

Cyberspazio (cyberspace)

ambiente digitale costituito dalla **interconnessione** fra reti, servizi, sistemi, persone, processi, organizzazioni, pubblici (e.g. Internet) o privati, che risiedono nell'ambiente digitale o lo attraversano

Cybersicurezza (cybersecurity):

la salvaguardia di **persone**, **società**, **organizzazioni** e **intere nazioni** da rischi cyber. In questo contesto, "salvaguardia" si intende come mantenere il rischio cyber ad un livello tollerabile.

Incidente Cyber (cyber incident) :

evento che **compromette** la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi , producendo **effetti diretti sull'organizzazione stessa** e/o su altri **stakeholders** ad essa collegati. Gli incidenti cyber possono influire su vari aspetti del ciclo di **business**, e la loro gestione può assumere tratti estremamente diversi a seconda della dimensione dell'organizzazione che ne è vittima.

02. Incidenti su larga scala

L'uso delle **tecnologie** di **comunicazione** moderne su larga scala costituisce un fattore abilitante per qualsiasi organizzazione, grande o piccola che sia, e consente l'esecuzione dei processi di business con un livello di efficienza enormemente superiore a quanto poteva essere osservato solamente 10 anni fa. Casi di successo come **Amazon** (ed in particolare l'efficienza raggiunta dalla sua logistica), **Airbnb** (l'efficienza raggiunta dal suo sistema di booking e customer care) e Apple (e la pervasività raggiunta dal suo **AppStore**) testimoniano come queste tecnologie possano produrre profitto e in generale aumentare enormemente la produttività degli utenti. Questo implica una dipendenza estrema dall'operatività dell'infrastruttura IT adottata da queste organizzazioni: qual è il danno prodotto dalla ridotta o completa indisponibilità del sistema logistico di Amazon a livello mondiale? O il danno di immagine (e la responsabilità legale) prodotto dalla perdita dei dati personali dei clienti di Airbnb? O quello prodotto dalla presenza di un virus in un'applicazione distribuita dall'AppStore di Apple?. Questi banali **esempi di incidente cyber** portano alla luce almeno due fattori rilevanti per il tema di questo articolo riportati di seguito.

1) La necessità di un approccio sistemico alla gestione degli incidenti

Con effetti potenziali così ampi, ed in un contesto dove una singola organizzazione non può **organizzare economicamente** i mezzi per affrontare correttamente le minacce cyber, è necessario un approccio sistemico in cui ogni singola organizzazione può contare sul supporto di operatori pubblici e privati in caso di bisogno. In altri termini, il lavoro portato avanti da **organizzazioni internazionali** (Unione Europea, Nazioni Unite, etc.) e **nazionali** a vari livelli diviene essenziale per supportare il settore privato e i singoli cittadini nella gestione delle minacce cyber

2) La dimensione del danno

Le società occidentali sono largamente **dipendenti dai servizi erogati da operatori pubblici e privati** attraverso le reti di telecomunicazione. Non si tratta solamente di perdita di efficienza e/o di profitto, ma anche e soprattutto di effetti di secondo e terzo ordine che impattano interi sistemi economici, a livello nazionale e/o sovranazionale

Queste considerazioni sono alla base delle azioni intraprese da varie organizzazioni internazionali per stimolare un maggiore sensibilità a questi elementi. Ad esempio, negli ultimi anni l'Unione Europea ha approvato direttive di rilievo come il **GDPR**, la NIS (e la recente **NIS2**). Nella stessa direzione vanno i decreti legislativi adottati negli ultimi anni in Italia a proposito del perimetro di **sicurezza cibernetica** e della creazione dell'Agenzia di Cybersicurezza Nazionale.

03. Elementi distintivi chiave

Il **livello di complessità degli incidenti di sicurezza** diviene rilevante in grandi organizzazioni pubbliche o private, dove gli elementi seguenti hanno un ruolo chiave:

Gestione del rischio. La gestione di incidenti dovrebbe sempre essere orientata dall'**analisi** e **gestione del rischio** generato dall'incidente. Le competenze e la sensibilità necessaria a interpretare gli eventi generati da un incidente cyber in questa ottica sono rare e spesso vengono poste in secondo piano rispetto ad obiettivi immediati, quali il ripristino dei processi aziendali e la tutela della reputazione dell'organizzazione.

Complessità infrastruttura ICT. L'incremento nella **qualità** e **quantità** di **servizi** offerti all'utenza ha generato una grande quantità di applicazioni, piattaforme e dispositivi interconnessi. Questi sistemi sono spesso il risultato di anni di **sviluppo**, in gran parte "organico" (ovvero non gestito in maniera strategica), che ha portato alla creazione di un ecosistema frammentato e con diversi grandi di **maturità**.

Integrazione con altre Organizzazioni. Il livello di integrazione fra diverse organizzazioni aziendali (ad esempio, appartenenti alla stessa supply chain) implica una serie di **interdipendenze** e effetti incrociati durante la gestione di un incidente. La gestione di questo elemento richiede professionalità e sensibilità raramente disponibili in un contesto aziendale non specializzato.

Scala del potenziale impatto. La gestione di incidenti dovrebbe sempre essere orientata dall'analisi e gestione del rischio generato dall'incidente. Le **competenze** e la **sensibilità** necessaria a interpretare gli eventi generati da un incidente cyber in questa ottica sono rare e spesso vengono poste in **secondo piano** rispetto ad obiettivi immediati, quali il ripristino dei processi aziendali e la tutela della **reputazione** dell'organizzazione.

Team e responsabilità distribuite. Le responsabilità per la **sicurezza ICT** sono distribuite e frammentate tra team e dipartimenti diversi, spesso con **interpretazioni** diverse e contrastanti di ciascuna area di competenza. Ciò può portare a problemi di **coordinamento** e **comunicazione**, e alla **perdita** di un centro unico di responsabilità durante la gestione di un incidente.

Requisiti di Compliance. La gestione dei dati attraverso reti ICT deve seguire una varietà di **normative**, fra cui quelle sulla **protezione dei dati** e sulla **sicurezza delle informazioni**. La gestione degli incidenti deve tenere conto di questi **requisiti normativi**, che possono variare a seconda del **settore** e della **giurisdizione**.

04. Gestione del rischio

La **gestione del rischio** durante un incidente di cybersecurity differisce dalla gestione del rischio in condizioni normali per la sua natura dinamica e per i ridotti tempi decisionali. L'obiettivo è **bilanciare la necessità di azioni rapide** con una **valutazione ponderata degli impatti** di ogni decisione sui processi di business e considerando gli effetti di primo, secondo e terzo livello. Durante la gestione di un incidente, la disponibilità di strumenti adeguati è **essenziale** per una valutazione **rapida** e **efficace**: questi devono essere predisposti e testati specificamente nella fase di preparazione, ovvero fuori dal contesto operativo di gestione di un incidente.

Struttura decisionale rapida ed efficiente, basata su:

- una **catena di comando** chiara per decisioni legate al rischio;
- la definizione di **soglie di rischio** per l'escalation delle decisioni ai livelli superiori;
- l'implementazione di un **processo di revisione** per le decisioni più critiche.

Analisi costi-benefici in tempo reale, che richiede a sua volta:

- meccanismi di **valutazione** rapida dei costi delle azioni di mitigazione (rispetto ai costi di potenziali danni);
- la considerazione degli **effetti** di secondo e terzo ordine;
- il **bilanciamento** della necessità di un'azione rapida con i suoi effetti.

Utilizzo di scenari e simulazioni, basati su:

- Preparare in **anticipo** scenari di rischio per **guidare** il processo decisionale
- Utilizzare simulazioni in **tempo reale** per valutare l'**impatto** potenziale delle decisioni
- Aggiornare **continuamente** gli scenari in base alle nuove informazioni **emergenti**

Monitoraggio e adattamento continuo, ad esempio usando le tecniche seguenti:

- monitoraggio in tempo reale, usando dashboard e **Key Risk Indicators (KRI)** creati specificamente per l'incidente;
- adattamento delle **strategie** di **mitigazione**, rivedere e adattare le strategie di mitigazione in base ai feedback e ai **risultati** osservati, in particolare quando l'incidente evolve in direzioni completamente inaspettate.

Comunicazione continua del livello di rischio, ad esempio:

- fornendo **aggiornamenti** regolari sullo stato del rischio agli stakeholder chiave;
- adattando la **comunicazione del rischio** in base all'audience (es. management, team tecnico, clienti);
- utilizzando **tool specifici** per comunicare rapidamente stato e trend

05. Analisi del rischio

L'**analisi del rischio** durante la gestione di incidenti risente fortemente della scarsità e **imprecisione delle informazioni** generate e condivise durante la gestione, e richiede una sensibilità e una professionalità specifica. Le **tecniche** per l'identificazione dei rischi sono:

- utilizzo di **checklist** predefinite per una rapida identificazione dei rischi più comuni;
- implementazione di **strumenti di analisi** per rilevare anomalie e potenziali minacce;
- coinvolgimento di vari **livelli aziendali** con varie professionalità (ICT, sicurezza, operations, legal) per una **valutazione completa del rischio.**

Una volta identificati i **rischi** emergenti dall'incidente, questi devono essere categorizzati per assicurare una gestione più efficiente. Ad esempio, possono essere utilizzate le categorie, quali: rischi di **sicurezza** (es. perdita di dati, compromissione di sistemi), **operativi**, **legali** e di **compliance**, **reputazionali** e **finanziari**. Ciascuna categoria di rischio richiede professionalità e sensibilità specifiche per arrivare ad una valutazione adeguata di **impatti** e **probabilità**. Durante un incidente cyber, le strategie di gestione del rischio si riducono a:

Trasferimento

comporta il **trasferimento** degli **effetti** della manifestazione del rischio ad un altro operatore, tipicamente usando una **polizza assicurativa** oppure trasferire temporaneamente in outsourcing un processo.

Accettazione

Una **decisione strategica** che si basa sull'accettazione degli **impatti** quantificati e della probabilità che il rischio si manifesti. In molti casi, durante un incidente l'accettazione è l'unica strategia possibile per procedere nella gestione dell'incidente

Mitigazione

Mitigare un rischio implica **identificare** una o più **azioni** per limitare l'impatto o la probabilità che esso si manifesti. Mitigare un rischio durante la gestione di un incidente può comportare l'uso di una o più tecniche quali: **contenimento** immediato, **misure di isolamento**, attivazione di **piani di continuità operativa**, applicazione di **patch di sicurezza**, prioritizzazione di attività per la **protezione di asset critici**, etc.

Chiusura

La gestione del rischio non termina con la chiusura dell'incidente, ma richiede diverse **considerazioni** sull'**efficacia** delle attività di risposta, eventuali **miglioramenti** sulla gestione, aggiornamento del **risk posture** ed eventuali **misure addizionali di sicurezza** da mettere in atto per aumentare la **resilienza.**

06. Rilevamento e gestione

Ogni incidente è unico e richiede una **gestione dedicata**. L'entità degli effetti di un incidente non corrisponde necessariamente con l'evidenza con cui lo stesso si manifesta, in particolare durante le fasi iniziali. Incidenti che originano direttamente nel cyberspazio (ad esempio, legati ad una vulnerabilità software o legati all'azione di un **Threat Actor** particolarmente sofisticato) possono essere particolarmente difficili da rilevare.

Cisco Systems riportava nel **2016** un **tempo medio di 240 giorn**i per la rilevazione, ovvero un intervallo di 240 giorni fra il momento in cui un Threat Actor completava l'infiltrazione in un'organizzazione e il momento in cui l'infiltrazione veniva rilevata. Anche se ad oggi questo tempo medio è più breve (si parla di un **intervallo inferiore** ai **100 giorni**), questo fattore è indice della complessità con cui alcuni incidenti vengono rilevati. In altri casi (ad esempio, attacchi **DDoS**), un incidente può essere più evidente e comportare un'attivazione immediata del processo di gestione.

In generale, la **gestione di un incidente cyber** implica un ciclo composto di **tre fasi.**

1) PREPARAZIONE

In questa fase si predispongono **strumenti** e **risorse adeguati** (in particolare risorse umane, tecnologiche e di processo). Il livello di preparazione, l'investimento necessario, la tempistica ed altri fattori sono **direttamente proporzionali** al ***risk appetite*** dell'organizzazione.

2) GESTIONE

Il processo vero e proprio di gestione di un incidente si basa sugli **elementi predisposti nella fase precedente**, e dipende fortemente dalla loro qualità

3) RECUPERO

Alla gestione vera e propria segue una fase dove gli effetti di secondo e terzo livello vengono gestiti e un ulteriore **crescita nel livello di maturità cyber** viene pianificato e preparato per l'esecuzione.

Il rilevamento accurato ed efficace di un incidente è essenziale e dipende strettamente dalla **qualità** della **preparazione** effettuata: durante la gestione di un incidente, gli strumenti predisposti dall'organizzazione sono costanti e costituiscono il vero limite all'efficacia della gestione.

Problemi e opportunità di **miglioramento** osservati durante la **gestione** costituiscono un elemento di crescita essenziale e devono essere rilevati e gestiti accuratamente. Una volta rilevato un incidente, il primo passo è l'attiv**azione del processo di gestione del rischio**, basato sulla valutazione di impatto e il suo costante aggiornamento. Questo processo dovrebbe essere standardizzato e basato su criteri predefiniti che considerino fattori come il tipo di sistemi interessati, la sensibilità dei dati coinvolti e il potenziale impatto sull'operatività aziendale.

Il team di gestione dell'incidente

La costituzione del **team** di gestione dell'incidente è essenziale e dovrebbe derivare da una preparazione adeguata, dove la struttura del team di gestione e le principali linee di intervento vengono definite in dettaglio. Il team porta avanti le operazioni di gestione basandosi su criteri di gestione del rischio: ogni azione, ogni decisione deve essere valutata e adottata in base all'impatto sulla risk posture e considerando il risk appetite delle Organizzazioni, monitorando in modo costante l'impatto seguendo i principi indicati nel capitolo precedente. Data la complessità dell'ecosistema di riferimento e dell'impatto di incidenti di larga scala, il team deve lavorare in **parallelo** su diverse linee di intervento. Ogni linea di intervento viene costituita con un obiettivo specifico e richiede un team dedicato. In alcuni casi, possono essere costituiti team specifici dedicati a ciascuna linea, sotto il coordinamento del team principale.

Analisi tecnica

Analisi degli **elementi tecnici** legati all'incidente, ad esempio analisi del malware rilevato, analisi forense.

First Response

Definizione delle **azioni tecniche** di **risposta**, quali isolamento di un host o di un'intera rete, riconfigurazione di apparati di rete, modifica delle regole di IPS o IDS, etc.

Comunicazione Interna

Definizione delle **linee di responsabilità** interne e dei processi di aggiornamento e integrazione fra diversi livelli di responsabilità aziendale.

Compliance

Monitoraggio degli **effetti dell'incidente** e delle azioni intraprese per gestirlo, in ottica di **compliance** con **regolamentazione nazionale** e **internazionale**.

Analisi dell'impatto

Monitoraggio costante degli **effetti dell'incidente sui processi di business** e impatti diretti, con possibile quantificazione economica.

Rispetto della Compliance

Verifica costante della compliance con **policy interne**, **schemi legislativi** e **framework** legali. Non soltanto gli effetti dell'incidente ma le azioni intraprese per la sua gestione potrebbero avere **impatto** sulla compliance.

Ogni incidente è unico e può richiedere solo alcune delle linee indicate, ovvero altre che possono essere identificate in base alla situazione o al contesto organizzativo.

La costituzione del team in tempi brevi e con le professionalità necessarie è un fattore essenziale per il successo della gestione dell'incidente.

La gestione tecnica

La gestione tecnica di un incidente può assumere dimensioni rilevanti e richiedere professionalità e strumenti dal costo rilevante. Il mercato ICT offre varie possibilità per integrare le risorse disponibili all'intero dell'organizzazione con operatori esterni, che devono essere considerate appropriatamente dal management.

La **complessità** di queste considerazioni e della gestione tecnica degli incidenti va al di là degli obiettivi di questo articolo, ed è qui limitata alle considerazioni seguenti:

L'indagine sull'incidente e l'analisi delle cause principali sono passi fondamentali nel processo di gestione. Il technical investigator deve raccogliere ed analizzare un ampio spettro di informazioni per comprendere la natura e l'estensione dell'incidente.

Le **strategie di contenimento** variano a seconda del tipo di incidente e del risk appetite dell'organizzazione. In alcuni casi, **l'isolamento immediato** dei sistemi affetti potrebbe essere uno step essenziali; in altri, invece, potrebbe comportare **conseguenze** troppo ampie.

L'eradicazione rappresenta una fase cruciale nella gestione delle minacce informatiche, poiché implica la rimozione completa del malware identificato o la chiusura dei punti di accesso sfruttati dal Threat Actor per penetrare nel sistema.
Questo processo richiede un'analisi dettagliata e l'implementazione di misure tecniche specifiche per garantire che non rimangano tracce della minaccia all'interno della rete.
Spesso, l'eradicazione comporta anche il ripristino dei sistemi compromessi e **l'aggiornamento** delle **configurazioni** di sicurezza per prevenire futuri attacchi dello stesso tipo.

Tuttavia, in molti casi non è possibile raggiungere una certezza assoluta sull'avvenuta eradicazione, soprattutto quando il malware utilizza tecniche avanzate di offuscamento o mantiene una presenza latente nel sistema. Questa **incertezza** rende indispensabile un approccio strutturato alla gestione del rischio, che includa il monitoraggio continuo delle attività di rete, la verifica dell'integrità dei sistemi e l'adozione di strategie di mitigazione per ridurre l'impatto potenziale di eventuali residui dell'attacco.

07. Effetti di secondo e terzo ordine

Nell'ambito della **gestione** degli **incidenti** di cybersecurity, è fondamentale considerare non solo gli impatti immediati e diretti (effetti di primo ordine), ma anche quelli che si manifestano successivamente e in modo **indiretto** (effetti di secondo e terzo ordine). Un incidente di cybersecurity può avere effetti che si propagano ben oltre l'impatto iniziale, influenzando vari **aspetti** dell'organizzazione e dei suoi **stakeholder**. Ad esempio, gli effetti sulla supply sono particolarmente importanti in un mondo interconnesso. Un incidente può influenzare fornitori, partner e clienti, creando un effetto domino che richiede una gestione attenta e puntuale. La valutazione dei **danni reputazionali** è un altro aspetto critico spesso sottovalutato: un incidente mal gestito può danneggiare la fiducia dei clienti e degli stakeholder, con conseguenze a lungo termine per il business.

Questa visione più ampia permette una **gestione** più **efficace** e **completa** dell'incidente, ed assicura una preparazione più efficace per gestire incidenti futuri. Oltre a specifici effetti diretti dell'incidente, si possono quindi distringere gli effetti seguenti:

EFFETTI DI SECONDO ORDINE

Sono **effetti indiretti** che derivano specificamente dall'incidente o dalle azioni intraprese per gestirlo, e si manifestano generalmente a breve o medio termine. Ad esempio:

Interruzione della supply chain

Un attacco che compromette i **sistemi** di **gestione** degli ordini potrebbe causare ritardi nelle consegne ai clienti o nell'approvvigionamento di materie prime.

Perdita di produttività

Le **misure di contenimento**, come la disattivazione di **sistemi critici**, possono portare a una significativa riduzione della produttività aziendale.

Danno reputazionale immediato

La notizia dell'incidente può causare una **perdita immediata di fiducia** da parte dei clienti e dei partner commerciali.

Costi imprevisti

L'implementazione di **misure di sicurezza aggiuntive** o l'assunzione di consulenti esterni può comportare spese impreviste.

EFFETTI DI TERZO ORDINE

Sono **effetti indiretti** che si manifestano a lungo termine che si verificano come risultato degli effetti di **secondo ordine** o dell'evoluzione complessiva della situazione post-incidente.

Cambiamenti normativi

Un incidente su **larga scala** potrebbe portare a nuove **regolamentazioni** nel settore, richiedendo adeguamenti significativi alle pratiche aziendali.

Relazioni con i Clienti

La perdita di **fiducia** potrebbe portare a una diminuzione della fedeltà dei clienti nel lungo periodo.

Impatto sul valore azionario:

Per le aziende **quotate in borsa**, gli effetti a lungo termine dell'incidente potrebbero influenzare negativamente il valore delle azioni.

Cambiamenti nella cultura organizzativa:

L'incidente potrebbe portare a una trasformazione significativa nella **cultura aziendale** riguardo alla sicurezza informatica.

Importanza di una visione unitaria

La gestione efficace degli effetti di **secondo e terzo ordine** richiede una visione unitaria della gestione degli incidenti cyber, che va ben oltre il dipartimento IT. È necessario un **approccio interdisciplinare** che coinvolga:

- **Leadership Aziendale**
- **Esperti di Sicurezza Informatica**
- **Responsabili Gestione Rischio**
- **Team Legale e Conformità**

Relazioni Pubbliche e Comunicazione

Responsabili Catena di Approvvigionamento

La **collaborazione** fra questi livelli aziendali permette di identificare e gestire in modo **proattivo** gli effetti di secondo e terzo ordine, abilitando una **gestione del rischio** efficace e sfruttando potenziali opportunità che possono emergere dalla gestione efficace dell'incidente.

08. Strategie di gestione

La gestione degli **effetti** di **secondo** e **terzo ordine** assume quindi una rilevanza cruciale nella gestione del rischio cyber e richiede una valutazione attenta e puntuale. Esempi di strategia di gestione di questi effetti includono:

ANALISI PREDITTIVA

Utilizzare **strumenti di analisi predittiva** per anticipare potenziali effetti a cascata dell'incidente, coinvolgendo vari livelli di management e esponendo il risultato al top management.

MAPPATURA DELLE INTERDIPENDENZE

Creare una mappa dettagliata delle interdipendenze tra **sistemi**, **processi** e **stakeholder** per comprendere meglio come un incidente può propagarsi e come i suoi effetti possano essere analizzati.

INTERAZIONE CON LA VITTIMA

Quando l'utente (vittima) visita la pagina, crede di trovarsi su un sito legittimo e inserisce le proprie **credenziali**.

COMUNICAZIONE PROATTIVA

Mantenere una **comunicazione aperta** e trasparente con **stakeholder interni** ed **esterni** durante e oltre la fine dell'incidente, gestendo le aspettative e mitigando potenziali effetti negativi.

CATENA DI APPROVVIGIONAMENTO

Sviluppare **piani** di **continuità** che includano fornitori e partner commerciali per mitigare gli effetti a cascata, includendoli ad esempio nell'analisi di scenario nel test.

REPUTAZIONE A LUNGO TERMINE

Implementare **strategie** di **gestione** della reputazione che vadano oltre la fase immediata post-incidente.

ADATTABILITÀ ORGANIZZATIVA

Coltivare una **cultura organizzativa** che sia flessibile e adattabile ai cambiamenti indotti dagli effetti a lungo termine degli incidenti.

La gestione degli effetti di secondo e terzo ordine è un aspetto critico ma spesso trascurato nella risposta agli incidenti di

cybersecurity. Un'organizzazione che è in grado di anticipare e gestire efficacemente questi **effetti** non solo minimizza i danni potenziali, ma può anche emergere più forte e resiliente da un incidente. Questa capacità diventa un **vantaggio competitivo** in un panorama di minacce informatiche sempre più complesso e in evoluzione.

09. Conclusione

La **gestione degli incidenti di cybersecurity** in ambienti Enterprise richiede un approccio olistico che va ben oltre la gestione tecnica e basato su una pianificazione attenta, una gestione del rischio efficace, una **gestione strategica** degli effetti di primo, secondo e terzo ordine e una cultura organizzativa che prioritizzi la sicurezza. Il panorama delle minacce informatiche è in continua evoluzione, con **nuove sfide** che emergono costantemente: le organizzazioni, pubbliche e private, devono rimanere vigili, adattabili e proattive nel loro approccio alla sicurezza informatica. Le istituzioni nazionali e sovranazionali devono supportare continuamente cittadini e organizzazioni nel mantenimento di un livello di rischio cyber accettabile. L'invito all'azione per le organizzazioni è chiaro: **investire** nella **preparazione**, sviluppare **capacità robuste** di **risposta** agli **incidenti** e **promuovere** una **cultura** di **consapevolezza** della **sicurezza** a **tutti** i **livelli.** Solo attraverso questi sforzi concertati, organizzazioni di ogni taglio (ed in particolare quelle più complesse) possono sperare di navigare con successo le acque turbolente del cyberspazio. La gestione degli **incidenti di cybersecurity** non è solo una necessità tecnica, ma una componente critica della **strategia aziendale** complessiva: le organizzazioni che eccellono in questa area proteggono meglio i loro asset e la loro reputazione, mantenendo un un vantaggio competitivo essenziale prosperare nell'era digitale

Autore

Mario Beccia

Mario Beccia è un esperto di cybersecurity con oltre vent'anni di esperienza nel settore IT, attualmente Vice Chief Information Officer per la sicurezza informatica presso la NATO. Dopo aver ottenuto una laurea in Economia e Management e un MBA in gestione dell'innovazione, ha conseguito diverse certificazioni di alto livello nel campo della cybersecurity e della gestione dei progetti, tra cui PMP, CISM e CISSP. Nel 2006 è entrato a far parte del NATO Allied Command Transformation, contribuendo al programma NATO Computer Incident Response Capability e il Successivamente, tra il 2018 e il 2021, ha ricoperto il ruolo di Chief Information Security Officer presso l'Agenzia Europea per la Difesa, nel 2021 ha fatto ritorno alla NATO per guidare i programmi di trasformazione della sicurezza informatica all'interno dell'organizzazione.

OWASP Top Ten – Dalla Teoria alla Pratica

Autore: Antonio Minnella

01. Vulnerabilità Software

Una vulnerabilità software è una **debolezza** o un errore intrinseco nel codice di un'applicazione che può essere sfruttato da un **aggressore** per ottenere accesso non autorizzato o per causare danni al sistema. Queste debolezze generalmente comprendono errori di programmazione, difetti di progettazione o configurazioni errate, e presentano falle nella sicurezza che possono essere sfruttate da utenti malintenzionati per scopi malevoli. L'attività di scoperta e la conseguente correzione tempestiva delle vulnerabilità riscontrate è di primaria importanza per garantire la sicurezza delle applicazioni software e allo stesso tempo per proteggere i **dati** e i **sistemi** da potenziali minacce.

Il processo di identificazione delle minacce riveste estrema importanza per proteggere le applicazioni dalle stesse. Questo processo avviene attraverso diversi metodi:

- **Revisione del codice**: analisi manuale del codice sorgente, effettuata da sviluppatori o esperti di sicurezza, per identificare bug, vulnerabilità, inefficienze e violazioni delle linee guida di sviluppo sicuro. Sebbene richieda molte risorse, è un'attività efficace per individuare debolezze e problemi nel codice;
- **Penetration Test (PT)**: simulano attacchi informatici per identificare vulnerabilità e valutare l'efficacia delle difese del sistema. Questo approccio offre una visione realistica delle minacce, individuando punti deboli e proponendo misure di mitigazione. Le analisi includono la mappatura delle risorse, l'identificazione e lo sfruttamento di vulnerabilità, l'escalation dei privilegi e la documentazione dei risultati con raccomandazioni.
- **Analisi Statica (SAST)**: analizza il codice sorgente di un'applicazione senza eseguirlo per identificare vulnerabilità come buffer overflow, SQL injection e XSS. Fornisce feedback immediato agli sviluppatori durante lo sviluppo, permettendo di correggere tempestivamente eventuali falle di sicurezza;
- **Analisi Dinamica (DAST)**: analizza applicazioni web in esecuzione simulando attacchi esterni senza accedere al codice sorgente. Identifica vulnerabilità come SQL injection, XSS e configurazioni errate, valutando l'applicazione dal punto di vista dell'attaccante per garantirne la robustezza contro attacchi reali.

Entrambe le tipologie di analisi (**SAST** e **DAST**) vengono condotte mediante all'ausilio di strumenti software specifici che permettono di eseguire le scansioni. La statica sul codice sorgente senza eseguirlo, l'analisi dinamica, invece, sull'applicazione mentre il software è in esecuzione.

Le vulnerabilità software possono emergere da varie fonti di scoperta. Tra queste abbiamo le segnalazioni che posso giungerci da:

- gli **utenti**: in quanto esperti utilizzatori possono rilevare problemi e segnalarli agli sviluppatori o i fornitori (caso poco simpatico).
- I **team di sicurezza** interni o esterni che eseguono attivamente test e valutazioni delle applicazioni per scoprire vulnerabilità prima che possano essere sfruttate da malintenzionati.
- la **community** di ricerca sulla sicurezza è composta ricercatori e hacker etici che studiano sistemi e applicazioni alla ricerca di debolezze e le segnalano ai rispettivi proprietari o manutentori per l'adozione delle opportune correzioni. Questo comportamento contraddistingue l'hacker «etico» da quello «malintenzionato».

Per ridurre il rischio di vulnerabilità nelle applicazioni software, è necessario adottare una serie di pratiche consigliate. Tra le principali di queste pratiche citiamo:

- **Aggiornamento regolare delle librerie di terze parti:** mantenere tutte le librerie di terze parti aggiornate. Le nuove versioni spesso includono correzioni di sicurezza per le vulnerabilità note.
- **Formazione degli sviluppatori sulla sicurezza:** offrire formazione continua ai membri del team di sviluppo è fondamentale. Gli sviluppatori devono essere istruiti sulle best practice di codifica sicura, sulla gestione delle vulnerabilità e sulla consapevolezza delle minacce.
- **Implementazione di politiche di codifica sicura:** definire e applicare politiche di codifica sicura all'interno dell'organizzazione. Queste politiche dovrebbero includere linee guida specifiche sulla scrittura del codice, suggerimenti per la prevenzione delle vulnerabilità più comuni e direttive sulla gestione delle librerie di terze parti.
- **Analisi statica e dinamica del codice:** utilizzare strumenti di analisi statica e dinamica per identificare e correggere le vulnerabilità. Questi strumenti sono preziosi per individuare debolezze nascoste.
- **Gestione delle vulnerabilità:** Implementare un processo di gestione delle vulnerabilità che includa la registrazione, la prioritizzazione e la risoluzione delle vulnerabilità garantendo che le minacce vengano affrontate in modo sistematico e tempestivo.

02. OWASP 2021 Summary

OWASP (Open Web Application Security Project) è un'organizzazione no-profit globale che si dedica alla **sicurezza** delle applicazioni web. Uno dei principali contributi messi a disposizione da OWASP per contrastare i pericoli del web è il report "**OWASP Top Ten**" che contiene l'elenco delle dieci **principali vulnera**bilità di sicurezza applicativa.

1. Broken Access Control

Si verifica quando un'applicazione non gestisce correttamente l'accesso, permettendo a utenti **non autorizzati** di accedere o manipolare risorse **protette**. Questo può causare **divulgazione**, **modifica** o **distruzione** di dati e azioni non autorizzate. La prevenzione richiede una **rigorosa gestione** degli accessi.

2. Cryptographic Failure

Per proteggere i dati in transito e a riposo, è essenziale identificare le **esigenze di protezione**, soprattutto per informazioni sensibili come **password**, **dati finanziari**, **cartelle cliniche** e **segreti aziendali**, spesso soggette a normative come il GDPR. È fondamentale applicare adeguati livelli di crittografia per garantire la sicurezza dei dati.

3. Injection

L'injection è una vulnerabilità **critica** causata dalla mancata validazione dei dati di input, che consente l'inserimento di **codice malevolo** eseguibile nell'applicazione. Tra i tipi più comuni figurano **SQL Injection** (SQLi), **Cross-Site Scripting** (XSS) e **Command Injection**.

4. Insecure Design

L'**Insecure Design** rende le applicazioni vulnerabili ad attacchi come **SQL injection**, **XSS** e **accessi non autorizzati**, causato dalla scarsa attenzione alla sicurezza durante la progettazione. Problemi comuni includono **controlli di accesso inadeguati**, **gestione scorretta delle sessioni** e **mancata validazione dell'input**. Per prevenire questo rischio, è essenziale integrare la sicurezza fin dalla **progettazione**, identificando minacce, **valutando i rischi**, seguendo **pratiche di sviluppo sicuro** e verificando continuamente la sicurezza lungo il ciclo di vita dell'applicazione.

5. Security Misconfiguration

Le **Security Misconfiguration** derivano da **configurazioni errate** o **non sicure** in componenti, sistemi o risorse cloud, consentendo **accessi non autorizzati**, **esposizione di dati sensibili** o **compromissioni dell'applicazione**. Le cause includono **errori umani**, **impostazioni di default non sicure**, **autorizzazioni eccessive** o **mancata applicazione** di patch. Per mitigare i rischi, è fondamentale seguire le **best practice**: ridurre i privilegi di accesso, aggiornare regolarmente le configurazioni, gestire le patch e applicare il principio del minimo privilegio.

6. Identification and Authentication Failures

Le **Identification and Authentication Failures** includono vulnerabilità legate all'**autenticazione** e **identificazione** degli utenti, come **password deboli**, assenza di **autenticazione a più fattori** (2FA), e credenziali **non protette**. Per mitigare questi rischi, è essenziale adottare politiche di password **robuste**, implementare l'autenticazione a due fattori, **proteggere** le credenziali e garantire **controlli di accesso** adeguati.

7. Vulnerable and Outdated Components

L'uso di librerie di terze parti accelera lo sviluppo software, ma può introdurre vulnerabilità, specialmente attraverso componenti **obsoleti** o **non controllati**. Questi rischi possono compromettere l'applicazione e il sistema, spesso senza che gli sviluppatori siano consapevoli delle falle. Per mitigare il rischio di **Vulnerable and Outdated Components**, è fondamentale monitorare le **notifiche di sicurezza**, applicare tempestivamente **patch** e **aggiornamenti**, e condurre regolarmente **analisi statiche** e **dinamiche** del codice per identificare eventuali vulnerabilità.

8. Software and Data Integrity Failures

Le **Software and Data Integrity Failures**, introdotte nel 2021, riguardano l'**incapacità** di garantire l'**integrità** di dati e codice, causando rischi come **manomissioni**, **corruzioni** e **problemi di accesso**. La mitigazione include **firme digitali**, **crittografia**, **verifica dell'integrità**, **gestione sicura delle sessioni** e **controlli di accesso rigorosi.**

9. Security Logging and Monitoring Failures

I **Security Logging and Monitoring Failures** derivano da lacune nei processi di **registrazione** e **monitoraggio** delle attività di sicurezza, favorendo **minacce** e **violazioni**. Questi includono mancata **registrazione** di eventi critici, **assenza di avvisi** o **risposta inadeguata** ad attività sospette. Per mitigare il rischio, è necessario implementare un sistema completo per **registrare** eventi rilevanti, **archiviare** i registri in sicurezza, **configurare** avvisi e **definire** procedure di risposta agli incidenti, con personale adeguatamente formato.

10. Server-Side Request Forgery

La **Server-Side Request Forgery** (SSRF) si verifica quando un'applicazione web permette a un attaccante di inviare **richieste HTTP** a risorse **interne** o **esterne** senza un adeguato controllo, consentendo di ottenere informazioni sensibili o attaccare la rete. Per mitigare il rischio di SSRF, è importante **validare** e **filtrare** tutte le richieste, **limitare** i privilegi dell'applicazione e **prevenire** l'accesso non autorizzato a risorse o server esterni. La **Top 10 OWASP** è una risorsa fondamentale per migliorare la sicurezza delle applicazioni, aiutando a identificare e mitigare le vulnerabilità più critiche.

La **Top 10 OWASP** rappresenta una risorsa cruciale per migliorare la sicurezza delle applicazioni web, fornendo una guida dettagliata sulle vulnerabilità più critiche che possono compromettere la **protezione dei dati** e la **privacy degli utenti**. Questa lista aiuta sviluppatori e professionisti della sicurezza a identificare **tempestivamente** le minacce più comuni e ad adottare **misure preventive** e **correttive** per mitigarle. Utilizzarla come punto di riferimento consente di progettare e sviluppare applicazioni più **sicure**, riducendo i rischi di attacchi e migliorando la **resilienza** dei sistemi, proteggendo in modo efficace sia le risorse aziendali che quelle degli utenti.

Tecniche di attacco cyber e investigazione

Autore: Simone Fortin

01. Introduzione

Negli ultimi anni, gli attacchi cyber sono diventati una delle **principali** minacce per le organizzazioni di ogni settore. Con l'aumento della **digitalizzazione** e la crescente **interconnessione** dei sistemi, le superfici d'attacco si sono ampliate, offrendo ai cybercriminali opportunità senza precedenti per sfruttare **vulnerabilità tecnologiche** e **umane**.

L'obiettivo della presente trattazione è fornire una panoramica generale sull'evoluzione degli attacchi cyber, anche tramite tre casi studio su alcuni dei principali attacchi cyber che hanno segnato la storia recente, analizzandone le dinamiche e le fasi d'attacco, al fine di comprendere e identificare, retrospettivamente, le misure di sicurezza che avrebbero potuto prevenirli o mitigarne gli impatti.

Il 2023 ha visto un incremento del **12%** negli attacchi cyber a livello globale rispetto all'anno precedente, secondo il **Rapporto Clusit** sulla sicurezza ICT in Italia. Di questi attacchi, **l'81%** è stato classificato con severità **elevata** o **critica**, indicando l'alto livello di rischio per le organizzazioni. Anche l'Italia ha registrato un numero significativo di attacchi di grave portata, pari all'**11%** del totale.

Analizzando più nello specifico questi attacchi, si evince come gli attori delle minacce seguano una strategia comune articolata in quattro fasi:

- **Reconnaissance** (ricognizione), dove identificano e studiano le informazioni delle organizzazioni target;
- **Attack** (attacco), durante il quale ottengono accesso alla rete aziendale;
- **Expansion** (espansione), che consiste in movimenti laterali all'interno dei sistemi target;
- **Obfuscation** (offuscamento), in cui mascherano le tracce per evitare analisi forensi. Questi passaggi riflettono una sofisticazione sempre maggiore, richiedendo contromisure **proattive** ed **efficaci** per mitigare i rischi.

02. Casi Studio

Caso nr.1 : Operation Dream Job

Operation Dream Job, attacco di cyberspionaggio, attribuito al **Lazarus Group**, ha colpito settori critici tra il 2019 e il 2020, usando false offerte di lavoro per infiltrarsi in reti e monetizzare l'accesso. Dal 2022, è un termine ombrello per operazioni simili, con misure di sicurezza individuate per contrastarne le fasi. Nella tabella seguente è riportato il dettaglio del flusso di attacco in relazione alle fasi della **Kill Chain**:

Fasi	Descrizione della Fase	Misure preventive e di contrasto
Initial Access	I Threat Actors hanno usato tecniche di social engineering su LinkedIn, inviando offerte di lavoro false con **allegati malevoli** per compromettere i dispositivi delle vittime.	• Awareness • Red Teaming • Threat Intelligence
Execution	Il malware creava una cartella nascosta, rinominava **utility legittime di Windows** e sfruttava script remoti per garantire persistenza e accesso all'ambiente target tramite PowerShell e brute force sugli account privilegiati.	• Email Security • End-Point Protection • Credential Protection
Defence Evasion	Tecniche di ***living off the land*** e ***masquerading*** con strumenti personalizzati e open-source per nascondere attività dannose tra processi legittimi.	• Antimalware AI-Based • SIEM AI-based • Threat Intelligence
Exfiltration	Informazioni raccolte venivano archiviate in file compressi (**RAR**) e trasferite usando un client Dropbox modificato, sebbene gli obiettivi specifici dei documenti esfiltrati rimangano incerti.	• Data Management • Data Loss Prevention • SIEM AI-Based
Lateral Movement	Probabile utilizzo di **comandi WMI** e masquerading per spostarsi attraverso i sistemi compromessi.	• Segmentation • SIEM AI-Based • Forensic Analysis
Impact	I Threat Actors sfruttavano account compromessi per **campagne BEC**, fingendo di essere la vittima e truffando i clienti tramite richieste di pagamento fraudolente.	• Awareness • Red Teaming • Threat Intelligence

Caso nr.2 : Colonial Pipeline

Nel maggio 2021, il **gruppo Ransomware DarkSide** ha attaccato Colonial Pipeline, interrompendo le operazioni lungo **5.500 miglia di oleodotto negli Stati Uniti**. Per mitigare l'attacco, l'azienda ha disattivato i sistemi e **pagato 4,4 milioni di dollari** ai criminali, evidenziando la necessità di solide misure di sicurezza per prevenire incidenti. Nella tabella seguente è riportato il dettaglio del flusso di attacco in relazione alle fasi della **Kill Chain:**

Fasi	Descrizione della Fase	Misure preventive e di contrasto
Initial Asset	Il **Threat Actor** ha sfruttato credenziali VPN obsolete trovate sul **Dark Web**, agevolato dall'assenza di autenticazione a più fattori, accedendo così alla rete aziendale e raccogliendo informazioni preliminari.	• Threat Intelligence • Multi-Factor • Account Management
Lateral Movement	Sono state utilizzate tecniche come il trasferimento di strumenti laterali e condivisione di **file tramite SMB** o **Remote Desktop Protocol** per spostarsi nei sistemi interni.	• Segmentation • SIEM • Detection & Response
Defence Evasion	Attraverso masquerading e manipolazione di task schedulati, il **Threat Actor** ha camuffato le proprie attività, ricorrendo anche a tecniche di **deoffuscamento** per evitare il rilevamento.	• Antimalware AI-Based • Account Management • Threat Intelligence
Exfiltration/ Execution	I dati sono stati esfiltrati tramite protocolli alternativi e successivamente sono stati impiegati comandi **PowerShell** per eseguire azioni malevole.	• Network Filtering • Data Loss Prevention • SIEM AI-Based
Impact	I sistemi sono stati criptati utilizzando tecniche di **Data Encrypted for Impact**, bloccando l'accesso ai dati. Il 7 maggio, **DarkSide** ha lasciato una richiesta di riscatto su uno dei computer della società.	• Crisis Management • Back-up Offline • Disaster Recovery

Caso nr.3 : Solar Winds

Nel 2020, **APT29** ha sfruttato una vulnerabilità di **SolarWinds** per un attacco alla supply chain, colpendo enti governativi e organizzazioni globali, incluse istituzioni dell'UE e statunitensi. L'operazione ha esposto dati sensibili e sembra parte di una campagna più ampia, con tattiche attribuite al gruppo. Nella tabella seguente è riportato il dettaglio del flusso di attacco in relazione alle fasi della **Kill Chain:**

Fasi	Descrizione della Fase	Misure preventive e di contrasto
Initial Infiltration	Il **Threat Actor** ha sfruttato una vulnerabilità nel servizio di autenticazione per ottenere persistenza, esaminare e-mail e profilare sviluppatori target.	• Vulnerability Management • SIEM AI-Based
Spear Phishing	Dopo aver raccolto informazioni, il Threat Actor ha condotto **campagne di spear phishing** mirate, compromettendo le credenziali degli sviluppatori e accedendo ai sistemi aziendali.	• Awareness • Threat Intelligence
Weaponization	Inserendo **codice malevolo** nel sorgente di SolarWinds e firmandolo digitalmente, il Threat Actor ha creato un software apparentemente legittimo pronto per il rilascio.	• Secure Development • SIEM AI-Based
Infiltration of Downstream Users	Il malware è stato distribuito tramite patch compromesse, attivando una **DLL** malevola che comunicava con il server **C&C** del Threat Actor, propagandosi tra migliaia di utenti.	• Antimalware AI-Based • Data Protection

03. Misure, prevenzione e contrasto

All'interno del presente paragrafo è riportata una descrizione di dettaglio delle misure di prevenzione e contrasto associate alle singole fasi d'attacco dei casi studio descritti sopra.

01. Awareness

Incentivare la *cyber awareness* dei dipendenti attraverso regolari corsi di formazione e simulazioni di **Phishing** e **Social Engineering**.

02. Threat Intelligence

Eseguire attività di threat intelligence, incluse investigazioni **OSINT** e **CLOSINT** al fine di rilevare eventuali credenziali compromesse.

03. Antimalware AI-Based

Implementare **soluzioni antimalware**, possibilmente **AI-based**, in grado di sfruttare funzionalità avanzate, quali analisi comportamentale e threat intelligence ***cloud-based.***

04. Vulnerability Management

Utilizzare **strumenti di scansione**, sia periodica che on-demand, delle vulnerabilità su tutte le **risorse IT/OT.** Implementare, inoltre, un processo di patching e **fixing** delle vulnerabilità strutturato ed efficiente.

05. Secure Development

Implementare un processo di Secure **System Development Life Cycle** con step di validazione pre-rilascio e soluzioni di code review automatizzata (**SAST** e **DAST**).

06. Multi-Factor Authentication

Implementare **soluzioni di protezione degli account e delle password** e, in particolare, soluzioni di autenticazione a più fattori (**MFA**).

07. Account Management

Implementare soluzioni e processi per la disabilitazione degli account inattivi e/o **dismessi**. Limitare, inoltre, i privilegi degli account utente e correggere i vettori di escalation dei privilegi.

08. Segmentation

Segmentare la rete aziendale per limitare la diffusione dei malware e implementare sistemi di monitoraggio della rete, rilevamento e prevenzione delle intrusioni (**IDS/IPS**).

09. SIEM/SOC AI-Based

Dotarsi di una soluzione di analisi, correlazione e monitoraggio dei Log. Se possibile, affidarsi a strumenti AI-based in grado di sfruttare le **funzionalità avanzate**.

10. Detection & Response

Implementare soluzioni di Network Detection and Response (**NDR**) al fine di eseguire attività di **real-time monitoring** e analisi del **traffico di rete**.

11. E-mail Security

Implementare funzionalità di **filtering** e **scansione** avanzata delle **e-mail** per rilevare e bloccare gli allegati e i link dannosi.

12. Network Filtering

Implementare soluzioni di Network Traffic Filtering (**NFC**), come i **proxy**, e utilizzare server dedicati per il **DNS**, al fine di consentire solo a questi sistemi di comunicare sulle rispettive **porte/protocolli**.

13. Crisis Management

Implementare dei **processi** di gestione delle crisi con ruoli e responsabilità definiti, pianificare ed eseguire delle attività **periodiche di simulazione** e **gestione delle crisi.**

14. Off-line Backup

Implementare delle **soluzioni di backup off-line** in modo da impedire la propagazione di ransomware e conservare delle copie aggiornate dei propri dati.

15. Disaster Recovery

Implementare soluzioni di **Disaster and Recovery** che prevedano l'esecuzione e la verifica periodica del ripristino e restore dell'infrastruttura e dei backup.

16. Red Teaming

Pianificare ed eseguire attività di Red Teaming con l'obiettivo di identificare **vulnerabilità tecniche**, **organizzative** e che incidono sul **fattore umano**.

17. Data Management

Adottare un approccio strutturato di analisi, **classificazione** ed **etichettatura dei dati** e delle informazioni aziendali. Implementare, parallelamente, soluzioni di Data Loss Prevention (**DLP**) per gestire in maniera efficace i diritti di **accesso** e il **trasferimento dei dati.**

18. Credential Protection

Utilizzare tecnologie di protezione delle credenziali (es. **Windows Credential Guard**) e verificare regolarmente gli account e le credenziali per garantire l'accesso solo agli utenti autorizzati.

19. Endpoint Protection

Implementare soluzioni di **protezione degli endpoint** efficaci in grado di rilevare e bloccare i payload dannosi.

04. Trends e Conclusioni

Nel 2023, il costo medio di un attacco cyber ha raggiunto i **4,45 milioni di dollari**, con un impatto maggiore sulle infrastrutture critiche (danno medio di **circa 5,04 Mln USD**). In media, il movimento laterale all'interno di una rete compromessa richiede solo 84 secondi, mentre il ciclo di vita complessivo di una violazione dura **227 giorni**. Le principali tipologie di attacco includono malware **(25%)** e attacchi distruttivi **(24%),** con credenziali compromesse e phishing come vettori d'attacco predominanti.

In tale contesto, è interessante evidenziare che organizzazioni che investono in strumenti di cybersecurity basati su AI riescono a ridurre sia il costo medio della violazione (-1,76 milioni di dollari) sia la **durata della violazione (108 giorni**). Al contrario, quelle che non coinvolgono le forze dell'ordine nei casi di ransomware registrano un aumento dei costi (+470.000 dollari) e una maggiore durata delle violazioni **(+33 giorni).**

I dati evidenziano che l'automazione e la cooperazione con le forze dell'ordine sono cruciali per mitigare i costi e la durata degli attacchi. La rapida propagazione degli attacchi dimostra l'importanza di un rilevamento tempestivo e di una risposta rapida, rendendo le soluzioni avanzate di cybersecurity fondamentali per proteggere le organizzazioni moderne da minacce sempre più sofisticate.

Autore

Simone Fortin

Simone Fortin, **Group Chief Information Security Office (CISO)** presso **MSC Cruises** con sede a Ginevra, ha sviluppato conoscenze approfondite in ambito Cyber e Information Security con particolare riferimento al **settore marittimo**. Durante la sua carriera ha anche ricoperto il ruolo di Cyber Security and Infrastructure advisor for Financial and Telco companies, presso un'importante azienda di consulenza, e di Executive Partner & Cyber Security Consulting Director presso un'azienda specializzata nel settore della Cyber Security and **Digital Transformation Technology**.

Inquadramento giuridico internazionale delle operazioni malevole nel cyberspazio

Autore: Annita Larissa Sciacovelli

01. Le attività illecite compiute nel cyberspazio

L'*intensità*, la *sofisticazione* e la *pervasività* delle operazioni malevoli compiute da attori statali e non nel cyber spazio, quali attacchi e reati informatici, compiuti ai danni di infrastrutture critiche, enti pubblici e aziende hanno spinto gli Stati e le organizzazioni internazionali – fra cui l'**Organizzazione delle Nazioni Unite (ONU)**, il **Consiglio d'Europa e l'Unione europea (UE)** - a elaborare un quadro giuridico di principi, norme e procedure per la loro prevenzione e repressione.

Si tratta di operazioni malevoli, spesso di carattere transnazionale che possono minacciare sia la sicurezza interna di uno Stato sia la pace internazionale, soprattutto quando causano crisi internazionali.

Obiettivo di tali operazioni è quello di alterare, degradare, distruggere o interrompere, parzialmente o totalmente, il funzionamento dei sistemi di informazione e di comunicazione (ICT), specie di infrastrutture critiche e strategiche, nonché di alterare, distruggere o compromettere, anche in modo irreversibile, la riservatezza, l'integrità e la disponibilità dei dati digitali. È noto che i sistemi ICT sono alla base del funzionamento di enti governativi, civili e militari, e di aziende private che rientrano o meno nel perimetro nazionale di sicurezza cibernetica (D.P.C.M. 30 luglio 2020 n. 131). Si pensi, ad esempio, al blocco del sistema sanitario nazionale, dei servizi bancari e finanziari, dei grandi complessi industriali automatizzati nel settore energetico e manifatturiero, dei trasporti, delle **telecomunicazioni** e degli acquedotti. Tali enti e **infrastrutture** sono assets indispensabili sia per l'erogazione di servizi essenziali per la popolazione civile sia per il regolare esercizio delle funzioni governative degli Stati. La loro compromissione può indebolire il sistema economico, politico e democratico di uno Stato, minare l'unità nazionale e la fiducia della popolazione civile, con gravi ripercussioni sulla sicurezza nazionale. A tal fine, un esempio è il ransomware lanciato ai danni della compagnia petrolifera statunitense **Colonial Pipeline** nel 2021 dalla cyber-gang DarkSide, e con ogni probabilità sponsorizzato dalla Federazione russa, che è stato definito dal Presidente degli Stati Uniti una questione di sicurezza nazionale. In senso analogo, nel 2022 il Costarica, vittima di una serie di attacchi informatici seriali di tipo DDoS, ha dichiarato lo stato di emergenza nazionale. Per condurre cyber operazioni illecite, gli Stati sono soliti utilizzare gli apparati militari e di intelligence sebbene, nella maggior parte dei casi, essi ricorrono a gruppi di hacker criminali o anche ad aziende di **sicurezza private** (proxies) contribuendo a spingere sempre di più verso la 'privatizzazione' delle capacità offensive degli Stati. Questi gruppi di hacker sono altamente organizzati, al pari di vere e proprie multinazionali del crimine e, come

evidenziato dall'ONU, dispongono di arsenali di armi cibernetiche superiori agli stessi Stati. Essi, pertanto, sono definiti cyber mercenari. Gli scopi perseguiti dai gruppi di hacker sostanzialmente possono essere sia di natura economica, perché finalizzati all'autofinanziamento grazie alla realizzazione di ingenti proventi derivanti dalla perpetrazione di **reati informatici**, sia di **natura politica**, in quanto finalizzati a mettere in atto le strategie criminose (anche militari) degli Stati. Infatti, questi ultimi di sovente tollerano, sponsorizzano o, addirittura, coordinano le attività degli hacker.

Le operazioni malevoli compiute nel cyber spazio possono essere distinte in due categorie in base alla "**teoria del cumulo degli effetti": sopra soglia** (superano la soglia della misura del divieto dell'uso della forza nelle relazioni tra gli Stati) e **sotto soglia** (non superano tale soglia). La soglia in esame si ritiene superata qualora un'azione minacci o impieghi la forza armata sia "contro l'integrità o l'indipendenza politica di qualsiasi Stato, sia in qualunque altra maniera incompatibile con i fini delle Nazioni Unite", ai sensi dell'**art. 2, par. 4, della Carta ONU.**

Operazioni Sopra Soglia

Le operazioni sopra soglia costituiscono una minaccia alla pace e alla sicurezza internazionale e, quindi, a seconda delle circostanze del caso, possono legittimare il ricorso alla **legittima difesa** da parte dello Stato vittima.

Da un punto di vista temporale...

il **primo attacco informatico massiccio** è stato realizzato nel **2007 contro l'Estonia** (attacco DDoS). Esso ha paralizzato quasi l'intera infrastruttura informatica estone e, con ogni probabilità, è stato sponsorizzato dalla Federazione Russa. Successivamente, azioni ostili sono state compiute, probabilmente sempre di matrice russa, contro l'Ucraina sia durante la guerra di Crimea (2014), sia poche ore prima dell'aggressione del, nel 24 febbraio 2022. In tale data, un attacco cibernetico ha bloccato il sistema informativo **satellitare della compagnia statunitense Ka-Viasat**, interrompendo le comunicazioni civili e militari. Da cui deriva che, il conflitto ucraino rappresenta così è il primo a essere **iniziato e combattuto anche nel dominio cibernetico.** È necessaria un'attenta valutazione della minaccia informatica anche per quanto riguarda la sicurezza dei cavi sottomarini, alla luce degli ultimi avvenimenti che hanno visto il danneggiamento ad opera di una nave commerciale cinese con equipaggio russo dei cavi che collegano Taiwan alla terraferma e quelli del Mar Baltico.

Ai casi precedentemente elencati si aggiungono poi gli attacchi cibernetici

di **tipo distruttivo** condotti contro l'Albania (luglio, settembre 2022) con l'obiettivo di bloccare i sistemi informatici governativi e cancellarne i dati digitali, come riportato nella dichiarazione dell'**Organizzazione del Trattato Nord Atlantico** (NATO) **dell'8 settembre 2022**, di cui l'Albania è Stato membro.

Tali attacchi sono stati definiti dal **Primo Ministro albanese** un'aggressione informatica di Stato che sarebbe stata sponsorizzata dall'Iran tramite alcuni gruppi hacker. Nel caso in esame, il **Segretario generale della NATO** non ha escluso il ricorso all'art. 5 del Trattato NATO, relativo a un'azione di difesa collettiva a tutela dell'Albania.

Operazioni Sotto Soglia

Rappresentano invece lo strumento di una nuova strategia militare: la c.d. guerra ibrida. Si tratta di una strategia offensiva il cui obiettivo è minare la sicurezza nazionale di un Paese basandosi sull'impiego di strumenti non convenzionali, quali, ad esempio, gli attacchi e i reati informatici, le campagne di disinformazione, l'ingerenza nei processi elettorali e la strumentalizzazione dei flussi migratori irregolari. In tal senso depone la dichiarazione di **settembre 2024** del presidente **Vladimir Putin** che, alla revoca delle restrizioni all'uso da parte dell'Ucraina di missili NATO a lungo raggio per attaccare la Russia, ha risposto che ciò avrebbe significato che i Paesi dell'Alleanza Atlantica fossero in guerra con la Russia e che per questo motivo, tenendo presente il cambiamento nell'*essenza* del conflitto «**saranno prese decisioni appropriate in risposta alle minacce che saranno poste**».

Quanto detto evidenzia il sempre maggiore impiego del cyber spazio quale nuova dimensione di conflitto asimmetrico e a bassa intensità, costringendo a rivedere la **tradizionale dicotomia esistente** nel diritto internazionale tra 'pace e guerra'. Infatti, i reati informatici, compiuti su larga scala contro le infrastrutture di rete di enti pubblici e aziende di uno Stato, possono essere una delle fasi o delle operazioni rientranti in una più ampia e complessa strategia militare.

02. Il Diritto Internazionale applicabile alle operazioni cibernetiche

Occorre quindi indicare quali sono i **principi di diritto internazionale** applicabili alle attività ostili nel cyber spazio. Sul punto, occorre segnalare però l'assenza di un trattato internazionale in merito e la circostanza che il dominio cibernetico si caratterizza per la mancanza di **confini fisici**, il quasi totale anonimato garantito agli attori che vi operano e la complessità e sofisticazione delle operazioni cyber che possono avere **carattere** diffuso e decentralizzato nel tempo e nello spazio.

Attualmente, tra gli Stati vi è consenso unanime riguardo all'applicazione del diritto internazionale alle attività ostili nel dominio cibernetico, sebbene vi siano difformità riguardo alla **concreta applicazione** con riferimento ai singoli istituti. Il quadro normativo di riferimento è stato definito dall'ONU ed invita degli Stati a un uso responsabile delle **ICT**, in conformità con il

diritto internazionale e la **Carta ONU**, come elaborato dal Group of Experts on advancing responsible state Behaviour in cyberspace in the context of international security (**GGE**) e dall'Open Ended Working Group on security of and in the use of ICT **(OEWG)**. Risultato principale delle attività dei due gruppi indicati è un Decalogo di norme volontarie sul comportamento responsabile degli Stati nell'uso delle tecnologie nel cyber spazio pubblicato nel 2015 (Decalogo). I principi indicati in tale Decalogo, espressione del diritto internazionale vigente, vertono su:

- Mantenimento della pace e sicurezza internazionale in linea con le finalità dell'Organizzazione delle Nazioni Unite.
- Divieto agli Stati di utilizzare e di consentire consapevolmente l'uso del proprio territorio per attività ICT proibite dal diritto internazionale e che danneggiano infrastrutture critiche
- Garanzia dell'uso pacifico delle ICT nel rispetto dei diritti umani, compreso il diritto alla privacy e alla libertà di espressione.
- Obbligo di impedire la proliferazione di tecnologie e l'uso di funzioni informatiche nascoste dannose (backdoor).

A ciò si aggiungono i principi relativi al rispetto della **sovranità statale**, al divieto dell'uso della forza, all'obbligo di soluzione pacifica delle controversie internazionali e al divieto di ingerenza negli affari interni ed esterni degli Stati attraverso le ICT. La principale questione verte sostanzialmente sull'individuazione delle caratteristiche che consentono di definire un'operazione cibernetica transnazionale un "attacco armato".

Per la Corte internazionale di giustizia, solo la più grave forma di uso della forza implica la violazione dell'art. 2, par. 4, della Carta ONU, allorquando, nello specifico , per intensità, durata, e gravità essa comporti danni simili a quelli causati dalla distruzione fisica (principio dell'equivalenza cinetica).

Sul punto, in termini generali gli Stati assumono due posizioni distinte.

De minimis, tra cui l'Italia, e che richiedono l'accertamento di una soglia minima e sufficiente di danni anche fisici causati dall'interruzione, dal blocco o da un'interferenza al normale funzionamento dei sistemi ICT.

Valutazione caso per caso, ai fini della violazione della sovranità statale, ogni tipo di intrusione nelle reti informatiche dello Stato. Ad esempio, nel caso del blocco del funzionamento del sistema informatico della borsa valori accaduto in Francia.

In tal senso, il Manuale di Tallinn 2.0 sul diritto internazionale applicabile alle operazioni cibernetiche (**Manuale di Tallinn 2.0 - Regola 69**), che rappresenta la principale opera collettanea di dottrina sul tema, afferma che un'operazione cibernetica viola il divieto dell'uso della forza qualora la sua portata e gli effetti siano paragonabili a quelli di una operazione cinetica 'sopra soglia'. In tal caso, non assumerebbero rilevanza né la natura violenta dell'attacco, né lo strumento impiegato quanto, piuttosto, i suoi effetti. Questi ultimi sono intesi quali danni ai beni materiali e immateriali (ad es. ai dati digitali)

Anche per la NATO occorre valutare i criteri relativi all'entità e agli effetti dell'attacco (*scale and effects*), con particolare attenzione all'interferenza sulla funzionalità delle infrastrutture critiche, alla gravità, alla reversibilità e alla pervasività degli effetti, all'immediatezza delle conseguenze e alla natura (civile o militare) dell'obiettivo dell'attacco.

Un esempio può essere fornito dalla **manomissione dei sistemi informatici delle infrastrutture critiche nel settore della Operational Technology (OT).** Si pensi a dighe, centrali elettriche e nucleari, o al sistema di controllo del traffico aereo di un aeroporto, il cui malfunzionamento o la manomissione possono causare incidenti di vaste proporzioni e, quindi, avere effetti - diretti, indiretti e prevedibili - sulla popolazione civile e, quindi, sulla sicurezza di uno Stato.

03. La responsabilità internazionale degli Stati

La scelta degli Stati di esternalizzare il compimento di attacchi cibernetici usando **proxies** è finalizzata a non risultare responsabili a livello internazionale di aver compiuto un illecito internazionale, al pari di quanto già accade riguardo alla sponsorizzazione del terrorismo internazionale, in cui gli Stati preferiscono non usare i propri funzionari, bensì gli agenti di fatto. Questi ultimi sono gli individui che materialmente pongono in essere l'illecito ma che non hanno alcun rapporto organico di **dipendenza** con lo **Stato**, sebbene essi agiscano per conto suo. Si tratta di una scelta favorita dalla natura del cyberspazio che ne garantisce l'anonimato e rende complesso individuare responsabili e mandanti di attività illecite poiché non possono essere usate le categorie giuridiche di attribuzione dell'**illecito** del diritto internazionale applicabili nel mondo fisico.

In tale disciplina, l'attribuzione dell'illecito del diritto internazionale a uno Stato si basa, tra l'altro, sul supporto alla logistica, sul finanziamento e, sulla direzione e sulle istruzioni fornite dallo Stato, circa le strategie di attacco e i bersagli da colpire. In altre parole, deve risultare il controllo da parte dello Stato dei delle proxies in modo effettivo o nel suo complesso, salvo che tale attività non sia riconosciuta ex post dallo Stato medesimo come propria (v. artt. 5, 8 e 11 del Progetto di articoli sulla Responsabilità internazionale degli Stati, 2001, Commissione di Diritto internazionale). Nel caso in esame, tali requisiti non rilevano riguardo alle operazioni malevoli messe in atto dai gruppi di hacker poiché spesso essi operano senza ricevere né istruzioni, né supporto logistico, né danaro dallo Stato. Ad ogni buon conto, pur nell'ipotesi in cui lo Stato non sia responsabile della sponsorizzazione o del controllo delle attività di gruppi di hacker, esso nondimeno è responsabile in base al principio di *due diligence* (diligenza dovuta) per non aver disposto, nei limiti della ragionevolezza, tutte le misure necessarie onde evitare l'uso improprio, da parte di gruppi criminosi, delle infrastrutture di rete che insistono sul suo territorio.

04. Conclusione

In conclusione, posto che i reati e gli incidenti informatici sono destinati a crescere, anche dato il basso costo di produzione delle armi cyber, un argine a tale situazione è fornita dalla cooperazione di polizia e giudiziaria tra gli Stati in materia di indagini ai sensi della Convenzione di Budapest sul crimine informatico del **2001** del Consiglio d'Europa, firmata dal 68 Stati. È necessaria però l'entrata in vigore del suo II Protocollo addizionale del 2021 sulla cooperazione in materia di raccolta delle prove digitali, aperta alla firma degli Stati dal 2022, oltre a una disciplina comune tra i **27 Stati membri dell'UE** circa tempi, modalità e procedure di raccolta e conservazione delle prove digitali e la regolamentazione delle criptovalute.

Autore

Annita Larissa Sciacovelli

Annita Larissa Sciacovelli è professore associato di Diritto internazionale presso l'Università degli Studi di Bari Aldo Moro e membro dell'Advisory Group dell'Agenzia dell'Unione Europea per la Cybersecurity (ENISA). Ha conseguito un dottorato di ricerca in Diritto internazionale e ricopre incarichi di docenza anche presso la Scuola di Polizia economica e finanziaria della Guardia di finanza e presso l'Istituto Superiore di Stato Maggiore Interforze del Ministero della Difesa. È stata Cyber Research Fellow presso il Jerusalem Institute for Strategy and Security in Israele e docente presso l'Università degli Studi Internazionali di Roma, trattando tematiche legate alla sicurezza e alle relazioni internazionali. Il suo impegno nella sicurezza cibernetica a livello europeo e internazionale le è valso il premio "Femme dans les métiers Annexes de la Cybersécurité" a Parigi nel 2023. Riconosciuta esperta nel suo campo, è impegnata a promuovere la consapevolezza e la preparazione e la gestione delle minacce digitali, combinando ricerca, didattica e consulenza istituzionale.

Gli incidenti informatici e i piani di risposta agli eventi avversi: azione e reazione

Autore: Claudio Tinelli

01. Introduzione

Gli incidenti informatici rappresentano, con un trend in costante crescita negli ultimi anni, uno dei principali pericoli per l'operatività di aziende, amministrazioni, infrastrutture e servizi e la corretta definizione di un piano di risposta a questi eventi è fondamentale ai fine di una adeguata gestione delle problematiche che ne derivano.

Nello specifico definiamo un incidente come segue:

> **«ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici.»**
>
> **art. 1, comma 1, lett. h) del DPCM n. 81/2021**

L'incidente informatico è pertanto un evento (o serie di eventi) che viola le politiche di sicurezza definite dall'organizzazione e che viene causato con la deliberata intenzione di procurarsi un vantaggio e/o causare un danno.
In questo scenario, la presenza di un **Incident Response Plan** costituisce un importante fattore di mitigazione del rischio e determina una capacità di azione e reazione che può risultare strategica nell'affrontare le avversità legate al mondo cyber.

02. Le principali minacce

Secondo l' «ENISA Threat Landscape 2024» le principali minacce informatiche risultano essere le seguenti:

- **Ransomware**
- **Malware**
- **Social Engineering**
- **Threats against data**
- **Threats against availability: Denial of Service**
- **Information manipulation and interference**
- **Supply chain attacks**

In particolare, i **Ransomware** rappresentano uno degli attacchi più diffusi e pericolosi, con l'obiettivo di inibire l'accesso ai dati dell'attaccato mediante tecniche crittografiche, con l'obiettivo di richiedere un riscatto per la decrittazione. Questo tipo di attacco è frequente nei settori dove la disponibilità del dato costituisce un fattore critico, come ad esempio nel settore sanitario o finanziario, con impatti operativi estremamente significativi.

Nell'ambito della Social Engineering, le strategie mirano a indurre gli utenti a condividere informazioni sensibili o a compiere azioni dannose mediante azioni ingannevoli.

Nell'ambito delle minacce orientate ai dati, il Data Breach (Violazione dei Dati) si orienta prevalentemente verso database aziendali e informazioni riservate con il risultato di una fuga di dati personali e/o aziendali (esfiltrazioni) sia per un diretto interesse e beneficio da parte dell'attaccante che per ottenere proventi illeciti attraverso la commercializzazione delle informazioni sul dark web.

I **Distributed Denial of Service** (**DDoS**) mirano a interrompere l'operatività di reti e servizi creando traffico **automatizzato** e artificiale con impatti che possono renderli inaccessibili agli utenti legittimi, tipicamente contro infrastrutture **critiche** e grandi aziende.

Negli attacchi di tipo **Supply Chain** invece si adotta una strategia differente sfruttando le vulnerabilità di subfornitori, dotati di minori strumenti di difesa, invece di attaccare direttamente l'obiettivo finale.

Infine, una vasta categoria di minacce ricade nel contesto degli **Exploits** e delle **Vulnerabilità Zero-Day**, attraverso le quali si ricercano attivamente e si sfruttano le vulnerabilità nei software e nei sistemi non ancora **risolte** dai fornitori o non ancora mitigate dai clienti finali nonostante il rilascio delle opportune **patch** di sicurezza.

03. Cos'è un Incident Response Plan?

Un **Incident Response Plan** è un insieme strutturato di **procedure** e **direttive** che un'organizzazione adotta per gestire con successo e reagire prontamente a eventuali incidenti informatici o situazioni di emergenza relative alla sicurezza.
Nello specifico, fornisce istruzioni dettagliate su come **identificare** l'incidente, **rispondere** alle azioni ostili, **contenere** i danni e **impostare** un processo di recovery che possa portare con successo al **ripristino** della situazione **ex ante**.

1. Preparazione

Catalogazione degli asset sensibili, identificazione delle minacce, esecuzione di valutazioni periodiche del rischio.

2. Rilevamento e Analisi

Monitoraggio del traffico di rete, analisi dei log, rilevamento di compromissioni, verifica della consistenza di dati e procedure, etc.

3. Contenimento, Sradicamento e Ripristino

Isolare le reti, eliminare le minacce, ripristinare i sistemi.

4. Attività Post-Incidente

Miglioramento continuo del piano, aggiornamento delle misure di sicurezza.

Nello specifico, la fase di preparazione prevede l'individuazione e la catalogazione di tutti gli asset sensibili e le possibili minacce, con l'obiettivo di definire una strategia basata sulle **priorità** in base all'impatto degli eventi sull'organizzazione.
Per prevenire e ridurre i danni, è necessario mettere in sicurezza l'infrastruttura IT, realizzare **Risk Assessment** periodici, adottare policy adeguate, effettuare il *patching* continuo, etc. L'attività di rilevamento e analisi prevede invece che all'interno dell'*Incident Response* Plan siano previste procedure per rilevare e identificare tempestivamente un attacco analizzando i vettori più frequenti e maggiormente pertinenti per il contesto all'interno del quale si sta operando.
Ad esempio, uno dei metodi di attacco più comunemente utilizzati è il cosiddetto *Business Email Compromise* attraverso il quale vengono perpetrate azioni fraudolente mediante azioni di sostituzione di identità che possono indurre i destinatari a compiere attività (decisionali, finanziarie, etc) in grado di determinare un danno aziendale e un illecito beneficio per l'attaccante. Un'azione di rilevamento e analisi di questo tipo di attacco potrebbe pertanto tradursi nel **monitoraggio** dei comportamenti sospetti nelle email, nella analisi e rimozione degli allegati, nella valutazione dello stile di scrittura, nella 'marcatura' dei messaggi provenienti dall'esterno dell'organizzazione.
Analogamente, il monitoraggio potrebbe consentire di individuare eventuali comportamenti anomali all'interno del sistema email aziendale, come l'invio di messaggi a destinatari non abituali, richieste di pagamento insolite o modifica delle informazioni di pagamento. La analisi dei rischi può inoltre rivelarsi fondamentale ai fini della definizione di procedure in grado di contenerli e mitigarne l'impatto. Inoltre, al fine di garantire una adeguata efficacia nella fase di rilevamento, la definizione di procedure di *reporting* degli incidenti, attraverso canali dedicati per la **segnalazione** di eventuali attacchi o tentativi **sospetti**, consente una gestione **sicura**, **tempestiva** e **appropriata** dell'evento.
A sostegno delle attività di analisi, un ruolo importante viene svolto dai penetration test, che offre diversi vantaggi:

- Identificazione delle vulnerabilità
- Valutazione della resilienza
- Sviluppo e miglioramento delle competenze
- Verifica delle procedure di risposta.

Per quanto concerne le azioni di **contenimento**, **sradicamento** e **ripristino**, possiamo sicuramente individuare, in prima istanza, una fase di **isolamento** e mitigazione che consenta, scoperto l'attacco, di circoscrivere il perimetro di azione dell'attaccante con interventi mirati e specifici. Ad esempio, nel caso di un attacco di tipo Business Email Compromise, si può prevedere la sospensione immediata degli account compromessi e la revoca dell'accesso agli utenti colpiti.
Relativamente alle attività post-incidente, è importante effettuare una valutazione critica dell'efficacia dell'Incident Response Plan in essere al fine di individuare i punti di miglioramento, anche in considerazione della continua evoluzione delle tecniche di individuazione delle vulnerabilità e di attacco.

04. Conclusione

L'Incident Response Plan rappresenta uno strumento importante per una corretta gestione del rischio di incidente informatico e coinvolge persone, sistemi, network e applicazioni, oltre a rappresentare la prima linea di difesa contro gli attacchi informatici, garantendo che l'organizzazione sia preparata a rispondere agli incidenti, minimizzando i danni e migliorando continuamente le sue strategie di sicurezza.
In sintesi, i punti di forza possono essere riassunti in:

- Business Continuity: Migliora la continuità operativa anche durante le crisi.
- Conformità Normativa: Molti enti regolatori richiedono un IRP per garantire che le organizzazioni possano rispondere prontamente agli incidenti.

Al fine di garantire una adeguata efficacia, un Incident Response Plan richiede quindi che siano individuati e catalogati tutti gli asset sensibili e venga predisposta una strategia con le varie priorità in funzione dell'impatto che gli eventi potrebbero avere sull'organizzazione, determinando la matrice dei rischi.
Per ridurre gli eventuali danni, dovrà essere messa in sicurezza tutta l'infrastruttura IT attraverso la definizione di policy adeguate, il patching continuo di applicazioni e sistemi operativi, la messa in sicurezza del network e la tenuta dell'intero sistema dovrà essere verificata con Risk Assessment (Penetration Test) periodici.

Autore

Claudio Tinelli

Claudio Tinelli è il co-fondatore e co-CEO di Eulogic NT SpA, azienda specializzata nella sicurezza informatica, e attuale presidente del Distretto Produttivo dell'Informatica Pugliese. La sua carriera nel settore ICT è iniziata con 17 anni di esperienza nella pubblica amministrazione, durante i quali ha sviluppato competenze significative nella progettazione e gestione di infrastrutture informatiche. Nel 2010, ha co-fondato Eulogic Srl, che, dopo la fusione con SIM NT Srl, è diventata Eulogic NT SpA, consolidando la sua posizione nel campo della cybersecurity. Tinelli è riconosciuto come esperto.

Resilienza Operativa

Autore: Federico Spadaro

01. Introduzione

Nel mondo di oggi, la sicurezza cibernetica è diventata una priorità cruciale per tutte le organizzazioni, comprese le forze dell'ordine. Le crescenti minacce digitali, che vanno dagli attacchi di ransomware alle operazioni di hacking sponsorizzate da stati, pongono sfide significative. In questo contesto, la **resilienza operativa**, ovvero la capacità di mantenere la continuità delle operazioni e rispondere efficacemente a eventi imprevisti, si rivela fondamentale per proteggere sia le **i**nfrastrutture critiche che la sicurezza pubblica. Le minacce informatiche evolvono rapidamente, rendendo necessaria una preparazione continua.

Ad esempio, il caso di «*WannaCry*», un attacco globale che ha paralizzato migliaia di aziende e istituzioni, dimostra l'importanza di avere piani di risposta rapidi e backup sicuri. Un altro caso emblematico è quello di Sony Pictures, dove una risposta tempestiva e la resilienza organizzativa hanno permesso di mitigare un attacco devastante.

La resilienza operativa è la capacità di un'organizzazione di adattarsi e continuare a funzionare **durante** e **dopo** eventi critici, come attacchi informatici, disastri naturali o guasti tecnici. Secondo il *World Economic Forum*, "La resilienza operativa è una capacità fondamentale per le istituzioni moderne, poiché la **sicurezza** e la **continuità** delle operazioni sono essenziali per rispondere in modo efficace alle crisi globali"

Essa richiede un'adeguata preparazione, una gestione **efficace** delle risorse durante la crisi e la capacità di riprendersi rapidamente senza compromettere l'efficacia operativa. La resilienza non riguarda solo la tecnologia, ma include anche la cultura organizzativa e la gestione del **capitale umano**.

02. L'importanza della *resilience*

Le forze dell'ordine devono essere sempre pronte a **rispondere a eventi imprevedibili** che potrebbero compromettere la sicurezza pubblica. La resilienza operativa, in questo contesto, permette di garantire la continuità operativa, anche in caso di attacchi informatici o emergenze.

Gli elementi fondamentali della resilienza operativa sono:

01.

Protezione Infrastrutture Critiche

Le aziende devono proteggere le infrastrutture tecnologiche critiche attraverso un approccio di sicurezza a più livelli, che includa strumenti come crittografia e autenticazione a più fattori, per evitare che vulnerabilità compromettano i sistemi. È essenziale mantenere aggiornati i software con patch di sicurezza regolari e monitorare costantemente le attività per rilevare minacce in tempo reale. I dati sensibili vanno protetti con crittografia e backup sicuri, e devono essere testati piani di ripristino. La formazione continua del personale sulla sicurezza cibernetica e la preparazione di piani di emergenza e continuità operativa sono altre misure cruciali per affrontare le crisi e gli attacchi.

02.

Mantenimento della sicurezza durante la crisi

Mantenere la sicurezza durante le crisi è cruciale per garantire la continuità operativa. È fondamentale sviluppare e testare piani di risposta alle emergenze, che prevedano scenari realistici come attacchi informatici e disastri naturali, e garantire una comunicazione sicura e continua tramite reti criptate e canali di emergenza. Inoltre, è necessario formare team dedicati per una risposta rapida e tempestiva agli attacchi e alle crisi. Il supporto psicologico e la gestione dello stress sono importanti per mantenere il personale operativo. L'uso di tecnologie avanzate di monitoraggio, come l'intelligenza artificiale, e la collaborazione con agenzie esterne e comunità locali migliora la capacità di risposta e gestione delle emergenze.

03.

Sicurezza delle Informazioni

La protezione dei dati sensibili è essenziale per garantire la sicurezza e la privacy, evitando che informazioni cruciali vengano compromesse. È fondamentale implementare politiche di classificazione dei dati per identificare e trattare in modo sicuro le informazioni riservate.

L'adozione di tecnologie avanzate di protezione, come la **Data Loss Prevention (DLP),** aiuta a prevenire la perdita di dati. Inoltre, è importante verificare periodicamente l'integrità dei dati, archiviare le informazioni sensibili in sistemi sicuri e attuare politiche di eliminazione sicura quando non sono più necessarie. L'accesso fisico alle informazioni deve essere controllato e monitorato, e **audit di sicurezza** regolari devono essere condotti per garantire l'efficacia delle misure di protezione.

«Le forze di polizia di tutto il mondo devono dotarsi di un piano di resilienza operativa che vada oltre la protezione dei dati, ma includa anche la prontezza nell'affrontare eventi che possano minare la sicurezza del paese.»

Cybersecurity and Infrastructure Security Agency (CISA)

03. Preparazione e gestione della crisi

La **preparazione** è essenziale per garantire che un'organizzazione possa rispondere adeguatamente a eventi imprevisti. In un contesto di **resilienza operativa**, la preparazione prevede le seguenti attività.

PIANI DI EMERGENZA

Ogni forza di polizia deve avere un piano di emergenza ben strutturato per gestire crisi come attacchi informatici, disastri naturali e violenze urbane. Il piano dovrebbe iniziare con una chiara definizione degli obiettivi, come la protezione del personale e la continuità delle operazioni. Un'analisi dei rischi identifica le minacce e guida la pianificazione delle risposte. Ogni membro deve avere ruoli e responsabilità definiti, con una gestione efficace dei turni e delle risorse. La comunicazione sicura è essenziale, così come le procedure di risposta specifiche per ogni tipo di emergenza. Infine, una gestione adeguata delle risorse e un supporto psicologico per il personale sono fondamentali per garantire un'efficace risposta alla crisi. Un piano completo aiuta a preparare le forze dell'ordine ad affrontare imprevisti riducendo l'impatto sulla sicurezza pubblica.

COMUNICAZIONE EFFICACE

Durante una crisi, le forze dell'ordine devono garantire una comunicazione rapida, sicura e senza interruzioni sia internamente che con partner esterni. È essenziale utilizzare canali sicuri, come reti criptate e avere sistemi di comunicazione ridondanti, come radio sicure e linee telefoniche di emergenza.

I piani di comunicazione devono essere chiari e ben definiti per ogni **dipartimento** e **partner** coinvolto, con un forte coordinamento tra le diverse unità. La formazione continua del personale è cruciale per garantire una risposta tempestiva ed efficiente. Un esempio importante è l'attacco ransomware subito dalla Polizia di Atlanta nel 2018, che ha sottolineato l'importanza di una risposta rapida per minimizzare i danni e garantire la continuità operativa. Secondo il **NIST**, una gestione efficace delle crisi dipende dalla preparazione e dalla comunicazione accurata.

FORMAZIONE E SIMULAZIONI

La formazione continua e le simulazioni pratiche sono essenziali per preparare le forze dell'ordine a rispondere rapidamente e in modo coordinato durante le emergenze. Attraverso esercitazioni realistiche e variegate, il personale impara a gestire scenari critici, migliorando competenze, comunicazione e lavoro di squadra. Queste attività aiutano a identificare e ottimizzare le procedure operative, garantendo una risposta più efficace e sicura per la comunità.

04. Problemi comuni nella sicurezza informatica

Le forze dell'ordine affrontano quotidianamente vari problemi comuni nel mantenimento della sicurezza informatica:

- **Intrusioni nella rete**: Gli attacchi come phishing, ransomware e DDoS possono compromettere la sicurezza delle comunicazioni e dei dati sensibili.
- **Difficoltà nell'identificare tempestivamente gli attacchi**: Spesso, gli attacchi informatici avanzati come il malware evasivo o gli attacchi DDoS vengono individuati troppo tardi, causando danni significativi.
- **Gestione dei falsi positivi**: Gli allarmi generati dai sistemi di sicurezza possono essere troppo generici o troppo frequenti, rendendo difficile distinguere tra minacce reali e normali attività di sistema.
- **Bilanciamento tra reattività e proattività**: Le forze dell'ordine devono trovare il giusto equilibrio tra reagire rapidamente agli attacchi e pianificare azioni preventive per evitare futuri attacchi.

Autore

Federico Spadaro

Con oltre 20 anni di esperienza nel settore della cybersecurity, Federico Spadaro, è un **Senior Manager** e attuale **CISO Deputy**. coordina team multidisciplinari e guida progetti strategici per migliorare resilienza e compliance aziendale. Oltre alle sue competenze tecniche, si dedica al coaching, formando leader e creando team ad alte prestazioni.È attivamente coinvolto nella comunità professionale della sicurezza informatica, contribuendo come autore per il capitolo italiano dell'(ISC), dove ha pubblicato articoli su vari aspetti della cybersecurity. Partecipa a eventi e conferenze del settore, condividendo la sua esperienza e le migliori pratiche per affrontare le sfide legate alla sicurezza informatica nelle organizzazioni moderne.La sua dedizione alla formazione e allo sviluppo di competenze nel campo della cybersecurity sottolinea il suo impegno nel promuovere una cultura della sicurezza all'interno delle organizzazioni.

Considerazioni Conclusive

Vice Questore Aggiunto della Polizia di Stato
Christian Falliano

Le principali minacce al settore pubblico

In conclusione, di questa prima edizione, appare opportuno evidenziare - ancora una volta - che l'obiettivo di questo Quaderno è stato quello di offrire uno spaccato attuale del mondo cibernetico, soffermandosi, in particolare, sui profili di rilevazione della matrice criminale di azioni illecite perpetrate in tale contesto. L'analisi si è avvalsa dello studio e dell'approfondimento tecnico-giuridico di professori appartenenti al mondo accademico, di personalità in ambito privato e di stimati colleghi che, nell'arco di svolgimento dei seminari tenutisi lo scorso anno con i Centri Operativi per la Sicurezza Cibernetica del Servizio Polizia Postale, hanno messo a disposizione tutte le proprie competenze e professionalità.

Il contributo dello scrivente a questo importante format si è basato principalmente sull'esperienza personale e professionale maturata durante il servizio prestato all'interno del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.), quale Centro specialistico del Servizio Polizia Postale deputato alla prevenzione e repressione dei crimini informatici, nonché - da ultimo - al Servizio per la Sicurezza Cibernetica del Ministero dell'Interno, che occupandosi a mezzo del Computer *Emergency Response Team* (C.E.R.T.) della gestione immediata delle attività di risposta alle minacce, agli incidenti e agli attacchi finalizzati a compromettere la sicurezza informatica del Ministero dell'Interno, sta delineando nuove e importanti prospettive di analisi e ricerca nel contesto cyber. Il punto di partenza è scontato e quasi banale: la società contemporanea è in continua evoluzione per effetto, principalmente, della crescente digitalizzazione dei processi e dei contenuti informatici. L'introduzione e la rapida adozione di tecnologie innovative hanno reso necessario l'elaborazione di un programma strategico per garantire una transizione digitale efficace e appropriata, che consenta l'implementazione funzionale di questi strumenti e favorisca al contempo la realizzazione della persona (attraverso una maggior interconnessione tra gli individui, le organizzazioni e l'ambiente in cui essi vivono) all'interno del più ampio contesto in cui si sviluppano le complesse dinamiche politiche, sociali, finanziarie e umane che la contraddistinguono.

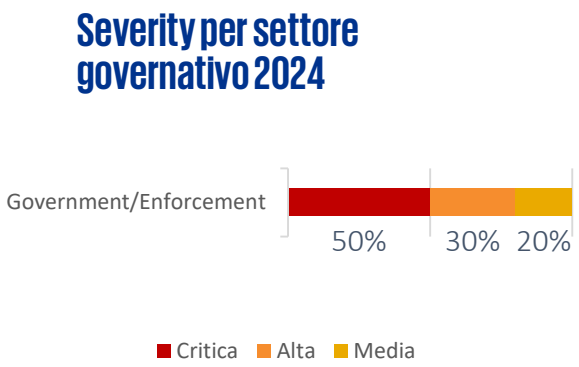
La diffusione e l'evoluzione delle tecnologie ICT hanno provocato una crescita esponenziale del cyberspazio, che si presenta quale ambiente sempre più complesso, multiforme, pervasivo e onnipresente, frutto dell'interazione tra attori, tecnologie, processi, pratiche e servizi a più livelli. In questo contesto, il cyberspazio si configura non solo come uno spazio fisico in cui è necessario garantire lo sviluppo pacifico e la protezione dei valori fondamentali e delle capacità dei suoi membri, ma anche come un circuito in cui si manifestano sempre più chiaramente fenomeni e comportamenti dannosi o potenzialmente dannosi, come gli attacchi informatici.

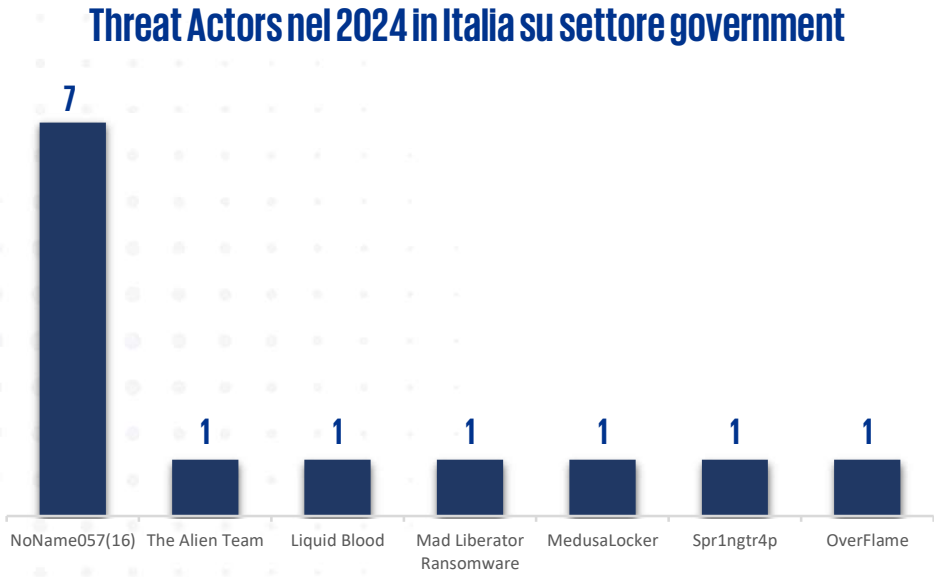
L'entità, la frequenza e l'impatto degli incidenti di sicurezza cibernetica sono in costante crescita, sia a livello mondiale, che europeo e, a cascata, italiano. Tali azioni ostili rappresentano una grave minaccia per il funzionamento delle reti e dei sistemi informativi, in quanto potenzialmente idonei a interrompere l'erogazione di servizi pubblici fondamentali e lo svolgimento di attività economiche, nonché a compromettere i sistemi democratici.

Invero, lo sviluppo delle tecnologie digitali e l'evoluzione dell'ambiente online rappresentano un fattore cruciale e strategico per la protezione di beni vitali, come l'interesse nazionale e la sicurezza dei cittadini. Tuttavia, questo non deve implicare una contrapposizione tra innovazione e sicurezza, bensì una visione integrata, poiché la digitalizzazione crescente offre opportunità di crescita economica e nuove modalità organizzative (si pensi, ad esempio, al lavoro da remoto), ma comporta anche un incremento di rischi e di vulnerabilità. Le sfide legate a queste incognite richiedono l'adozione di iniziative mirate a rafforzare la sicurezza dei sistemi e delle infrastrutture critiche del nostro Paese, attraverso interventi tecnologici innovativi e riforme strutturali tese a migliorare la resilienza dello spazio cibernetico. In quest'ottica va intesa anche la pianificazione di nuove assunzioni di personale, sia nelle aree di pubblica sicurezza che di polizia giudiziaria, dedicate alla prevenzione e investigazione del crimine informatico diretto contro singoli cittadini e preposte a difendere il Paese da minacce cibernetiche, irrobustendo gli asset e le unità cyber incaricate della protezione delle infrastrutture tecnologiche critiche delle pubbliche amministrazioni. intesi oramai nella loro più ampia accezione. Proprio l'esperienza maturata durante il servizio svolto al CNAIPIC e al CERT ha consentito una visione privilegiata in occasione della gestione operativa di queste nuove forme di minaccia cibernetica. Inoltre, la sinergia tra le strutture - che lavorano sempre più a stretto contatto, attraverso le piattaforme di comunicazione dedicate

e riservate - ha consentito un'azione effettiva mediante la condivisione delle informazioni in tempo reale e la successiva ricerca di soluzioni immediate, il più possibile risolutive. Queste peculiari postazioni hanno permesso, nel corso dell'ultimo anno, di usufruire di un punto di osservazione avanzato sui principali obiettivi scelti dalle compagini criminali che si concentrano sostanzialmente in due settori, ritenuti maggiormente appetibili per la loro importanza e rilevanza strategica: quello governativo, per ciò che attiene il comparto pubblico e quello sanitario, in ambito privato. Per quanto riguarda i *threat actors*, l'Italia è sempre più esposta ad azioni ostili condotte prevalentemente da gruppi altamente specializzati di natura statuale o sponsorizzati da Stati (APT- acronimo di *Advanced Persistent Threat*), in grado di condurre attacchi mirati e persistenti, portati avanti da avversari dotati di notevole expertise tecnica e che dispongono di ingenti risorse economiche. Più nello specifico, negli ultimi tempi, il settore governativo italiano è stato uno dei principali obiettivi di attacchi informatici, con un'esposizione crescente a minacce di rilevanza critica. La maggior parte degli attacchi cibernetici rivolti al settore pubblico ha avuto un impatto significativo, coinvolgendo sia Enti ministeriali che istituzioni preposte alla difesa nazionale. Tra gli incidenti di maggiore rilevanza, si segnalano numerosi casi di data leak, tra cui la divulgazione di dati sensibili nel dark web. Le campagne generalizzate di phishing, attuate sempre più frequentemente mediante l'utilizzo di tecniche di social engineering, sono ancora oggi molto diffuse e destano non poche preoccupazioni, in quanto la partecipazione di numerosi attori statali sponsorizzati e l'estensione delle operazioni a livello internazionale amplifica in modo esponenziale le conseguenze dannose per gli utenti. Nelle figure sottostanti, si riportano alcuni dati significativi, tratti dalla piattaforma di *threat intelligence* che supporta le attività del CERT, a dimostrazione dei trend maggiormente rilevati all'interno delle minacce che riguardano il settore pubblico. Come risulta dai grafici, nonostante il cybercrime orientato al guadagno economico continui a rappresentare la principale causa di attacchi informatici, negli ultimi anni si sta osservando un aumento significativo di azioni di *hacktivism*, che sono invece guidate da motivazioni essenzialmente politiche. Gli hacktivisti tentano, con ogni espediente, di utilizzare il cyberspazio come mezzo per diffondere e amplificare la portata di messaggi di protesta e di cambiamento sociale, o anche solo politicamente orientati, facendo emergere questioni ideologiche che potrebbero non avere alcun risalto tramite i media tradizionali. Il gruppo di hacktivisti filorusso conosciuto come NoName057(16),

ad esempio, è emerso come uno dei principali attori minacciosi contro il settore governativo, perpetrando attacchi di tipo DDoS («Distributed Denial of Service») mirati a saturare le risorse dei siti istituzionali e militari.

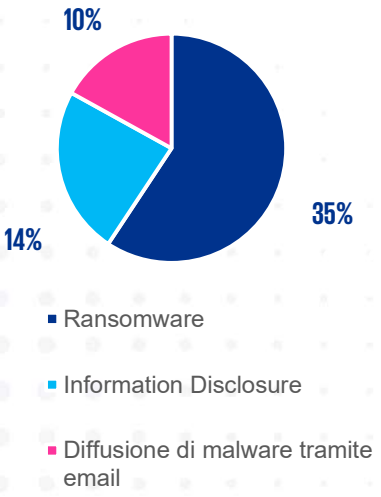




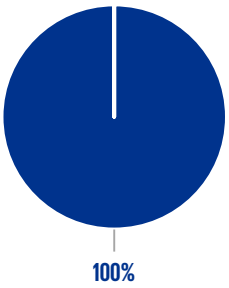
Talle gruppo promuove una propaganda favorevole al Cremlino con l'intento di causare destabilizzazione nei servizi pubblici e di generare disagi tra i cittadini. Inoltre, tale gruppo criminale sta estendendo la propria rete di influenza, attraverso alleanze con altri collettivi hacktivisti ideologicamente affini, e ciò potrebbe esporre il settore governativo italiano a maggiori rischi. Gli attacchi informatici al settore sanitario tendono, invece, nel breve periodo, ad interrompere la capacità dei sistemi sanitari di accedere alle cartelle cliniche elettroniche o ad altri network based services, comportando ad una riduzione della capacità delle strutture di offrire cure tempestive ai pazienti, con gravi conseguenze sulla salute di questi ultimi. A causa della perdita di dati, i sistemi ospedalieri potrebbero dover fronteggiare ritardi nella prestazione di servizi diagnostici o di assistenza anche per settimane o mesi dopo un attacco informatico.

ransomware, è la tecnica di attacco preferita dai criminali informatici, attraverso cui vengono criptati i dati dei pazienti per poi richiedere un riscatto affinché vengano sbloccati. Negli ultimi tempi, i principali sistemi sanitari sotto attacco informatico sono stati quelli di Francia, Spagna, Germania, Paesi Bassi e Italia, che hanno registrato più del 60% dei casi. Questo trend è destinato a crescere a causa del continuo interesse dei cybercriminali per questo settore pervaso di dati sensibili e, per molti aspetti legati alla sicurezza proattiva, certamente da migliorare. I grafici sottostanti riportano le tipologie delle minacce e degli attori ostili più attivi, con

Tipologie di minacce sul settore nel 2023



Tipologie di attaccanti sul settore nel 2024

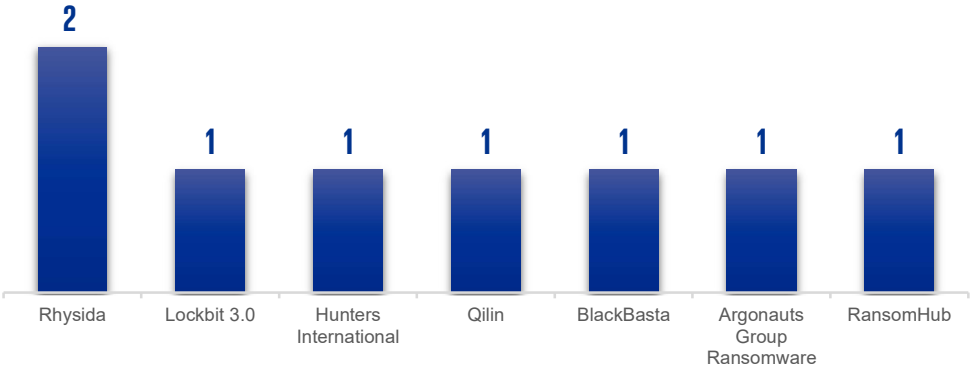


$ 10,93M costo medio di una violazione dei dati nel settore sanitaria a livello mondiale

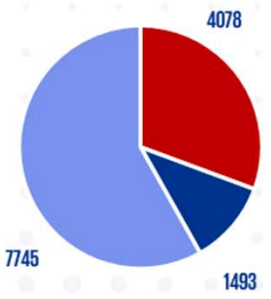
l'indicazione del costo medio di una violazione dati rivenduta nei canali oscuri. A differenza del settore governativo, la principale motivazione dietro gli attacchi informatici al settore sanitario è di natura esclusivamente economica. I dati sanitari sono estremamente ricercati e lucrativi nel mercato del dark web, in quanto includono informazioni personali sensibili come le credenziali di accesso a sistemi sanitari e le informazioni finanziarie relative a trattamenti o assicurazioni sanitarie, particolarmente ricercati nel mercato illecito dai criminali per ovvi motivi. I dati sanitari, infatti, sono estremamente dettagliati e unici e possono essere utilizzati per falsificare identità, accedere a fondi pubblici o privati, per frode assicurativa. Tale tipologia di dati, essendo meno soggetta a modifiche, ha una durata più lunga e costituisce una risorsa stabile e di maggior valore per i criminali,

rispetto ad altre informazioni personali (come numeri di carte di credito o account bancari) che possono essere facilmente annullate o bloccate.

Threat Actors Attivi in Attacchi in Italia sul settore-2024



Vulnerabilità Riscontrate



- Esposizione di servizi non necessari su internet → Seppur le **più critiche**, si è osservato che sono in leggera diminuzione
- Vulnerabilità di software non aggiornati → Si sono ridotte significativamente, indicando una maggiore attenzione agli aggiornamenti
- Errate configurazioni → Sono la vulnerabilità **più frequente** che unita alla più critica comporta un **rischio molto elevato**.

Il settore governativo necessita di maggiore coordinamento interistituzionale, mentre quello sanitario richiede investimenti urgenti nell'aggiornamento delle infrastrutture.

Più nel dettaglio, si osserva che, al verificarsi di un'azione ostile, la reazione di Polizia alle minacce nei due settori suindicati si concretizza, in chiave preventiva, attraverso un costante monitoraggio dei canali e delle piattaforme che erogano i servizi. In caso di attacchi cyber con impatti, vengono attivate, a seconda dei casi, le due Sale operative (CNAIPIC e CERT), che agendo ciascuna nell'ambito di propria competenza ma in maniera coordinata e sinergica, in tempo reale, riescono ad emettere preallarmi, diramano alert, annunci anche sui canali social e si impegnano nella divulgazione di informazioni strategiche agli operatori interessati (soprattutto attraverso interlocuzioni dirette, frutto di atti convenzionali che prevedono canali dedicati di comunicazione) per coordinare una risposta integrata, mediante una gestione organizzata ed efficiente degli eventi, al fine di evitare o, quanto meno, mitigare il più possibile gli effetti di un'azione ostile e scongiurare che la stessa abbia

impatti significativi sulla sicurezza delle reti e dei sistemi informativi nazionali. Nello svolgimento di quest'opera continuativa, la Polizia sostiene il lavoro degli operatori specialistici mettendo loro a disposizione piattaforme di lavoro tecnologicamente avanzate, che consentono l'identificazione delle tecniche e delle tattiche utilizzate, il monitoraggio e la raccolta dei dati delle minacce, degli incidenti informatici e delle vulnerabilità di sistema. Un ulteriore progresso verso una **postura di sicurezza avanzata**, che implica un aumento della qualità e rapidità dell'info-sharing, è rappresentato dall'implementazione di soluzioni per una consapevolezza e allerta precoce, di investimenti in formazione congiunta e di un incremento della comprensione interna delle minacce informatiche, nonché dall'armonizzazione dei sistemi normativi di riferimento, al fine di creare un **quadro regolamentare coerente** e **coordinato**, in grado di affrontare a livello transnazionale le sfide globali. Infine, è di cruciale importanza migliorare la **qualità** e la **rapidità dell'informazione condivisa** tra le **Autorità di contrasto**, attraverso un approccio integrato e collaborativo, che consenta di **rispondere alle minacce informatiche** in **modo proattivo e sostenibile**. A tal proposito, nell'ambito del gruppo *Lawful Access*, i Paesi aderenti al G7 si sono impegnati a **promuovere un dialogo più efficace** con le società di tecnologia, al fine di agevolare il pieno accesso delle istituzioni alle informazioni legittimamente detenute, in conformità alle discipline normative nazionali vigenti e nel rispetto del principio di tutela della privacy.

Tra le iniziative intraprese dalla rappresentanza italiana in seno al citato gruppo, proprio al fine di agevolare il dialogo costante tra le istituzioni, la più rilevante - che ove accolta rappresenterebbe un considerevole passo in avanti nello sviluppo della strategia di difesa e risoluzione degli attacchi e a cui il sottoscritto ha fornito il proprio personale contributo - consiste nella redazione di un Codice etico contenente i principi fondamentali di collaborazione a cui gli Internet service provider dovrebbero attenersi, nel presupposto di creare un ambiente sicuro di circolazione delle informazioni utili a rilevare le minacce, individuarne gli autori e consentire una rapida risposta agli attacchi malevoli. L'obiettivo comune è quello di definire regole chiare, procedure e valori morali condivisi (la pubblica sicurezza della comunità, la protezione dai crimini e la relativa persecuzione, la libertà e la privacy dei cittadini, l'integrità delle istituzioni, la pubblica efficienza, la trasparenza dei servizi, l'affidabilità delle imprese, la solidità dei rapporti sociali) per prevenire e contrastare la commissione di illeciti, mitigare le minacce relative a

vulnerabilità ed incidenti in danno della regolarità dei servizi per la conservazione e la successiva acquisizione di dati informatici, che nella prassi risultano indispensabili per la ricostruzione dei crimini commessi online, nonché per la prevenzione da minacce impellenti concernenti la pubblica sicurezza e l'integrità della persona nel dispiegarsi di un'azione corale e trasversale che superi i confini delle nazioni. Nello specifico, l'auspicata promulgazione del Codice consentirà di poter impegnare le società di telecomunicazioni che vi aderiranno ad ottemperare ad ogni richiesta proveniente dalle Forze di Polizia nell'ambito delle rispettive funzioni di vigilanza, fornendo - ove richiesto - piena collaborazione ed evitando comportamenti di tipo ostruzionistico, nonché garantendo una pronta collaborazione nell'ambito delle istruttorie intercorrenti con Agenzie e/o Autorità pubbliche affinché non siano presentate informazioni non veritiere ovvero omissive.

In conclusione, questo Quaderno ha cercato di mettere in luce l'importanza di un approccio integrato e multidisciplinare alla sicurezza cibernetica. Abbiamo esplorato il Perimetro Nazionale di Sicurezza Cibernetica (PNSC), le normative che regolano la protezione delle infrastrutture critiche e l'impegno necessario da parte delle Organizzazioni per garantire la resilienza digitale. Tuttavia, ciò che emerge con chiarezza è che la **protezione cibernetica** non può essere raggiunta attraverso misure tecniche isolate ma richiede un **impegno costante** che coinvolge persone, tecnologie e processi, dal momento che la cybersecurity è un obiettivo caratterizzato da molteplici aspetti e richiede un processo continuo (e globale) di miglioramento. Le Organizzazioni devono quindi investire in sicurezza informatica: si tratta di una necessità tecnica e di una componente strategica per assicurare la continuità delle operazioni, nonché la protezione dei dati e delle infrastrutture vitali.

Autore

Vice Questore Aggiunto Christian Falliano

Assegnato al Servizio per la Sicurezza Cibernetica del Ministero dell'Interno con il ruolo di responsabile degli Affari Generali dell'Ufficio e delle attività propedeutiche alla piena operatività del CERT, che ha il compito istituzionale di garantire le attività di prevenzione, di analisi e di gestione proattiva delle minacce, incidenti ed attacchi informatici contro le reti, i sistemi e le infrastrutture telematiche del Dicastero.

Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica

powered by:

KPMG